

HP Universal CMDB

per sistemi operativi Windows e Linux

Versione software: 9.02

Guida alla distribuzione

Data di rilascio del documento: ottobre 2010

Data di rilascio del software: ottobre 2010



Note legali

Garanzia

Le sole garanzie per i prodotti e i servizi HP sono esplicitate nelle dichiarazioni di garanzia espressa che accompagnano tali prodotti e servizi. Nulla contenuto nel presente documento deve essere interpretato come garanzia aggiuntiva. HP non è responsabile di errori tecnici ed editoriali o di omissioni contenuti nel presente documento.

Le informazioni contenute nel presente documento sono soggette a modifica senza preavviso.

Legenda diritti limitati

Software riservato. Licenza valida rilasciata da HP richiesta per il possesso, l'uso e la copia. Conformemente alle disposizioni di FAR 12.211 e 12.212, il software per computer commerciale, la documentazione sul software per computer e i dati tecnici per articoli commerciali sono concessi al governo degli Stati Uniti con licenza commerciale standard del fornitore.

Note sul copyright

© Copyright 2005 - 2010 Hewlett-Packard Development Company, L.P

Note sui marchi

Adobe® e Acrobat® sono marchi di Adobe Systems Incorporated.

AMD e il simbolo AMD Arrow sono marchi di Advanced Micro Devices, Inc.

Google™ e Google Maps™ sono marchi di Google Inc.

Intel®, Itanium®, Pentium® e Intel® Xeon® sono marchi di Intel Corporation negli Stati Uniti e negli altri paesi.

Java™ è un marchio statunitense di Sun Microsystems, Inc.

Microsoft®, Windows®, Windows NT®, Windows® XP e Windows Vista® sono marchi registrati negli Stati Uniti di Microsoft Corporation.

Oracle è un marchio registrato di Oracle Corporation e/o sue affiliate.

UNIX® è un marchio registrato di The Open Group.

Riconoscimenti

- Questo prodotto include software sviluppato da Apache Software Foundation (<http://www.apache.org/licenses>).
- Questo prodotto include il codice OpenLDAP di OpenLDAP Foundation (<http://www.openldap.org/foundation/>).
- Questo prodotto include il codice GNU di Free Software Foundation, Inc. (<http://www.fsf.org/>).
- Questo prodotto include il codice JiBX di Dennis M. Sosnoski.
- Questo prodotto include il parser XPP3 XMLPull incluso nella distribuzione e utilizzato in JiBX di Extreme! Lab, Indiana University.
- Questo prodotto include la licenza Office Look and Feels di Robert Futrell (<http://sourceforge.net/projects/officelnfs>).
- Questo prodotto include il codice JEP - Java Expression Parser di Netaphor Software, Inc. (<http://www.netaphor.com/home.asp>).

Aggiornamenti alla documentazione

La pagina del titolo di questo documento contiene le seguenti informazioni identificative:

- Numero di versione del software che indica la versione del software.
- Data di rilascio del documento che cambia ogni volta che il documento viene aggiornato.
- Data di rilascio del software che indica la data di rilascio della versione del software.

Per cercare aggiornamenti recenti o verificare che il documento utilizzato sia il più recente, passare alla pagina:

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

Il sito richiede la registrazione a HP Passport e l'accesso. Per la registrazione a HP Passport, passare alla pagina:

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

Oppure fare clic sul collegamento **New users - please register** nella pagina di accesso HP Passport.

L'utente riceverà inoltre le edizioni aggiornate o nuove se si registra al relativo servizio di assistenza del prodotto. Rivolgersi al proprio rappresentante HP per i dettagli.

Supporto

Visitare il sito HP Software Support all'indirizzo:

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

Questo sito fornisce le informazioni di contatto e i dettagli sui prodotti, i servizi e l'assistenza offerti da HP Software.

L'assistenza online HP Software fornisce al cliente la possibilità di utilizzare soluzioni implementabili dall'utente mediante un accesso veloce ed efficiente agli strumenti di assistenza tecnica interattiva necessari per gestire la propria attività. In qualità di cliente qualificato dell'assistenza è possibile usufruire del sito Web di assistenza per le operazioni seguenti:

- Ricerca di documenti di interesse sulle caratteristiche
- Invio e traccia dei casi di assistenza e delle richieste di ampliamento
- Download delle patch del software
- Gestione dei contratti di assistenza
- Ricerca dei contatti di assistenza HP
- Riesame delle informazioni sui servizi disponibili
- Partecipazione alle discussioni con altri clienti software
- Ricerca e iscrizione alla formazione sul software

La maggior parte delle aree di assistenza richiedono la registrazione e l'accesso come utente di HP Passport. Molte inoltre richiedono un contratto di assistenza. Per la registrazione di un ID utente di HP Passport, visitare la pagina:

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

Per maggiori informazioni sui livelli di accesso, visitare la pagina:

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

Sommario

Introduzione alla guida	15
Organizzazione della guida	16
Destinatari della guida.....	17
HP Universal CMDB Documentazione online.....	17
Ulteriori risorse online	21
Aggiornamenti alla documentazione.....	22

PARTE I: INTRODUZIONE

Capitolo 1: Introduzione a HP Universal CMDB	25
Panoramica di HP Universal CMDB.....	26
HP Universal CMDB su VMware	31
Migrazione da versioni precedenti.....	31
Cambiare l'allocazione di memoria per le applet.....	32
Capitolo 2: Matrice di supporto di HP Universal CMDB	35
Requisiti hardware del server	36
Requisiti del software del server	38
Ambienti virtuali supportati del server	39
Requisiti del database del server.....	40
Requisiti del software del client	44
Requisiti del browser del client	45
Requisiti di pianificazione della capacità	45
Capitolo 3: Modello di licenza di HP Universal CMDB	47
Modello di licenza - Panoramica	48
Licenza di UCMDB Foundation	50
Licenza di UCMDB Integration Only.....	53
Licenza DDM Advanced Edition	54
Licenza di aggiornamento a Integration Only o DDM Advanced Edition.....	56
Risoluzione dei problemi e limitazioni	57

Capitolo 4: Introduzione a HP Universal CMDB	59
Pianificazione di redistribuzione.....	60
Avvio.....	63
Compiti di amministrazione di base.....	64

PARTE II: INSTALLAZIONE DEL SERVER UCMDB

Capitolo 5: Procedura di installazione	67
Procedura di installazione - Panoramica.....	68
Passaggi di installazione.....	69

Capitolo 6: HP Universal CMDB Installazione su una piattaforma Windows	71
Prerequisiti di installazione.....	72
Installare UCMDB	74
Configurare il server della posta di UCMDB.....	83
Disinstallare HP Universal CMDB.....	84

Capitolo 7: HP Universal CMDB Installazione su una piattaforma Linux	87
Prerequisiti di installazione.....	88
Installare HP Universal CMDB.....	90
Configurare il server della posta di UCMDB.....	99
Disinstallare UCMDB	99

Capitolo 8: Configurazione del server UCMDB	101
Scelta del database o dello schema.....	102
Informazioni richieste per l'impostazione dei parametri del database.....	103
Accedere alla procedura guidata di configurazione di UCMDB Server	106
Creare un database Microsoft SQL Server	106
Creare uno schema Oracle	111
Connettersi a un database Microsoft SQL Server esistente.....	115
Connettersi a uno schema Oracle esistente	116
Riavviare il server	116

Capitolo 9: Servizi di HP Universal CMDB	117
Visualizzare lo stato dei servizi del server HP Universal CMDB	118
Avviare e arrestare il servizio del server HP Universal CMDB.....	119
Servizi di HP Universal CMDB	120
Risoluzione dei problemi e limitazioni	122

Capitolo 10: Accedere ai comandi del server UCMDB	123
Accedere ai comandi su piattaforma Windows.....	124
Accedere ai comandi su piattaforma Linux	125

PARTE III: INSTALLAZIONE DELLA SONDA DEL FLUSSO DI DATI

Capitolo 11: Installazione della sonda del flusso di dati su piattaforma Windows	129
Installare la sonda del flusso di dati.....	130
Aggiornamento della sonda	139
Eseguire Probe Manager e Probe Gateway su computer separati.....	140
Configurare i componenti di Probe Manager e Probe Gateway	141
Connettere una sonda del flusso di dati per un cliente non predefinito	142
Requisiti per l'installazione della sonda del flusso di dati	143
Risoluzione dei problemi e limitazioni	145
Capitolo 12: Installazione della sonda del flusso di dati su piattaforma Linux.....	147
Installare la sonda del flusso di dati.....	148
Arrestare il server della sonda.....	157
Aggiornamento della sonda del flusso di dati.....	158
Connettere una sonda del flusso di dati per un cliente non predefinito	158
Requisiti per il supporto della sonda del flusso di dati	159
Risoluzione dei problemi e limitazioni.	159

PARTE IV: AGGIORNAMENTO DI HP UNIVERSAL CMDB DALLA VERSIONE 8.0X A 9.0X

Capitolo 13: Aggiornamento di HP Universal CMDB dalla versione 8.0x alla versione 9.0x.....	163
Aggiornamento - Panoramica	164
Aggiornare HP Universal CMDB - Riepilogo	165
Aggiornamento a UCMDB 9.02	171
Terminare la procedura di aggiornamento	178
Risoluzione dei problemi e limitazioni	179
Capitolo 14: Processo di aggiornamento: descrizioni tecniche	181
Parametri di input per il processo di aggiornamento	182
File di registro per il processo di aggiornamento	183
Passaggi di aggiornamento	184

Capitolo 15: Aggiornamento dei pacchetti dalla versione 8.04 alla 9.02	257
Utilità di migrazione pacchetto - Panoramica	258
Migrare un pacchetto personalizzato	259
Risoluzione dei problemi e limitazioni	262

PARTE V: DISPONIBILITÀ ELEVATA E PIANIFICAZIONE DELLA CAPACITÀ

Capitolo 16: Installazione della modalità disponibilità elevata	265
Procedure consigliate per la disponibilità elevata di HP Universal CMDB.....	266
Transizione tra server attivo e passivo	267
Installare HP Universal CMDB in modalità disponibilità elevata	268
Configurare la disponibilità elevata della rete	273
Configurare il sito completo	274
Capitolo 17: Pianificazione della grande capacità di HP Universal CMDB	275
Pianificazione della grande capacità - Panoramica	276
Nodi gestiti e CI correlati ai nodi	277
Configurazione del server UCMDB	278
Configurazione del database Oracle.....	278
Configurazione del test di sistema	279
Risultati del test di sistema.....	280

PARTE VI: PROTEZIONE AVANZATA DI HP UNIVERSAL CMDB

Capitolo 18: Introduzione alla protezione avanzata	283
Protezione avanzata - Panoramica	284
Preparazione della protezione avanzata	286
Distribuire HP Universal CMDB in un'architettura protetta	287
Cambiare il nome utente o la password di sistema per la console JMX	288
Cambiare l'utente del servizio HP Universal CMDB Server	289

Capitolo 19: Abilitazione della comunicazione Secure	
Sockets Layer (SSL)	291
Attivare SSL sul computer server con certificato autofirmato	292
Abilitare SSL sul computer server con un certificato dall'Autorità di certificazione.....	295
Abilitare SSL sui computer client	297
Abilitare SSL sull'SDK del client	298
Abilitare l'autenticazione reciproca del certificato per SDK.....	298
Cambiare le password del keystore del server	301
Abilitare o disabilitare le porte HTTP/HTTPS	302
Mappare i componenti Web di UCMDB alle porte	304
Capitolo 20: Utilizzo di un proxy inverso	307
Proxy inverso - Panoramica.....	308
Aspetti di protezione nell'utilizzo di un server proxy inverso	310
Configurare un proxy inverso utilizzando le impostazioni dell'infrastruttura	311
Configurare un proxy inverso utilizzando la console JMX	312
Apache 2.0.x - Configurazione di esempio	313
Capitolo 21: Gestione credenziali del flusso di dati	315
Gestione credenziali del flusso di dati - Panoramica	316
Metodi dei dati delle credenziali (Direzione dei dati: verso HP Universal CMDB)	320
Metodi dei dati delle credenziali (Direzione dei dati: verso HP Universal CMDB)	321
Configurare le impostazioni dell'autenticazione e della crittografia del client CM sul server UCMDB	322
Configurare manualmente le impostazioni dell'autenticazione e della crittografia del client CM sulla sonda	324
Configurare la cache del client Confidential Manager (CM)	329
Esportare e importare le informazioni sulle credenziali e sull'intervallo in formato crittografato	332
Cambiare il livello di messaggi del file di registro del client CM	334
Generare o aggiornare la chiave di crittografia	336
Impostazioni della crittografia di CM	342

Capitolo 22: Protezione avanzata della sonda del flusso di dati	345
Impostare la password crittografata del database MySQL	346
Impostare la password crittografata della console JMX	348
Abilitare il protocollo SSL tra il server UCMDB e la sonda del flusso di dati con l'autenticazione reciproca	350
Abilitare l'autenticazione nella sonda del flusso di dati con autenticazione HTTP di base	358
Connettere la sonda del flusso di dati mediante il proxy inverso ...	359
Controllo della posizione del file domainScopeDocument.....	361
Creare un keystore per la sonda del flusso di dati	362
Crittografare le password del keystore e del truststore della sonda..	362
Keystore e truststore predefiniti della sonda del flusso di dati	364
Capitolo 23: Autenticazione Lightweight Single Sign-On (LW-SSO) – Riferimenti generali.....	367
Autenticazione LW-SSO - Panoramica	368
Requisiti di sistema di LW-SSO	370
Avvisi di protezione LW-SSO	371
Risoluzione dei problemi e limitazioni	373
Capitolo 24: Autenticazione per l'accesso a HP Universal CMDB	377
Impostazione del metodo di autenticazione.....	378
Abilitare e definire il metodo di autenticazione LDAP	379
Impostare una connessione protetta con il protocollo SSL (Secure Sockets Layer).....	380
Utilizzare la console JMX per verificare le connessioni LDAP	382
Configurare le impostazioni LDAP utilizzando la console JMX	382
Abilitare l'accesso a HP Universal CMDB con LW-SSO.....	383
Ripristinare la configurazione LW-SSO corrente nell'ambiente distribuito	385
Capitolo 25: Confidential Manager	387
Confidential Manager - Panoramica	388
Considerazioni sulla protezione.....	389
Configurare il server HP Universal CMDB.....	390
Definizioni.....	392
Proprietà di crittografia	393

PARTE VII: RIPRISTINO DI EMERGENZA

Capitolo 26: Impostazione del ripristino di emergenza.....	397
Ripristino di emergenza - Panoramica	398
Preparare l'ambiente del ripristino di emergenza	399
Preparare l'istanza di failover di HP Universal CMDB per l'attivazione.....	402
Eseguire la procedura di pulizia all'avvio	403

PARTE VIII: INTRODUZIONE A HP UNIVERSAL CMDB

Capitolo 27: Accesso a HP Universal CMDB mediante il server Web IIS.....	407
Accesso a HP Universal CMDB mediante IIS - Panoramica	408
Impostazione di IIS per consentire l'accesso a UCMDB - Windows 2003	409
Impostazione di IIS per consentire l'accesso a UCMDB - Windows 2008	413
Configurare la sonda del flusso di dati	416
Capitolo 28: Accesso a HP Universal CMDB.....	417
Accesso a HP Universal CMDB - Panoramica.....	418
Modalità di installazione locale	419
Accesso a HP Universal CMDB e ai rispettivi componenti	420
Abilitare l'accesso automatico	422
Cambiare il limite di tempo predefinito per la disconnessione dell'utente a causa di inattività	423
Capitolo 29: Spostamento in HP Universal CMDB	425
Spostamento nell'interfaccia utente di HP Universal CMDB.....	426
Utilizzo della documentazione di HP Universal CMDB	428
Menu e opzioni	431
Capitolo 30: Risoluzione dei problemi delle risorse disponibili	433
Risoluzione dei problemi delle risorse.....	433
Capitolo 31: Utilizzo di impostazioni internazionali non in lingua inglese	435
Problemi di installazione e distribuzione.....	436
Problemi relativi all'ambiente del database	437
Problemi relativi all'amministrazione	437
Problemi relativi ai report	437
Supporto per Multi-Lingual User (MLU) Interface.....	438
Indice	443

Introduzione alla guida

Introduzione alla guida di distribuzione di HP Universal CMDB. La presente guida di introduzione a HP Universal CMDB fornisce informazioni sull'avvio, descrive l'installazione del server e la rispettiva protezione avanzata e descrive in dettaglio il processo di aggiornamento.

Il capitolo si suddivide in:

- Organizzazione della guida a pag. 16
- Destinatari della guida a pag. 17
- HP Universal CMDB Documentazione online a pag. 17
- Ulteriori risorse online a pag. 21
- Aggiornamenti alla documentazione a pag. 22

Organizzazione della guida

La guida si suddivide nelle parti seguenti:

Parte I Introduzione

Introduce i componenti installati in fase di installazione di HP Universal CMDB e fornisce il workflow di installazione e le scelte di distribuzione.

Parte II Installazione del server UCMDB

Descrive la procedura di installazione del server HP Universal CMDB, compresa la configurazione del database.

Parte III Installazione della sonda del flusso di dati

Descrive la procedura di installazione della sonda del flusso di dati.

Parte IV Aggiornamento di HP Universal CMDB dalla versione 8.0x a 9.0x

Spiega le procedure di aggiornamento (migrazione) di HP Universal CMDB alla versione 9.02 e di migrazione dei pacchetti dalla versione 8.0x alla 9.02.

Parte V Disponibilità elevata e pianificazione della capacità

Descrive le procedure di installazione, di avvio e di configurazione per eseguire HP Universal CMDB versione 9.02 in un ambiente a elevata disponibilità.

Parte VI Protezione avanzata di HP Universal CMDB

Spiega le procedure per la protezione avanzata del server HP Universal CMDB e la sonda del flusso di dati.

Parte VII Ripristino di emergenza

Descrive i principi di base e le linee guida sull'installazione del sistema di ripristino di emergenza.

Parte VIII Introduzione a HP Universal CMDB

Include informazioni sull'accesso a HP Universal CMDB la prima volta subito dopo l'installazione e il menu di avvio. Include anche informazioni sull'accesso a UCMDB tramite il server Web IIS.

Destinatari della guida

La guida è rivolta agli utenti seguenti di HP Universal CMDB:

- Amministratori di HP Universal CMDB
- Amministratori della piattaforma di HP Universal CMDB
- Amministratori delle applicazioni di HP Universal CMDB
- Amministratori della gestione dei dati di HP Universal CMDB

I lettori di questa guida devono avere una buona conoscenza dell'amministrazione del sistema enterprise, avere familiarità con i concetti ITIL e avere una buona conoscenza di HP Universal CMDB.

HP Universal CMDB Documentazione online

HP Universal CMDB comprende la documentazione online seguente:

Leggimi. Fornisce un elenco delle limitazioni delle versioni e degli ultimi aggiornamenti. Dalla directory principale del DVD di HP Universal CMDB, fare doppio clic su **readme.html**. È anche possibile accedere alla versione più aggiornata del file Leggimi dal sito Web HP Software Support.

Novità. Fornisce un elenco delle nuove funzionalità e degli elementi di rilievo delle versioni. In HP Universal CMDB, selezionare **Guida > Novità**.

Documentazione per la stampa. Selezionare **Guida > Guida di UCMDB**. Le seguenti guide sono pubblicate solo in formato PDF:

- *Guida alla distribuzione di HP Universal CMDB* in PDF. Illustra i requisiti hardware e software necessari per impostare HP Universal CMDB, la procedura di installazione o di aggiornamento di HP Universal CMDB, la procedura per la protezione avanzata del sistema e la procedura per effettuare l'accesso all'applicazione.
- *Guida al database di HP Universal CMDB* in PDF. Illustra come impostare il database (MS SQL Server o Oracle) richiesto da HP Universal CMDB.

- ▶ *HP Universal CMDB Discovery and Integration Content Guide* in PDF. Illustra come eseguire l'individuazione per individuare le applicazioni, i sistemi operativi e i componenti di rete nel proprio sistema. Illustra inoltre come individuare i dati su altri repository di dati tramite l'integrazione.

La guida in linea di HP Universal CMDB comprende:

- ▶ **Guida alla modellazione.** Consente di gestire il contenuto del proprio modello Universo IT.
- ▶ **Guida di Gestione flusso di dati.** Consente di integrare HP Universal CMDB con altri repository di dati e come impostare HP Universal CMDB per individuare i componenti di rete.
- ▶ **Guida all'amministrazione.** Illustra come utilizzare HP Universal CMDB.
- ▶ **Guida di riferimento per lo sviluppatore.** Per gli utenti con una conoscenza avanzata di HP Universal CMDB. Illustra come definire e utilizzare gli adattatori e come utilizzare le API per l'accesso ai dati.

La Guida in linea è disponibile dalle finestre specifiche di HP Universal CMDB facendo clic nella finestra e sul pulsante **Guida**.

È possibile visualizzare e stampare le documentazioni in linea utilizzando Adobe Reader, che può essere scaricato dal sito Web Adobe (www.adobe.com).

Tipi di argomenti

All'interno della guida, ciascuna area di interesse è organizzata in argomenti. Un argomento contiene un modulo distinto di informazioni per un oggetto. In genere gli argomenti sono classificati in base al tipo di informazioni che contengono.

Questa struttura è stata progettata per creare un accesso più semplice a informazioni specifiche, suddividendo la documentazione in tipi diversi di informazioni che possono essere necessarie di volta in volta.

Sono utilizzati tre tipi di argomenti principali: **Concetti**, **Compiti** e **Riferimenti**. I tipi di argomenti sono stati differenziati visivamente tramite l'uso di icone.

Tipo di argomento	Descrizione	Utilizzo
Concetti 	Informazioni di background, descrittive o concettuali.	Conoscere informazioni generali su una funzionalità.
Compiti 	<p>Compiti di istruzione. Guida dettagliata per l'utilizzo dell'applicazione e il completamento degli obiettivi. Alcuni passaggi dei compiti comprendono esempi con l'utilizzo di dati campione. I passaggi dei compiti possono essere numerati o non numerati:</p> <ul style="list-style-type: none"> ▶ Passaggi numerati. Compiti che vengono eseguiti seguendo ogni passaggio in ordine consecutivo. ▶ Passaggi non numerati. Un elenco di operazioni complete che si possono eseguire in qualsiasi ordine. <p>Compiti di uno scenario nei casi di utilizzo. Esempi di come eseguire un compito per una situazione specifica.</p>	<ul style="list-style-type: none"> ▶ Imparare il workflow completo di un compito. ▶ Seguire i passaggi elencati in un compito numerato per completare un compito. ▶ Eseguire operazioni indipendenti completando i passaggi in un compito non numerato. <p>Imparare come potrebbe essere eseguito un compito in uno scenario realistico.</p>

Tipo di argomento	Descrizione	Utilizzo
Riferimenti 	Riferimenti generali. Elenchi e spiegazioni dettagliati di materiale orientato ai riferimenti.	Cercare una parte specifica di informazioni sui riferimenti rilevanti per un contesto particolare.
	Riferimenti dell'interfaccia utente. Argomenti su riferimenti specializzati che descrivono una determinata interfaccia utente nel dettaglio. Selezionando Guida per questa pagina dal menu della Guida nel prodotto in genere si aprono gli argomenti dell'interfaccia utente.	Cercare informazioni specifiche su cosa inserire o come utilizzare uno o più elementi specifici dell'interfaccia utente, come ad esempio una finestra, una finestra di dialogo o una procedura guidata.
Risoluzione dei problemi e limitazioni 	Risoluzione dei problemi e limitazioni. Argomenti su riferimenti specializzati che descrivono i problemi comunemente incontrati e le relative soluzioni e che elencano le limitazioni di una funzionalità o di un'area di prodotto.	Aumentare il riconoscimento di problemi importanti prima di utilizzare una funzionalità oppure se si incontrano problemi di usabilità nel software.

Ulteriori risorse online

Risoluzione dei problemi & Knowledge Base consente di accedere alla pagina Risoluzione dei problemi sul sito Web HP Software Support dove è possibile effettuare ricerche nella Knowledge Base con soluzioni implementabili dall'utente. Selezionare **Guida > Risoluzione dei problemi & Knowledge Base**. L'URL del sito Web è <http://h20230.www2.hp.com/troubleshooting.jsp>.

HP Software Support consente di accedere al sito Web HP Software Support. Il sito consente di esplorare la knowledge base con soluzioni implementabili dall'utente. È inoltre possibile registrare un messaggio o cercare forum di discussione tra utenti, inoltrare richieste di assistenza, scaricare patch e documentazione aggiornata e così via. Selezionare **Guida > HP Software Support**. L'URL del sito Web è www.hp.com/go/hpsupport.

La maggior parte delle aree di assistenza richiedono la registrazione e l'accesso come utente di HP Passport. Molte inoltre richiedono un contratto di assistenza.

Per maggiori informazioni sui livelli di accesso, visitare la pagina:

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

Per la registrazione di un ID utente di HP Passport, visitare la pagina:

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

Il sito Web HP Software consente di accedere al sito Web HP Software. In questo sito sono presenti le informazioni più aggiornate sui prodotti software HP. Sono compresi anche nuove versioni software, seminari, fiere, assistenza clienti e così via. Selezionare **Guida > Sito Web HP Software**. L'URL del sito Web è www.hp.com/go/software.

Aggiornamenti alla documentazione

HP Software aggiorna costantemente la documentazione sui prodotti aggiungendo nuove informazioni.

Per cercare aggiornamenti recenti o verificare che il documento utilizzato sia il più recente, visitare il sito Web sui manuali dei prodotti software HP (<http://h20230.www2.hp.com/selfsolve/manuals>).

Parte I

Introduzione

1

Introduzione a HP Universal CMDB

Questo capitolo comprende:

Concetti

- Panoramica di HP Universal CMDB a pag. 26
- HP Universal CMDB su VMware a pag. 31
- Migrazione da versioni precedenti a pag. 31

Compiti

- Cambiare l'allocazione di memoria per le applet a pag. 32

Concetti

Panoramica di HP Universal CMDB

In questo capitolo viene illustrato HP Universal CMDB, i passaggi principali dell'installazione di HP Universal CMDB, viene presentato il workflow di installazione, vengono fornite informazioni sui prerequisiti di hardware, software e configurazione e viene spiegato come procedere con l'avvio.

In questa sezione vengono trattati i seguenti argomenti:

- “Informazioni su HP Universal CMDB” a pag. 26
- “Architettura di sistema di HP Universal CMDB” a pag. 28
- “HP Universal CMDB Distribuzione” a pag. 28
- “Configuration Management Database (CMDB)” a pag. 29
- “Mappatura di Gestione flusso di dati” a pag. 29
- “Topology Query Language (TQL)” a pag. 30
- “Convenzioni relativi ai documenti” a pag. 30

Informazioni su HP Universal CMDB

HP Universal CMDB è composto da un modello di dati basato sul servizio aziendale con individuazione incorporata di elementi di configurazione (CI, configuration item) e dipendenze dei CI, visualizzazione e mappatura dei servizi aziendali e il tracciamento dei cambiamenti di configurazione.

HP Universal CMDB consente di gestire tutti i CI contenuti in un ambiente gestito. Un ambiente gestito si riferisce a qualsiasi ambiente completo che può essere descritto utilizzando un modello di topologia (definito con il linguaggio Topology Query Language (TQL) di HP). Ad esempio, l'infrastruttura di una grande azienda IT rappresenta un ambiente gestito dove la topologia comprende più livelli quali reti, protocolli, database, sistemi operativi e così via. Le viste vengono gestite per visualizzare le informazioni esattamente nel formato richiesto.

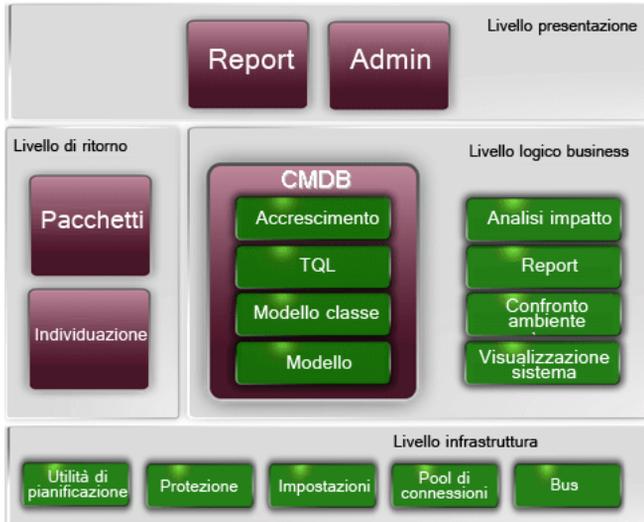
Inoltre le informazioni contenute nei risultati di ciascuna TQL vengono aggiornate automaticamente con l'immissione dei dati più recenti nel database di gestione della configurazione (CMDB, configuration management database). In questo modo, una volta definita una TQL e una vista, queste continuano a fornire informazioni aggiornate sullo stato corrente dell'ambiente gestito. Le viste vengono visualizzate in mappe a più livelli che consentono di identificare i CI chiave, a seconda delle esigenze. È inoltre possibile creare report, in formato HTML, Excel o tabella, sulle informazioni raccolte dal sistema.

HP Universal CMDB soddisfa le esigenze operative e funzionali seguenti:

- ▶ **Allineamento delle risorse e delle applicazioni IT.** Individuazione automatica delle risorse IT e delle rispettive interdipendenze da una prospettiva di servizio aziendale.
- ▶ **Risoluzione dei problemi.** Comprensione delle relazioni di causa tra CI per individuare e risolvere la causa principale dei problemi di infrastruttura per ridurre il tempi di risoluzione dei problemi.
- ▶ **Controllo della gestione degli asset e dei cambiamenti.** Rilevamento automatico dei cambiamenti dell'infrastruttura per consentire l'aggiornamento automatico di tutti i sottosistemi rilevanti.
- ▶ **Gestione dello stato personalizzato (prestazione, cambiamento).** Capacità di definire uno stato per la gestione dei CI.
- ▶ **Gestione delle prestazioni e pianificazione delle capacità.**
- ▶ **Pianificazione dell'architettura e dell'infrastruttura.**
- ▶ **Dati di federazione e riconciliazione.** Recuperati da repository esistenti e altri CMDB.

Architettura di sistema di HP Universal CMDB

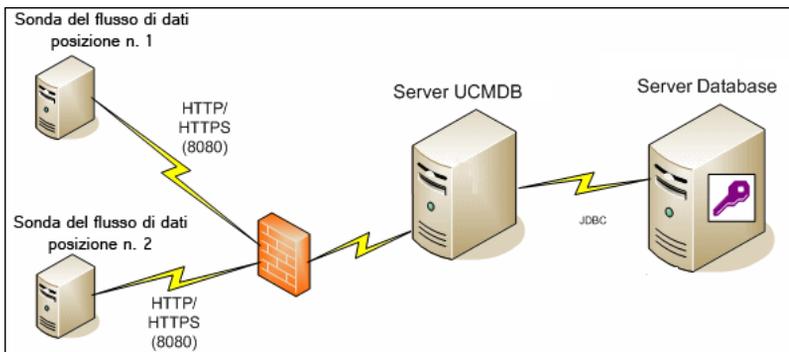
Nel diagramma seguente viene fornita una panoramica grafica dell'architettura di sistema di HP Universal CMDB:



Per impostare un metodo di autenticazione LDAP per eseguire l'accesso, consultare "Autenticazione per l'accesso a HP Universal CMDB" a pag. 377.

HP Universal CMDB Distribuzione

Nel diagramma seguente viene fornita una panoramica grafica di una distribuzione tipica del sistema di HP Universal CMDB.



Configuration Management Database (CMDB)

Il CMDB è un repository centrale per le informazioni di configurazione raccolte dalle varie applicazioni e strumenti di HP Universal CMDB e di terze parti.

Il CMDB contiene CI e relazioni creati automaticamente dal processo di individuazione o inseriti manualmente. I CI e le relazioni rappresentano un modello dei componenti del mondo IT in cui funziona la propria azienda.

Il CMDB consente inoltre di archiviare e gestire i dati dell'infrastruttura raccolti e aggiornati da Gestione flusso di dati.

Il modello IT può avere grandi dimensioni e contenere migliaia di CI. Per facilitarne la gestione di questi CI, utilizzare i CI in una vista che fornisce un subset di tutti i componenti del mondo IT.

Utilizzare le viste (le viste predefinite fornite con HP Universal CMDB o definite nella Mappa topologica) per visualizzare e gestire i CI e le relazioni nel CMDB. Le viste consentono di concentrarsi su determinate aree IT.

Il CMDB contiene inoltre le definizioni di query TQL utilizzate per interrogare e recuperare dati dal CMDB per la presentazione in:

- viste sequenza (viste basate su TQL)
- modello del tipo di elemento di configurazione (CIT, configuration item type) (repository di tutte le definizioni delle relazioni e dei i tipi di CI)

Nota: è possibile connettersi al CMDB da altri prodotti HP. Per i dettagli consultare la documentazione sull'installazione del prodotto.

Mappatura di Gestione flusso di dati

Il processo di individuazione è il meccanismo che consente di raccogliere dati sul sistema mediante l'individuazione delle risorse dell'infrastruttura IT e le rispettive interdipendenze (relazioni). Il flusso di dati è in grado di individuare le risorse, ad esempio applicazioni, database, periferiche di rete, diversi tipi di server e così via. Ciascuna risorsa IT individuata viene fornita e memorizzata nel database di gestione della configurazione (CMDB) dove viene rappresentata come elemento di configurazione gestito (CI).

Topology Query Language (TQL)

TQL è un linguaggio e uno strumento per l'individuazione, l'organizzazione e la gestione dei dati dell'infrastruttura IT. Viene utilizzato per creare query per il recupero di determinati dati dal CMDB e la rispettiva visualizzazione.

TQL esegue costantemente ricerche sul CMDB per individuare i cambiamenti occorsi allo stato delle risorse gestite, fornisce informazioni e aggiorna i sottosistemi rilevanti.

TQL estende il linguaggio query tradizionale aggiungendo due importanti funzioni:

- ▶ TQL consente a HP Universal CMDB di tracciare relazioni concettuali tra CI che rappresentano le reali interdipendenze. Utilizzando operatori predefiniti, è possibile stabilire i diversi tipi d'interconnessioni esistenti tra i CI e, di conseguenza, presentare con maggiore precisione il design e le prestazioni dell'infrastruttura. Questa rappresentazione funge da base e modello per la scoperta, l'organizzazione, l'interrogazione e la gestione di complesse infrastrutture.
- ▶ TQL comprende un aspetto grafico composto di simboli visivi e sintassi che rappresentano le risorse e le relative interconnessioni. La visualizzazione di un'infrastruttura IT semplifica la comprensione, il monitoraggio e la gestione delle operazioni aziendali IT.

Convenzioni relativi ai documenti

- ▶ Nella documentazione di HP Universal CMDB si presume che HP Universal CMDB Server e Data Flow Probe siano installati nel percorso predefinito, ovvero **C:\hp\UCMDB\UCMDBServer** e **C:\hp\UCMDB\DataFlowProbe**.
- ▶ Le istruzioni di accesso ai componenti dell'applicazione indicano sempre il percorso nel menu a sinistra, ad esempio per visualizzare la query topologica di Active Directory: **Modellazione > Studio di modellazione > Risorse > Root > Application > Active Directory**.

HP Universal CMDB su VMware

Se si sta distribuendo HP Universal CMDB su una piattaforma VMware non si applicano le linee guida sul dimensionamento per un'installazione normale. Le restrizioni e i consigli generali seguenti si applicano a un'installazione VMware:

- Si può prevedere che le prestazioni di HP Universal CMDB su VMware saranno più lente rispetto a un'installazione normale. Per una distribuzione aziendale di HP Universal CMDB si sconsiglia quindi una piattaforma VMware, che è supportata solo per distribuzioni standard. Per i requisiti della distribuzione consultare “Requisiti hardware del server” a pag. 36.
- Le capacità e le prestazioni di HP Universal CMDB variano in base alle diverse risorse del server come CPU, memoria e larghezza della banda di rete, allocate ai componenti di HP Universal CMDB.
- Si consiglia di utilizzare ESX Server versione da 3.5 a 4.0.
- Utilizzare una scheda di rete gigabit.
- Si consiglia di non eseguire un server di database contenente HP Universal CMDB su VMware se i file del database risiedono su un disco virtuale VMware.
- VMware è l'unica tecnologia di virtualizzazione supportata da HP Universal CMDB per Windows.

I componenti di HP Universal CMDB seguenti sono supportati su VMware ESX Server versioni da 3.5 a 4.0:

- HP Universal CMDB
- Sonda del flusso di dati

Migrazione da versioni precedenti

Per i dettagli sull'aggiornamento di HP Universal CMDB dalla versione 8.0x alla 9.02 consultare “Aggiornamento di HP Universal CMDB dalla versione 8.0x alla versione 9.0x” a pag. 163.

Per i dettagli sull'aggiornamento di HP Universal CMDB dalla versione 7.0x e 7.5x a 8.0x consultare la documentazione sulla versione 8.04.

Compiti

Cambiare l'allocazione di memoria per le applet

Nota: questa sezione è pertinente solo se si sta eseguendo la connessione a HP Universal CMDB da un client che utilizza JRE 6u9 o versione precedente.

Per utilizzare correttamente le applet di HP Universal CMDB è possibile che sia necessaria maggiore memoria di quella allocata per impostazione predefinita, specialmente quando si visualizzano mappe topologiche di grandi dimensioni oppure si utilizza l'applet per un lungo periodo senza riavviare il browser.

Per cambiare l'allocazione di memoria, modificare un file sul client (il computer dell'utente che utilizza l'applet):

- 1 Su computer Windows aprire il file: ...**Documents and Settings**\%userprofile%\ApplicationData\Sun\Java\Deployment\deployment.properties.
- 2 Cambiare la riga con l'ultima versione di Java aggiungendo il testo **-XmxYYYm** alla fine dove **YYY** è la quantità di memoria (in megabyte) da allocare all'applet Java. Ad esempio:

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

alloca 256 MB di memoria all'applet.

Il valore predefinito (se non esiste alcun parametro **-Xmx**) è 64 MB. È possibile provare con i valori 128 MB e 256 MB. Si consiglia di non utilizzare più di 256 MB. Se Java non è in grado di acquisire la memoria indicata, il caricamento non avviene. In questo caso, impostare l'allocazione di memoria su un valore inferiore.

È inoltre possibile eseguire questo cambiamento selezionando **Start > Impostazioni > Pannello di controllo**. Fare doppio clic sull'icona Java e fare clic sulla scheda **Java**. Fare clic sul pulsante **Visualizza** per Runtime settings are used when an applet is executed. Apportare i cambiamenti nel campo Java Runtime Parameters in base alle istruzioni precedenti.

Nota:

- A causa di restrizioni tecnologiche, quando si cambia modalità (ad esempio da Admin a Application) o si cambiano Gestori prima di aver scaricato tutte le applet nel browser, è possibile che venga visualizzato il messaggio di errore **Errore irreversibile**. In questo caso cancellare la cache di Java.
 - Per visualizzare l'avanzamento del download dei jars dell'applet, nella finestra Java Console immettere **5**.
 - Per i dettagli sull'installazione o l'aggiornamento di Java sul client consultare "Updating the Java Configuration" on page 177.
-

2

Matrice di supporto di HP Universal CMDB

Questo capitolo comprende:

Riferimenti

- Requisiti hardware del server a pag. 36
- Requisiti del software del server a pag. 38
- Ambienti virtuali supportati del server a pag. 39
- Requisiti del database del server a pag. 40
- Requisiti del software del client a pag. 44
- Requisiti del browser del client a pag. 45
- Requisiti di pianificazione della capacità a pag. 45

Riferimenti

Requisiti hardware del server

<p>Computer/ processore</p>	<p>Windows/Linux:</p> <p>Per soddisfare i requisiti della CPU, è necessario disporre di uno dei processori seguenti:</p> <ul style="list-style-type: none"> ▶ Intel Dual Core Xeon Processor 2.4 GHz o superiore ▶ AMD Opteron Dual Core Processor 2.4 GHz o superiore <p>Oltre ai requisiti precedenti, è necessario disporre dei seguenti numeri di CPU Core, a seconda della configurazione della distribuzione:</p> <ul style="list-style-type: none"> ▶ Distribuzione piccola: 1 CPU ▶ Distribuzione standard: 4 CPU ▶ Distribuzione enterprise: 8 CPU <p>Nota: Poiché le prestazioni di HP Universal CMDB dipendono dalla velocità del processore, per garantire prestazioni adeguate di HP Universal CMDB si consiglia di utilizzare la velocità maggiore possibile per il processore.</p>
<p>Memoria</p>	<p>Windows/Linux:</p> <ul style="list-style-type: none"> ▶ Distribuzione piccola: 4 GB RAM ▶ Distribuzione standard: 8 GB RAM ▶ Distribuzione enterprise: 16 GB RAM

<p>Memoria virtuale/ file di memoria swap</p>	<p>Windows:</p> <ul style="list-style-type: none"> ➤ Distribuzione piccola: 6 GB (supportati) ➤ Distribuzione standard: 12 GB ➤ Distribuzione enterprise: 24 GB <p>Linux:</p> <ul style="list-style-type: none"> ➤ Distribuzione piccola: 4 GB (supportati) ➤ Distribuzione standard: 8 GB ➤ Distribuzione enterprise: 16 GB <p>Nota:</p> <ul style="list-style-type: none"> ➤ La memoria virtuale per Windows deve essere almeno 1,5 volte le dimensioni della memoria fisica. ➤ Il file swap Linux deve essere uguale alle dimensioni della memoria fisica.
<p>Spazio libero su disco rigido</p>	<p>Minimo 30 GB (per registri, dump di memoria e così via)</p>
<p>Display</p>	<p>Windows: impostazione della tavolozza dei colori su almeno 256 colori (consigliati: 32.000 colori)</p>

Requisiti del software del server

Piattaforma hardware	Tipo di sistema operativo	Versione ed edizione SO	Supportato	Consigliato
x86-64	Windows 2003	Enterprise SP2 e R2 SP2, 64-bit	Sì	
x86-64	Windows 2008	Enterprise SP2 e R2, 64-bit	Sì	Sì
x86-64	Red Hat Linux 5	Enterprise/Advanced, 64-bit	Sì	
Qualsiasi	SUSE Linux 9, 10, 11	Enterprise	No	
x86	Windows 2000, 2003/2008		No	64-bit obbligatorio
Sun SPARC	Solaris 8, 9 or10		No	
Qualsiasi	Red Hat Linux 3, 4	Enterprise	No	
Itanium 64	Red Hat Linux 5	Enterprise/Advanced	No	

Nota:

- Le configurazioni non supportate sono elencate per garantire che non ci sia ambiguità riguardo l'ambito della matrice di supporto.
- Si consiglia di abilitare e configurare in modalità automatica il Dr. Watson (dopo aver eseguito almeno una volta il Dr. Watson, Drwtsn32.exe). Per impostare la modalità automatica cercare `\\HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\AeDebug` nel registro di Windows e impostare il valore del parametro automatico su **1**.
- A prescindere alla versione del sistema operativo, sono richiesti l'intera distribuzione (con supporto OEM) e l'ultima versione del cluster della patch consigliata.

Ambienti virtuali supportati del server

Ambiente virtuale	Versione ed edizione SO	Supportato	Consigliato
VMware ESX 4.0	<ul style="list-style-type: none"> ▶ Windows 2003 Enterprise SP2 e R2 SP2, 64-bit ▶ Windows 2008 Enterprise SP2 e R2, 64-bit ▶ Red Hat Linux 5 Enterprise/Advanced, 64-bit 	Sì	Sì
VMware ESX version 3.5 o versione 3.x	<ul style="list-style-type: none"> ▶ Windows 2003 Enterprise SP2 e R2 SP2, 64-bit ▶ Windows 2008 Enterprise SP2 e R2, 64-bit ▶ Red Hat Linux 5 Enterprise/Advanced, 64-bit 	Sì	Versione di ESX 3.x precedenti potrebbero non fornire una prestazione adeguata e potrebbero non essere supportate su tutte le versioni del sistema operativo.
MS Hyper-V Server 2008 v1 e R2	Qualsiasi	No	
Xen Hypervisor 3.x	Qualsiasi	No	
ESXi	Qualsiasi	No	

Requisiti del database del server

Questa sezione descrive i server del database supportati per l'utilizzo di HP Universal CMDB.

In questa sezione vengono trattati i seguenti argomenti:

- “Requisiti di sistema Oracle” a pag. 40
- “Requisiti di sistema di Microsoft SQL Server” a pag. 42

Requisiti di sistema Oracle

Nella tabella seguente sono elencati gli Oracle Server supportati per l'utilizzo con HP Universal CMDB. Se un'opzione è supportata significa che il personale HP addetto al controllo qualità ha eseguito con esito positivo i test di base su tale opzione.

Versione del database	
Versione	Tipo di sistema
Oracle 10.2 (10.2.0.4 o numero di versione superiore specifica per il componente 10.2.0.X) Enterprise Edition	64-bit
Oracle 10.2 (10.2.0.4 o numero di versione superiore specifica per il componente 10.2.0.X) RAC Enterprise Edition	64-bit
Oracle 11.1.0.7 Enterprise Edition	64-bit
Oracle 11.2 (11g R2) Standard Edition	64-bit
Oracle 11.2 (11g R2) Enterprise Edition	64-bit
Oracle 11.2 (11g R2) RAC Enterprise Edition	64-bit

Nota:

- Si consiglia di applicare le patch Oracle critiche più recenti per ogni sistema operativo. Per i dettagli consultare la documentazione Oracle.
- Consultare la documentazione Oracle per le piattaforme supportate.
- È necessario abilitare l'opzione di partizione Oracle.

Esempi di distribuzioni testate

Nella tabella seguente sono forniti i dettagli sugli ambienti di distribuzione sottoposti a test rigorosi da parte del personale HP addetto al controllo qualità.

Versione del database		Sistema operativo
Versione	Tipo di sistema	
Oracle 11.2 (11g R2) Enterprise Edition	64-bit	Linux Enterprise Edition RHEL 5
Oracle 11.2 (11g R2) RAC Enterprise Edition	64-bit	Linux Enterprise Edition RHEL 5
Oracle 10.2.0.4 Enterprise Edition	64-bit	Linux Enterprise Edition RHEL 5
Oracle 11.2 (11g R2) Enterprise Edition	64-bit	Solaris 10

Requisiti di sistema di Microsoft SQL Server

Nella tabella seguente sono elencati i Microsoft SQL Server supportati per l'utilizzo con HP Universal CMDB. Se un'opzione è supportata significa che il personale HP addetto al controllo qualità ha eseguito con esito positivo i test di base su tale opzione.

Versione del database		
Versione	Tipo di sistema	Service Pack
Microsoft SQL Server 2008 Enterprise Edition	32-bit	Service Pack 1
Microsoft SQL Server 2008 Enterprise Edition	64-bit	Service Pack 1
Microsoft SQL Server 2008 Standard Edition	32-bit	Service Pack 1
Microsoft SQL Server 2008 Standard Edition	64-bit	Service Pack 1
Microsoft SQL Server 2005 Enterprise Edition	32-bit	Service Pack 3
Microsoft SQL Server 2005 Enterprise Edition	64-bit	Service Pack 3

Nota:

- ▶ Installare soltanto i service pack supportati con le patch più recenti.
 - ▶ Consultare la documentazione Microsoft per le piattaforme supportate.
-

Esempi di distribuzioni testate

Nella tabella seguente sono forniti i dettagli sugli ambienti di distribuzione sottoposti a test rigorosi da parte del personale HP addetto al controllo qualità.

Versione del database			Sistema operativo
Versione	Tipo di sistema	Service Pack	
Microsoft SQL Server 2008 Enterprise Edition	32-bit	Service Pack 1	Windows 2008 Enterprise Edition Service Pack 1
Microsoft SQL Server 2008 Enterprise Edition	64-bit	Service Pack 1	Windows 2008 Enterprise Edition Service Pack 1 (64-bit)

Requisiti del software del client

Risoluzione schermo	Risoluzione minima: 1024x768. Si consiglia di utilizzare 1280x1024. Per gli schermi grandi (ad es. per laptop 15.4") la risoluzione migliore è 1600x1050.
Java Runtime Environment (per la visualizzazione dell'applet)	<p>Famiglia 1.6: La versione consigliata è 6u20 e la versione richiesta è 6u4 o successive. 6u19 non è consigliata poiché a ogni caricamento dell'applet si apre una finestra pop-up con un messaggio che comunica che l'applet contiene un mix di codice firmato e non.</p> <p>Nota: la versione JRE consigliata è 6u20, inclusa anche sul server UCMDDB per il download di rete locale.</p> <p>Per cambiare la JRE disponibile in locale:</p> <ol style="list-style-type: none"> collocare il file eseguibile della nuova distribuzione di JRE in: C:\hp\UCMDDB\UCMDDBServer\deploy\ucmdb-ui\static\JRE Riavviare il server. <p>Per i dettagli sull'utilizzo delle applet consultare "Cambiare l'allocazione di memoria per le applet" a pag. 32.</p> <p>Se si utilizza Microsoft Internet Explorer, è possibile scaricare Sun JRE dal sito Web di Java (http://java.com/).</p> <p>Dopo l'installazione, verificare che il browser utilizzi la versione di Java corretta. Fare clic sulla scheda Strumenti > Opzioni Internet > Avanzate e selezionare la casella di controllo Java (Sun). Fare clic su OK, chiudere il browser e riaprirlo.</p>
Java caching	Abilitare il caching di Java sul computer client: Pannello di controllo > Java > scheda Generale > File temporanei Internet > Impostazioni > Archivia i file temporanei sul computer.
Supporto dei tag dell'applet	<p>Le applet di UCMDDB supportano soltanto la distribuzione del tag dell'applet.</p> <p>Per verificare che il computer client supporti i tag dell'applet, aprire il pannello di controllo di Java. Fare clic sulla scheda Avanzate e aprire Java predefinito per browser. Verificare che sia selezionato Microsoft Internet Explorer.</p>
Flash Player (per visualizzare i grafici nei report)	Acrobat Flash 8 o successivo.
Microsoft Excel (per visualizzare i dati esportati)	Versioni 2003, 2007 e 2010
Adobe PDF (per visualizzare i dati esportati)	Versioni 7.0, 8.1 e 9.1

Requisiti del browser del client

Browser	Versione ed edizione SO	Supportato	Consigliato
Internet Explorer 7 o superiore	Windows XP 32/64-bit Windows Vista 32/64-bit Windows 7 32/64-bit Windows 2003 32/64-bit Windows 2008 32/64-bit	Sì	Sì
Internet Explorer 8	Windows XP 32/64-bit Windows Vista 32/64-bit Windows 7 32/64-bit Windows 2003 32/64-bit Windows 2008 32/64-bit	Sì	
Google Chrome	Windows XP Windows Vista Windows 7	Sì	
Firefox 3.5 o superiore	Windows XP Windows Vista Windows 7 Windows 2003 Linux	Sì	
Safari 4.x	Windows	No	
Internet Explorer 6	Windows	No	

Requisiti di pianificazione della capacità

Per i dettagli consultare “Pianificazione della grande capacità di HP Universal CMDB” a pag. 275.

3

Modello di licenza di HP Universal CMDB

Questo capitolo:

Concetti

- ▶ Modello di licenza - Panoramica a pag. 48
- ▶ Licenza di UCMDB Foundation a pag. 50
- ▶ Licenza di UCMDB Integration Only a pag. 53
- ▶ Licenza DDM Advanced Edition a pag. 54

Compiti

- ▶ Licenza di aggiornamento a Integration Only o DDM Advanced Edition a pag. 56

Riferimenti

- ▶ Risoluzione dei problemi e limitazioni a pag. 57

Concetti

Modello di licenza - Panoramica

Il modello di licenza di HP Universal CMDB si basa su tre tipi complementari di licenza o livelli di licenza. Il primo, noto come Licenza di UCMDB Foundation, viene concesso gratuitamente ai clienti idonei. Gli altri due livelli (Licenza di UCMDB Integration Only e DDM Advanced Edition) sono a pagamento.

In questa sezione vengono trattati i seguenti argomenti:

- ▶ “Livelli di licenza” a pag. 48
- ▶ “Unità di misura” a pag. 49

Livelli di licenza

▶ **Licenza di UCMDB Foundation**

Questa licenza concede il diritto di:

- ▶ utilizzare UCMDB come componente principale di prodotti BTO selezionati
- ▶ integrare le istanze di UCMDB con le altre
- ▶ integrare i prodotti BTO con UCMDB utilizzando vari tipi di integrazioni

▶ **Licenza di UCMDB Integration Only**

Questa licenza concede il diritto di integrare prodotti di terze parti (non-HP) con UCMDB utilizzando vari tipi di integrazioni.

▶ **Licenza DDM Advanced Edition**

Questa licenza concede il diritto di:

- utilizzare tutte funzionalità di Discovery and Dependency Mapping (DDM) per popolare UCMDB
- integrare prodotti BTO e di terze parti (non-HP) con UCMDB utilizzando qualsiasi tipo di integrazione

Nella tabella seguente viene fornita una panoramica di funzionalità permesse a seconda delle varie licenze:

Licenza/Integrazione	Integrazioni con altri prodotti BTO	Integrazioni con prodotti di terze parti	Integrazioni personalizzate di tipo individuazione	Tutte le funzionalità di individuazione
UCMDB Foundation	Permessa	No	No	No
UCMDB Integration Only	No	Permessa	No	No
DDM Advanced Edition	Permessa	Permessa	Permessa	Permessa

Unità di misura

➤ Istanza del sistema operativo

Ogni implementazione di un programma di avvio che si può installare su un sistema fisico o una partizione nel sistema fisico. Un sistema fisico può contenere più istanze del sistema operativo.

➤ Server gestito

Un sistema o partizione di sistema dove è installato un programma di avvio, esclusi personal computer o computer per un singolo individuo.

Nota: stampanti e periferiche di rete non sono considerate server gestiti.

Licenza di UCMDB Foundation

Questa è una licenza gratuita per il prodotto UCMDB che viene concessa automaticamente a qualsiasi cliente HP che acquista HP Discovery and Dependency Mapping (DDM), HP Service Manager (SM) o HP Asset Manager (AM).

Questa sezione include inoltre:

- ▶ “Integrazioni BTO standard” a pag. 50
- ▶ “Altre integrazioni” a pag. 51
- ▶ “Numero di CI e relazioni” a pag. 51
- ▶ “Numero di istanze di UCMDB” a pag. 52
- ▶ “Numero di istanze della sonda del flusso di dati” a pag. 52
- ▶ “Caso particolare di BSM” a pag. 52

Integrazioni BTO standard

Questa licenza consente di integrare i seguenti prodotti BTO con UCMDB:

- ▶ HP Universal CMDB * (istanza diversa)
- ▶ HP Asset Manager *
- ▶ HP Service Manager *
- ▶ HP DDM Inventory
- ▶ HP Network Node Manager
- ▶ HP Storage Essentials
- ▶ HP Systems Insight Manager

(*) integrazione bidirezionale

I flussi di dati tra questi prodotti vengono implementati per mezzo di adattatori preimpostati forniti con HP Universal CMDB o con la soluzione SACM. La maggior parte degli adattatori può usufruire dell'infrastruttura della sonda del flusso di dati di HP Universal CMDB, salvo quelli che supportano un flusso di dati di federazione o il flusso di dati di invio da UCMDB a SM a causa di una limitazione di tipo tecnico.

Nota: il flusso di dati da UCMDB ad Asset Manager si basa su un connettore Connect-It che viene concesso in licenza gratuitamente ai clienti di AM.

Il diritto concesso dalla licenza di UCMDB Foundation per l'integrazione dei prodotti BTO con UCMDB non elimina la necessità per i clienti di ottenere una licenza idonea di questi prodotti.

Altre integrazioni

Questa licenza consente inoltre di integrare i prodotti BTO con UCMDB utilizzando:

- ▶ integrazioni standard fornite dai partner HP (si possono applicare ulteriori costi)
- ▶ le integrazioni per lo scambio di dati personalizzati (ovvero l'adattatore generico del database, l'adattatore Push generico e gli adattatori Java personalizzati)
- ▶ l'API del servizio Web di HP Universal CMDB e l'API (Java) di HP Universal CMDB
- ▶ ma non integrazioni di tipo individuazione (ovvero quelle create utilizzando gli adattatori Jython)

Numero di CI e relazioni

La licenza di UCMDB Foundation non limita il numero di CI e relazioni che si possono memorizzare in UCMDB o scambiare tra UCMDB e altri prodotti BTO. L'unica limitazione è la capacità fisica e la prestazione.

Numero di istanze di UCMDDB

La licenza di UCMDDB Foundation non limita il numero di istanze di UCMDDB che si possono distribuire in un ambiente del cliente a scopo di implementazione di sviluppo, test, produzione, piattaforme HA e/o DR. Si potrebbero comunque applicare limitazioni tecniche riguardo la modalità di gestione e lo scambio dei dati in un'installazione di tipo multi-istanza. I server individuati mediante DDM o originati da un prodotto di terze parti devono essere conteggiati una sola volta nella licenza di DDM Advanced Edition o UCMDDB Integration Only anche se sono presenti in più istanze di UCMDDB a scopo di gestione operativa.

Numero di istanze della sonda del flusso di dati

La licenza di UCMDDB Foundation non limita il numero di istanze della sonda del flusso di dati che si possono distribuire in un ambiente del cliente a scopo di servizi di hosting di adattatori di individuazione o integrazione. Si potrebbero comunque applicare limitazioni tecniche riguardo il numero di sonde che si possono utilizzare con UCMDDB. Inoltre, come indicato in precedenza, alcuni adattatori non possono essere ospitati da una sonda.

Caso particolare di BSM

I clienti che acquistano HP Application Performance Manager (APM) versione 9.0x o successiva ricevono automaticamente una licenza gratuita per l'utilizzo del componente UCMDDB incorporato etichettato come Runtime Service Model (RTSM) e l'integrazione dei prodotti BTO con RTSM. Di conseguenza i clienti APM non hanno necessità di una licenza di UCMDDB Foundation.

Nota: APM era noto in precedenza con il nome HP Business Availability Center versione 8.0x (BAC) e RTSM come Operational Database (ODB).

Licenza di UCMDB Integration Only

Questa licenza si basa sull'unità di misura del server gestito (per i dettagli consultare “Unità di misura” a pag. 49). I clienti che devono integrare prodotti di terze parti con UCMDB devono acquistare un numero adeguato di queste licenze.

Questa sezione include inoltre:

- “Regole di licenza” a pag. 54
- “Tipi validi di integrazioni” a pag. 53

Regole di licenza

Un licenza d'uso, License To Use (LTU), deve essere acquistata per ogni server gestito definito in un prodotto di terze parti e la cui definizione viene copiata in UCMDB per la registrazione sotto forma di CI. La licenza di UCMDB Integration Only richiede un acquisto minimo iniziale di 100 LTU.

Tipi validi di integrazioni

Questa licenza consente di integrare i prodotti di terze parti con UCMDB utilizzando:

- integrazioni standard fornite da HP
- integrazioni standard fornite dai partner HP (si possono applicare ulteriori costi)
- le integrazioni per lo scambio di dati personalizzati (ovvero l'adattatore generico del database, l'adattatore Push generico e gli adattatori Java personalizzati)
- l'API del servizio Web di HP Universal CMDB e l'API (Java) di HP Universal CMDB
- ma non integrazioni di tipo individuazione (ovvero quelle create utilizzando gli adattatori Jython)

Nota: HP Universal CMDB fornisce gli adattatori preimpostati per prodotti di terze parti Microsoft SCCM e BMC Atrium CMDB.

Licenza DDM Advanced Edition

Questa licenza si basa sull'unità di misura dell'istanza del sistema operativo (per i dettagli consultare “Unità di misura” a pag. 49). I clienti che devono accedere a tutte le funzioni di Discovery and Dependency Mapping di DDM devono acquistare un numero adeguato di queste licenze.

Questa sezione include inoltre:

- ▶ “Regole di licenza” a pag. 54
- ▶ “Discovery and Dependency Mapping” a pag. 54
- ▶ “Integrazioni” a pag. 55
- ▶ “Diritto gratuito per DDM Inventory con DDM Advanced Edition” a pag. 55

Regole di licenza

Un licenza d'uso, License To Use (LTU), deve essere acquistata per ogni istanza del sistema operativo individuato da DDM e registrato in UCMDB sotto forma di CI. La licenza di DDM Advanced Edition richiede un acquisto minimo iniziale di 100 LTU.

Esempio: un VMware ESX Server che ospita una macchina virtuale richiede due licenze d'uso(LTU).

I server individuati da DDM e originati da un prodotto di terze parti (per raccogliere dati aggiuntivi) non devono essere conteggiati nella licenza di UCMDB Integration Only. La licenza di DDM Advanced Edition copre lo scenario di utilizzo.

Discovery and Dependency Mapping

Questa licenza consente l'utilizzo del Pannello di controllo dell'individuazione e altre funzioni correlate per usufruire di tutto il contenuto di individuazione preimpostato disponibile. Inoltre è possibile creare nuovi adattatori Jython per individuare altre risorse.

Integrazioni

Questa licenza consente di utilizzare lo studio di integrazione per creare punti di integrazione con prodotti BTO e di terze parti utilizzando le integrazioni di tipo individuazione (adattatori Jython personalizzati).

Diritto gratuito per DDM Inventory con DDM Advanced Edition

Per ogni LTU acquistata con la licenza di DDM Advanced Edition per un determinato server, si ottiene una licenza gratuita di DDM Inventory per raccogliere i dati di inventario sullo stesso server.

Compiti

Licenza di aggiornamento a Integration Only o DDM Advanced Edition

Quando si installa HP Universal CMDB si riceve la licenza di Universal CMDB Foundation. Per ottenere un file necessario per la licenza di aggiornamento a Integration Only o DDM Advanced Edition rivolgersi a HP Software Support quindi eseguire la procedura seguente:

Per l'aggiornamento della licenza:

- 1** Ottenere il file adeguato da HP Software Support.
- 2** Sostituire il file **ucmdb_license.xml** nella cartella C:\hp\UCMDB\UCMDBServer\conf\. Il nome del file deve essere **ucmdb_license.xml**.
- 3** Utilizzare la console JMX per forzare il cambio di licenza:
 - a** Avviare il browser Web e specificare l'indirizzo del server come segue: **http://<nome host del server UCMDB oppure IP>:8080/jmx-console**.
 - b** Quando viene richiesto immettere le credenziali di autenticazione della console JMX (se non si dispone di queste credenziali rivolgersi all'amministratore di sistema). Il nome e la password predefiniti sono **sysadmin/sysadmin**.
 - c** In **UCMDB** fare clic su **service=Server Services** per aprire la pagina Operazioni.
 - d** Individuare **getLicense** e immettere le informazioni seguenti:

Nella casella Valore per il parametro **customerID** immettere **1**.

Fare clic su **Invoke**.

Vengono visualizzate le informazioni sul tipo di licenza, il nome del cliente, i pacchetti consentiti e l'eventuale blocco delle applicazioni.

Riferimenti

Risoluzione dei problemi e limitazioni

Questa sezione descrive la risoluzione dei problemi e le limitazioni per la licenza di UCMDB.

- **Problema.** quando si integra UCMDB con HP Storage Essentials, non è possibile eseguire il processo **SE Integration by SQL** con licenza di Foundation.

Soluzione. Eseguire la procedura descritta in “Discover the SE Oracle Database” nella *HP Universal CMDB Discovery and Integration Content Guide* in PDF.

- **Problema.** Quando si integra UCMDB con HP Network Node Manager (NNMi) non è possibile eseguire il processo **Layer2 by NNM** con licenza di Foundation.

Soluzione. Per i dettagli consultare “*Network Node Manager i (NNMi) Integration*” nella *HP Universal CMDB Discovery and Integration Content Guide* in PDF.

4

Introduzione a HP Universal CMDB

Questo capitolo comprende:

Concetti

- Pianificazione di predistribuzione a pag. 60

Compiti

- Avvio a pag. 63
- Compiti di amministrazione di base a pag. 64

Concetti

Pianificazione di predistribuzione

La distribuzione di HP Universal CMDB in un ambiente di rete d'impresa è un processo che richiede la pianificazione delle risorse, il design dell'architettura di sistema e una strategia di distribuzione ben ponderata. L'elenco di controllo seguente descrive alcune delle problematiche di base che devono essere prese in considerazione prima dell'installazione. Per la documentazione complessiva sulle procedure consigliate relative alla pianificazione della distribuzione, consultare HP Professional Services.

Utilizzare l'elenco di controllo seguente per esaminare le problematiche di base che la propria organizzazione dovrebbe prendere in considerazione in fase di pianificazione della distribuzione di HP Universal CMDB.

✓	Passaggio
	Definire gli obiettivi del progetto.
	Definire i protocolli da utilizzare per Gestione flusso di dati (GFD) e accertarsi che tali protocolli siano disponibili per l'utilizzo.
	Verificare di disporre dei diritti di accesso per i protocolli da utilizzare per GFD. Chiedere all'amministratore di sistema il nome utente e la password per i protocolli rilevanti.
	Definire la velocità e l'utilizzo delle sottoreti della rete da individuare. È possibile che sia necessario aumentare i timeout per alcuni protocolli.
	<p>Verificare se le applicazioni seguenti utilizzano le porte predefinite. Se non utilizzano le porte predefinite, verificare quali porte utilizzano.</p> <ul style="list-style-type: none"> ➤ FTP ➤ IBM HTTP Server ➤ IIS ➤ Microsoft SQL Server ➤ Oracle Server ➤ SAP ➤ SNMP ➤ Siebel ➤ WebLogic ➤ WebSphere
	<p>Identificare i componenti da individuare:</p> <ul style="list-style-type: none"> ➤ Piattaforma hardware del server ➤ Sistema operativo e versione del server ➤ Tipi di periferiche di rete

✓	Passaggio
	<p>Installare gli strumenti e le utilità seguenti per l'analisi dei processi di individuazione:</p> <ul style="list-style-type: none"> ▶ Strumento SNMP ▶ Strumento WMI ▶ Browser LDAP ▶ Tailer dei file di registro (ad esempio BareTail for Windows oppure un'utilità tail di UNIX)
	<p>Definire le operazioni da eseguire con HP Universal CMDB:</p> <ul style="list-style-type: none"> ▶ Mappatura dei componenti di sistema ▶ Analisi della causa principale ▶ Analisi impatto ▶ Riposizionamento/consolidamento data center
	<p>Analizzare i processi IT e la struttura organizzativa e la cultura che può influenzare o può essere influenzata dalla distribuzione.</p>
	<p>Analizzare gli obiettivi dell'organizzazione e identificare i processi aziendali chiave abilitati all'ambiente IT per raggiungere questi obiettivi.</p>
	<p>Identificare gli utenti di destinazione (quelli con un interesse legittimo nei processi aziendali), ad esempio gli esecutivi, i manager LOB, i proprietari delle applicazioni, gli amministratori di sistema e i revisori della protezione.</p>
	<p>Allineare il progetto con le pratiche di gestione delle prestazioni correnti.</p>
	<p>Definire i risultati finali del progetto compresa l'impostazione delle aspettative relative alle misurazioni, le funzioni, l'obiettivo della distribuzione e i livelli di maturità.</p>
	<p>Identificare la funzionalità adeguata di HP Universal CMDB.</p>
	<p>Creare una roadmap della distribuzione.</p>
	<p>Definire i criteri per stabilire il successo del progetto.</p>
	<p>Decidere la frequenza di esecuzione di GFD. Per i dettagli consultare "Finestra di dialogo Utilità di pianificazione individuazione" nella <i>Guida alla gestione del flusso di dati di HP Universal CMDB</i>.</p>

Compiti

Avvio

Questa sezione fornisce la roadmap di base passo passo per l'avvio di HP Universal CMDB.

1 Leggere dove reperire le informazioni.

Informarsi sulle diverse fonti di assistenza, compresi HP Professional Services e HP Software Support nonché la documentazione su HP Universal CMDB. Per i dettagli consultare “Introduzione alla guida” a pag. 15.

2 Learn about the HP Universal CMDB components.

Informarsi sui componenti che alimentano il sistema HP Universal CMDB. Per i dettagli consultare “Panoramica di HP Universal CMDB” a pag. 26.

3 Pianificare la distribuzione di HP Universal CMDB.

Creare un piano di distribuzione completa prima di installare HP Universal CMDB. Utilizzare l'elenco di controllo di Pianificazione di predistribuzione come punto di riferimento. Per le procedure consigliate di pianificazione della distribuzione completa, rivolgersi al proprio rappresentante di HP Professional Services. Per i dettagli consultare “Pianificazione di predistribuzione” a pag. 60.

4 Installare i componenti di HP Universal CMDB.

Installare il server (su un sistema Windows o) e la sonda del flusso di dati. Per i dettagli consultare Parte II, “Installazione del server UCMDB.”

5 Accedere a HP Universal CMDB.

Avviare HP Universal CMDB. Per i dettagli consultare “Accesso a HP Universal CMDB” a pag. 417.

6 Avviare l'amministrazione di sistema.

Installare il sistema HP Universal CMDB. Per i dettagli consultare “Amministrazione” nella *Guida all'amministrazione di HP Universal CMDB*.

Compiti di amministrazione di base

Questa sezione fornisce un elenco di controllo per i compiti di amministrazione di configurazione. Utilizzare questo elenco di controllo per esaminare i compiti di amministrazione richiesti per l'installazione del sistema HP Universal CMDB.

1 Installazione di Gestione flusso di dati (GFD).

Gli utenti con licenza di DDM possono eseguire il processo di individuazione per identificare le risorse IT nell'infrastruttura di rete. Per i dettagli consultare *Guida alla gestione del flusso di dati di HP Universal CMDB*.

2 Quando si installa GFD richiedere all'amministratore di sistema quanto segue:

- Credenziali del sistema operativo
- Credenziali del protocollo di rete
- Credenziali dell'applicazione

3 Impostazione utenti.

Definire le autorizzazioni per le viste. Le autorizzazioni consentono o negano l'accesso degli utenti alle viste, alle TQL e ad altri componenti. Per i dettagli consultare "Impostazione e utilizzo degli utenti" nel "Gestione protezione" e nella *Guida all'amministrazione di HP Universal CMDB*.

4 Configurare i destinatari dei report pianificati, compreso il metodo di consegna.

Per i dettagli consultare "Report" nella *Guida alla modellazione di HP Universal CMDB*.

5 Creare manualmente il proprio modello di universo IT definendo gli elementi di configurazione (CI) e le relazioni dei CI nel modello.

Dividere il modello in viste che rappresentano i sottoinsiemi logici dell'intero modello. Aggiungere i CI in base alle risorse di rete individuate oppure definire manualmente i componenti dell'infrastruttura.

Per i dettagli consultare:

- "Gestione Universo IT" nella *Guida alla modellazione di HP Universal CMDB*
- "Studio di modellazione" nella *Guida alla modellazione di HP Universal CMDB*

Parte II

Installazione del server UCMDB

5

Procedura di installazione

Questo capitolo include:

Concetti

- ▶ Procedura di installazione - Panoramica a pag. 68
- ▶ Passaggi di installazione a pag. 69

Concetti

Procedura di installazione - Panoramica

Durante l'installazione verranno installati i componenti di HP Universal CMDB seguenti:

- ▶ Server HP Universal CMDB
- ▶ Configuration management database (CMDB)
- ▶ Database Cronologia
- ▶ Pacchetti di HP Universal CMDB
- ▶ Sonda Gestione flusso di dati (GFD) (se è disponibile la rispettiva licenza - per i dettagli consultare “Modello di licenza di HP Universal CMDB” a pag. 47)

Importante: HP Universal CMDB **non** deve essere installato più di una volta su un server anche se le istanze sono installate in cartelle diverse o sono versioni diverse.

Passaggi di installazione

Il workflow di installazione prevede i principali passaggi seguenti:

1 Installazione dei database CMDB e Cronologia.

Installare HP Universal CMDB su Microsoft SQL Server oppure su Oracle Server.

Per i dettagli consultare “Deploying and Maintaining the Microsoft SQL Server Database” e “Deploying and Maintaining the Oracle Server Database” nella *Guida al database di HP Universal CMDB* in PDF.

2 Ottenere la licenza di HP Universal CMDB.

Posizionare la licenza su un computer accessibile dal computer sul quale si sta installando HP Universal CMDB.

Per i dettagli consultare “Modello di licenza di HP Universal CMDB” a pag. 47.

3 Installare il server HP Universal CMDB.

Per i dettagli consultare “HP Universal CMDB Installazione su una piattaforma Windows” a pag. 71 o “HP Universal CMDB Installazione su una piattaforma Linux” a pag. 87

Al termine dell'installazione del server, la procedura di installazione continua direttamente con l'installazione dei database (CMDB e Cronologia). È possibile creare un nuovo database (Microsoft SQL Server) o schema (Oracle Server) oppure connettersi a un database o schema esistente. Per i dettagli consultare “Configurazione del server UCMDB” a pag. 101.

Nota: I pacchetti predefiniti vengono distribuiti automaticamente solo una volta al primo avvio del server.

4 Installare gli strumenti di raccolta (sonde del flusso di dati). Per i dettagli consultare “Installazione della sonda del flusso di dati su piattaforma Windows” a pag. 129 o “Installazione della sonda del flusso di dati su piattaforma Linux” a pag. 147

5 Installare le autorizzazioni di accesso per il server UCMDB e la sonda del flusso di dati.

Per i dettagli consultare Parte VI, “Protezione avanzata di HP Universal CMDB.”

6 Installare le autorizzazioni di autenticazione del servizio del server UCMDB.

7 Avviare HP Universal CMDB.

Per i dettagli consultare “Accedere ai comandi del server UCMDB” a pag. 123.

6

HP Universal CMDB Installazione su una piattaforma Windows

Importante: se si sta installando una versione di service pack (ad es. 9.02), consultare le note sulla versione per le istruzioni più aggiornate.

Questo capitolo comprende:

Concetti

- Prerequisiti di installazione a pag. 72

Compiti

- Installare UCMDB a pag. 74
- Configurare il server della posta di UCMDB a pag. 83
- Disinstallare HP Universal CMDB a pag. 84

Concetti

Prerequisiti di installazione

Tenere presente i consigli seguenti prima di installare HP Universal CMDB:

- ▶ Si consiglia di leggere attentamente l'introduzione a questa guida prima di avviare l'installazione. Per i dettagli consultare “Introduzione a HP Universal CMDB” a pag. 25.
- ▶ Non installare HP Universal CMDB su un'unità mappata a una risorsa di rete.
- ▶ A causa delle limitazioni del browser Web, i nomi dei server che eseguono il server HP Universal CMDB devono comprendere soltanto caratteri alfanumerici (a-z, A-Z, 0-9), tratti (-) e punti (.

Se i nomi dei computer che eseguono i server HP Universal CMDB contengono caratteri di sottolineatura, potrebbe non essere possibile accedere a HP Universal CMDB. In questo caso si consiglia di utilizzare l'indirizzo IP del computer anziché il nome del computer.

- ▶ **Importante:** HP Universal CMDB **non** deve essere installato più di una volta su un server anche se le istanze sono installate in cartelle diverse o sono versioni diverse.
- ▶ I nomi e le password degli utenti del database possono contenere caratteri alfanumerici del set di caratteri del database e il carattere di sottolineatura. I nomi devono iniziare con un carattere alfabetico e non devono superare 30 caratteri.
- ▶ La directory dei programmi di HP Universal CMDB non può contenere caratteri non inglesi.
- ▶ Per i dettagli sulla licenza consultare “Modello di licenza di HP Universal CMDB” a pag. 47.
- ▶ Per i dettagli sulla risoluzione dei problemi di accesso consultare “Risoluzione dei problemi delle risorse disponibili” a pag. 433.

- ▶ **Importante:** Se si sta eseguendo l'aggiornamento della versione corrente a 9.02, leggere il capitolo “Aggiornamento di HP Universal CMDB dalla versione 8.0x alla versione 9.0x” a pag. 163 prima di installare la versione corrente. In questo capitolo la sezione “Eeguire le procedure post-aggiornamento” a pag. 169 spiega come evitare di perdere i file di configurazione dell'adattatore.
- ▶ Tenere a portata di mano le informazioni seguenti prima di avviare l'installazione:
 - ▶ Informazioni sull'impostazione dei parametri del database CMDB e Cronologia. Se si pianifica di impostare questi database durante l'installazione del server, consultare “Configurazione del server UCMDB” a pag. 101.
 - ▶ Se si pianifica di eseguire il server UCMDB su una piattaforma con protezione avanzata (compreso l'utilizzo del protocollo HTTPS), esaminare le procedure di protezione avanzata descritte in Parte VI, “Protezione avanzata di HP Universal CMDB.”
 - ▶ Indirizzo e-mail dell'amministratore. (Facoltativo)
 - ▶ Nome del server della posta SMTP. (Facoltativo)
 - ▶ Nome mittente SMTP. Questo nome viene visualizzato nelle allerte inviate da UCMDB. (Facoltativo)

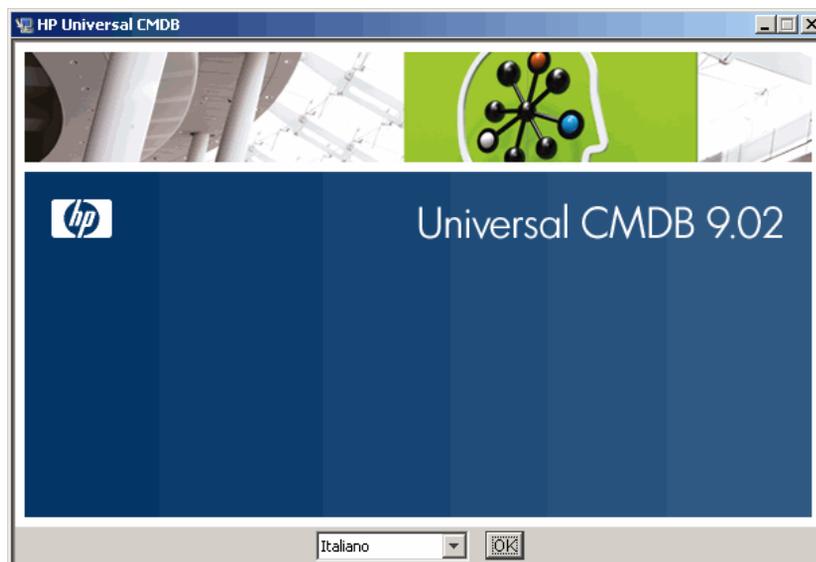
Compiti

Installare UCMDB

La procedura seguente spiega come installare HP Universal CMDB.

- 1 Se si sta installando da un'unità di rete, eseguire il collegamento.
- 2 Individuare il file eseguibile di UCMDB: **HPUCMDB_Server_902.exe**.
- 3 Fare doppio clic sul file per aprire la schermata iniziale.

Se la firma digitale è valida, si apre la schermata iniziale:

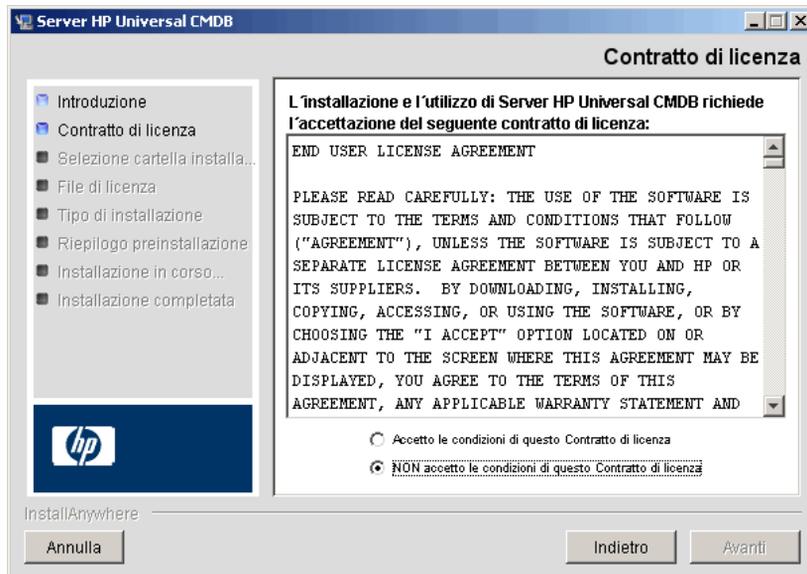


- 4 Selezionare la lingua delle impostazioni internazionali e fare clic su **OK**.

Si apre la finestra di dialogo Introduzione.



5 Fare clic su **Avanti** per aprire la finestra di dialogo Contratto di licenza.



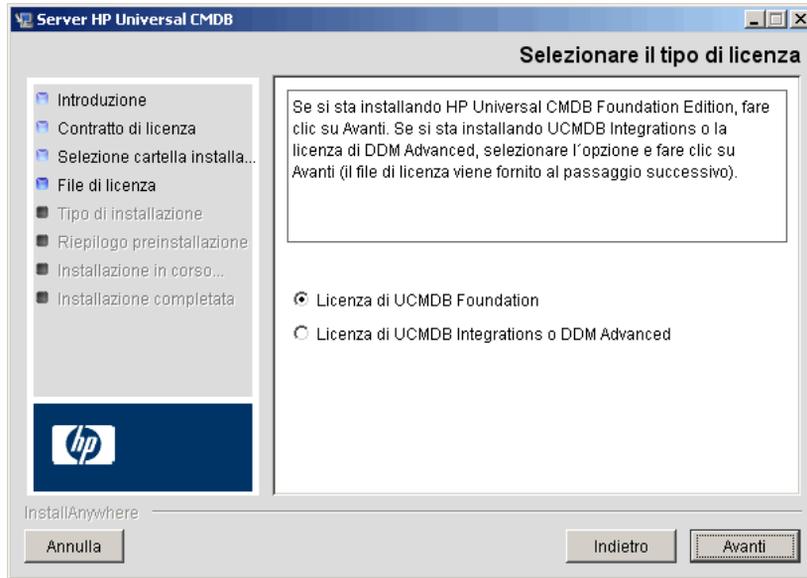
Accettare i termini della licenza e fare clic su **Avanti** per aprire la finestra di dialogo Selezione della cartella di installazione.



Accettare la voce predefinita oppure fare clic su **Scegli** per visualizzare una finestra di dialogo predefinita Sfoglia. Per installare una directory diversa, individuarla e selezionare la cartella di installazione. Il percorso di installazione non può contenere spazi.

Suggerimento: per visualizzare di nuovo la cartella di installazione predefinita, fare clic su **Ripristina cartella predefinita**.

- 6 Fare clic su **Avanti** per aprire la finestra di dialogo Selezionare il tipo di licenza.



Per installare la licenza di Foundation accettare la voce predefinita. Per installare la licenza di Integrazioni o DDM selezionare **Licenza di UCMDB Integrations o DDM Advanced**. Per i dettagli sulla licenza consultare “Modello di licenza di HP Universal CMDB” a pag. 47.

Se si seleziona **Licenza UCMDB Foundation**, passare al passaggio 7 a pag. 79.

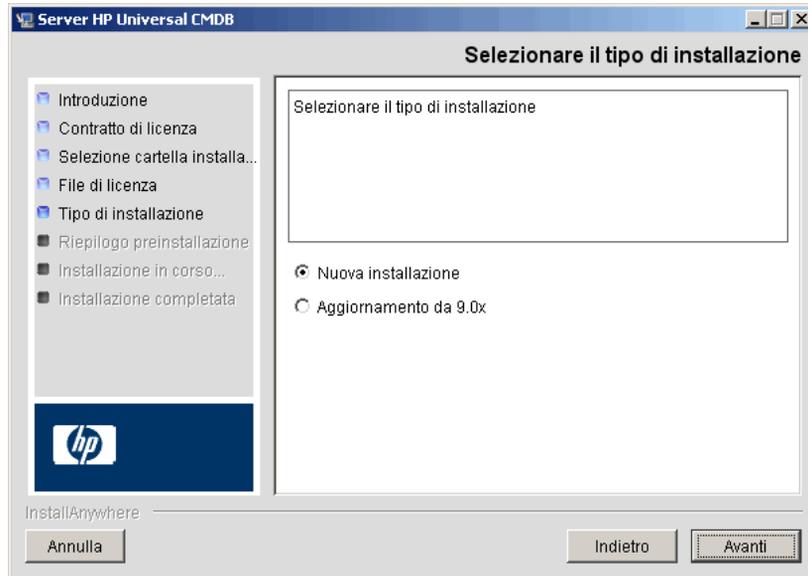
Se si seleziona **Licenza di UCMDB Integrations o DDM Advanced**, fare clic su **Avanti** per aprire la finestra di dialogo Selezionare il file di licenza.



Accettare la voce predefinita oppure fare clic su **Scegli** per visualizzare una finestra di dialogo predefinita Sfoglia. Individuare e selezionare la cartella del file di licenza. Selezionare il file di licenza (**ucmdb_license.xml**).

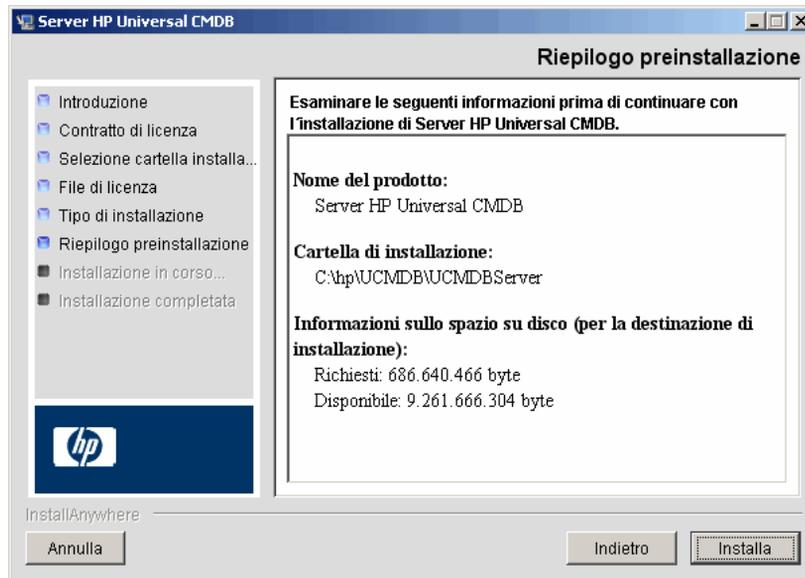
Suggerimento: per visualizzare di nuovo la cartella di installazione predefinita, fare clic su **Ripristina file predefinito**.

- 7 Fare clic su **Avanti** per aprire la finestra di dialogo Selezionare il tipo di installazione.



Selezionare **Nuova installazione** quando si esegue una installazione completa del prodotto. Selezionare **Aggiornamento da 9.0x** quando si esegue una installazione della patch.

- 8 Fare clic su **Avanti** per aprire la finestra di dialogo Riepilogo preinstallazione per l'elenco delle opzioni selezionate.



- 9 Se il riepilogo è corretto, fare clic su **Installa**. Viene visualizzato un messaggio che indica che l'installazione è in corso.
- 10 Al termine dell'installazione, viene visualizzato il messaggio Configurare server HP Universal CMDB:

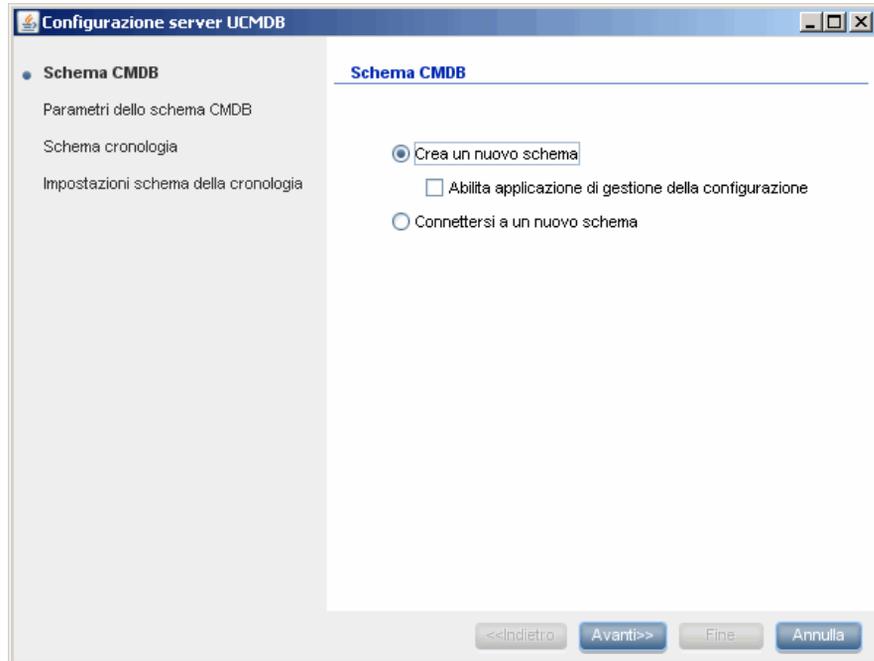


Il passaggio successivo della procedura prevede l'avvio della procedura guidata di configurazione di UCMDB Server (per l'installazione del database o dello schema). Fare clic su **Sì** per continuare con la configurazione.

Se si sta eseguendo un aggiornamento dalla versione 8.0x a 9.02, fare clic su **No** e continuare con la procedura in “Installare la versione 9.02 della sonda del flusso di dati” a pag. 170.

È possibile installare il database o lo schema in un secondo momento. In tal caso accedere alla procedura guidata di configurazione di UCMDB Server dalla menu Start di Windows.

Si apre la finestra di dialogo Configurazione server UCMDB.



Durante i passaggi seguenti scegliere se creare un nuovo database o schema (Microsoft SQL Server oppure Oracle Server) oppure connettersi a un database o schema esistente. Verrà probabilmente scelto di creare un nuovo database o schema per una nuova installazione di HP Universal CMDB con connessione a un schema o database esistente durante la reinstallazione di un server o l'installazione di un server aggiuntivo.

- Per l'introduzione alla creazione o alla connessione a un database, consultare “Scelta del database o dello schema” a pag. 102.
- Per la procedura di creazione del database Microsoft SQL Server, consultare “Creare un database Microsoft SQL Server” a pag. 106.

- ▶ Per la procedura di creazione dello schema Oracle, consultare “Creare uno schema Oracle” a pag. 111.
 - ▶ Per la procedura di connessione a un database Microsoft SQL Server esistente, consultare “Connettersi a un database Microsoft SQL Server esistente” a pag. 115.
 - ▶ Per la procedura di connessione a uno schema Oracle esistente, consultare “Connettersi a uno schema Oracle esistente” a pag. 116.
- 11** Al termine della configurazione seguendo la procedura guidata, si apre la finestra di dialogo Installazione completata.



- 12** Fare clic su **Eseguito** per completare l'installazione.

Configurare il server della posta di UCMDB

Eseguire questa procedura dopo aver installato HP Universal CMDB.

Per configurare il server della posta di UCMDB:

- 1** Selezionare **Amministrazione > Impostazioni infrastruttura > Impostazioni posta**.
- 2** Definire l'impostazione **Server SMTP**: immettere il nome del server SMTP.
- 3** Modificare l'impostazione **Porta server SMTP**: il valore predefinito è 25.
- 4** Come backup per il server SMTP principale è possibile fornire le informazioni su un server alternativo. Ripetere i passaggi 2 e 3 ma fornire il nome del **Server SMTP alternativo** e la **Porta server SMTP alternativa**.
- 5** Modificare le impostazioni per **Mittente e-mail** con il nome da visualizzare nei report inviati da HP Universal CMDB.
- 6** Per abilitare gli utenti a cambiare il nome **Mittente e-mail** all'interno del modulo che invia la posta, cambiare il valore di **Modificabilità mittente** in **True**. In caso contrario lasciare il valore impostato su **False**.

Disinstallare HP Universal CMDB

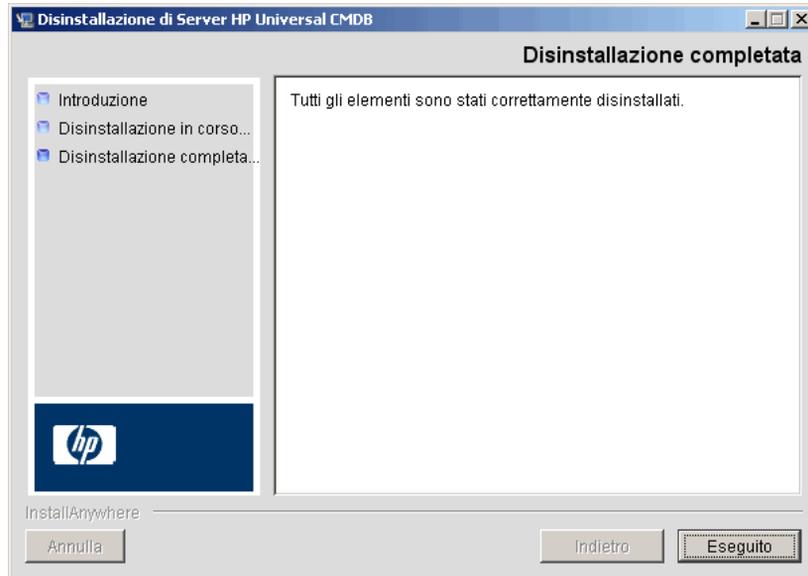
La procedura seguente spiega come disinstallare HP Universal CMDB.

- 1 Da menu Start menu selezionare **Tutti i programmi > HP UCMDB > Avvio HP Universal CMDB Server > Disinstalla HP Universal CMDB Server**. Si apre la finestra di dialogo Disinstalla HP Universal CMDB Server.



- 2 Fare clic su **Disinstalla**.

Al termine della disinstallazione, viene visualizzato un messaggio di conferma:



3 Fare clic su **Eseguito**.

7

HP Universal CMDB Installazione su una piattaforma Linux

Importante: se si sta installando una versione di service pack (ad es. 9.02), consultare le note sulla versione per le istruzioni più aggiornate.

Questo capitolo comprende:

Concetti

- Prerequisiti di installazione a pag. 88

Compiti

- Installare HP Universal CMDB a pag. 90
- Configurare il server della posta di UCMDB a pag. 99
- Disinstallare UCMDB a pag. 99

Concetti

Prerequisiti di installazione

Tenere presente i consigli seguenti prima di installare HP Universal CMDB:

- ▶ Si consiglia di leggere attentamente l'introduzione a questa guida prima di avviare l'installazione. Per i dettagli consultare "Introduzione a HP Universal CMDB" a pag. 25.
- ▶ A causa delle limitazioni del browser Web, i nomi dei server che eseguono il server HP Universal CMDB devono comprendere soltanto caratteri alfanumerici (a-z, A-Z, 0-9), tratti (-) e punti (.).

Se i nomi dei computer che eseguono i server HP Universal CMDB contengono caratteri di sottolineatura, potrebbe non essere possibile accedere a HP Universal CMDB. In questo caso si consiglia di utilizzare l'indirizzo IP del computer anziché il nome del computer.

- ▶ **Importante:** HP Universal CMDB **non** deve essere installato più di una volta su un server anche se le istanze sono installate in cartelle diverse o sono versioni diverse.
- ▶ Applicare la configurazione seguente al computer Linux:
 - ▶ /etc/sysctl.conf. Add or update the **fs.file-max** value to **fs.file-max = 300000**
 - ▶ /etc/security/limits.conf. Alla fine del file aggiungere:
 - * **soft nofile 20480**
 - * **hard nofile 20480**

Nota: probabilmente saranno necessari i privilegi di modifica per questi file. Sarà necessario riavviare il computer Linux per applicare i cambiamenti.

- I nomi e le password degli utenti del database possono contenere caratteri alfanumerici del set di caratteri del database e il carattere di sottolineatura. I nomi devono iniziare con un carattere alfabetico e non devono superare 30 caratteri.
- La directory dei programmi di HP Universal CMDB non può contenere caratteri non inglesi.
- Per i dettagli sulla licenza consultare “Modello di licenza di HP Universal CMDB” a pag. 47.
- Per i dettagli sulla risoluzione dei problemi di accesso consultare “Risoluzione dei problemi delle risorse disponibili” a pag. 433.
- Tenere a portata di mano le informazioni seguenti prima di avviare l'installazione:
 - Informazioni sull'impostazione dei parametri del database CMDB e Cronologia. Se si pianifica di impostare questi database durante l'installazione del server, consultare “Configurazione del server UCMDB” a pag. 101.
 - Se si pianifica di eseguire il server UCMDB su una piattaforma con protezione avanzata (compreso l'utilizzo del protocollo HTTPS), esaminare le procedure di protezione avanzata descritte in Parte VI, “Protezione avanzata di HP Universal CMDB.”

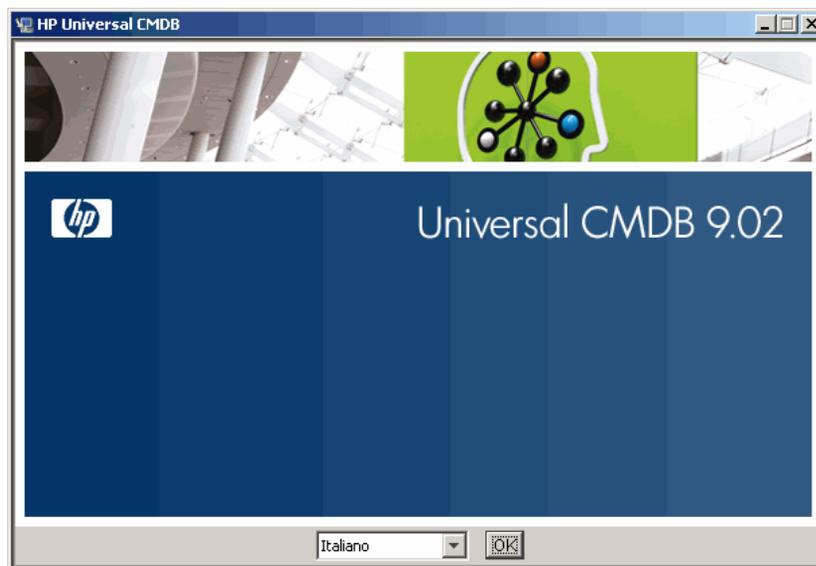
Compiti

Installare HP Universal CMDB

La procedura seguente spiega come installare HP Universal CMDB.

- 1** L'installazione di HP Universal CMDB Linux funziona come un'installazione basata su grafico. Prima di eseguire il programma di installazione, configurare la variabile d'ambiente **DISPLAY** in modo che punti a un'istanza in esecuzione di un X Windows Server.
- 2** Individuare il file eseguibile di UCMDB: **HPUCMDB_Server_902.bin**.
- 3** Eseguire l'eseguibile seguente: **sh <percorso del file di installazione>/HPUCMDB_Server_902.bin**.

Si apre la schermata iniziale:

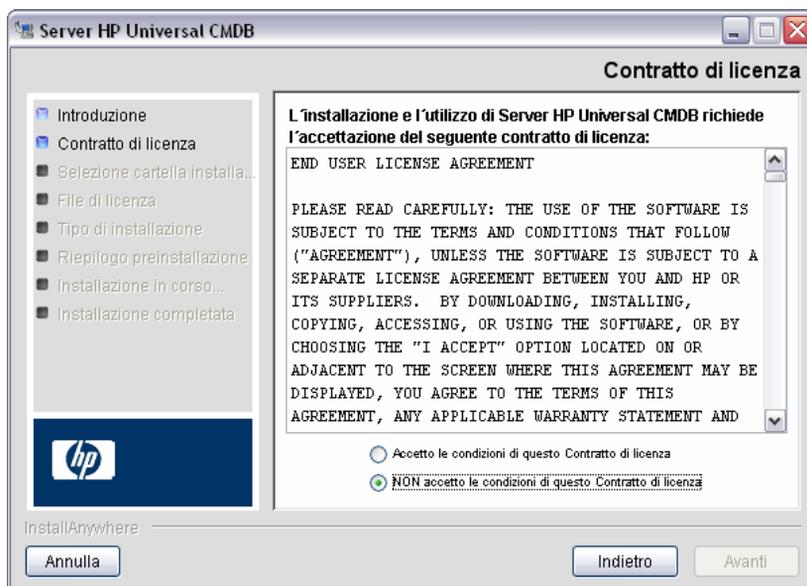


- 4** Selezionare la lingua delle impostazioni internazionali e fare clic su **OK**.

Si apre la finestra di dialogo Introduzione.



5 Fare clic su **Avanti** per aprire la finestra di dialogo Contratto di licenza.



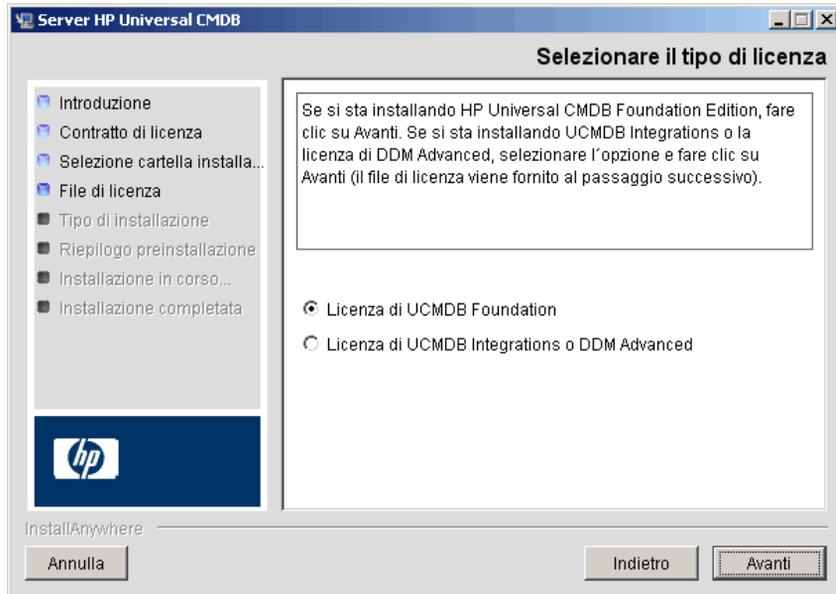
Accettare i termini della licenza e fare clic su **Avanti** per aprire la finestra di dialogo Selezione della cartella di installazione.



Immettere un percorso diverso oppure fare clic su **Scegli** per visualizzare una finestra di dialogo predefinita Sfoglia. Per installare una directory diversa, individuarla e selezionare la cartella di installazione. Il percorso di installazione non può contenere spazi.

Suggerimento: per visualizzare di nuovo la cartella di installazione predefinita, fare clic su **Ripristina cartella predefinita**.

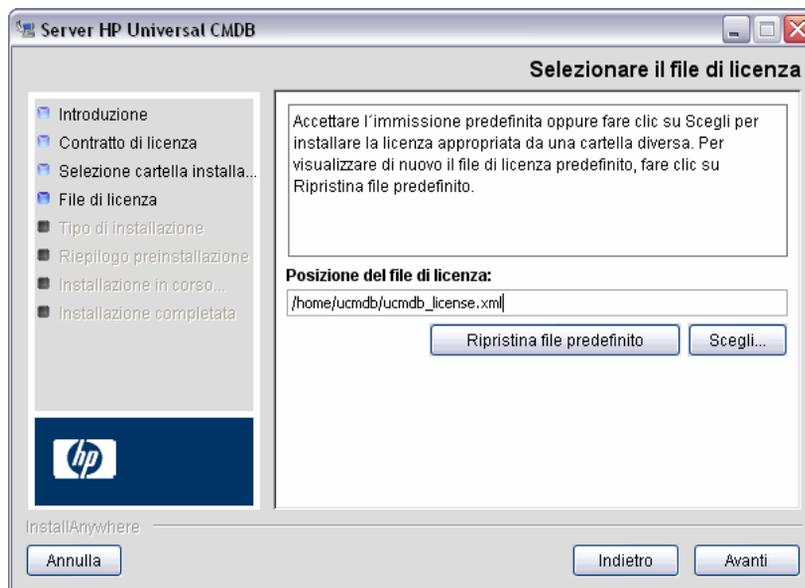
- 6 Fare clic su **Avanti** per aprire la finestra di dialogo Selezionare il tipo di licenza.



Per installare la licenza di Foundation accettare la voce predefinita. Per installare la licenza di Integrazioni o DDM selezionare **Licenza di UCMDB Integrations o DDM Advanced**. Per i dettagli sulla licenza consultare “Modello di licenza di HP Universal CMDB” a pag. 47.

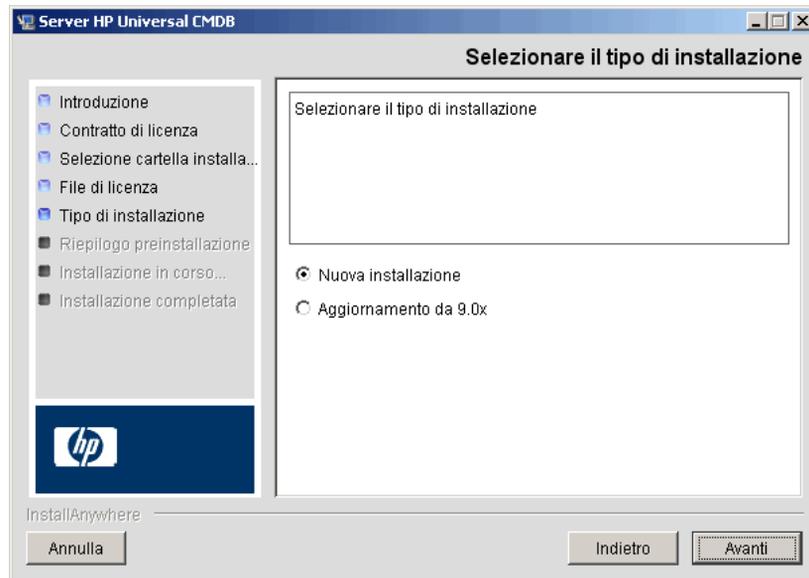
Se si seleziona **Licenza UCMDB Foundation**, passare al passaggio 8.

Se si seleziona **Licenza di UCMDB Integrations o DDM Advanced**, fare clic su **Avanti** per aprire la finestra di dialogo Selezionare il file di licenza.



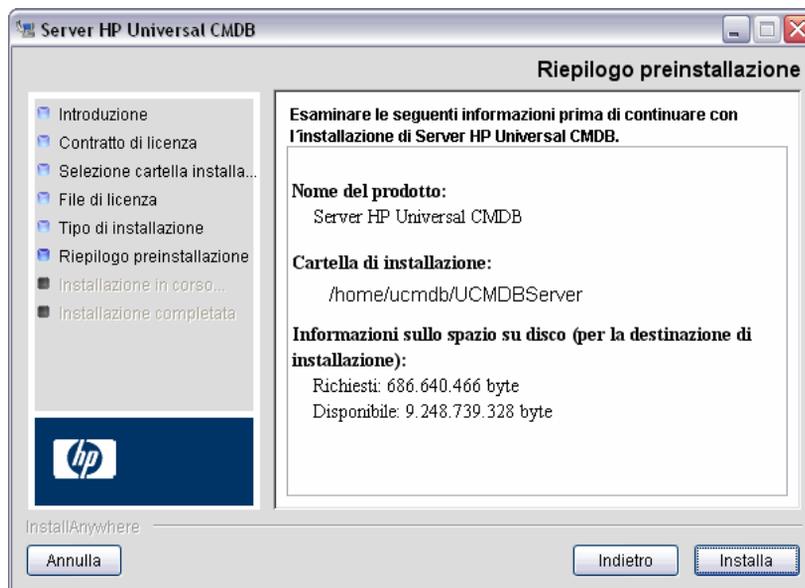
Fare clic su **Scegli** per visualizzare una finestra di dialogo predefinita Sfoglia. Individuare e selezionare la cartella del file di licenza. Selezionare il file di licenza (**ucmdb_license.xml**).

- 7 Fare clic su **Avanti** per aprire la finestra di dialogo Selezionare il tipo di installazione.



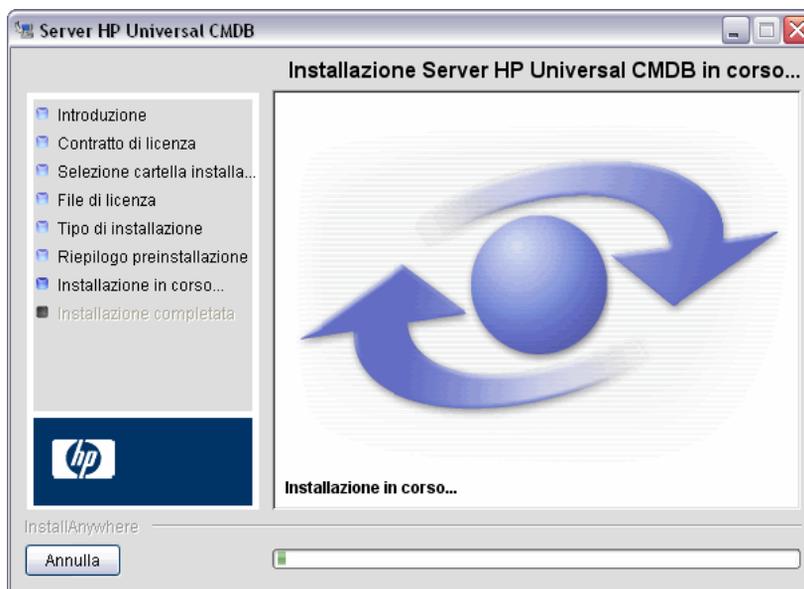
Selezionare **Nuova installazione** quando si esegue una installazione completa del prodotto. Selezionare **Aggiornamento da 9.0x** quando si esegue una installazione della patch.

- 8 Fare clic su **Avanti** per aprire la finestra di dialogo Riepilogo preinstallazione per l'elenco delle opzioni selezionate.



Se il riepilogo è corretto, fare clic su **Installa**.

- 9 Viene visualizzato un messaggio che indica che l'installazione è in corso.



Viene visualizzato il messaggio Configurare server HP Universal CMDB:



- 10 Fare clic su **Sì** per continuare con la configurazione e aprire la finestra di dialogo di avvio della configurazione del server HP Universal CMDB.
- È possibile, a scelta, installare il database o lo schema in un secondo momento. In questo caso eseguire lo script **configure.sh** che si trova nella sottocartella **bin** della cartella di installazione.

- 11** Durante i passaggi seguenti scegliere se creare un nuovo database o schema (Microsoft SQL Server oppure Oracle Server) oppure connettersi a un database o schema esistente. Verrà probabilmente scelto di creare un nuovo database o schema per una nuova installazione di HP Universal CMDB con connessione a un schema o database esistente durante la reinstallazione di un server o l'installazione di un server aggiuntivo. Per l'introduzione alla creazione o alla connessione a un database, consultare "Scelta del database o dello schema" a pag. 102.
- 12** Al termine della configurazione seguendo la procedura guidata, si apre la finestra di dialogo Installazione completata. Fare clic su **Eseguito** per completare l'installazione.



Configurare il server della posta di UCMDB

- 1 Selezionare **Amministrazione > Impostazioni infrastruttura > Impostazioni posta**.
- 2 Definire l'impostazione **Server SMTP**: immettere il nome del server SMTP.
- 3 Modificare l'impostazione **Porta server SMTP**: il valore predefinito è 25.
- 4 Come backup per il server SMTP principale è possibile fornire le informazioni su un server alternativo. Ripetere i passaggi 2 e 3 ma fornire il nome del **Server SMTP alternativo** e la **Porta server SMTP alternativa**.
- 5 Modificare le impostazioni per **Mittente e-mail** con il nome da visualizzare nei report inviati da HP Universal CMDB.
- 6 Per abilitare gli utenti a cambiare il nome **Mittente e-mail** all'interno del modulo che invia la posta, cambiare il valore di **Modificabilità mittente** in **TRUE**. In caso contrario lasciare il valore impostato su **FALSE**.

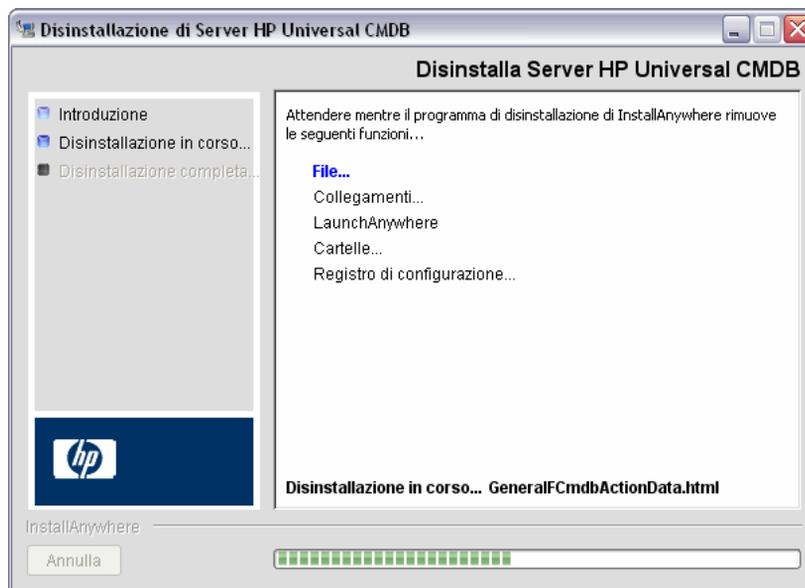
Disinstallare UCMDB

La procedura seguente indica i passaggi per disinstallare UCMDB.

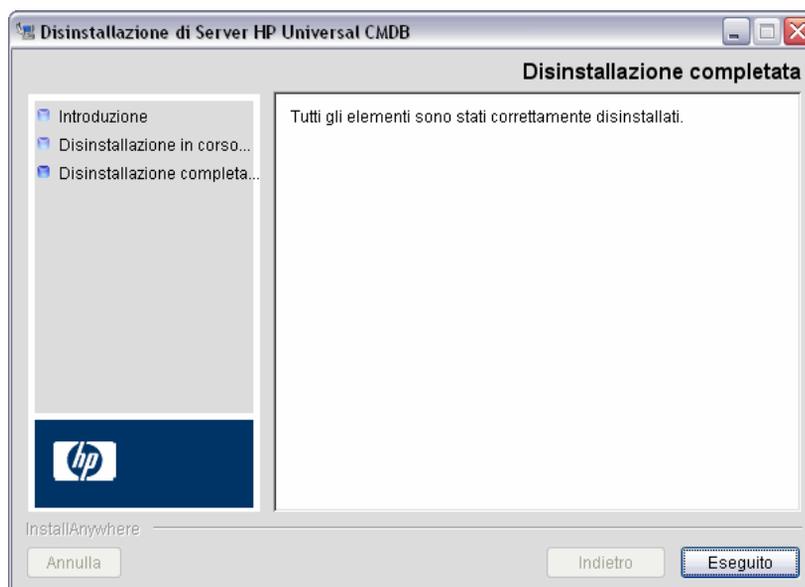
- 1 Eseguire lo script **Uninstall_UCMDBServer** dalla sottocartella **UninstallerData** della cartella di installazione.



- 2 Dallo stesso percorso selezionare **Disinstalla** per disinstallare HP Universal CMDB Server.



- 3 Fare clic su **Eseguito** per completare il processo di disinstallazione.



8

Configurazione del server UCMDB

Questo capitolo comprende:

Concetti

- Scelta del database o dello schema a pag. 102
- Informazioni richieste per l'impostazione dei parametri del database a pag. 103

Compiti

- Accedere alla procedura guidata di configurazione di UCMDB Server a pag. 106
- Creare un database Microsoft SQL Server a pag. 106
- Creare uno schema Oracle a pag. 111
- Connettersi a un database Microsoft SQL Server esistente a pag. 115
- Connettersi a uno schema Oracle esistente a pag. 116
- Riavviare il server a pag. 116

Concetti

Scelta del database o dello schema

In questo capitolo viene descritto il secondo passaggio della procedura di installazione per avviare la procedura guidata di configurazione di UCMDB Server (per l'installazione del database o dello schema). Per i dettagli sul primo passaggio dell'installazione consultare “HP Universal CMDB Installazione su una piattaforma Windows” a pag. 71 oppure “HP Universal CMDB Installazione su una piattaforma Linux” a pag. 87.

Nota: Si consiglia di leggere attentamente l'introduzione a questa guida prima di avviare l'installazione. Per i dettagli consultare “Introduzione a HP Universal CMDB” a pag. 25.

Durante l'installazione è necessario decidere se si desidera creare gli utenti del database oppure utilizzare gli utenti predefiniti. HP Universal CMDB consente di operare questa scelta nel momento in cui si sceglie il database che esegue l'applicazione:

Scegliere di creare un utente del database o dello schema nei casi seguenti:

- ▶ Non esistono utenti del database.
- ▶ Esistono utenti del database ma non si desidera inizializzare i contenuti predefiniti del database.

Scegliere di connettersi a utente del database o dello schema esistente nei casi seguenti:

- ▶ Si desidera eseguire l'aggiornamento a una versione più recente di HP Universal CMDB e utilizzare i contenuti del database della versione precedente di HP Universal CMDB.

- Non si desidera cambiare i contenuti predefiniti del database, ad esempio poiché si dispone dei dati del database o dello schema di un'installazione precedente della stessa release. In questo caso, l'installazione aggiorna i file di configurazione del server necessari con i dettagli del database e aggiornare i file di configurazione degli script del database. Per i dettagli consultare la *Guida al database di HP Universal CMDB* in PDF.
- L'amministratore del database fornisce in anticipo le istruzioni per la creazione di utenti del database in base ai criteri adottati dall'azienda. Per la creazione manuale di database Microsoft SQL Server o schemi Oracle, consultare la *Guida al database di HP Universal CMDB* in PDF.

Informazioni richieste per l'impostazione dei parametri del database

Prima di impostare i parametri del database CMDB e cronologia, è necessario preparare le informazioni descritte nelle sezioni seguenti.

Distribuzione di Microsoft SQL Server

Per la creazione di nuovi database e la connessione a quelli esistenti sono necessarie le informazioni seguenti:

- **Nome host.** Il nome del computer su cui è installato Microsoft SQL Server. Se si sta eseguendo la connessione a un'istanza di Microsoft SQL Server non predefinita, immettere quanto segue: <nome_host>\<nome_istanza>
- **Porta.** Porta TCP/IP di Microsoft SQL Server. HP Universal CMDB visualizza automaticamente la porta predefinita, **1433**.
- **Nome database (schema).** Il nome del database esistente o il nome che sarà assegnato al nuovo database (ad esempio Cronologia_UCMDB).
- **Nome utente e password.** (se si utilizza l'autenticazione Microsoft SQL Server) Il nome utente e la password di un utente con diritti amministrativi su Microsoft SQL Server. Il nome utente predefinito dell'amministratore di Microsoft SQL Server è **sa**. Tenere presente che è necessario fornire una password.

È possibile creare e connettersi a un database utilizzando l'autenticazione anziché l'autenticazione Microsoft SQL Server. Per eseguire questa operazione è necessario accertarsi che l'utente Windows che esegue il servizio HP Universal CMDB disponga delle autorizzazioni necessarie per accedere al database Microsoft SQL Server. Per informazioni sull'assegnazione di un utente Windows a eseguire il servizio HP Universal CMDB consultare “Cambiare l'utente del servizio HP Universal CMDB Server” a pag. 289. Per informazioni sull'aggiunta di un utente Windows a Microsoft SQL Server consultare “Using Windows Authentication to Access Microsoft SQL Server Databases” nella *Guida al database di HP Universal CMDB* in PDF.

Distribuzione di Oracle Server

Prima di impostare i parametri del database CMDB e cronologia CMDB, accertarsi di aver creato almeno uno spazio tabella predefinito per ciascuno schema utente ai fini della persistenza dei dati e che sia assegnato almeno uno spazio tabella temporaneo a ciascuno schema utente.

Per la creazione di un nuovo schema utente e la connessione a quello esistente sono necessarie le informazioni seguenti:

- ▶ **Nome host.** Il nome del computer host su cui è installato Oracle Server.
- ▶ **Porta.** Porta listener di Oracle. HP Universal CMDB visualizza automaticamente la porta predefinita, **1521**.
- ▶ **SID.** Il nome dell'istanza di Oracle che identifica in modo univoco l'istanza del database Oracle utilizzata da HP Universal CMDB.
- ▶ **Nome e password dello schema.** Il nome e la password dello schema utente esistente o il nome assegnato al nuovo schema utente (ad esempio UCMDB_FOUNDATION).

Se si sta creando un nuovo schema utente sono necessarie le informazioni aggiuntive seguenti:

- **Nome utente e password dell'amministratore** (per connettersi come amministratore). Il nome e la password di un utente con autorizzazioni amministrative su Oracle Server (ad esempio un utente di sistema).
- **Spazio tabella predefinito.** Il nome dello spazio tabella predefinito creato per lo schema utente. Per i dettagli sulla creazione di uno spazio tabella di HP Universal CMDB consultare "Manually Creating the Oracle Server Database Schemas" nella *Guida al database di HP Universal CMDB* in PDF.
- **Spazio tabella temporaneo.** Il nome dello spazio tabella temporaneo assegnato allo schema utente. Lo spazio tabella Oracle temporaneo è **temp**.

Nota: per creare un nuovo schema utente è necessario disporre dei privilegi utente per la creazione.

Compiti

Accedere alla procedura guidata di configurazione di UCMDB Server

Se il database o lo schema non sono stati installati durante l'installazione, è possibile impostarli accedendo alla procedura guidata di configurazione di UCMDB Server dal menu Start di Windows e selezionare **Start > Tutti i programmi > HP UCMDB > Avvio della procedura guidata di configurazione di HP Universal CMDB Server**.

Creare un database Microsoft SQL Server

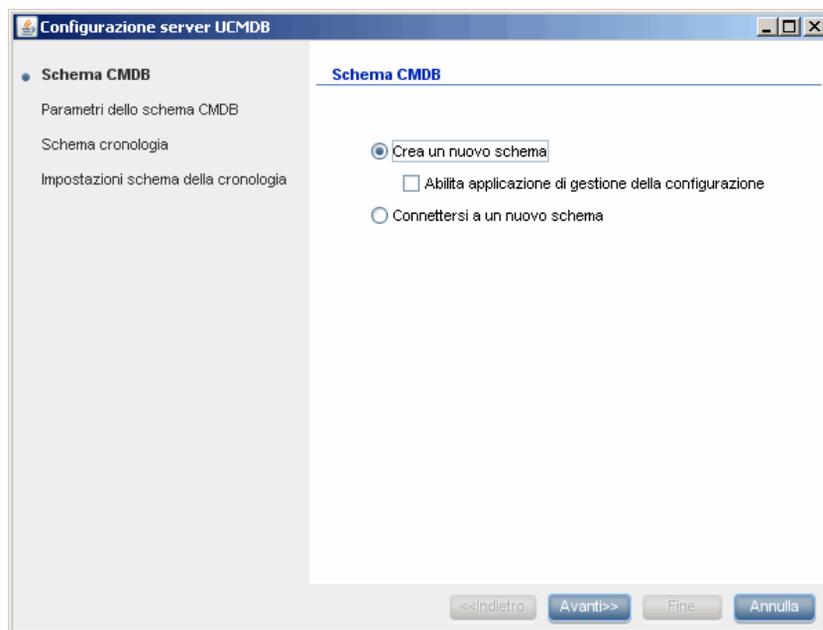
In questa sezione viene spiegato come impostare il database Microsoft SQL Server. Questo passaggio di installazione-impostazione dei database CMDB e cronologia si suddivide in due parti.

Nota: in UCMDB versione 9.00 o successiva i database Foundations e CMDB sono combinati. Per informazioni sull'aggiornamento consultare "Aggiornamento di HP Universal CMDB dalla versione 8.0x alla versione 9.0x" a pag. 163.

Per impostare il database Microsoft SQL Server:

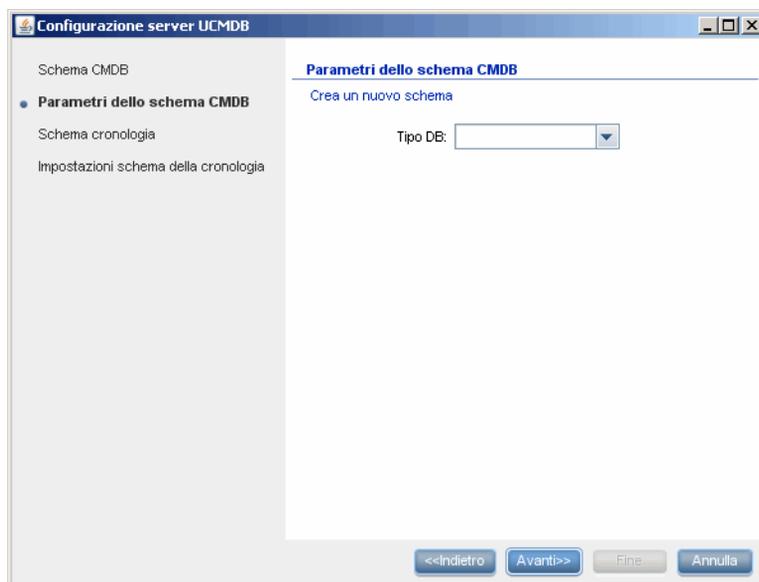
- 1 Seguendo l'installazione fare clic su **Avanti** per aprire la finestra di dialogo Schema CMDB.

Nota: al termine dell'installazione è possibile accedere alla procedura guidata di configurazione di UCMDB Server dalla menu Start di Windows. Per i dettagli consultare “Accedere alla procedura guidata di configurazione di UCMDB Server” a pag. 106.



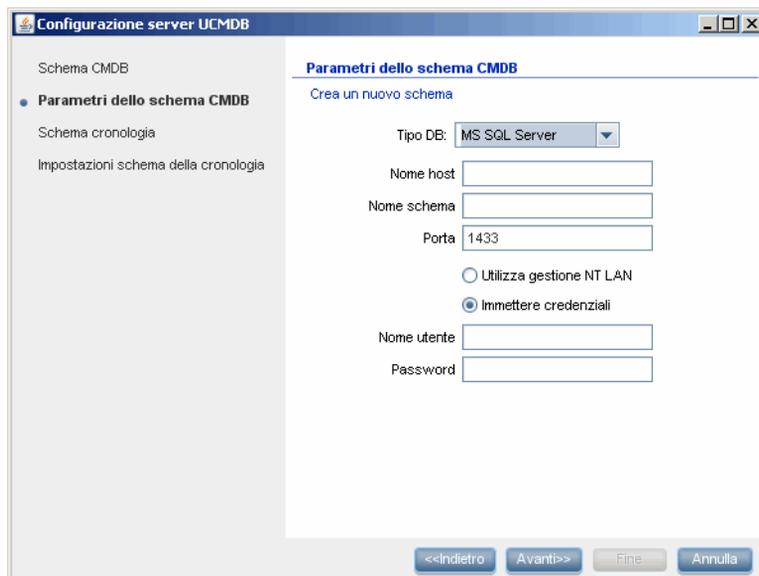
Selezionare **Crea un nuovo schema**.

- 2 Fare clic su **Avanti** per aprire la finestra di dialogo Schema CMDB.

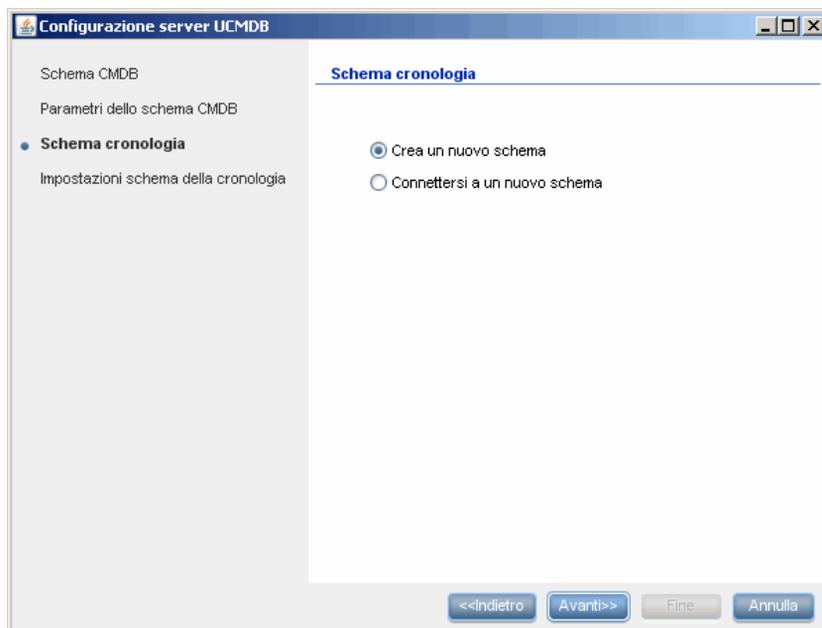


Selezionare **MS SQL Server**.

- 3 Nella finestra di dialogo vengono visualizzati altri campi.

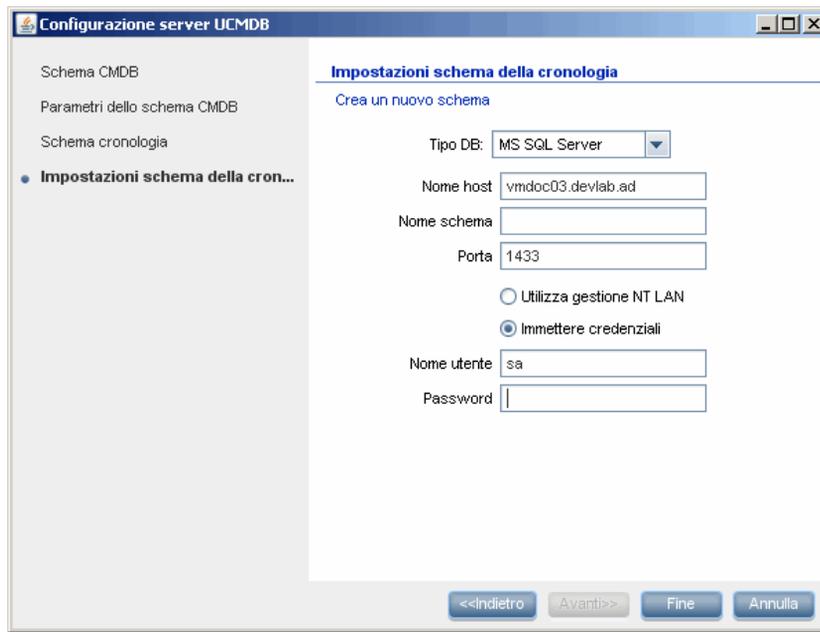


- 4 Immettere il nome host e il nome del database e stabilire l'autenticazione da utilizzare con HP Universal CMDB per la connessione al server del database. Per i dettagli sull'autenticazione Windows, consultare “Using Windows Authentication to Access Microsoft SQL Server Databases” nella *Guida al database di HP Universal CMDB* in PDF.
- 5 Fare clic su **Avanti**. Viene creato il database CMDB. Viene visualizzata la finestra di dialogo Schema cronologia.



Selezionare **Crea un nuovo schema**.

- 6 Fare clic su **Avanti** per aprire la finestra di dialogo Impostazioni schema della cronologia.



Selezionare **MS SQL Server**. I valori immessi per le impostazioni del CMDB vengono visualizzati nella casella.

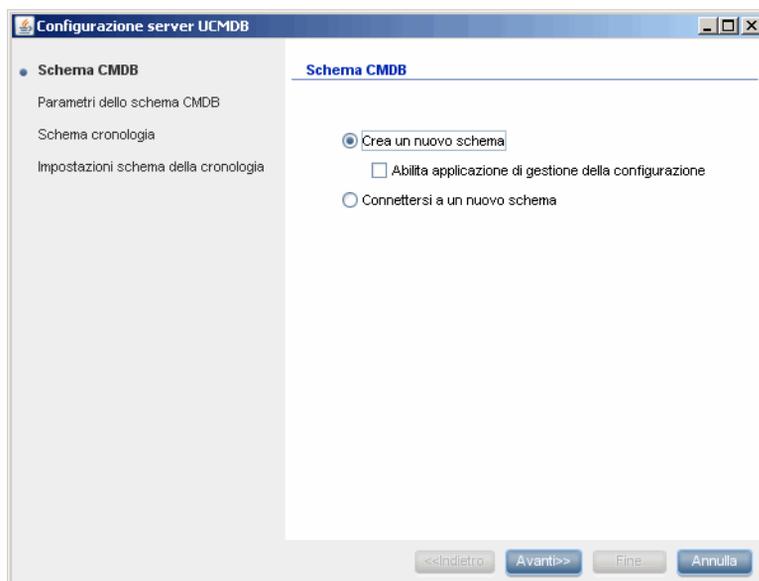
- 7 Fare clic su **Fine**. Viene creato il database Cronologia CMDB.

Creare uno schema Oracle

In questa sezione viene spiegato come impostare lo schema Oracle. Questo passaggio di installazione-impostazione degli schemi CMDB e cronologia si suddivide in due parti.

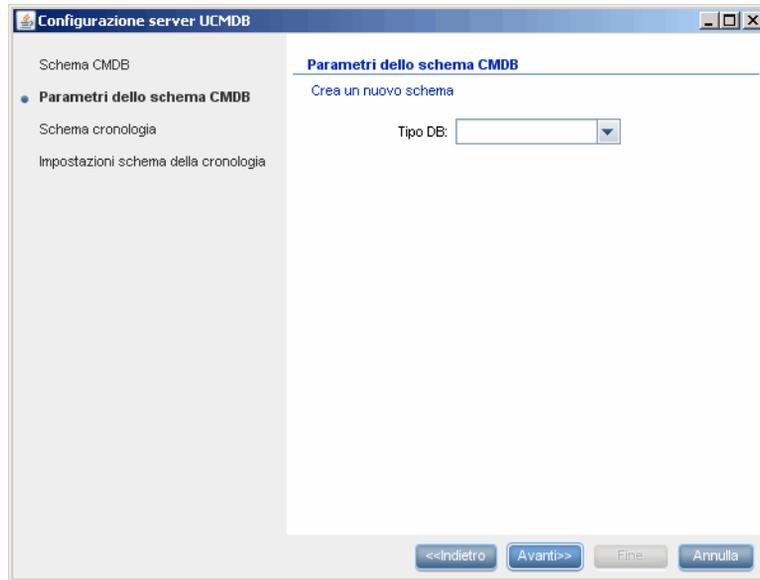
Per impostare lo schema Oracle:

- 1 Seguendo l'installazione fare clic su **Avanti** per aprire la finestra di dialogo Schema CMDB.



Selezionare **Crea un nuovo schema**.

2 Fare clic su **Avanti** per aprire la finestra di dialogo Schema CMDB.



Selezionare **Oracle**.

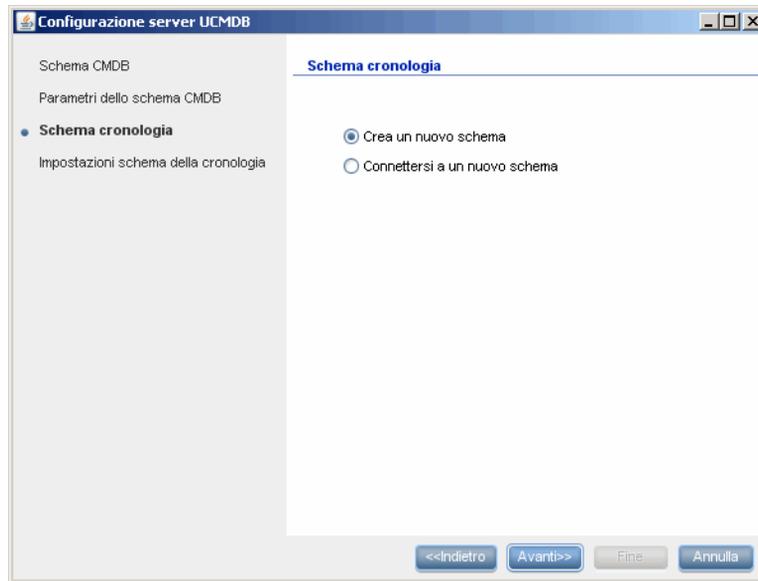
3 Nella finestra di dialogo vengono visualizzati altri campi.

The screenshot shows a Windows-style dialog box titled "Configurazione server UCMDB". On the left is a sidebar with three items: "Schema CMDB", "Parametri dello schema CMDB" (which is selected with a blue dot), "Schema cronologia", and "Impostazioni schema della cronologia". The main area of the dialog is titled "Parametri dello schema CMDB" and contains the sub-header "Crea un nuovo schema". Below this, there are several input fields: "Tipo DB:" with a dropdown menu showing "Oracle"; "Nome host" (empty text box); "Nome schema" (empty text box); "Password schema" (empty text box); "Conferma password" (empty text box); "Porta" with the value "1521"; "SID" (empty text box); "Nome amministrazione" (empty text box); "Password amministrazione" (empty text box); "Spazio tabella predefinito" (empty text box); and "Spazio tabella temporaneo" (empty text box). At the bottom of the dialog are four buttons: "<<Indietro", "Avanti>>", "Fine", and "Annulla".

Immettere i dettagli dello schema.

- **Nome dello schema.** Il nome dello schema deve essere univoco.
- **Spazio tabella predefinito.** Aggiornare questo campo.
- **Spazio tabella temporaneo.** Se l'amministratore del database ha creato uno spazio tabella temporaneo non predefinito immettere questo nome, in caso contrario immettere **temp**.

4 Fare clic su **Avanti** per aprire la finestra di dialogo Schema cronologia.



Selezionare **Crea un nuovo schema**.

- 5 Fare clic su **Avanti** per aprire la finestra di dialogo Impostazioni schema della cronologia.

Selezionare **Oracle**. I valori immessi per le impostazioni del CMDB vengono visualizzati nella casella.

- 6 Fare clic su **Fine**. Viene creato il database Cronologia CMDB.

Connettersi a un database Microsoft SQL Server esistente

In questa sezione viene spiegato come connettersi a un database Microsoft SQL Server esistente. Questo passaggio di installazione-connessione al database CMDB e cronologia si suddivide in due parti.

Seguire le istruzioni per la creazione del database Microsoft SQL Server salvo i passaggi seguenti:

- Nel passaggio 1 a pag. 107 selezionare **Connettersi a un nuovo schema** e fare clic su **Avanti**.
- Nel passaggio 5 a pag. 109 selezionare **Connettersi a un nuovo schema** e fare clic su **Avanti**.

Connettersi a uno schema Oracle esistente

In questa sezione viene spiegato come connettersi a uno schema Oracle Server esistente. Questo passaggio di installazione-connesione allo schema CMDB e cronologia si suddivide in due parti.

Seguire le istruzioni per la creazione dello schema Oracle Server salvo i passaggi seguenti:

- ▶ Nel passaggio 1 a pag. 111 selezionare **Connettersi a un nuovo schema** e fare clic su **Avanti**.
- ▶ Nel passaggio 4 a pag. 114 selezionare **Connettersi a un nuovo schema** e fare clic su **Avanti**.

Riavviare il server

Se è stata eseguita la procedura guidata di configurazione di UC MDB Server nell'ambito dell'installazione di HP Universal CMDB è necessario riavviare HP Universal CMDB sul server solo dopo aver correttamente impostato i parametri di tutti i database.

Se è stata eseguita la procedura guidata di configurazione di UC MDB Server per la modifica dei tipi di database definiti in precedenza o dei parametri di connessione, riavviare HP Universal CMDB Server e Data Flow Probe dopo aver completato correttamente il processo di modifica dei parametri.

9

Servizi di HP Universal CMDB

Questo capitolo comprende:

Compiti

- ▶ Visualizzare lo stato dei servizi del server HP Universal CMDB a pag. 118
- ▶ Avviare e arrestare il servizio del server HP Universal CMDB a pag. 119

Riferimenti

- ▶ Servizi di HP Universal CMDB a pag. 120

Compiti

Visualizzare lo stato dei servizi del server HP Universal CMDB

Selezionare **Start > Tutti i programmi > HP UCMDB > Stato server HP Universal CMDB**. Viene visualizzato lo stato e lo stato dettagliato di tutti i servizi:

Status

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

Detailed Status

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

La colonna Cliente indica se tutti i servizi di HP Universal CMDB sono in esecuzione (**Su**) oppure se alcuni non sono attivi ().

Nota: se qualche servizio non è in esecuzione, rivolgersi a HP Software Support per cercare di risolvere il problema.

Avviare e arrestare il servizio del server HP Universal CMDB

Accedere alla finestra **Servizi** di Windows e individuare il servizio **UCMDB_Server**. Si apre la finestra di dialogo Proprietà di **UCMDB Server (computer locale)** e si apre il servizio. Se necessario, cambiare il tipo di avvio in **Automatico**.

Per i dettagli sull'avvio e l'arresto del server UCMDB consultare “Accedere ai comandi su piattaforma Windows” a pag. 124 oppure “Accedere ai comandi su piattaforma Linux” a pag. 125.

Riferimenti

Servizi di HP Universal CMDB

I servizi del server HP Universal CMDB sono descritti nella tabella seguente:

Nome del servizio	Descrizione del servizio
autodiscovery	Responsabile dei servizi relativi a Gestione flusso di dati.
classModel	Responsabile della gestione del modello di classe nel CMDB.
cmdb_mod_not	Responsabile delle notifiche dei cambiamenti che si verificano nel CMDB.
cmdb_sys_tqls	Responsabile delle condizioni applicate ai nodi TQL e dei risultati delle condizioni memorizzati nella TQL di sistema.
cmdb_view	Responsabile del calcolo delle definizioni della vista in base ai risultati della TQL (la trasformazione dal grafico alla struttura viene data alla definizione della vista).
configuration	Responsabile delle istantanee, delle query dei cambiamenti CI e della query della TQL/cronologia della vista.
content-install	
data-acquisition	
enrichment	Responsabile dell'esecuzione degli accrescimenti ad hoc e attivi.
fcmdb	Responsabile del controllo degli adattatori, del popolamento e dei flussi di invio di dati, della federazione dei dati e dell'individuazione da un modulo di livello superiore.
fcmdb-config	Meccanismo della cache per i dati federati che consentono i servizi FCMDB di base prima del caricamento completo di FCMDB.
fcmdb-management	Responsabile della gestione degli adattatori, della federazione e del flusso di invio dei dati.

Nome del servizio	Descrizione del servizio
folders	Responsabile della gestione della gerarchia delle cartelle per ogni tipo di risorsa.
framework	
grouping	Responsabile della gestione dei diversi pacchetti che consentono la classificazione delle risorse.
historyDB	
impact	Responsabile dell'impatto, della causa principale e dei sottosistemi di correlazione di HP Universal CMDB.
mapping-engine	
model	Responsabile della mappatura dei CI dalle origini di dati esterne ai CI locali di CMDB.
model_update	Responsabile della gestione degli aggiornamenti del modello di classe nel CMDB.
packaging	Responsabile dei pacchetti. I pacchetti sono file zip che contengono le risorse che sono strutturate in sottodirectory organizzate predefinite.
reconciliation	Servizio di riconciliazione del popolamento di dati del CMDB. Responsabile del motore di riconciliazione di HP Universal CMDB.
report	Responsabile dei servizi di report di HP Universal CMDB, ad esempio l'aggiunta, la modifica e la rimozione dei report di sistema, il calcolo dei report Asset e Dipendenza nodo.
utilità di pianificazione	
protezione	
state_management	
tql	Responsabile dei calcoli TQL.
tql_res_utils	Responsabile della manutenzione dei risultati TQL (attiva) e recupero del layout.
view	Responsabile della parte della logica aziendale di Studio di modellazione, compreso "watch".

Nome del servizio	Descrizione del servizio
world	Repository centrale per le informazioni di configurazione raccolte dalle varie applicazioni e strumenti di HP Universal CMDB e di terze parti. Tali informazioni vengono utilizzate per la creazione delle viste di HP Universal CMDB. Nota: il servizio di CMDB non è necessariamente eseguito dal processo mercury_as.

Risoluzione dei problemi e limitazioni

Problema: UCMDB non si avvia automaticamente al riavvio del sistema.

Soluzione:

- 1** Selezionare **Start > Tutti i programmi > HP UCMDB > Avvia server HP Universal CMDB**.
- 2** Aprire la finestra di dialogo **Servizi** di Windows e selezionare il servizio **UCMDB_Server**.
- 3** Si apre la finestra di dialogo **Proprietà di UCMDB Server (computer locale)**.
- 4** Nella scheda **Generale**, accertarsi di quanto segue:
 - Il campo **Percorso dell'eseguibile** punta al percorso dell'eseguibile corretto.
 - Il servizio è configurato per l'avvio automatico (**Tipo di avvio è Automatico**).
- 5** Nella scheda **Accesso**, accertarsi di quanto segue:
 - Il servizio utilizza l'utente corretto per l'accesso. Per i dettagli sul cambiamento dell'utente del servizio, consultare “Cambiare l'utente del servizio HP Universal CMDB Server” a pag. 289.
- 6** Nella scheda **Dipendenze**, accertarsi di quanto segue:
 - Il servizio è configurato per non avere dipendenze (<**Nessuna dipendenza**>).

10

Accedere ai comandi del server UCMDB

Questo capitolo comprende:

Compiti

- Accedere ai comandi su piattaforma Windows a pag. 124
- Accedere ai comandi su piattaforma Linux a pag. 125

Compiti

Accedere ai comandi su piattaforma Windows

Durante l'installazione di HP Universal CMDB viene aggiunto un menu di avvio alle impostazioni del computer sul quale è stato installato UCMDB. È possibile avviare e arrestare il server UCMDB, accedere alla procedura guidata di configurazione del database, visualizzare lo stato del servizio del server e disinstallare il server.

Nota: Per i dettagli sull'avvio e l'arresto del server UCMDB come servizio consultare “Avviare e arrestare il servizio del server HP Universal CMDB” a pag. 119.

Per accedere al menu di avvio di HP Universal CMDB selezionare **Start > Programmi > HP UCMDB**. Nel menu sono comprese le opzioni seguenti:

- ▶ **Avvio della procedura guidata di configurazione di HP Universal CMDB Server.** Consente di eseguire la procedura guidata per il collegamento a un database o schema esistente oppure per la creazione di un nuovo database o schema. Per i dettagli consultare “Scelta del database o dello schema” a pag. 102.
- ▶ **Avvio di HP Universal CMDB Server.** Fare clic per avviare il servizio del server.
- ▶ **Interrompi HP Universal CMDB Server.** Fare clic per arrestare il servizio del server.
- ▶ **Stato di HP Universal CMDB Server.** Fare clic per aprire una pagina Web con le informazioni sul server. Per i dettagli consultare “Servizi di HP Universal CMDB” a pag. 120.
- ▶ **Disinstallazione di HP Universal CMDB Server.** Fare clic per disinstallare il server.

Accedere ai comandi su piattaforma Linux

Eeguire i comandi seguenti per avviare e arrestare il server UCMDB, accedere alla procedura guidata di configurazione del database, lo stato del servizio del server e disinstallare il server.

Nota:

- Per i dettagli sull'avvio e l'arresto del server UCMDB come servizio consultare “Avviare e arrestare il servizio del server HP Universal CMDB” a pag. 119.
- I comandi seguenti presumono che UCMDB sia installato nel percorso predefinito, ovvero **/opt/hp**. Se il server è installato altrove, sostituire il percorso suddetto..

-
- Per avviare il server HP Universal CMDB:

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

- Per arrestare il server HP Universal CMDB:

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

- Per chiamare la procedura guidata di configurazione di HP Universal CMDB Server:

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

- Per accedere alla pagina Web sullo stato del server UCMDB, aprire una pagina del browser e immettere l'URL seguente: **http://<nome host o IP di UCMDB Server>:8080/status**.

Nota: è possibile accedere alla pagina sullo stato da qualsiasi computer e non solo dal computer Linux che ospita il server UCMDB.

- Per disinstallare il server UCMDB:

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

Parte III

Installazione della sonda del flusso di dati

11

Installazione della sonda del flusso di dati su piattaforma Windows

Questo capitolo comprende:

Compiti

- Installare la sonda del flusso di dati a pag. 130
- Aggiornamento della sonda a pag. 139
- Eseguire Probe Manager e Probe Gateway su computer separati a pag. 140
- Configurare i componenti di Probe Manager e Probe Gateway a pag. 141
- Connettere una sonda del flusso di dati per un cliente non predefinito a pag. 142

Riferimenti

- Requisiti per l'installazione della sonda del flusso di dati a pag. 143
- **Risoluzione dei problemi e limitazioni** a pag. 145

Compiti

Installare la sonda del flusso di dati

Nota: si consiglia di leggere attentamente “Introduzione a HP Universal CMDB” a pag. 25 prima di iniziare l'installazione. Per maggiori informazioni sulla Gestione flusso di dati leggere “Introduzione a Gestione flusso di dati” nella *Guida alla gestione del flusso di dati di HP Universal CMDB*.

La procedura seguente spiega come installare la sonda del flusso di dati su una piattaforma Windows.

La sonda può essere installata prima o dopo l'installazione del server HP Universal CMDB. Durante l'installazione della sonda è necessario fornire il nome del server quindi è preferibile installare il server prima di installare la sonda.

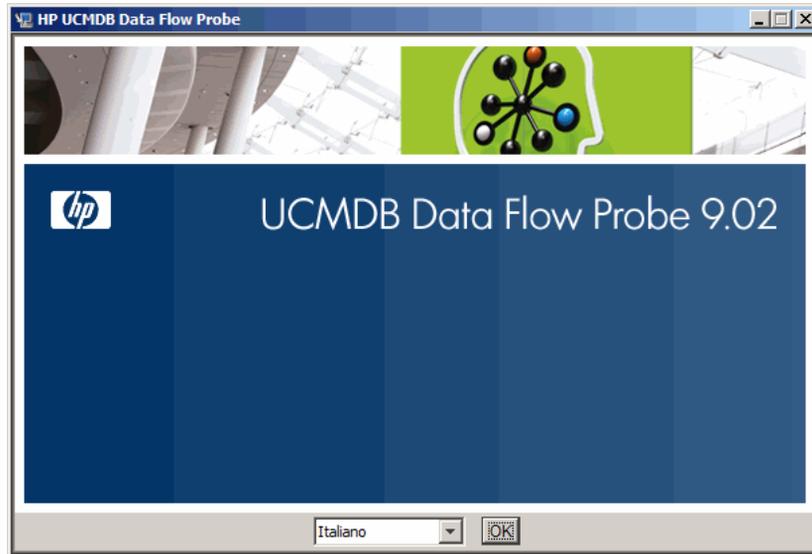
Verificare di disporre di spazio disponibile sufficiente su disco prima di iniziare l'installazione. Per i dettagli consultare “Requisiti per l'installazione della sonda del flusso di dati” a pag. 143.

Nota: per i dettagli sulla licenza consultare “Modello di licenza di HP Universal CMDB” a pag. 47.

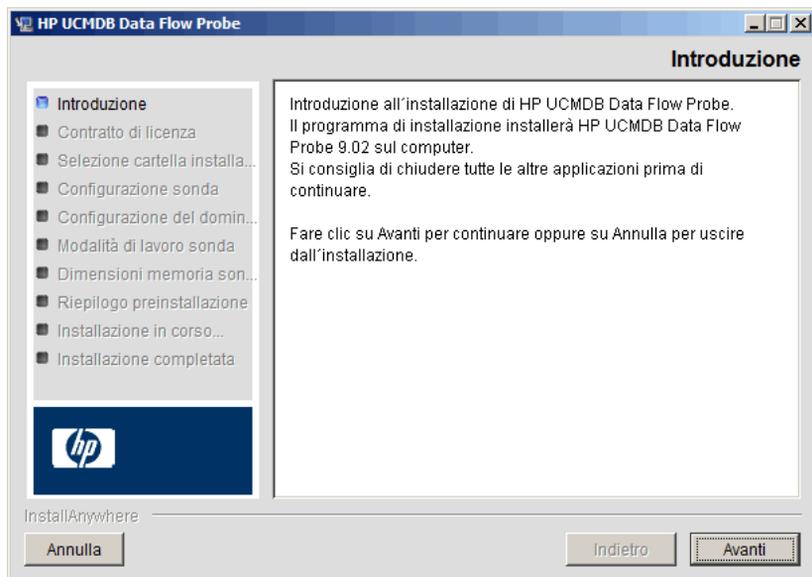
Per installare la sonda del flusso di dati di UCMDB:

- 1** Inserire il DVD di Windows per l'installazione di **HP Universal CMDB 9.02** nell'unità dalla quale si sta installando la sonda. Se si sta installando da un'unità di rete, eseguire il collegamento.
- 2** Fare doppio clic sul file della cartella principale del <DVD >\UCMDB902\HPUCMDB_DataFlowProbe_902.exe.

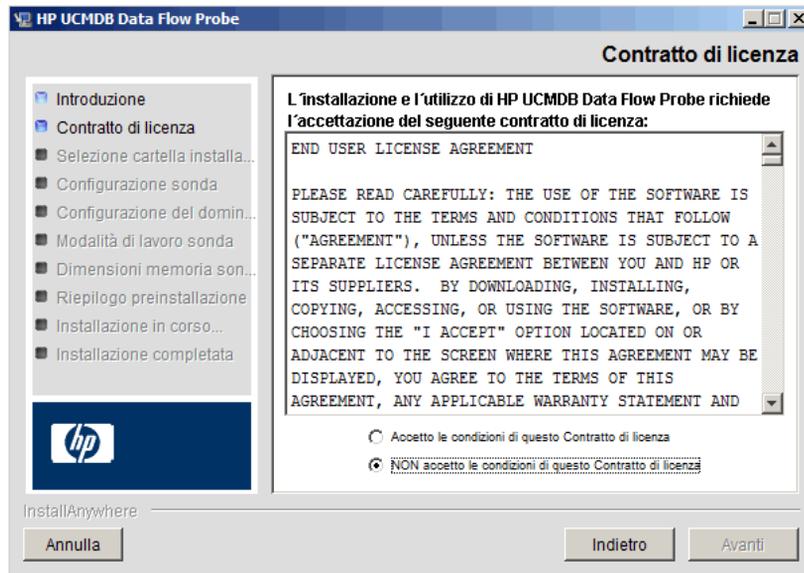
Viene visualizzata una barra di avanzamento. Al termine del processo si apre la schermata iniziale.



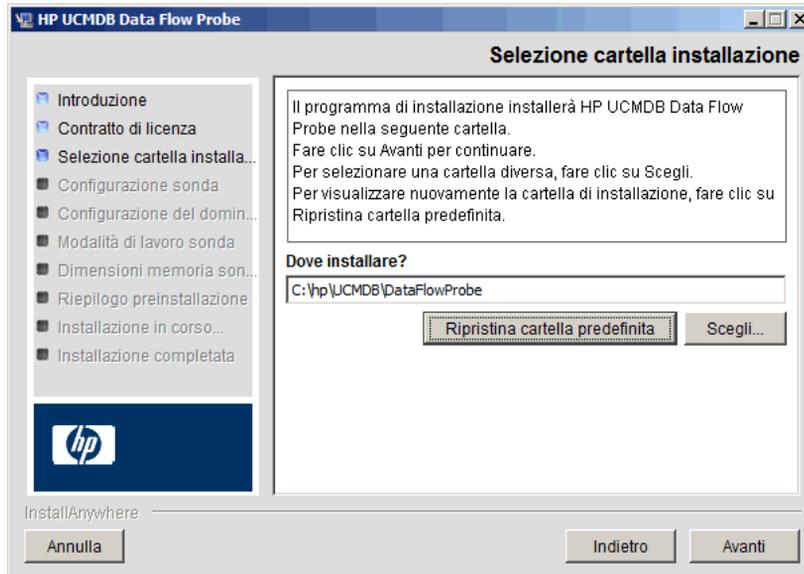
- 3 Selezionare la lingua delle impostazioni internazionali e fare clic su **OK** per aprire la finestra di dialogo Introduzione.



4 Fare clic su **Avanti** per continuare con il Contratto di licenza.



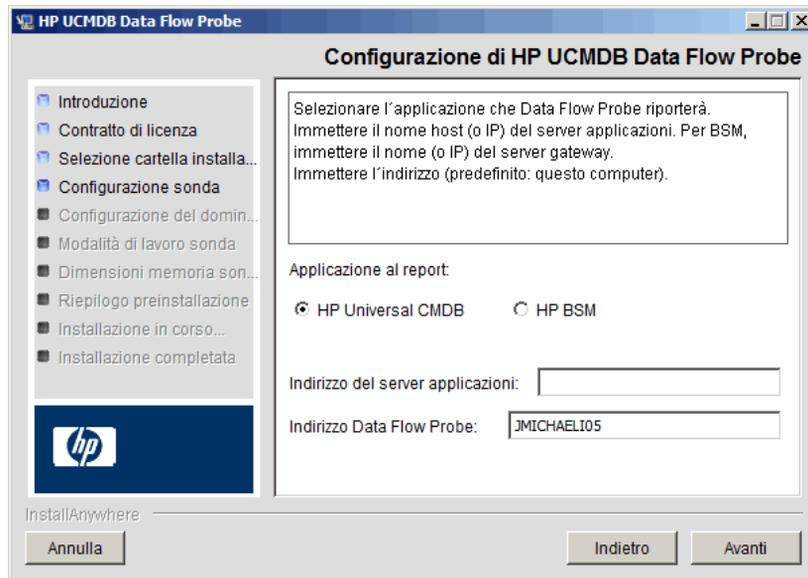
5 Accettare i termini del contratto e fare clic su **Avanti** per aprire la finestra di dialogo Selezione della cartella di installazione.



- 6 Accettare la voce predefinita oppure fare clic su **Scegli** per visualizzare una finestra di dialogo predefinita Sfoglia. Per installare una directory diversa, individuarla e selezionare la cartella di installazione.

Nota: per ripristinare la directory di installazione predefinita, dopo aver selezionato una directory nella finestra di dialogo Sfoglia fare clic su **Ripristina cartella predefinita**.

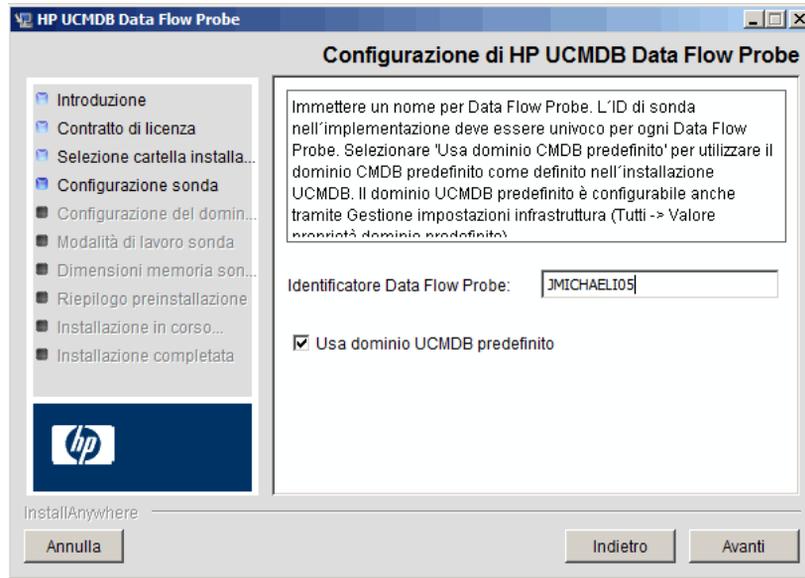
- 7 Fare clic su **Avanti** per aprire la finestra di dialogo Configurazione di HP UCMDB Data Flow Probe.



- ▶ **Applicazione al report.** Selezionare il server delle applicazioni che si sta utilizzando. È possibile utilizzare la sonda con HP Universal CMDB o Business Service Management.
 - ▶ Se si seleziona **HP Universal CMDB** nella casella **Indirizzo del server applicazioni** immettere il nome o l'indirizzo IP del server HP Universal CMDB al quale si deve connettere la sonda.
 - ▶ Se si seleziona HP BSM, nella casella **Indirizzo del server applicazioni** immettere l'IP o il nome DNS del server gateway.
- ▶ Nella casella **Indirizzo Data Flow Probe** immettere l'indirizzo IP oppure il nome DNS del computer sul quale si sta installando la sonda oppure accettare i valori predefiniti.
- 8 Se non si immette l'indirizzo del server della applicazioni, viene visualizzato un messaggio. È possibile scegliere di continuare a installare la sonda senza immettere l'indirizzo oppure tornare alla pagina precedente e aggiungere l'indirizzo.



- 9 Fare clic su **Avanti** per aprire la finestra di dialogo Configurazione di HP UCMDB Data Flow Probe.



- Nella casella **Identificatore Data Flow Probe** immettere un nome della sonda utilizzato per identificarla nel proprio ambiente.

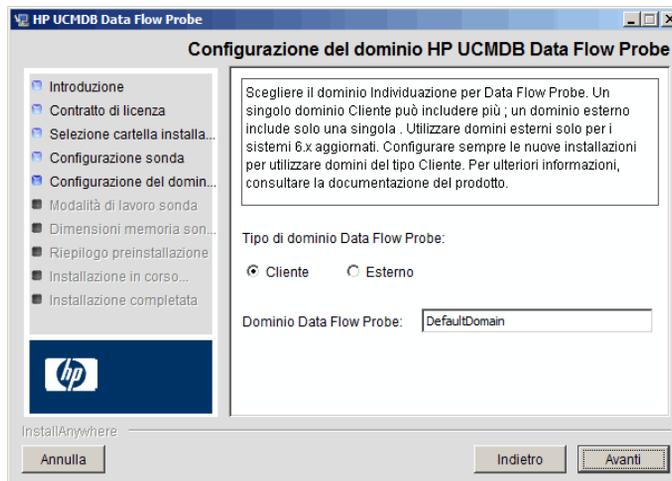
Importante:

- l'identificatore della sonda di UCMDB deve essere univoco per ciascuna sonda della distribuzione.
 - Quando si installa la sonda in modalità separata, ovvero Probe Gateway e Probe Manager sono installati su computer separati, è necessario dare lo stesso nome al Probe Gateway e a tutte le rispettive gestioni. Questo nome viene visualizzato in UCMDB come singolo nodo della sonda. In caso di errore nell'assegnazione del nome potrebbe impedire la corretta esecuzione dei processi.
-

- Selezionare **Usa dominio CMDB predefinito** per utilizzare l'indirizzo IP predefinito di UCMDB oppure il nome del computer come definito nell'installazione del server UCMDB.

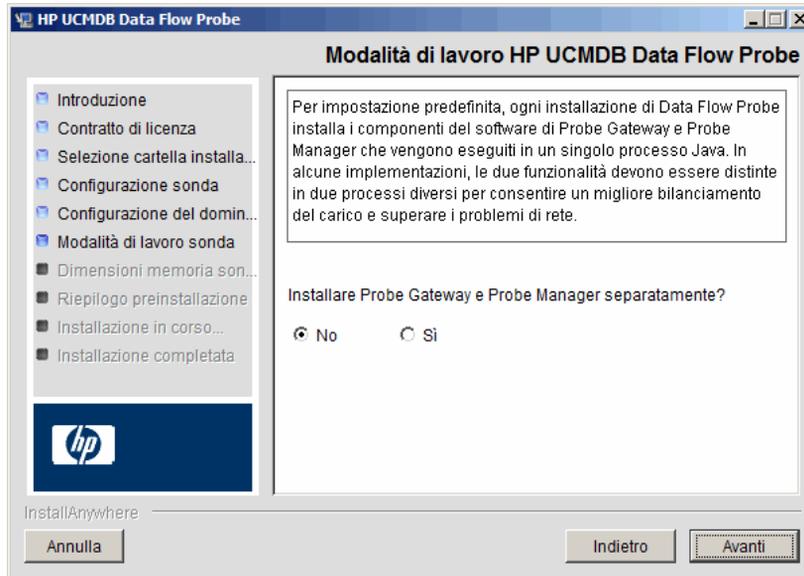
Il dominio predefinito di UCMDB è configurabile anche tramite l'opzione Impostazioni infrastruttura disponibile dopo l'installazione di HP Universal CMDB (**Amministrazione > Impostazioni infrastruttura > Impostazioni modello di classe > Valore predefinito della proprietà dominio**).

- 10** Fare clic su **Avanti**. Se la casella **Usa dominio CMDB predefinito** è stata deselezionata nella finestra di dialogo Configurazione di HP UCMDB Data Flow Probe, viene visualizzata la finestra di dialogo Configurazione del dominio di HP UCMDB Data Flow Probe.



- **Tipo di dominio Data Flow Probe.** Scegliere tra **Cliente** e **Esterno** a seconda del tipo di dominio sul quale deve essere eseguita la sonda:
 - **Cliente.** Selezionare se si sta installando una o più sonde nella propria distribuzione.
 - **Esterno.** Selezionare se si sta eseguendo l'aggiornamento da sistemi della versione 6.x.
- Importante:** per le nuove installazioni selezionare sempre **Cliente**.
- **Dominio Data Flow Probe:** Se non si sta utilizzando il dominio predefinito definito in UCMDB immettere qui il nome del dominio.

- 11 Fare clic su **Avanti** per aprire la finestra di dialogo Modalità di lavoro di HP UCMDB Data Flow Probe.

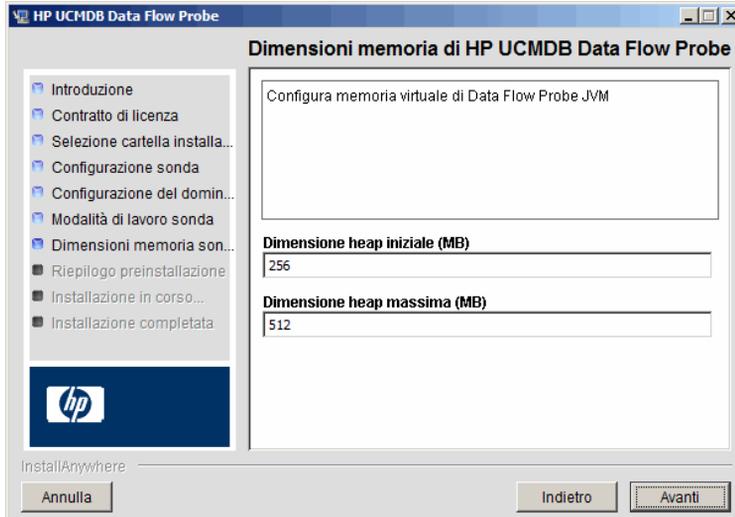


È possibile eseguire Probe Gateway e Manager come un processo Java o come processi separati. È probabile eseguirli come processi separati in distribuzioni che richiedono un migliore bilanciamento del carico e di risolvere i problemi di rete.

Fare clic su **No** per eseguire Probe Gateway e Probe Manager come processo unico.

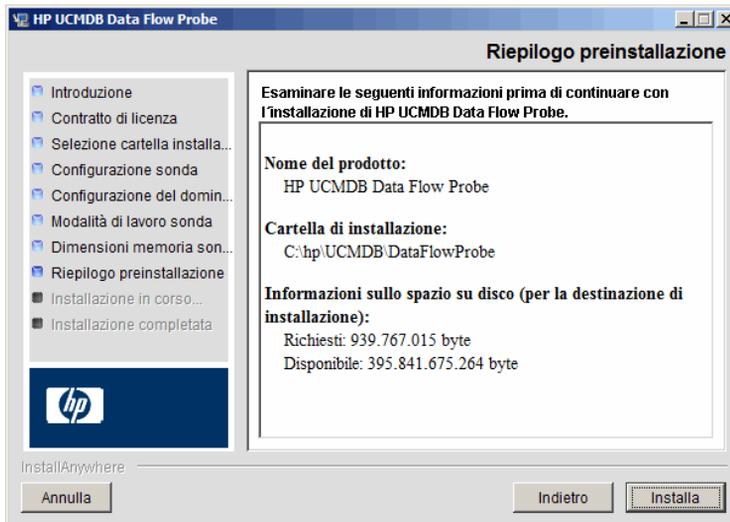
Fare clic su **Sì** per eseguire Probe Gateway e Probe Manager come due processi. Per i dettagli sulla procedura consultare “Eseguire Probe Manager e Probe Gateway su computer separati” a pag. 140.

- 12 Fare clic su **Avanti** per aprire la finestra di dialogo Dimensioni memoria di HP UCMDB Data Flow Probe.



Definire la memoria minima e massima da allocare per la sonda. I valori sono misurati in megabyte.

- 13 Fare clic su **Avanti** per aprire la finestra di dialogo Riepilogo preinstallazione e riesaminare le selezioni eseguite.



- 14** Fare clic su **Installa** per completare l'installazione della sonda. Al termine dell'installazione, viene visualizzata la pagina Installazione completata.

Eventuali errori durante l'installazione vengono scritti nel file seguente:
C:\hp\UCMDB\DataFlowProbe\HP_UCMDB_Data_Flow_Probe_Install Log.log.

- 15** Fare clic su **Eseguito**. Il menu di scelta rapida seguente viene aggiunto al menu **Start** di Windows:

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

- 16** Per attivare la sonda selezionare la scelta rapida.

È possibile eseguire la sonda in una console. Per i dettagli consultare “Avvio della sonda in una console” nella *Guida alla gestione del flusso di dati di HP Universal CMDB*.

La sonda viene visualizzata in HP Universal CMDB: accedere a **Gestione flusso di dati > Impostazione della sonda del flusso di dati**. Per i dettagli consultare “Requisiti per l'installazione della sonda del flusso di dati” a pag. 143.

Aggiornamento della sonda

Questo compito descrive come eseguire l'aggiornamento della sonda del flusso dati.

1 Disinstallare la sonda precedente

Disinstallare tutte le sonde esistenti Se una sonda è in esecuzione arrestarla prima di disinstallarla:

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

2 Installare la nuova sonda

Installare la nuova sonda con la stessa configurazione, ovvero utilizzare lo stesso ID della sonda, nome di dominio e nome server dell'installazione della sonda precedente.

Eseguire Probe Manager e Probe Gateway su computer separati

Durante l'installazione è possibile scegliere di separare i processi di Probe Manager e Probe Gateway in modo da eseguirli su computer separati. È necessario:

- 1** Installare la sonda su entrambi i computer seguendo la procedura descritta in “Installare la sonda del flusso di dati” a pag. 130.
- 2** Scegliere **Sì** nel passaggio 11 a pag. 137.
- 3** Eseguire la configurazione in “Configurare i componenti di Probe Manager e Probe Gateway” a pag. 141.

Nota:

- Deve essere installato almeno un componente di Probe Gateway. Gateway è connesso al server UCMDB, riceve i compiti dal server e comunica con gli strumenti di raccolta (Probe Manager).
 - Si possono installare diversi Probe Manager. I gestori eseguono i processi e raccolgono informazioni dalle reti.
 - Probe Gateway deve contenere l'elenco dei gestori collegati.
 - I Probe Manager devono sapere a quale Gateway sono collegati.
-

Configurare i componenti di Probe Manager e Probe Gateway

In questa sezione viene spiegato come installare la sonda del flusso di dati quando Probe Manager e Probe Gateway sono eseguiti come processi separati su due computer.

In questa sezione vengono trattati i seguenti argomenti:

- “Configurazione del computer di Probe Gateway” a pag. 141
- “Configurazione del computer di Probe Manager” a pag. 142
- “Avviare i servizi” a pag. 142

1 Configurazione del computer di Probe Gateway

a Aprire il seguente file:

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

b Individuare la riga che inizia con `<probeMgr ip=` e aggiungere il nome del computer del Manager o l'indirizzo IP, ad esempio:

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

c Aprire il seguente file:

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

d Individuare le righe che iniziano con `appilog.collectors.local.ip =` e `appilog.collectors.probe.ip =` e immettere il nome del computer del Gateway o l'indirizzo IP, ad esempio:

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

2 Configurazione del computer di Probe Manager

- a In `C:\hp\UCMDB\DataFlowProbe\conf\DiscoveryProbe.properties` individuare la riga che inizia con `appilog.collectors.local.ip = e` e immettere il nome del computer del Manager o l'indirizzo IP, ad esempio:

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

- b Individuare la riga che inizia con `appilog.collectors.probe.ip = e` e immettere il nome del computer del Gateway in maiuscolo, ad esempio:

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

3 Avviare i servizi

- a Sul computer di Probe Manager avviare il servizio Manager: **Start > Tutti i programmi > UCMDB > Avvia sonda del flusso di dati.**
- b Sul computer di Probe Gateway avviare il servizio Gateway: **Start > Tutti i programmi > UCMDB > Avvia sonda del flusso di dati (console).**

Connettere una sonda del flusso di dati per un cliente non predefinito

È possibile connettere una sonda del flusso di dati per un cliente che non è predefinito. L'ID del cliente predefinito è 1.

- 1 Aprire il file seguente in un editor di testo:
`C:\hp\UCMDB\DataFlowProbe\conf\DiscoveryProbe.properties.`
- 2 Individuare la voce `customerID`.
- 3 Aggiornare il valore con l'ID del cliente, ad esempio `customerID = 2`.
- 4 Riavviare la sonda per aggiornarla con i cambiamenti.

Riferimenti

Requisiti per l'installazione della sonda del flusso di dati

In questa sezione vengono trattati i seguenti argomenti:

- “Requisiti hardware” a pag. 143
- “Requisiti software” a pag. 143
- “Requisiti ambiente virtuale” a pag. 144

Requisiti hardware

Computer/ processore	Windows: processore Pentium IV 2.4 GHz o successivo
Memoria	Windows: minimo 1 GB RAM (consigliata: 2 GB RAM)
Memoria virtuale (per distribuzione Windows)	Minimo 2 GB Nota: La dimensione della memoria virtuale deve essere almeno due volte la dimensione della memoria fisica.
Spazio libero su disco rigido	Windows: minimo 4 GB (almeno 4 GB per il software del database e i file di dati) (consigliato: 20 GB disco rigido)
Display	Windows: impostazione della tavolozza dei colori su almeno 256 colori (consigliati 32.000 colori)

Requisiti software

Piattaforma hardware	Tipo di sistema operativo	Versione ed edizione SO	Supportato	Consigliato
x86	Windows 2008	SP2, Standard/Enterprise edition, 32-bit	Sì	
x86-64	Windows 2008	SP2, Standard/Enterprise edition, 64-bit	Sì	Sì

Piattaforma hardware	Tipo di sistema operativo	Versione ed edizione SO	Supportato	Consigliato
x86-64	Windows 2008	R2, Standard/Enterprise edition, 64-bit	Sì	
x86	Windows 2003	SP2 e R2 SP2, Standard/Enterprise edition, 32-bit	Sì	
x86-64	Windows 2003	SP2 e R2 SP2, Standard/Enterprise edition, 64-bit	Sì	
	Windows 7	Professional/Enterprise	No	
	Windows 2000		No	

Requisiti ambiente virtuale

Piattaforma	Versione ed edizione SO	Supportato	Consigliato
VMware ESX 3.x	<ul style="list-style-type: none"> ▶ Windows 2003 Standard/Enterprise edition SP2 e R2 SP2, 32/64-bit ▶ Windows 2008 Standard/Enterprise SP2, 32/64-bit e R2, 64-bit 	Sì	
VMware ESX 4.0	<ul style="list-style-type: none"> ▶ Windows 2003 Standard/Enterprise edition SP2 e R2 SP2, 32/64-bit ▶ Windows 2008 Standard/Enterprise SP2, 32/64-bit e R2, 64-bit 	Sì	Sì
Pre ESX 3.5 (come le versioni 3.0.x)	<ul style="list-style-type: none"> ▶ Potrebbe non fornire prestazioni adeguate ▶ Non supporta Windows 2008 o Windows 7 	No	
ESXi VMware	Tutte le piattaforme	No	
MS Hyper-V	Server 2008 v1 e R2	No	
Xen Hypervisor 3.x	Tutte le piattaforme	No	

Risoluzione dei problemi e limitazioni

Il database MySQL della sonda del flusso di dati potrebbe danneggiarsi senza possibilità di ripristino, ad esempio poiché è stato arrestato il computer ma non il servizio MySQL.

Per riparare il problema:

- 1** Arrestare la sonda.
- 2** Eseguire lo strumento **repair_mysql.bat** dalla cartella seguente:
C:\hp\UCMDB\DataFlowProbe\tools\.
- 3** Avviare la sonda.

Se questa procedura non risolve il problema rivolgersi a HP Software Support.

12

Installazione della sonda del flusso di dati su piattaforma Linux

Questo capitolo comprende:

Compiti

- Installare la sonda del flusso di dati a pag. 148
- Arrestare il server della sonda a pag. 157
- Aggiornamento della sonda del flusso di dati a pag. 158
- Connettere una sonda del flusso di dati per un cliente non predefinito a pag. 158

Riferimenti

- Requisiti per il supporto della sonda del flusso di dati a pag. 159
- **Risoluzione dei problemi e limitazioni.** a pag. 159

Compiti

Installare la sonda del flusso di dati

Importante:

- ▶ Questa sonda è progettata solo ai fini dell'integrazione e non può essere utilizzata per l'individuazione. Pertanto non viene visualizzata nella finestra Impostazione della sonda del flusso di dati.
- ▶ Non è possibile eseguire un'istanza del database Microsoft My SQL sul computer nel quale si sta installando la sonda del flusso di dati. Se è in corso un'istanza è necessario disabilitarla.
- ▶ Per installare la sonda del flusso di dati è necessario disporre delle autorizzazioni principali sul computer Linux.

La procedura seguente spiega come installare la sonda del flusso di dati su una piattaforma Linux.

La sonda può essere installata prima o dopo l'installazione del server HP Universal CMDB. Durante l'installazione della sonda è necessario fornire il nome del server quindi è preferibile installare il server prima di installare la sonda.

Verificare di disporre di spazio disponibile sufficiente su disco prima di iniziare l'installazione. Per i dettagli consultare “Requisiti per il supporto della sonda del flusso di dati” a pag. 159.

Nota: per i dettagli sulla licenza consultare “Modello di licenza di HP Universal CMDB” a pag. 47.

Per installare la sonda del flusso di dati di UCMDB:

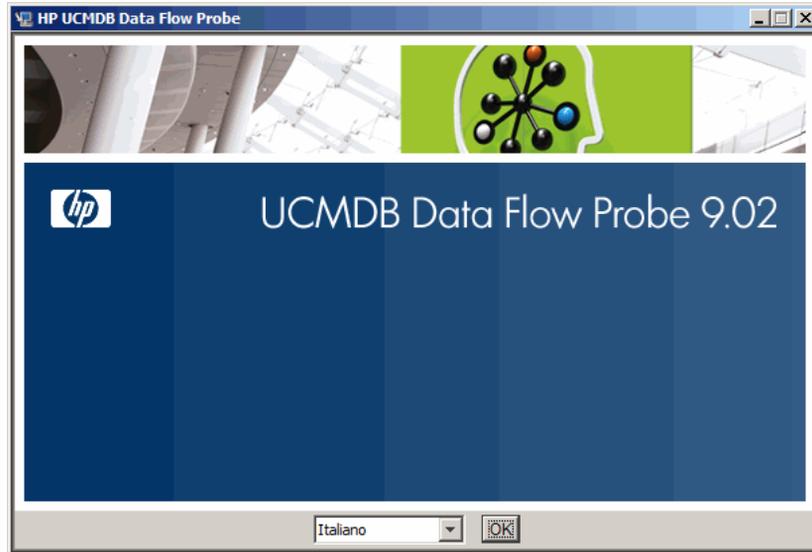
1 Per la procedura guidata all'installazione eseguire il comando seguente:

```
sh <percorso programma di  
installazione>/HPUCMDB_DataFlowProbe_902Linux.bin
```

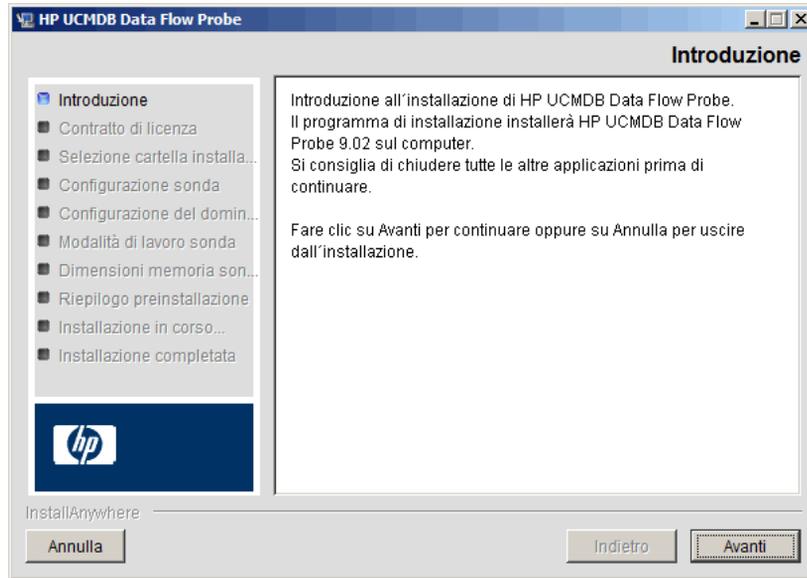
Vengono eseguiti di comandi seguenti:

```
Preparing to install...  
Extracting the JRE from the installer archive...  
Unpacking the JRE...  
Extracting the installation resources from the installer archive...  
Configuring the installer for this system's environment...  
Launching installer...
```

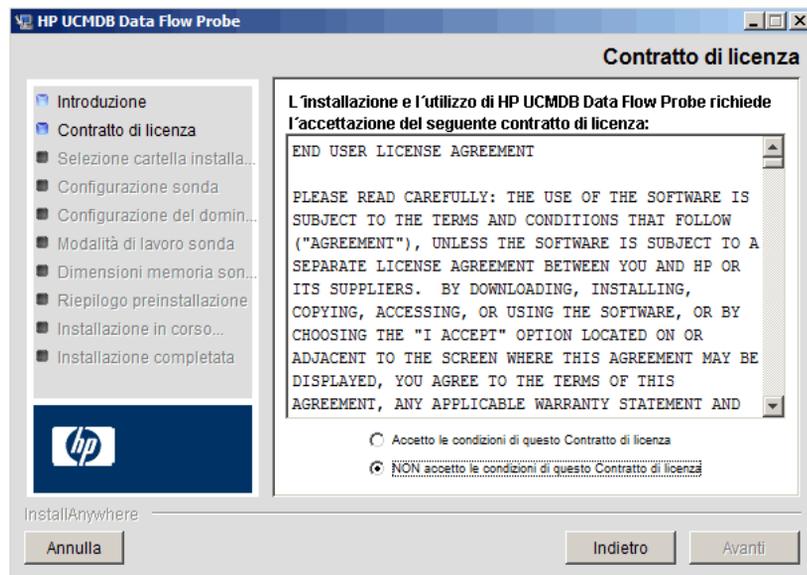
Al termine del processo si apre la schermata iniziale.



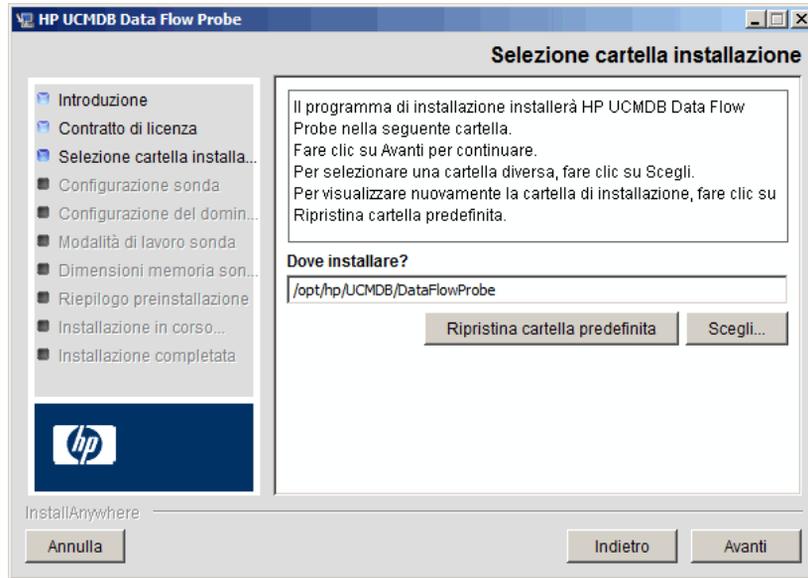
- 2 Selezionare la lingua delle impostazioni internazionali e fare clic su **OK** per aprire la finestra di dialogo Introduzione.



- 3 Fare clic su **Avanti** per continuare con il Contratto di licenza.



- 4 Accettare i termini del contratto e fare clic su **Avanti** per aprire la finestra di dialogo Selezione della cartella di installazione.

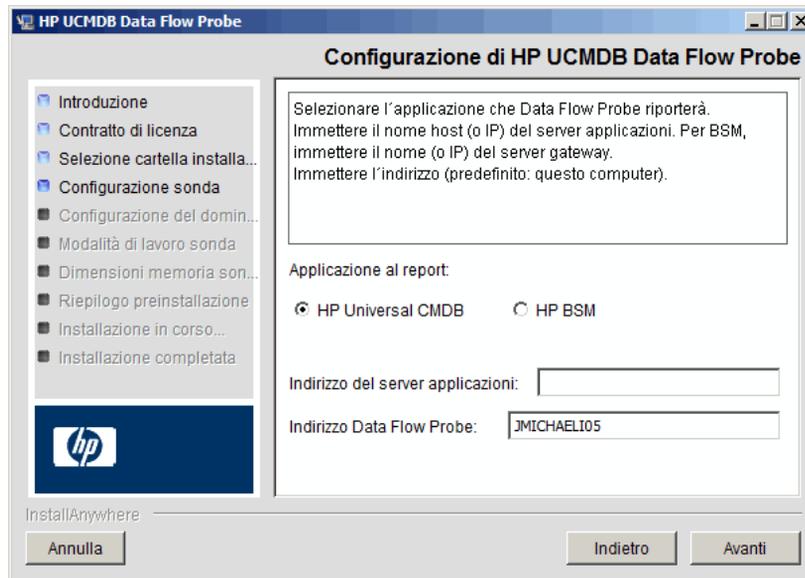


- 5 Accettare la voce predefinita oppure fare clic su **Scegli** per visualizzare una finestra di dialogo predefinita Sfoglia. Per installare una directory diversa, individuarla e selezionare la cartella di installazione.

Nota:

- È possibile cambiare il percorso dell'installazione ma la directory devono essere collocata in **/opt/**.
 - per ripristinare la directory di installazione predefinita, dopo aver selezionato una directory nella finestra di dialogo Sfoglia fare clic su **Ripristina cartella predefinita**.
-

- 6 Fare clic su **Avanti** per aprire la finestra di dialogo Configurazione di HP UCMDB Data Flow Probe.

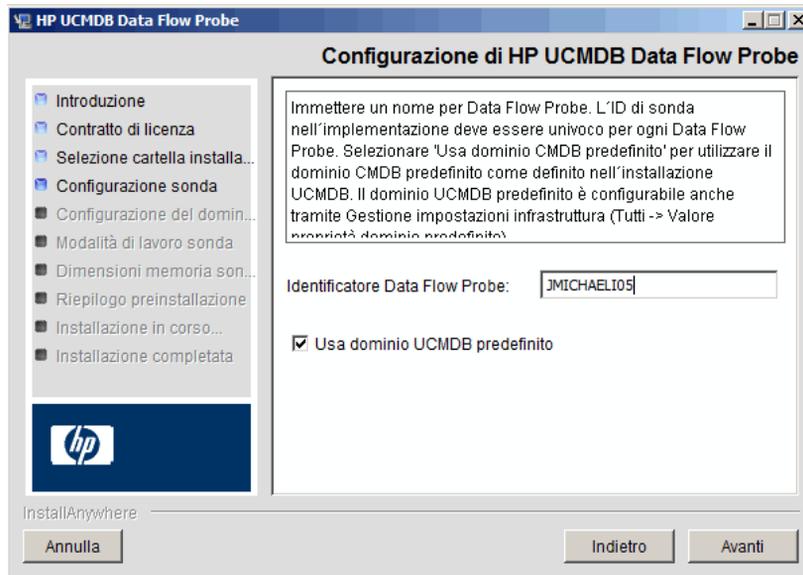


- **Applicazione al report.** Selezionare il server delle applicazioni che si sta utilizzando. È possibile utilizzare la sonda con HP Universal CMDB o Business Service Management.
 - Se si seleziona **HP Universal CMDB** nella casella **Indirizzo del server applicazioni** immettere il nome o l'indirizzo IP del server HP Universal CMDB al quale si deve connettere la sonda.
 - Se si seleziona HP BSM, nella casella **Indirizzo del server applicazioni** immettere l'IP o il nome DNS del server gateway.
- Nella casella **Indirizzo Data Flow Probe** immettere l'indirizzo IP oppure il nome DNS del computer sul quale si sta installando la sonda oppure accettare i valori predefiniti.

- 7 Se non si immette l'indirizzo del server della applicazioni, viene visualizzato un messaggio. È possibile scegliere di continuare a installare la sonda senza immettere l'indirizzo oppure tornare alla pagina precedente e aggiungere l'indirizzo.



- 8 Fare clic su **Avanti** per aprire la finestra di dialogo Configurazione di HP UCMDB Data Flow Probe.



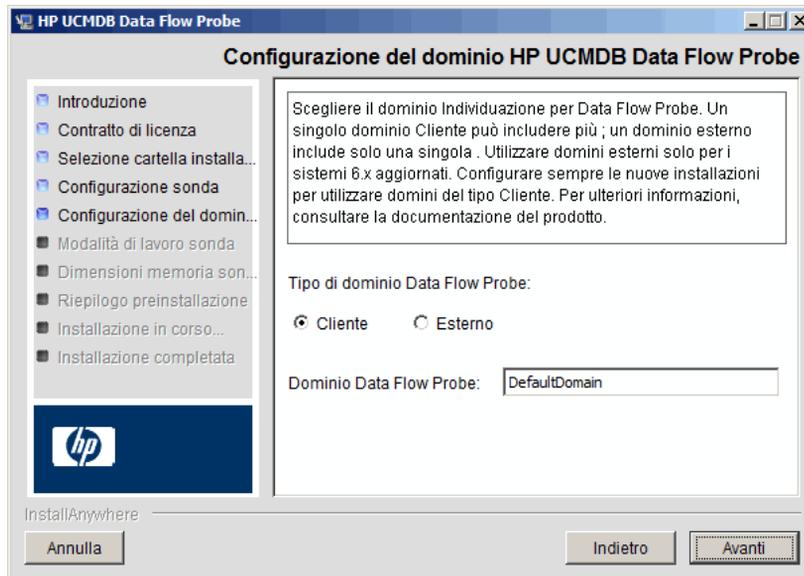
- Nella casella **Identificatore Data Flow Probe** immettere un nome della sonda utilizzato per identificarla nel proprio ambiente. Questo è il nome che viene visualizzato nella finestra di dialogo Punto di integrazione. Per i dettagli consultare “Finestra di dialogo Crea nuovo punto di integrazione/Modifica punto di integrazione” nella *Guida alla gestione del flusso di dati di HP Universal CMDB*.

Importante: L'identificatore della sonda di UCMDB deve essere univoco per ciascuna sonda della distribuzione.

- Selezionare **Usa dominio CMDB predefinito** per utilizzare l'indirizzo IP predefinito di UCMDB oppure il nome del computer come definito nell'installazione del server UCMDB.

Il dominio predefinito di UCMDB è configurabile anche tramite l'opzione Impostazioni infrastruttura disponibile dopo l'installazione di HP Universal CMDB (**Amministrazione > Impostazioni infrastruttura > Impostazioni modello di classe > Valore predefinito della proprietà dominio**).

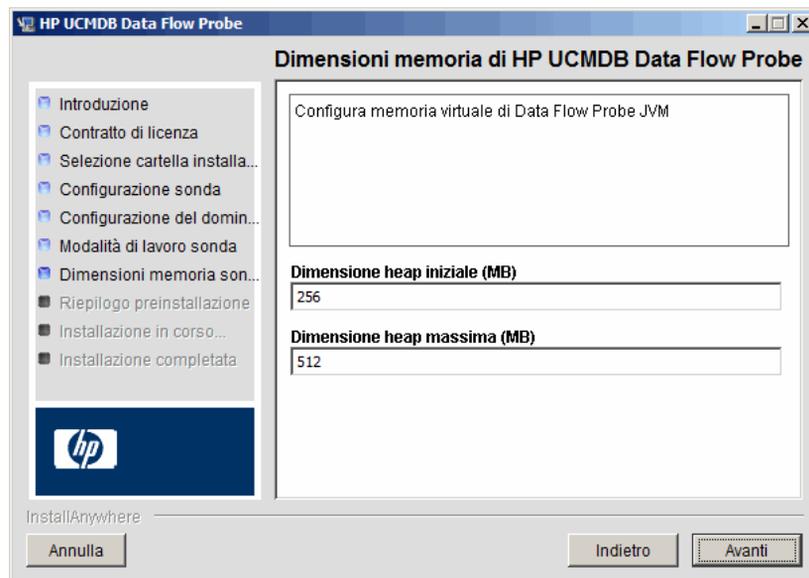
- 9 Fare clic su **Avanti**. Se la casella **Usa dominio CMDB predefinito** è stata deselezionata nella finestra di dialogo Configurazione di HP UCMDB Data Flow Probe, viene visualizzata la finestra di dialogo Configurazione del dominio di HP UCMDB Data Flow Probe.



- **Tipo di dominio Data Flow Probe.** Scegliere tra **Cliente** e **Esterno** a seconda del tipo di dominio sul quale deve essere eseguita la sonda:
 - **Cliente.** Selezionare se si sta installando una o più sonde nella propria distribuzione.
 - **Esterno.** Selezionare se si sta eseguendo l'aggiornamento da sistemi della versione 6.x.
- Importante:** per le nuove installazioni selezionare sempre **Cliente**.
- **Dominio Data Flow Probe:** Se non si sta utilizzando il dominio predefinito definito in UCMDB immettere qui il nome del dominio.

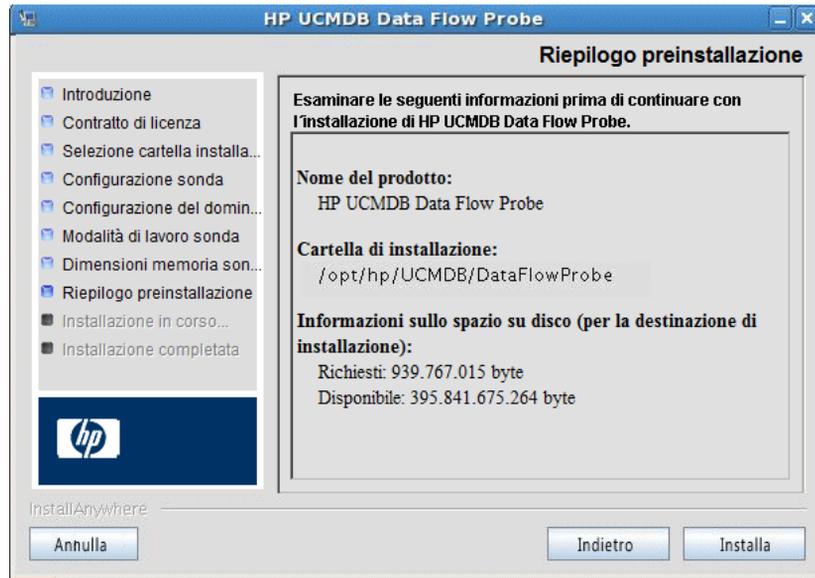
Nota: la procedura di installazione ignora la finestra di dialogo Modalità di lavoro HP UCMDB Data Flow Probe. Ciò è dovuto al fatto che Probe Gateway e Probe Manager devono essere eseguiti come un processo Java.

- 10** Fare clic su **Avanti** per aprire la finestra di dialogo Dimensioni memoria di HP UCMDB Data Flow Probe.



Definire la memoria minima e massima da allocare per la sonda. I valori sono misurati in megabyte.

- 11 Fare clic su **Avanti** per aprire la finestra di dialogo Riepilogo preinstallazione e riesaminare le selezioni eseguite.



- 12 Fare clic su **Installa** per completare l'installazione della sonda. Al termine dell'installazione, viene visualizzata la pagina Installazione completata.

Eventuali errori durante l'installazione vengono scritti nel file seguente: `/opt/hp/UCMDB/DataFlowProbe/HP_UCMDB_Data_Flow_Probe_InstallLog.log`. Se la sonda è stata installata in un'altra directory in `/opt/`, il file di registro si trova qui.

- 13 Fare clic su **Eseguito**.

- 14 Per attivare la sonda eseguire il comando seguente:
`/opt/hp/UCMDB/DataFlowProbe/bin/ProbeGateway.sh start`

Per attivare la sonda in una console, eseguire il comando seguente:
`/opt/hp/UCMDB/DataFlowProbe/bin/ProbeGateway.sh console`

La sonda installata viene visualizzata nella finestra di dialogo Nuovo punto di integrazione nell'elenco delle sonde. Per i dettagli consultare “Finestra di dialogo Crea nuovo punto di integrazione/Modifica punto di integrazione” nella *Guida alla gestione del flusso di dati di HP Universal CMDB*.

Nota: L'utente che esegue il servizio della sonda deve essere un membro del gruppo degli Amministratori.

Arrestare il server della sonda

Per arrestare il server della sonda, eseguire il comando seguente:

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

Aggiornamento della sonda del flusso di dati

Questo compito descrive come eseguire l'aggiornamento della sonda del flusso dati.

1 Disinstallare la sonda precedente

Disinstallare tutte le sonde esistenti. Se una sonda è in esecuzione arrestarla prima di disinstallarla.

O:

► Nella shell eseguire:

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

O:

► Fare doppio clic sul file `Uninstall_Discovery_Probe` nel file system.

2 Installare la nuova sonda

Installare la nuova sonda con la stessa configurazione, ovvero utilizzare lo stesso ID della sonda, nome di dominio e nome server dell'installazione della sonda precedente.

Connettere una sonda del flusso di dati per un cliente non predefinito

È possibile connettere una sonda del flusso di dati per un cliente che non è predefinito. L'ID del cliente predefinito è 1.

1 Aprire il file seguente in un editor di testo:

```
../DataFlowProbe/conf/DiscoveryProbe.properties.
```

2 Individuare la voce **customerID**.

3 Aggiornare il valore con l'ID del cliente, ad esempio **customerID = 2**

4 Riavviare la sonda per aggiornarla con i cambiamenti.

Riferimenti

Requisiti per il supporto della sonda del flusso di dati

Per i dettagli sui requisiti minimi consultare “Matrice di supporto di HP Universal CMDB” a pag. 35.

Risoluzione dei problemi e limitazioni.

Il database MySQL della sonda del flusso di dati potrebbe danneggiarsi senza possibilità di ripristino, ad esempio poiché è stato arrestato il computer ma non il servizio MySQL.

Per riparare il problema:

- 1** Arrestare la sonda.
- 2** Eseguire lo strumento **repair_mysql.sh** dalla cartella seguente:
`/opt/hp/UCMDB/DataFlowProbe/tools.`
- 3** Avviare la sonda.

Se questa procedura non risolve il problema rivolgersi a HP Software Support.

Parte IV

Aggiornamento di HP Universal CMDB dalla versione 8.0x a 9.0x

13

Aggiornamento di HP Universal CMDB dalla versione 8.0x alla versione 9.0x

Importante:

- se si sta installando una versione di service pack (ad es. 9.02), consultare le note sulla versione per le istruzioni più aggiornate.
 - Si consiglia di leggere attentamente questo capitolo prima di avviare la procedura di aggiornamento.
-

Questo capitolo comprende:

Concetti

- Aggiornamento - Panoramica a pag. 164

Compiti

- Aggiornare HP Universal CMDB - Riepilogo a pag. 165
- Aggiornamento a UCMDB 9.02 a pag. 171
- Terminare la procedura di aggiornamento a pag. 178

Riferimenti

- **Risoluzione dei problemi e limitazioni** a pag. 179

Concetti

Aggiornamento - Panoramica

Questo capitolo spiega come eseguire l'aggiornamento di HP Universal CMDB (UCMDB) dalla versione 8.0x alla versione 9.02.

Il processo di aggiornamento viene eseguito offline quando tutte le risorse e i dati vengono trasformati dal modello di classe 8.0x nel BDM (BTO Data Model). Per i dettagli sul modello di dati consultare "Introduzione al modello di dati di UCMDB" nella *Guida alla modellazione di HP Universal CMDB*.

È possibile eseguire l'aggiornamento delle risorse soltanto oppure eseguire l'aggiornamento completo:

- **Solo aggiornamento delle risorse.** Viene eseguito l'aggiornamento delle impostazioni, delle risorse e del modello di classe. Tutti i CI vengono eliminati poiché sono eventi di cronologia quindi è necessario reindividuare i dati.
- **Aggiornamento completo.** Viene eseguito l'aggiornamento dei dati e della cronologia oltre che delle risorse.

Compiti

Aggiornare HP Universal CMDB - Riepilogo

In questa sezione vengono descritti i passaggi necessari per il processo di aggiornamento.

Nota: se si pianifica di eseguire il server UCMDB su una piattaforma con protezione avanzata (compreso l'utilizzo del protocollo HTTPS), esaminare le procedure di protezione avanzata descritte in Parte VI, "Protezione avanzata di HP Universal CMDB."

Questo compito comprende i passaggi seguenti:

- "Prerequisiti" a pag. 166
- "Verificare i requisiti hardware e del sistema operativo" a pag. 166
- "Preparare i database" a pag. 166
- "Salvare gli adattatori di integrazione (federazione) modificati" a pag. 167
- "Disinstallare versioni precedenti di UCMDB" a pag. 167
- "Disinstallare le sonde precedenti" a pag. 168
- "Installare UCMDB versione 9.02" a pag. 168
- "Eseguire lo strumento di aggiornamento" a pag. 168
- "Eseguire le procedure post-aggiornamento" a pag. 169
- "Installare la versione 9.02 della sonda del flusso di dati" a pag. 170

1 Prerequisiti

- Se si dispone di una versione di HP Universal CMDB anteriore a 8.04 eseguire l'aggiornamento alla versione 8.04 o successiva. Se si sta eseguendo l'aggiornamento, HP Software consiglia di eseguirlo all'ultima versione 8.0x.
- Se si dispone di DDM Content Pack 6.00 o versione precedente, è necessario installare DDM Content Pack 7.00. Questo passaggio deve essere eseguito dopo l'aggiornamento alla versione 8.04 o successiva.

2 Verificare i requisiti hardware e del sistema operativo

Per i dettagli consultare "Matrice di supporto di HP Universal CMDB" a pag. 35.

3 Preparare i database

- L'aggiornamento richiede circa il 250% dello spazio di norma richiesto per lo schema del CMDB. Accertarsi di allocare questo spazio.
- Eseguire il backup di CMDB, database Cronologia e Foundation versione 8.0x. In UCMDB 9.02 gli schemi di Foundation e CMDB sono combinati. Eseguire singolarmente il backup dei tre schemi per garantire la connessione corretta durante l'aggiornamento alla versione 9.02.

Importante: come ulteriore precauzione eseguire la versione corrente di UCMDB rispetto agli schemi di backup per verificare che non siano danneggiati.

- Eseguire lo strumento di coerenza del database nell'installazione della versione 8.0x per pulire lo schema del CMDB dai seguenti dati danneggiati:
 - Collegamenti dove mancano gli oggetti delle estremità
 - CI con informazioni mancanti in alcune tabelle con gerarchia del modello di dati

Per i dettagli sull'utilizzo del CMDB consultare la *Guida al database di HP Universal CMDB* in PDF.

4 Salvare gli adattatori di integrazione (federazione) modificati

Per tutti gli adattatori preimpostati: se si modifica la configurazione di un adattatore nella versione 8.0x, si consiglia di salvare tutti i file dell'adattatore di tale versione e di rieseguire le modifiche sui file dell'adattatore della versione 9.02.

Per tutti gli adattatori non preimpostati: è necessario ridistribuire gli adattatori nella versione 9.02. Per i dettagli consultare "Gestione pacchetti" nella *Guida all'amministrazione di HP Universal CMDB*.

Importante: tutti gli adattatori devono essere compatibili con il nuovo modello BDM. Se si eseguono cambiamenti agli adattatori preimpostati esistenti, è necessario eseguire gli stessi cambiamenti ai file dell'adattatore della versione 9.00. Ovvero non copiare i file dalla versione 8.0x e sostituirli nella versione 9.00.

5 Disinstallare versioni precedenti di UCMDB

Eseguire la procedura seguente **solo se si intende installare il server UCMDB versione 9.02 sullo stesso computer della precedente versione 8.0x**. Se si stanno utilizzando uno o più server, non è necessario disinstallare la versione 8.0x prima dell'aggiornamento alla versione 9.02 ed è possibile passare al passaggio successivo ("Disinstallare le sonde precedenti" a pag. 168); è comunque necessario arrestare l'istanza 8.0x prima di installare la versione 9.02.

Nota: se è installata la versione 7.x eseguire l'aggiornamento da tale versione all'ultima versione 8.0x poi continuare con le procedure descritte nel presente capitolo. Per i dettagli sull'aggiornamento alla versione 8.0x consultare la rispettiva documentazione.

Per rimuovere il server UCMDB 8.0x:

- a** Arrestare il server UCMDB: **Start > Tutti i programmi > HP UCMDB > Interrompi HP Universal CMDB Server.**
- b** Disinstallare il server: **Start > Tutti i programmi > HP UCMDB > Disinstallazione di HP Universal CMDB Server.** Per i dettagli consultare "Disinstallare HP Universal CMDB" a pag. 84.
- c** Rimuovere l'intera cartella **C:\hp\UCMDB** dal server UCMDB.
- d** Riavviare il server UCMDB.

6 Disinstallare le sonde precedenti

Il requisito minimo per l'aggiornamento a UCMDB 9.02 è UCMDB versione 8.04 o successiva su cui è installato DDM Content Pack 7.00.

Arrestare e disinstallare le sonde DDM (o del flusso di dati). Per i dettagli consultare "Aggiornamento della sonda" a pag. 139 (Windows) o "Aggiornamento della sonda del flusso di dati" a pag. 158 (Linux).

7 Installare UCMDB versione 9.02

Per i dettagli consultare "HP Universal CMDB Installazione su una piattaforma Windows" a pag. 71 oppure "HP Universal CMDB Installazione su una piattaforma Linux" a pag. 87 nella *Guida alla distribuzione di HP Universal CMDB* in PDF per la versione 9.02.

Importante: non installare il database o lo schema. Al termine dell'installazione non continuare con la procedura guidata di configurazione di UCMDB Server (per l'installazione del database o dello schema). Fare clic su **No** al passaggio 12 a pag. 82. Continuare invece con il passaggio successivo di questa procedura.

8 Eseguire lo strumento di aggiornamento

È possibile eseguire l'aggiornamento completo oppure eseguire l'aggiornamento delle risorse soltanto. Per i dettagli consultare "Aggiornamento - Panoramica" a pag. 164.

Per i dettagli sull'esecuzione dell'aggiornamento, consultare "Aggiornamento a UCMDB 9.02" a pag. 171.

Per i dettagli sulle implicazioni in caso di errore e sui messaggi di registro consultare "Processo di aggiornamento: descrizioni tecniche" a pag. 181.

9 Eseguire le procedure post-aggiornamento

I passaggi seguenti possono essere necessari dopo l'aggiornamento.

- ▶ **Proxy inverso.** A meno che il sistema con aggiornamento venga eseguito nello stesso ambiente del sistema della versione 8.0x, riconfigurare il proxy inverso dopo l'aggiornamento. Per i dettagli sulla configurazione consultare "Utilizzo di un proxy inverso" a pag. 307.
- ▶ **SSL.** Reinstallare le configurazioni SSL. Per i dettagli consultare "Abilitazione della comunicazione Secure Sockets Layer (SSL)" a pag. 291.
- ▶ **LW-SSO.** Reinstallare LW-SSO. Per i dettagli consultare "Autenticazione Lightweight Single Sign-On (LW-SSO) – Riferimenti generali" a pag. 367 e "Abilitare l'accesso a HP Universal CMDB con LW-SSO" a pag. 383
- ▶ **LDAP.** Reinstallare la configurazione di LDAP e la mappatura tra gli utenti e i gruppi LDAP. Per i dettagli consultare "Sincronizzare i ruoli utenti di HP Universal CMDB con i gruppi LDAP" nella *Guida all'amministrazione di HP Universal CMDB*.
- ▶ **JMX Console.** Il nome e la password predefiniti dell'amministratore sono **sysadmin**. Per i dettagli sulla protezione avanzata della console JMX consultare "Cambiare il nome utente o la password di sistema per la console JMX" a pag. 288.
- ▶ **Eliminare lo schema Foundation.** Lo schema Foundation non viene più utilizzato dopo l'aggiornamento e può essere eliminato.
- ▶ **Rieseguire le modifiche sugli adattatori di integrazione (federazione).** tutti gli adattatori devono essere compatibili con il nuovo modello BDM. Se si eseguono cambiamenti agli adattatori preimpostati esistenti, è necessario eseguire gli stessi cambiamenti ai file dell'adattatore della versione 9.02. Ovvero non copiare i file dalla versione 8.0x e sostituirli nella versione 9.02. Per tutti gli adattatori non preimpostati è necessario ridistribuire gli adattatori. Per i dettagli consultare "Gestione pacchetti" nella *Guida all'amministrazione di HP Universal CMDB*.

- **Abilitare il meccanismo di aging.** Dopo l'aggiornamento il meccanismo di aging è disabilitato. Ciò impedisce l'eliminazione dei CI nel periodo di tempo in cui la sonda non raccoglie dati (tra l'esecuzione del processo di aggiornamento fino a quando l'individuazione inizia a segnalare tutti i CI).

Si consiglia quindi di attendere che il sistema si sia stabilizzato prima di riabilitare il meccanismo di aging. Per la verifica eseguire l'individuazione e controllare tutti i CI contrassegnati per l'eliminazione.

Per i dettagli sul meccanismo di aging consultare "Ciclo di vita del CI e meccanismo di aging" nella *Guida all'amministrazione di HP Universal CMDB*.

Per i dettagli sull'esecuzione dell'individuazione consultare "Pannello di controllo dell'individuazione - Workflow Modalità avanzata" nella *Guida alla gestione del flusso di dati di HP Universal CMDB*.

10 Installare la versione 9.02 della sonda del flusso di dati

Installare la sonda del flusso di dati versione 9.02. Per il percorso del file **HPUCMDB_DataFlowProbe_902.exe** consultare "Installazione della sonda del flusso di dati su piattaforma Windows" a pag. 129 oppure "Installazione della sonda del flusso di dati su piattaforma Linux" a pag. 147.

Aggiornamento a UCMDB 9.02

Questa sezione spiega come eseguire l'aggiornamento da UCMDB versione 8.04 o successiva alla versione 9.02.

Importante: è necessario eseguire la procedura di aggiornamento solo se UCMDB versione 8.04 o successiva è installato con DDM Content Pack 7.00 distribuito.

- 1** Individuare e avviare il file **aggiornamento:**
C:\hp\UCMDB\UCMDBServer\tools\upgrade.bat (Windows) o
upgrade.sh (Linux).
- 2** Si apre la procedura guidata **Preparazione dell'aggiornamento**. Fare clic su **Avanti** per aprire la finestra Aggiornamento server UCMDB.
- 3** Selezionare un database **Oracle** o **MS SQL Server** e impostare i parametri di connessione dello **Schema di Foundation**.

Il **Nome schema** deve corrispondere al nome dello schema **Foundations** di UCMDB 8.0x replicato in precedenza. Per maggiori dettagli sui parametri di connessione consultare "Informazioni richieste per l'impostazione dei parametri del database" a pag. 103.

Impostazioni schema di Foundation

Parametri di connessione dello schema Foundation

Tipo DB:	MS SQL Server
Nome host	labm3mam18.devlab.ad
Nome schema	Foundation
Porta	1433
	<input type="radio"/> Utilizza gestione NT LAN
	<input checked="" type="radio"/> Immettere credenziali
Nome utente	sa
Password	●●●

<<Indietro Avanti>> Fine Chiudi

- 4 Fare clic su **Avanti** e impostare i parametri di connessione dello **Schema CMDB**. Il **Nome schema** deve corrispondere al nome dello schema CMDB di UCMDB 8.0x replicato in precedenza.

Parametri dello schema CMDB

Parametri di connessione dello schema CMDB

Tipo DB: MS SQL Server

Nome host: labm3mam18.devlab.ad

Nome schema: CMDB

Porta: 1433

Utilizza gestione NT LAN

Immettere credenziali

Nome utente: sa

Password: ●●●

<<Indietro Avanti>> Fine Chiudi

- 5 Fare clic su **Avanti** e impostare i parametri di connessione dello **Schema cronologia**. Il **Nome schema** deve corrispondere al nome dello schema **Cronologia** di UCMDB 8.0x replicato in precedenza.

Impostazioni schema della cronologia

Parametri di connessione dello schema della cronologia

Tipo DB: MS SQL Server

Nome host: labm3mam18.devlab.ad

Nome schema: History

Porta: 1433

Utilizza gestione NT LAN

Immettere credenziali

Nome utente: sa

Password: ●●●

<<Indietro Avanti>> Fine Chiudi

6 Fare clic su **Avanti** e selezionare la Modalità aggiornamento:

Modalità aggiornamento

Modalità aggiornamento

Soltanto risorse
Aggiorna solo parti selezionate del database CMDB: impostazioni, risorse e modello di classe. Dati e cronologia vengono rimossi.

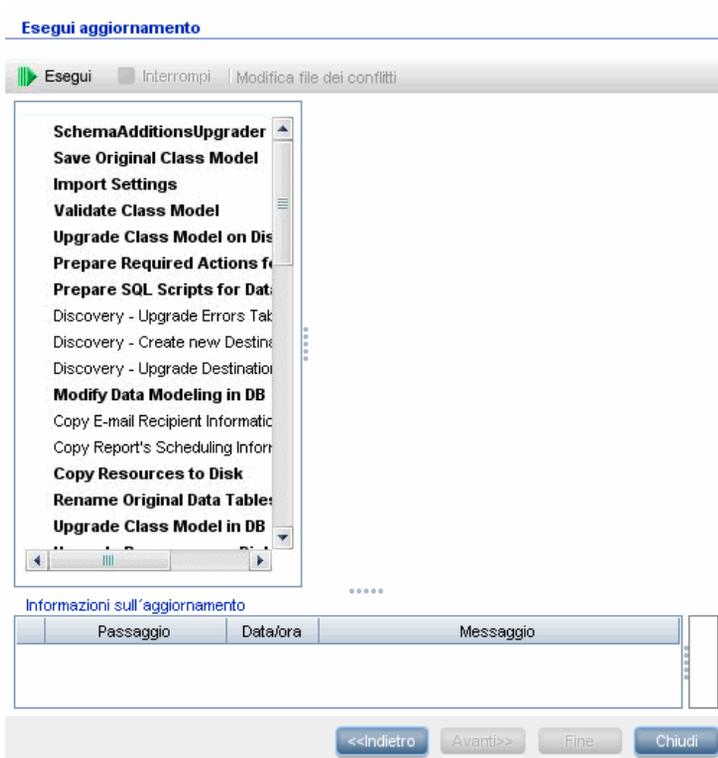
Aggiornamento completo
Aggiorna solo parti selezionate del database CMDB: impostazioni, risorse, modello di classe, dati e cronologia.

Questa impostazione verrà bloccata dopo l'avvio del processo di aggiornamento. Non può essere sbloccata - neanche per un nuovo aggiornamento. Per sbloccare questa schermata, eliminare il file **upgrademode.ui** dalla cartella runtime.

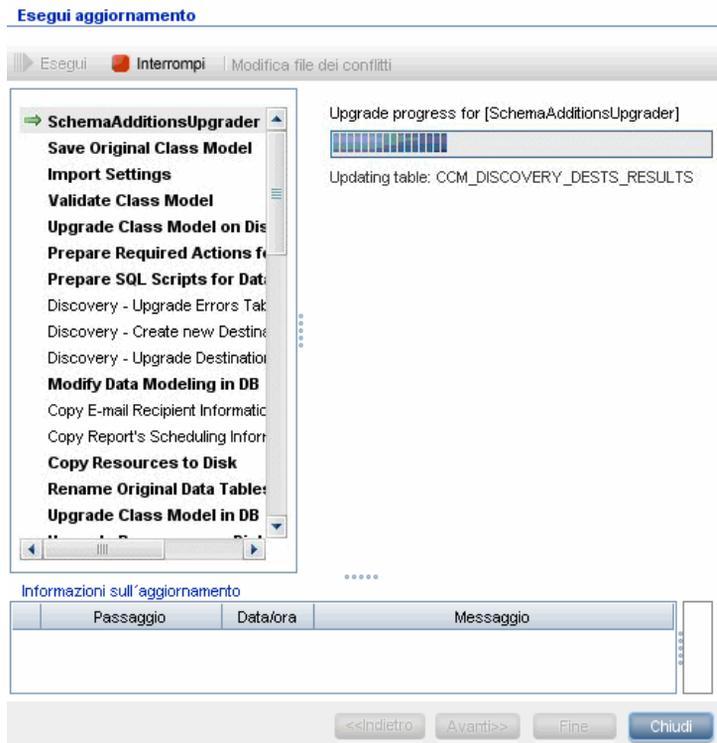
<<Indietro Avanti>> Fine Chiudi

- **Soltanto risorse.** Esegue solo l'aggiornamento delle parti selezionate del CMDB, esclusi dati e cronologia.
- **Aggiornamento completo.** Esegue l'aggiornamento dell'intero CMDB, compresi dati e cronologia.

- 7 Fare clic su **Avanti**. Nella schermata Esegui aggiornamento vengono elencati i passaggi di aggiornamento. Fare clic su **Esegui** per iniziare l'aggiornamento.



- 8 Nella schermata Esegui aggiornamento viene indicato l'avanzamento di ciascun passaggio.



Per i dettagli sulle implicazioni in caso di errore e sui messaggi di registro per ciascun passaggio, consultare "Passaggi di aggiornamento" a pag. 184.

Per i dettagli sulla convalida dei conflitti del modello di dati, consultare "Convalidare il conflitto del modello di dati" a pag. 179.

- 9 Per rieseguire un passaggio specifico fare clic con il pulsante destro del mouse nel riquadro **Passaggi** e selezionare **Esegui elementi selezionati**.

Importante: la riesecuzione di un passaggio di aggiornamento corretto deve avvenire solo per la risoluzione dei problemi.

Terminare la procedura di aggiornamento

L'aggiornamento può richiedere molto tempo prima del completamento. Per terminare l'aggiornamento in un determinato punto, fare clic sul pulsante rosso **Interrompi**:

Esegui aggiornamento



I passaggi completati con un avviso o che non riescono vengono registrati nel riquadro **Informazioni sull'aggiornamento**. Per visualizzare queste informazioni, evidenziare la riga quando viene visualizzato il passaggio di aggiornamento. Le informazioni rilevanti vengono visualizzate a destra.

Esegui aggiornamento

The screenshot shows the 'Esegui aggiornamento' window with a list of tasks on the left and a log of warnings on the right. The tasks list includes:

- Discovery - Upgrade Statistics
- Discovery - Upgrade Resources
- Load Upgraded Resources
- Upgrade Snapshots
- Discovery - Re Encrypt Domain Scope Document
- Discovery - Upgrade Domain Scope Document
- Discovery - Copy Credentials to Confidential Manager
- Discovery - Upgrade Credential Identifiers
- Copy Report Configuration
- Copy Snapshots Scheduling Information
- Copy LDAP Configuration
- Upgrade Settings
- Upgrade Security Model
- Clear Old Data
- User Vs. Factory
- Populate IPv6 Attribute
- Enrichment Driven Upgrade
- Define Key Attributes Reconciliation Rules
- Package Manager Upgrade
- CleanupRemoveColumnsUpgrader

The log shows several warnings from 'offlineResourceLoader' regarding upgraded resources that are not loaded since a different out-of-the-box resource with the same name was used:

Passaggio	Messaggio
offlineResourceLoader	WARN: Upgraded resource Weblogic_Topology_tql (TQL) is not loaded since a different out-of-the-box resource with the same name was used.
offlineResourceLoader	WARN: Upgraded resource Websphere_Topology_tql (TQL) is not loaded since a different out-of-the-box resource with the same name was used.
offlineResourceLoader	WARN: Upgraded resource Jboss_Topology_tql (TQL) is not loaded since a different out-of-the-box resource with the same name was used.
offlineResourceLoader	WARN: Upgraded resource DB2 (CMDB_VIEW) is not loaded since a different out-of-the-box resource with the same name was used.
offlineResourceLoader	WARN: Upgraded resource Apache_Topology (CMDB_VIEW) is not loaded since a different out-of-the-box resource with the same name was used.
offlineResourceLoader	WARN: Upgraded resource Host Storage Dependency (CMDB_VIEW) is not loaded since a different out-of-the-box resource with the same name was used.

Riferimenti

Risoluzione dei problemi e limitazioni

Questa sezione spiega la risoluzione dei problemi e le limitazioni dell'aggiornamento da UCMDDB 8.04 o versione successiva a UCMDDB 9.02.

Convalidare il conflitto del modello di dati

Il passaggio di convalida del modello di dati nell'aggiornamento utilizza come input il modello di classe precedente, le trasformazioni predefinite e i modelli di dati preimpostati e genera un modello di dati modificato (dopo aver aggiunto le entità del modello di dati mancanti) nel disco in

C:\hp\UCMDDB\UCMDDBServer\runtime\old-class-model.xml.

Se viene rilevato un conflitto, ad esempio quando un nuovo nome di classe o attributo definito dall'utente viene allocato a una nuova classe o attributo preimpostato, viene generato un altro file di trasformazione e salvato su disco in **C:\hp\UCMDDB\UCMDDBServer\runtime\added-class-model-changes.xml** e il processo di aggiornamento non riesce.

Il nuovo file di trasformazione definisce un'ulteriore trasformazione allo scopo di risolvere i conflitti rinominando le classi e gli attributi. Eseguire di nuovo l'aggiornamento per includere queste nuove trasformazioni e consentire la continuazione dell'aggiornamento.

Importante: se viene generato un altro file di trasformazione è necessario chiudere la procedura guidata per l'aggiornamento e riavviarla.

Le risorse non sono caricate nell'UCMDB con aggiornamento

Le risorse che utilizzano le classi rimosse durante l'aggiornamento non sono sottoposte ad aggiornamento e non sono caricate in UCMDB con aggiornamento. Allo stesso modo le query che utilizzano gli attributi come condizione di proprietà vengono anch'esse rimosse. A prescindere dalle trasformazioni del modello di dati applicate a queste risorse, vengono apportati i cambiamenti seguenti:

- Le viste vengono ridefinite per corrispondere alla nuova definizione di vista.
- I report Topologia vengono ridefiniti come viste. In UCMDB 9.02, i report e le viste vengono considerate come visualizzazioni diverse degli stessi dati.
- Le query vengono salvate in un formato XML semplice da usare.

14

Processo di aggiornamento: descrizioni tecniche

Questo capitolo comprende:

Riferimenti

- Parametri di input per il processo di aggiornamento a pag. 182
- File di registro per il processo di aggiornamento a pag. 183
- Passaggi di aggiornamento a pag. 184

Riferimenti

Parametri di input per il processo di aggiornamento

A seconda del tipo di aggiornamento che si esegue (**Completo** o **Soltanto risorse**), il processo di aggiornamento utilizza i componenti seguenti:

- ▶ Schema del database.
- ▶ File che descrivono la trasformazione del modello di classe eseguita durante l'aggiornamento. Sono i file che terminano con **_changes.xml** che si trovano nella directory **C:\hp\UCMDB\UCMDBServer\conf\upgrade**.
- ▶ Modello di classe predefinito della versione 8.04 e DDM Content Pack 6.00. Questa versione consente al processo di aggiornamento di aggiungere le entità del modello di classe mancanti prima dell'aggiornamento.
- ▶ Modello di dati predefinito della versione 9.00 e DDM Content Pack 6.00. Questa versione consente al processo di aggiornamento di aggiungere le entità del modello di classe mancanti dopo la procedura di aggiornamento e garantisce che il modello di classe sottoposto ad aggiornamento sia conforme a HP Universal CMDB e Business Service Management.

File di registro per il processo di aggiornamento

Durante l'aggiornamento vengono utilizzati i file di registro seguenti:

- **upgrade.detailed.log.** Questo è il file di registro principale per la procedura di aggiornamento. Tutte le operazioni di aggiornamento vengono scritte in questo registro (se non diversamente dichiarato in un passaggio di aggiornamento specifico). Di norma le dimensioni di questo file sono comprese tra 30 MB e 70 MB.
- **upgrade.short.log.** Riepilogo del registro dettagliato. Tutte le righe di questo file vengono visualizzate anche in **upgrade.detailed.log**. Questo file deve essere utilizzato come indice del file più dettagliato oppure come panoramica generale. Di norma le dimensioni di questo file sono inferiori a 5 MB.
- **upgrade.detailed.attribute_cleanup.log.** Questo file di registro visualizza l'avanzamento della pulizia completa del modello di dati in modo che un attributo viene definito una sola volta in una gerarchia di classi. Tutte le altre definizioni devono essere **attribute override** e tutti gli override di attributo (sostituzioni dell'attributo) non validi vengono rimossi. Questo processo si verifica diverse volte durante l'aggiornamento completo, durante la manipolazione del modello di classe (convalida con il modello di classe precedente, aggiornamento del modello di classe e convalida con il modello di classe di destinazione). Di norma la dimensione combinata di questi file di registro (file **.log** e tutti i file roll-over) può essere di centinaia di MB.
- **error.log.** Questo file non è specifico dell'aggiornamento e contiene tutti gli errori e gli avvisi inviati da qualsiasi altro registro (se non sono appositamente bloccati). Può essere utilizzato come mappa e come riepilogo generale del processo di aggiornamento.
- **mam.packaging.log.** Questo registro è rilevante solo per il passaggio relativo alla redistribuzione dei pacchetti base e comprende tutte le informazioni su questo passaggio. Per i dettagli consultare "Redistribuire i pacchetti di base" a pag. 240.

Passaggi di aggiornamento

In questa sezione vengono descritti i passaggi che comprendono il processo di aggiornamento completo. Per ciascun passaggio della procedura di aggiornamento viene descritto quanto segue:

- ▶ Descrizione del passaggio.
- ▶ Indicazione della criticità del passaggio. Un passaggio viene considerato critico nei casi seguenti:
 - ▶ Se viene saltato potrebbe impedire l'avvio del server UCMDB dopo l'aggiornamento.
 - ▶ Se viene saltato potrebbe rendere critica la configurazione o provocare perdita di dati che non si possono recuperare dopo l'aggiornamento.
 - ▶ Se viene saltato potrebbe impedire il funzionamento corretto di un componente critico dopo l'aggiornamento.
- ▶ Se il passaggio può essere rieseguito. In caso di errore durante l'aggiornamento viene indicato se è possibile rieseguire questo passaggio sugli stessi schemi.
- ▶ Implicazioni in caso di errore. Se questo passaggio di aggiornamento non riesce, quali sono gli effetti su UCMDB? Se è possibile rieseguire il passaggio, quali sono le operazioni per risolvere i problemi?
- ▶ File di registro. Messaggi importanti del file di registro che sono tipici di questo passaggio di aggiornamento e il significato di ciascun messaggio. Se non diversamente specificato, tutti i messaggi vengono visualizzati nei file di registro seguenti:
 - ▶ **C:\hp\UCMDB\UCMDBServer\runtime\log\upgrade.detailed.log**
 - ▶ **C:\hp\UCMDB\UCMDBServer\runtime\log\upgrade.short.log** (I messaggi di registro di questo file possono essere un duplicato dei messaggi del file **upgrade.detailed.log**.)

Per i dettagli sui registri consultare "File di registro per il processo di aggiornamento" a pag. 183.

Importante: i passaggi rilevanti per un aggiornamento di tipo **Soltanto risorse** vengono contrassegnati come tali.

La sezione è suddivisa nei passaggi seguenti:

- "Aggiornamento aggiunte allo schema" a pag. 187
- "Salvare il modello di classe originale" a pag. 187
- "Importare le impostazioni" a pag. 188
- "Convalidare il modello di classe" a pag. 189
- "Aggiornamento del modello di classe su disco" a pag. 195
- "Preparare le azioni richieste per l'aggiornamento dei dati" a pag. 198
- "Preparare gli script SQL per l'aggiornamento dei dati" a pag. 211
- "Individuazione - Aggiornamento tabella degli errori" a pag. 212
- "Individuazione - Creare una tabella di IP di nuova destinazione" a pag. 213
- "Individuazione - Aggiornamento tabella delle destinazioni" a pag. 214
- "Modificare la modellazione di dati nel database" a pag. 214
- "Copiare informazioni sui destinatari dell'e-mail" a pag. 215
- "Copiare informazioni sulla pianificazione dei report" a pag. 216
- "Copiare le risorse su disco" a pag. 217
- "Troncare le tabelle dei dati" a pag. 219
- "Rinominare le tabelle dei dati originali" a pag. 220
- "Aggiornare il modello di classe nel database" a pag. 221
- "Aggiornamento delle risorse su disco" a pag. 222
- "Dati di aggiornamento" a pag. 227
- "Creare tabella temporanea dei CI rimossi" a pag. 228
- "Popolare la tabella radice" a pag. 229
- "Aggiornamento della tabella degli attributi List" a pag. 229
- "Eliminare le tabelle di configurazione precedenti" a pag. 230
- "Aggiornamento del database cronologia" a pag. 230
- "Gestione dei dati non coerenti" a pag. 235

- "Ricalcolare gli ID generati non casualmente" a pag. 236
- "Popolare ID globali" a pag. 236
- "Individuazione - Configurazione dell'aggiornamento" a pag. 237
- "Federazione - Rimuovere la configurazione precedente" a pag. 239
- "Ridistribuire i pacchetti di base" a pag. 240
- "Convalidare il modello di classe aggiornato" a pag. 240
- "Individuazione - Statistiche dell'aggiornamento" a pag. 241
- "Individuazione - Aggiornamento delle risorse" a pag. 242
- "Caricare risorse aggiornate" a pag. 243
- "Aggiornamento delle istantanee" a pag. 244
- "Individuazione - Ricrittografare il documento dell'ambito del dominio" a pag. 245
- "Individuazione - Aggiornamento del documento dell'ambito del dominio" a pag. 247
- "Individuazione - Copiare le credenziali in Confidential Manager" a pag. 247
- "Individuazione - Aggiornamento degli identificatori delle credenziali" a pag. 248
- "Copiare la configurazione dei report" a pag. 249
- "Copiare informazioni sulla pianificazione delle istantanee" a pag. 249
- "Impostazioni di aggiornamento" a pag. 250
- "Aggiornamento del modello di protezione" a pag. 251
- "Eliminare dati precedenti" a pag. 251
- "Utente rispetto a valori predefiniti" a pag. 252
- "Popolare l'attributo IPv6" a pag. 254
- "Aggiornamento guidato dell'accrescimento" a pag. 254
- "Definire le regole di riconciliazione degli attributi chiave" a pag. 255
- "Aggiornamento Gestione pacchetti" a pag. 256

Aggiornamento aggiunte allo schema

Aggiunge al CMDB le nuove tabelle e colonne richieste.

È critico (S/N)	Può essere rieseguito (S/N)
S	S

Implicazioni in caso di errore

- Problemi di autorizzazioni (autorizzazioni insufficienti)
- Problemi di connettività del database (impossibile collegare il database)
- Blocco (impossibile modificare le tabelle)

File di registro

- Updating table: ... Quando viene aggiornata una determinata tabella nel database.
- Initializing default customer registration. Quando vengono aggiornate le informazioni globali sul cliente.

Salvare il modello di classe originale

Nota: solo aggiornamento delle risorse.

Salva il modello di classe completo, prima dell'aggiornamento, su disco in
C:\hp\UCMDB\UCMDBServer\runtime\original-class-model.xml.

È critico (S/N)	Può essere rieseguito (S/N)
S	S

Implicazioni in caso di errore

- ▶ Impossibile leggere dal CMDB il modello di classe utente esistente. Causa probabile: definizione di modello di classe danneggiata. Soluzione: modificare manualmente la definizione di modello di classe del database prima di riprovare la riesecuzione del passaggio.
- ▶ Il CMDB non dispone delle autorizzazioni per scrivere nella cartella **C:\hp\UCMDB\UCMDBServer\runtime**. Le autorizzazioni di cartella di **Read/Write/Create** sono necessarie per l'intera cartella di installazione (anche se la maggior parte dei comandi **Write** vengono eseguiti soltanto sulla cartella **C:\hp\UCMDB\UCMDBServer\runtime**).

File di registro

Gli errori nei file **cmdb.classmodel.log** o **error.log** possono indicare l'entità del modello di classe che ha segnalato il caricamento non riuscito.

Importare le impostazioni

Nota: solo aggiornamento delle risorse.

Copia le impostazioni rilevanti dal database Foundations nella tabella di gestione nel CMDB.

È critico (S/N)	Può essere rieseguito (S/N)
S	S

Implicazioni in caso di errore

Le impostazioni non sono state migrate correttamente e vengono utilizzati invece i valori preimpostati del CMDB. Se il meccanismo di aging è abilitato, gran parte del modello di dati del CMDB può essere rimossa quando il CMDB viene avviato per la prima volta.

Database Foundations configurato non correttamente (oppure non esistente). Soluzione: configurare il database Foundations utilizzando la procedura guidata di aggiornamento. Se il database è stato danneggiato o si desidera creare un nuovo database, creare un database Foundations vuoto utilizzando la procedura guidata del database UCMDB 8.0x.

File di registro

- **Fetch old settings.** Quando si recuperano le impostazioni dal database Foundations 8.0x.
- **Set new settings.** Quando vengono scritte le impostazioni nel nuovo database Management.
- **Aging mechanism has been disabled.** Per i dettagli sul meccanismo di aging consultare "Ciclo di vita del CI e meccanismo di aging" nella *Guida all'amministrazione di HP Universal CMDB*.

Convalidare il modello di classe

Nota: solo aggiornamento delle risorse.

Garantisce che il precedente modello di classe, letto da **C:\hp\UCMDB\UCMDBServer\runtime\original-class-model.xml**, venga allineato con il previsto modello di classe preimpostato. Ciò si rende necessario poiché il precedente modello di classe deve essere accessibile per le trasformazioni del modello di classe che rientrano nel processo di aggiornamento. Questo passaggio utilizza come input il modello di classe precedente, le trasformazioni predefinite e i modelli di classe preimpostati e genera un modello di classe modificato dopo aver aggiunto le entità del modello di classe mancanti al file **C:\hp\UCMDB\UCMDBServer\runtime\original-fixed-class-model.xml**.

Importante:

I file dei cambiamenti del modello di classe non devono essere modificati dopo il completamento di questo passaggio. Ciò si riferisce ai file preimpostati, al file di risoluzione automatica dei conflitti e a qualsiasi file posizionato manualmente in

C:\hp\UCMDB\UCMDBServer\conf\upgrade.

Se vengono cambiati i file dei cambiamenti del modello di classe, la procedura guidata dell'aggiornamento e il file di risoluzione automatica dei conflitti devono essere completamente chiusi e riaperti per applicare correttamente i cambiamenti.

È critico (S/N)	Può essere rieseguito (S/N)
S	S

Nota: se all'inizio di questo passaggio il file **original-class-model.xml** non esiste, esso viene riletto dal database.

Implicazioni in caso di errore

Se questo passaggio non riesce, verificare uno dei casi seguenti:

- ▶ **Discordanza dell'attributo.** Il tipo di **attributo** è diverso dai tipi di attributo del modello di classe preimpostato. La conversione del tipo non è supportata.
- ▶ **Conflitto di classe o attributo.** Il nuovo nome di classe o attributo definito dall'utente è allocato a una nuova classe o attributo preimpostato. Se ciò si verifica, un nuovo file di trasformazione viene automaticamente generato e salvato su disco in **C:\hp\UCMDB\UCMDBServer\runtime\added-class-model-changes.xml** e il processo di aggiornamento non riesce. Il nuovo file di trasformazione definisce un'ulteriore trasformazione allo scopo di risolvere i conflitti rinominando le classi e gli attributi. Eseguire di nuovo l'aggiornamento per includere queste nuove trasformazioni e consentire la continuazione dell'aggiornamento. Prima di rieseguire l'aggiornamento è anche possibile modificare manualmente queste operazioni, ad esempio selezionando nuovi nomi.

Nota: se è stato creato un file di risoluzione dei conflitti oppure se lo si modifica mediante l'interfaccia utente, è necessario chiudere completamente la procedura guidata dell'aggiornamento e riaprirla per ricaricare correttamente questi cambiamenti.

File di registro

- ▶ Un'entità mancante o altra entità non supportata nel modello di classe utente scrive un avviso nel file di registro. L'avviso include il tipo di entità, il nome, la posizione della gerarchia del modello di classe e l'azione adottata per gestire l'entità (se presente).
 - ▶ Attribute type change is not allowed. Attribute <nome> in Class <nome> change type from <vecchio-tipo> to <nuovo-tipo>. In caso di cambiamento di tipo di attributo, l'errore include il nome dell'attributo e la rispettiva classe.
 - ▶ Class hierarchy change may cause upgrade problems in Class <nome>. Il nome della classe ha cambiato posizione nella gerarchia del modello di classe. L'aggiornamento può gestire tipi specifici di cambiamento di gerarchia ma a questo punto nell'aggiornamento non ci sono informazioni sufficienti per decidere sul cambiamento.
 - ▶ Class removal is not allowed in Class <nome>. Class was added. Una classe predefinita manca nel modello di classe utente quindi la classe viene forzatamente riportata nel modello. Ciò può avvenire in seguito alla rimozione di una classe da parte dell'utente o in seguito a un errore di distribuzione del Content Pack 6.00.
 - ▶ Class Qualifier addition of type <nome> is not allowed. The qualifier was removed in Class <nome>. Certi tipi di qualificatori di classe non possono essere aggiunti dall'utente. Se un utente ha aggiunto uno di questi qualificatori, viene visualizzato il messaggio e il qualificatore di classe viene rimosso dalla classe.
 - ▶ Class Qualifier removal of type <nome> is not allowed in Class <nome>. The qualifier was added. Se un qualificatore manca nella classe preimpostata, esso viene aggiunto alla classe.
 - ▶ Attribute removal <nome> is not allowed. Attribute <nome> in Class <nome>. The Attribute was added. Un attributo predefinito manca nel modello di classe utente in una classe predefinita quindi l'attributo viene aggiunto alla classe. Ciò può avvenire in seguito alla rimozione di un attributo da parte dell'utente o in seguito a un errore di distribuzione del Content Pack 6.00.

- ▶ Attribute Qualifier addition of type <nome> in new attribute <nome> is not allowed. The qualifier was removed in Class <nome>. I nuovi attributi sono attributi aggiunti da un utente a una classe predefinita. Tuttavia, tipi specifici di qualificatori di attributo non possono essere aggiunti ai nuovi attributi quindi il qualificatore di attributo viene rimosso dall'attributo nel modello di classe utente.
- ▶ Attribute Qualifier addition of type <nome> in existing attribute <nome> is not allowed. The qualifier was removed in Class <nome>. Gli utenti non possono aggiungere tipi specifici di qualificatori di attributo agli attributi predefiniti. Il qualificatore di attributo quindi viene rimosso dall'attributo nel modello di classe utente.
- ▶ Attribute Qualifier addition of type <nome> in new attribute <nome> is not allowed. The qualifier was removed from the attribute override in Class <nome>. I nuovi attributi sono attributi creati da un utente per una classe predefinita. L'utente ha inoltre aggiunto un override sul nuovo attributo in una sottoclasse. Tuttavia specifici tipi di qualificatori di attributo non possono essere aggiunti ai nuovi attributi o ai rispettivi override. Quindi il qualificatore di attributo viene rimosso dall'override dell'attributo nel modello di classe utente.
- ▶ Attribute Qualifier addition of type <nome> in existing attribute <nome> is not allowed. The qualifier was removed from the attribute override in Class <nome>. Specifici tipi di qualificatori di attributo non possono essere aggiunti agli attributi predefiniti o ai rispettivi override. Quindi il qualificatore di attributo viene rimosso dall'override dell'attributo nel modello di classe utente.
- ▶ Attribute Qualifier removal <nome> is not allowed. Attribute <nome> in Class <nome>. Un utente ha rimosso un qualificatore di attributo fornito con il modello di classe preimpostato. Specifici tipi di qualificatori di attributo non possono essere rimossi dagli attributi predefiniti.
- ▶ Attribute Qualifier removal <nome> in override is not allowed. Attribute <nome> in Class <nome>. Un utente ha rimosso un qualificatore di attributo in un override di attributo incluso nel modello di classe preimpostato. Specifici tipi di qualificatori di attributo non possono essere rimossi dagli override dell'attributo predefiniti.

- ▶ Valid Link <nome> removal is not allowed. Un collegamento valido è stato rimosso da un utente o non è stato distribuito correttamente dal Content Pack 6.00. Il collegamento valido viene ripristinato nel modello di classe utente.
- ▶ Calculated Link <nome> removal is not allowed. Class <nome>. Un collegamento calcolato è stato rimosso dall'utente o non è stato distribuito correttamente dal Content Pack 6.00. Il collegamento calcolato viene restituito nel modello di classe utente.
- ▶ TypeDef <nome> removal is not allowed. Se la definizione di tipo predefinita (Factory TypeDef - Enum or List) manca nel modello di classe utente, essa viene restituita al modello. La definizione potrebbe mancare in seguito alla rimozione da parte dell'utente o in seguito a un errore di distribuzione del Content Pack 6.00.
- ▶ Enum entry removal is not allowed. Enum <nome> with Enum entry key <chiave> and Enum entry value <valore>. Se una voce **Enum** manca in una definizione di tipo **Enum**, la voce viene restituita alla definizione **Enum**. La voce Enum potrebbe mancare in seguito alla rimozione da parte dell'utente o in seguito a un errore di distribuzione del Content Pack 6.00.
- ▶ List entry removal is not allowed. List <nome> with List entry value <valore>. Se una voce List manca in una definizione di tipo List, la voce viene restituita a List. La voce List potrebbe mancare in seguito alla rimozione da parte dell'utente o in seguito a un errore di distribuzione del Content Pack 6.00.
- ▶ Enum entry addition can cause conflicts. Enum <nome> with Enum entry key <chiave> and Enum entry value <valore>. Un utente ha aggiunto una voce a una definizione di tipo **Enum**. A questo punto nell'aggiornamento non sono disponibili informazioni sufficienti per stabilire se la voce causa la non riuscita dell'aggiornamento.
- ▶ List entry addition can cause conflicts. List <nome> with List entry value <valore>. Un utente ha aggiunto una voce a una definizione di tipo List. A questo punto nell'aggiornamento non sono disponibili informazioni sufficienti per stabilire se la voce causa la non riuscita dell'aggiornamento.
- ▶ In caso di cambiamento di tipo di attributo, viene generato un errore con il nome dell'attributo e la rispettiva classe.

- I cambiamenti di gerarchia producono un avviso con il nome della classe che ha cambiato la classe padre.
- I problemi del modello di classe utente producono il messaggio di errore seguente: User class model is not valid for upgrade.
- I problemi con le trasformazioni del modello di classe producono il messaggio di errore seguente: Upgrade configuration files are not valid.

Aggiornamento del modello di classe su disco

Nota: solo aggiornamento delle risorse.

Utilizza il modello di classe generato nel passaggio Convalidare il modello di classe: **C:\hp\UCMDB\UCMDBServer\runtime\original-fixed-class-model.xml** con i file di trasformazione predefiniti per generare il modello di classe aggiornato. Il modello di classe aggiornato viene salvato su disco in **C:\hp\UCMDB\UCMDBServer\runtime\upgraded-class-model.xml**. Per i dettagli consultare "Convalidare il modello di classe" a pag. 189.

È critico (S/N)	Può essere rieseguito (S/N)
S	S

Implicazioni in caso di errore

Al momento il modello di classe non può essere aggiornato correttamente.

- **Soluzione 1:** modificare le classi problematiche nell'istanza UCMDB 8.0x e rieseguire l'aggiornamento.
- **Soluzione 2:** modificare i file dei cambiamenti del modello di classe. Per i dettagli consultare "Convalidare il modello di classe" a pag. 189. Se si modificano questi file, è necessario rieseguire il passaggio Convalidare il modello di classe prima di continuare con l'aggiornamento.

File di registro

- **Messaggi generali (tutte le entità del modello di classe a livello superiore):**
 - Adding non-modified <tipo entità> <nome entità>. L'entità non è stata modificata tra l'utente e il modello di classe di destinazione. Questo messaggio può essere visualizzato anche come Adding un-upgraded...
 - Adding <tipo entità> <nome>. L'entità aggiornata viene aggiunta al modello di classe di destinazione.
 - Skipping <tipo entità> <nome> - Dropped in upgrade. L'entità deve essere rimossa esplicitamente nell'aggiornamento. Questo messaggio può essere visualizzato anche come Not adding...
 - Skipping <tipo entità> <nome> - exists in new basic CM. L'entità esiste nel modello di classe di base e la rispettiva definizione viene utilizzata.
 - Adding new <tipo entità> <nome>. Una nuova entità, contrassegnata per l'aggiunta durante l'aggiornamento, viene aggiunta al modello di classe di destinazione.
 - Skipping adding new <tipo entità> <nome> - exists in new basic CM. Una nuova entità, contrassegnata per l'aggiunta durante l'aggiornamento, non viene aggiunta al modello di classe di destinazione poiché è stata specificata dal modello di classe di base.
- **Messaggi relativi ai collegamenti calcolati:**
 - Skipping calculated link <nome> - exists in new basic CM, adding only triplets. Il collegamento calcolato esiste nel modello di classe di base ma le terne del modello di classe utente vengono aggiunte per conservare i risultati della query (TQL).
- **Messaggi relativi alla classe:**
 - About to upgrade class <nome>. Questo messaggio viene scritto prima dell'aggiornamento di una classe. In caso di errore il messaggio può essere utilizzato per tracciare la classe che lo ha causato.
 - Skipping class <nome> - already added as a calculated link. La classe è già stata aggiunta come parte di un collegamento calcolato. Fare riferimento ai messaggi di registro precedenti per stabilire cosa si è effettivamente verificato con tale classe.
 - skipping adding new class <nome> extends <nome padre> which does not exist. La classe non è aggiunta al modello di classe poiché il padre non è stato trovato nel modello di classe di destinazione.

➤ **Messaggi relativi ai collegamenti validi:**

- **Skipping adding new valid link <nome> - <estremità> class <nome classe> does not exist.** Il collegamento valido non può essere aggiunto poiché non è possibile trovare una classe (**end1**, **end2** o **link**) nel modello di classe di destinazione.
- **Duplicate CITs found: <nomi>.** A causa di un errore, i CIT sono stati aggiunti due volte al modello di classe di destinazione. Questo errore non è recuperabile se non si modifica l'aggiornamento dei file dei cambiamenti del modello di classe e non si rieseguo i passaggi Convalidare il modello di classe e Aggiornare il modello di classe. Per i dettagli consultare "Convalidare il modello di classe" a pag. 189 e "Aggiornamento del modello di classe su disco" a pag. 195
- **Adding <nome precedente> > <nuovo nome> to rename map.** La mappa di ridenominazione viene utilizzata per identificare i nomi di classe precedenti e mapparli ai nuovi nomi di classe.
- **Mismatch between incremental rename map and changes util! Using incremental rename map. Incremental: <nome precedente> > <nuovo nome>. Util: <nome precedente2> > <nuovo nome2>.** La mappa di ridenominazione corrente e la definizione di aggiornamento non corrispondono. Si consiglia di prendere nota per la verifica poiché potrebbe indicare un problema nell'aggiornamento del modello di classe. Questo messaggio non arresta da solo il processo di aggiornamento.

➤ **Convalida dei collegamenti validi:**

- **Start removing invalid links.** I collegamenti validi devono essere verificati e quelli non validi vengono rimossi (ovvero nessuna classe **end1**, **end2** o **link**).
- **Link <nome> <entità> does not exist in target class model - Removing valid link <nome>.** L'entità del collegamento valido (**end1**, **end2** o **link** class) non esiste nel modello di classe di destinazione e quindi il collegamento valido deve essere rimosso per rendere valido l'intero modello di classe. Successivamente ciò potrebbe causare il mancato aggiornamento delle risorse (ad esempio TQL e viste).
- **Done removing invalid links.** Questo messaggio viene visualizzato quando questo sottopassaggio è completo.

- Per una classe utente con attributi chiave diversi dal rispettivo padre viene ripristinato il set completo di attributi chiave. Ciascun attributo chiave rimosso dai rispettivi predecessori preimpostato e aggiunto alla nuova classe utente produce il messaggio di informazioni di registro: Added ID qualifier to attribute <nome attributo> in class <nome classe>.

Preparare le azioni richieste per l'aggiornamento dei dati

Nota: solo aggiornamento delle risorse.

Utilizza il file **C:\hp\UCMDB\UCMDBServer\runtime\original-class-model.xml**, il file **C:\hp\UCMDB\UCMDBServer\runtime\upgraded-class-model.xml** e le trasformazioni del modello di classe per trovare le azioni richieste per l'esecuzione della trasformazione dei dati.

Salva i risultati di analisi su disco nel file seguente: **C:\hp\UCMDB\UCMDBServer\runtime\data-upgrade-actions.xml**. Questo passaggio salta i CIT che causano l'omissione dei dati durante l'aggiornamento dei dati che non si possono aggiornare. I CIT sono elencati in **C:\hp\UCMDB\UCMDBServer\upgrade\DataModelUpgradeConfig.xml (app-infra.jar)**.

È critico (S/N)	Può essere rieseguito (S/N)
S	S

Implicazioni in caso di errore

L'aggiornamento non può dedurre le azioni necessarie per trasformare il modello di dati dal modello di classe della versione precedente al modello di classe di destinazione. La configurazione e l'aggiornamento dei dati non possono continuare senza aver completato questo passaggio.

File di registro - Analisi iniziale

Nota: in questa sezione ED significa elementi dati: CI o collegamenti.

Informazioni generali

- ▶ Questo passaggio si riferisce alla configurazione dell'aggiornamento dei dati come serie di regole di copia con possibili trasformazioni e condizioni.
- ▶ L'origine di un attributo può essere:
 - ▶ Una proprietà nell'ED di origine.
 - ▶ Un valore costante per tutti gli ED di una determinata classe concreta.
- ▶ I registri di questo passaggio sono nidificati (utilizzando i rientri). Un messaggio di registro rientrato è preceduto di norma da un'intestazione che stabilisce il contesto dell'analisi.
- ▶ Tipi di regole di classe:
 - ▶ Modified, Moved, Merged. Gli ED che appartengono alle regole contrassegnate come una di queste devono essere copiate nel nuovo modello di dati (con trasformazioni possibili).
 - ▶ Added, Deprecated. Questi CIT sono nuovi. In quanto tali non possono avere alcun ED.
 - ▶ Removed. Questi CIT vengono rimossi in modo esplicito durante l'aggiornamento. I rispettivi ED non vengono copiati nel modello di classe di destinazione (se non diversamente annotato da un'altra regola).
- ▶ Tipi di regole di attributo:
 - ▶ Added. La regola definisce un attributo che può essere nuovo o che mantiene il proprio nome.
 - ▶ Deprecated, Modified. La regola definisce una trasformazione per un attributo esistente che viene rinominato.

- **Removed.** La regola definisce che questo attributo non deve esistere nell'ED di destinazione.
- La regola predefinita o l'azione predefinita. Definita su un determinato CIT. Ciò significa che il nome del CIT di destinazione è lo stesso del nome del CIT di origine. Gli attributi di ED definiti nel livello del CIT di destinazione vengono copiati dagli attributi con lo stesso nome a livello del CIT di origine. Gli attributi nel CIT padre utilizzano le regole del CIT padre.

Analisi generale della classe o della regola

- **Rule type for class <nome> is <tipo>.** L'analisi per la classe specificata sta per iniziare.
- **Class <nome> added to added CITs.** Il CIT è nuovo quindi non esistono ED. Viene aggiunto a un elenco di riferimento di CIT aggiunti nel file XML.
- **Class <nome> added to removed CITs.** Il CIT è contrassegnato per essere rimosso con tutti i rispettivi ED.
- **Change has empty class name.** Un avviso che la trasformazione richiesta non è valida e non ci sono azioni da eseguire. Causa: definizione di trasformazione non valida.
- **Target CIT name is <nome>, Source CIT name is <nome> (from <origine>).** Gli ED del CIT di origine devono essere copiati nel CIT di destinazione.
- **Target CIT <nome> does not exist in target class model, skipping rule!** Un avviso che indica che il CIT di destinazione non è stato creato correttamente. L'intera regola deve essere saltata poiché non può essere completata. Causa: definizione di trasformazione non valida o aggiornamento di modello di classe non corretto.
- **Source CIT <nome> does not exist in source class model, skipping rule!** Un avviso che indica che il CIT di origine non si trova nel modello di classe utente. L'intera regola deve essere saltata poiché non può essere completata. Causa: definizione di trasformazione non valida, aggiornamento del modello di classe non corretto oppure modello di classe utente (dopo le correzioni) non conforme al modello di classe della versione 8.0x.

- Source CIT <nome> does not exist in source class model, skipping rule, adding to added CITs! Un avviso che indica che le regole non corrispondono al modello di classe corrente. Non è possibile trovare il CIT di origine quindi il CIT di destinazione deve essere gestito come un nuovo CIT (ovvero non c'è un aggiornamento dei dati). Causa: definizione di trasformazione non valida, aggiornamento del modello di classe non corretto oppure modello di classe utente (dopo le correzioni) non conforme al modello di classe della versione 8.0x.
- Source CIT is empty, Target CIT is empty. Un avviso che indica che la regola di trasformazione non è valida. La regola viene saltata. Causa: definizione di trasformazione non valida.

Analisi della condizione di copia

- Could not create copy condition for source CIT <nome> - CIT does not exist in old class model. La classe ha un condizione dalla quale si devono copiare gli ED ma quel CIT di origine non esiste nel modello di classe utente. Un avviso che indica che la condizione deve essere ignorata. Causa: definizione di trasformazione non valida oppure modello di classe utente (dopo le correzioni) non conforme al modello di classe della versione 8.0x.
- Could not create copy condition for source CIT <nome> and attribute <nome attributo> - CIT exists but does not have the attribute. La classe ha un condizione dalla quale si devono copiare gli ED ma quell'attributo nel CIT di origine non esiste nel modello di classe utente. Un avviso che indica che l'istruzione di copia deve essere ignorata. Causa: definizione di trasformazione non valida oppure modello di classe utente (dopo le correzioni) non conforme al modello di classe della versione 8.0x.
- Copy condition attribute: <nome>, Type: <tipo>, Operator: <operatore>, Copy condition value: <valore> Per un ED da copiare (e non da eliminare), il valore dell'attributo deve conservare la condizione indicata (ad esempio **ipport not-equal to 3**).
- Attribute condition.attribute name is empty. Il nome dell'attributo è vuoto. Un avviso che indica che la condizione di copia non è valida e non deve essere utilizzata (tutti gli ED devono essere copiati). Causa: definizione di trasformazione non valida.

- ▶ Copy condition value is empty. Il valore della condizione di copia è vuoto. Un avviso che indica che la condizione di copia non è valida e non deve essere utilizzata (tutti gli ED devono essere copiati). Causa: definizione di trasformazione non valida.

Analisi dell'attributo generale

- ▶ Entering copy attribute analysis. L'analisi dell'attributo sta per iniziare.
- ▶ Rule type for attribute <nome precedente> > <nuovo nome> is <tipo di regola>. L'analisi per questa regola sta per iniziare. Nota: i tipi MERGED e MOVED non si applicano per le regole dell'attributo.
- ▶ Rule type changed from <tipo originale> to ADDED - no old name or oldName == Name. Anche se la regola viene definita come modificata, l'azione dei dati corrente deve trattare questo attributo come aggiunto poiché non c'è alcun cambiamento nel nome dell'attributo oppure non c'è alcun attributo precedente (la differenza tra il modello di classe utente e il modello di classe previsto versione 8.0x).
- ▶ No target class <nome> in new class model. Un avviso che indica non è possibile trovare la classe di destinazione nel modello di classe di destinazione e questo attributo deve essere saltato. Causa: aggiornamento del modello di classe non corretto.
- ▶ No target attribute <nome> in target class <nome classe> in new class model. Un avviso che indica non è possibile trovare l'attributo di destinazione nel modello di classe di destinazione e questa regola di attributo deve essere saltata. Causa: aggiornamento del modello di classe non corretto.
- ▶ Attribute <nome> in class <nome classe> in new class model is declared STATIC_ATTRIBUTE. Skipping rule. Gli attributi statici sono connessi al CIT e non all'ED corrente. In quanto tali non devono essere copiati durante l'aggiornamento dei dati.
- ▶ Attribute <nome> in class <nome classe> in new class model is of simple list type. Skipping rule. Gli elenchi di valori (valori multipli) sono gestiti in un passaggio di aggiornamento diverso e qui sono saltati.
- ▶ Attribute <nome> is a root class attribute that is not duplicated to concrete classes. Skipping rule. La regola specifica viene saltata poiché l'attributo non deve essere copiato nella tabella di classi concrete nel database.

Copiare l'attributo dall'analisi della classe

- Copy attribute from class. Questo valore dell'attributo viene determinato dalla classe concreta dell'ED.
- Attribute constant value: <valore>. Per questa classe concreta, il valore dell'attributo è il valore specificato nel messaggio.

Copiare l'attributo dall'analisi dell'attributo

- Copy attribute from attribute. Questo valore di attributo viene determinato da un altro attributo.
- Old attribute name: <nome>. Applicabile per un attributo aggiunto: l'attributo di origine è il nome specificato nel messaggio.
- Source attribute name (from enum): <nome>, Source attribute name (from OldName): <nome>. Applicabile per un attributo modificato: l'origine per questa regola è costante (from enum) oppure è un altro attributo (from OldName).
- **Trasformazione mappata all'interno di attributo di copia:**
 - Entering map transformation analysis. L'origine deve essere trasformata utilizzando un'origine per la mappatura di destinazione (dictionary).
 - Adding transformation: <valore precedente> > <valore nuovo>. Il valore precedente deve essere sostituito con il valore nuovo.
 - From value is empty. To value is empty. Il valore da/a è vuoto e questa trasformazione non si verifica. Causa: definizione di trasformazione non valida.

Analisi dell'attributo aggiunto (nuovo e non rinominato)

- Copy attribute from default value: <nome>. L'attributo non ha origine dell'attributo quindi il rispettivo valore viene determinato dal nuovo valore predefinito.
- Attribute name is empty, Attribute default value is empty. Questa regola di attributo non è valida e non viene utilizzata. Causa: definizione di trasformazione non valida.

Analisi dell'attributo modificato (rinominato)

- Copy attribute from source value: <nome>. Il nome dell'attributo viene determinato da un altro attributo nell'ED di origine.
 - Attribute name is empty, Attribute default value is empty. Questa regola di attributo non è valida e non viene utilizzata. Causa: definizione di trasformazione non valida.

Analisi dell'attributo comune

- Completing and adding. Un messaggio che indica che l'aggiornamento sta avviando la fase di analisi comune per questa regola di attributo.
- Attribute was not properly completed. La fase di analisi comune non è riuscita e la regola di attributo non viene utilizzata. Ciò viene preceduto da uno dei messaggi seguenti:
 - Target CIT empty. Il CIT di destinazione è vuoto. Causa: regola non valida.
 - Target CIT does not exist in new class model. Il CIT di destinazione è vuoto. Causa: regola non valida o aggiornamento di modello di classe non corretto.
 - Il nome dell'attributo di destinazione è vuoto. Il nome dell'attributo di destinazione è vuoto. Causa: regola non valida.
 - Target attribute <nome> does not exist in target CIT in new class model! Impossibile trovare l'attributo nel modello di classe di destinazione. Causa: regola non valida o aggiornamento di modello di classe non corretto.
 - Cannot determine target type <nome>. Il tipo dell'attributo di destinazione non è valido. Causa: aggiornamento del modello di classe non corretto.
 - Il nome del CIT di origine è vuoto. Il CIT di origine è vuoto. Causa: regola non valida, aggiornamento del modello di classe non corretto oppure errore precedente nell'analisi delle azioni dei dati.
 - Source attribute name is empty, Source attribute is null. Il CIT di origine è vuoto. Causa: regola non valida, aggiornamento del modello di classe non corretto oppure errore precedente nell'analisi delle azioni dei dati.

- Tipi:
 - Setting new type <tipo>, Setting old type <tipo>. È stato determinato che l'attributo sia del tipo specificato. Questo viene utilizzato successivamente per creare il cast di tipo SQL corretto.
 - Target attribute is <nome>, Source attribute is <nome>. Il nome dell'attributo è il nome specificato nel messaggio.
 - Constant value requires new type declaration. New type and old type are <tipo>. Per l'attributo deve essere fornito un valore costante con il tipo specificato.
- Valori predefiniti:
 - Target default value is <valore>. Il nome dell'attributo di destinazione ha un valore predefinito. Questo valore viene utilizzato se la proprietà dell'ED originale è vuota.
 - Source default value is <valore>. Se la proprietà dell'ED originale è uguale al valore predefinito precedente, questo viene trasformato nel valore nuovo predefinito.
- Limiti delle dimensioni:
 - New size set <dimensione> set from default, Constant value new size is <dimensione>. Il tipo dell'attributo di destinazione è di tipo string. In quanto tale deve avere un limite di dimensione. Non è stato specificato alcun limite quindi viene utilizzato il limite di dimensione predefinito (50 caratteri).
 - Old size is <dimensione>, setting truncate flag. Il limite di dimensione è inferiore al limite di dimensione di origine. I valori potrebbero essere troncati.
 - New size is <dimensione>. Viene specificato un nuovo limite di dimensione.

- ▶ **Attribute did not pass validation.** La convalida finale non è riuscita quindi la regola di attributo non viene utilizzata. Le cause effettive devono essere controllate per verificare i messaggi della creazione corrente dell'azione. Ciò deve essere preceduto da uno dei messaggi seguenti:
 - ▶ **No target attribute.** Per qualche motivo il nome dell'attributo di destinazione resta vuoto.
 - ▶ **Target attribute does not exist in target class model.** L'attributo di destinazione non esiste nel modello di classe di destinazione.
 - ▶ **No source.** L'origine dell'attributo (attributo di origine o valore costante) resta indeterminato.
 - ▶ **Source attribute does not exist in source class model**
 - ▶ **Source attribute size limit > Target attribute size limit but truncate needed flag is false.**
 - ▶ **Target attribute target type is missing.**
 - ▶ **Target attribute source type is missing.**
 - ▶ **Target attribute source and target types are not the same, but attribute source is of type CONSTANT_VALUE.**
 - ▶ **Instruction for target attribute already exists.** I valori dell'attributo di destinazione in questo CIT specifico sono già generati da un'altra regola.
 - ▶ **Value transformation source is empty, Value transformation target is empty.** La trasformazione della mappa di valori non è valida.

File di registro - Analisi successiva

Flattening regole. Le regole definite nei cambiamenti del modello di classe sono state convertite in azioni. Questa fase ora copia le regole dalle classi padri nelle classi figlie per creare un set di regole non semplici disconnesse dalla gerarchia di classi.

- Flatten rules stage. La fase ha inizio.
- Building class to direct children map. Avvio della creazione di una classe completa nel dizionario figlio.
 - Class <nome figlio> is a child of <nome padre>.
 - Class appeared twice. Avvisa che una classe è stata trovata due volte. Probabilmente il modello di classe non è valido.
- Building by target and by source rules map. Avvio della creazione di due dizionari classe-regole: uno è classe di origine-regola, l'altro è classe di destinazione-regola.
 - Found rule from <origine> to <destinazione>.
 - Adding this rule will corrupt the by target map, By source map already contains this CIT. Un avviso che indica che non è possibile aggiungere la regola alla mappa poiché un'altra istanza esiste già in una destinazione diversa o classe di origine. La regola viene ignorata per le classi figlie.
- Entering DFS over target class model. Avvio della fase flattening con passaggio sul modello di classe dall'alto verso il basso.
 - Visiting <classe> (added <figli> children). Avvio del trattamento della classe specifica. È stato trovato che questa classe ha i figli specificati e li tratta in un secondo momento.
 - No rule for <nome>, it exists in old class model and it was not explicitly added or removed - adding default rule. Viene utilizzata una regola predefinita per copiare gli ED di questo CIT.

- ▶ **Visiting rule from <nome classe di origine>**. Avvio della consultazione delle regole di attributo da parte del CIT di origine specificato. In questa fase, la struttura di origine viene verificata dal basso (CIT specificato) verso l'alto (radice) per raccogliere il set corretto di regole. La regola bottom-most che genera un valore per un attributo di destinazione è la sola utilizzata.
- ▶ **Visiting source class <nome>**. Classe di origine specificata da verificare.
- ▶ **Found rule from source class <origine> to <destinazione>**. Avvio della verifica della regola di copia attributo specificato.
- ▶ **Rule matches for flattening**. Si può applicare alla classe di destinazione (classe di destinazione è la classe di destinazione **current** o un padre di tale classe).
- ▶ **Going over source rules with targets: <destinazioni>**. Avvio dell'analisi della regola con gli attributi di destinazione indicati.

Rule to <destinazione> is not mapped - attribute exists in concrete source class and concrete target class. La regola non viene utilizzata poiché l'attributo esiste nella classe concreta di origine e nella classe concreta di destinazione (deve essere copiata nello stato in cui si trova).

Rule to <destinazione> is not mapped. L'attributo di destinazione specificato non ha ancora alcuna regola di generatore di valori.

Rule is not in ignore list - adding to target attribute rules. La regola specificata viene utilizzata per generare valori per l'attributo di destinazione.

Attribute did not pass validation. La regola di attributo non ha superato la convalida. Consultare la sezione precedente sui possibili messaggi di convalida e delle cause.

Rule is in ignore list - not added. L'attributo non può essere copiato (è contrassegnato in questo senso) quindi non può essere utilizzato.

- Going over ignore list: <attributi>. Se un attributo è stato rimosso, viene visualizzato in questo elenco. Gli attributi di questo elenco non devono essere copiati nell'attributo di destinazione. Poiché l'analisi viene eseguita dal basso verso l'alto, l'elenco viene creato e aggiunto a ciascun livello del CIT.

Adding ignored attribute <nome>. È stato trovato un attributo nell'elenco da non copiare. Aggiunta all'elenco corrente di elementi da ignorare in modo che questo attributo non viene copiato se presente nel CIT padre.

- Going over copy conditions. Copia le condizioni di copia (se gli ED devono essere effettivamente copiati). Viene copiato dalla classe padre (prevale la regola bottom-most).

Copy condition is for attribute name <nome>. È stata trovata una condizione di copia che dipende dall'attributo specificato.

Adding copy condition for attribute name <nome> with values <valori>. L'attributo non è stato ancora vincolato da alcun'altra condizione di copia. Ora è vincolato dalla condizione di copia 'current'.

Fase di eliminazione delle classi astratte. I CIT astratti non hanno ED (o tabelle sotto il nuovo modello di dati). Le regole che sono state create per questi CIT (processo flattening, errori e una discordanza tra il modello di classe della versione 8.0x e il risultato del modello di classe previsto) ora sono eliminate.

- Remove abstract classes stage. Questa fase sta iniziando.
- Removing rule from <nome di origine> to <nome di destinazione> - <origine/destinazione> is abstract in new class model. Questa regola di copia viene rimossa poiché il CIT di origine o il CIT di destinazione è contrassegnato come astratto.

Fase delle regole non semplici. Se un attributo con lo stesso nome esiste nel CIT di origine e il nome dell'attributo non fa parte della raccolta di attributi che non devono essere copiati, viene aggiunta una regola per questo attributo.

- ▶ Found rule from <classe di origine> to <classe di destinazione>. Elaborazione della regola specificata.
- ▶ Adding CMDB_ID rule. Tutti i CIT devono avere una regola per copiare la colonna CMDB_ID.
- ▶ Target class <nome classe> is a link. Adding <estremità1> and <estremità2> rules. Tutte le classi di collegamento devono avere due regole per copiare la colonna end1 ed end2.
- ▶ Checking attribute <nome>. Elaborazione dell'attributo specificato.
- ▶ Attribute <nome> has qualifier STATIC_ATTRIBUTE, skipping. L'attributo è statico quindi non deve essere copiato.
- ▶ Attribute <nome> is CmdbSimpleList, skipping. Gli attributi con più valori vengono trattati un passaggio di aggiornamento diverso quindi non è necessaria alcuna regola.
- ▶ Attribute <nome> appears in root, skipping. L'attributo viene visualizzato in una classe radice e non viene duplicato nelle tabelle foglie quindi non è necessaria alcuna regola.
- ▶ Attribute is not mapped, nor in 'do not copy' list. L'attributo deve essere copiato utilizzando una regola predefinita.
- ▶ Found source attribute with the same name - creating default copy rule. Un attributo con lo stesso nome è stato trovato nel modello di classe di origine quindi sarà l'origine della regola predefinita.
- ▶ No source attribute, checking default value, Found non empty default value - creating default constant copy rule. Valore predefinito: <valore>. No c'è alcun attributo di origine con lo stesso nome quindi il valore predefinito (se ne esiste uno) viene utilizzato come origine per la regola predefinita. Se il secondo messaggio non viene visualizzato allora non viene utilizzata alcuna regola e il valore dell'attributo resta vuoto.
- ▶ completing and adding. Attribute was not properly completed. Attribute did not pass validation. Questi messaggi hanno lo stesso significato della fase iniziale.

Preparare gli script SQL per l'aggiornamento dei dati

Nota: solo aggiornamento delle risorse.

Analizza il file `C:\hp\UCMDB\UCMDBServer\runtime\data-upgrade-actions.xml`, genera le istruzioni SQL correnti da eseguire nel database per l'aggiornamento dei dati e li salva su disco in

`C:\hp\UCMDB\UCMDBServer\runtime\data-upgrade-script.sql`.

È critico (S/N)	Può essere rieseguito (S/N)
S	S

Implicazioni in caso di errore

Un errore in questo passaggio significa che l'aggiornamento non ha convertito le azioni (del file XML) nelle istruzioni SQL necessarie per la trasformazione del modello di dati dal modello di classe della versione precedente nel modello di classe di destinazione. La configurazione e l'aggiornamento dei dati non possono continuare senza aver completato questo passaggio.

Possibili correzioni degli errori: rimuovere l'azione origine dell'errore (classe intera o solo l'attributo) dall'XML delle azioni di aggiornamento dei dati. Ciò potrebbe causare una perdita di dati (la classe / l'attributo potrebbero non essere copiati) ma consentirebbe all'aggiornamento di continuare.

File di registro

- ▶ Could not create cast for <classe di origine> > <classe di destinazione>, on <origine> > <attributo di destinazione>. Il generatore SQL non ha trovato il modo corretto di trasformare il tipo di origine (attributo o costante) nel tipo di attributo di destinazione. Le possibili cause sono cast di tipi non supportati (non tutte le conversioni di tipi possibili sono supportate) oppure un'analisi non corretta (errore / definizioni non corrette / cambiamenti di modello di classe utente imprevisti). L'effetto è che questi valori di attributo non sono cast. Durante la chiamata SQL corrente, potrebbe causare errore nell'istruzione. Questo errore non dovrebbe arrestare il processo di aggiornamento.
- ▶ Could not create copy condition for <class di origine> > <classe di destinazione>. Il generatore SQL non ha compreso la clausola di copia condizionale. Le possibili cause sono condizioni non supportate (non tutte le condizioni possibili sono supportate) oppure un'analisi non corretta (errore / definizioni non corrette / cambiamenti di modello di classe utente imprevisti). L'effetto è che questa condizione di copia non si verifica e tutti i CI del tipo CIT di origine vengono copiati. Questo errore non dovrebbe arrestare il processo di aggiornamento.
- ▶ Default value exceeding 4000 characters is ignored. Table: <tabella>. Column: <colonna>. Questo set di valori predefiniti per questa colonna è troppo grande per adattarsi all'istruzione SQL. La possibile causa è un valore predefinito troppo alto nel modello di classe utente. L'effetto è come se non esistesse alcun valore predefinito per questa colonna. Questo errore non dovrebbe arrestare il processo di aggiornamento.

Individuazione - Aggiornamento tabella degli errori

Esegue l'aggiornamento dei dati degli errori di individuazione (memorizzati nella tabella **CCM_DISCOVERY_ERRORS** nel CMDB). Questa tabella sostituisce i messaggi di errore in base ai codici errore con i parametri (informazioni sul runtime di individuazione).

È critico (S/N)	Può essere rieseguito (S/N)
N	S

Implicazioni in caso di errore

Le informazioni sugli errori di individuazione sono andate perdute. Se si salta questo passaggio è necessario troncare la tabella **CCM_DISCOVERY_ERRORS** nel CMDB e riattivare tutti i processi di individuazione dopo aver eseguito il backup del server.

File di registro

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

Individuazione - Creare una tabella di IP di nuova destinazione

Crea una nuova tabella nel CMDB denominata **CCM_DISCOVERY_DEST_IPS**. La nuova tabella contiene gli IP di ciascuna destinazione. Le informazioni vengono estratte dalla tabella **CCM_DISCOVERY_DESTS** (informazioni sul runtime di individuazione).

È critico (S/N)	Può essere rieseguito (S/N)
N	S

Implicazioni in caso di errore

Le informazioni sulle destinazioni di individuazione sono andate perdute. Se si salta questo passaggio è necessario troncare la tabella **CCM_DISCOVERY_DEST_IPS** nel CMDB e riattivare tutti i processi di individuazione dopo aver eseguito il backup del server.

File di registro

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

Individuazione - Aggiornamento tabella delle destinazioni

Rinomina i tipi CI nella tabella **CCM_DISCOVERY_DESTS** nel CMDB (informazioni sul runtime di individuazione).

È critico (S/N)	Può essere rieseguito (S/N)
N	S

Implicazioni in caso di errore

Le informazioni sulle destinazioni di individuazione sono andate perdute. Se si salta questo passaggio è necessario troncare la tabella **CCM_DISCOVERY_DESTS** nel CMDB e riattivare tutti i processi di individuazione dopo aver eseguito il backup del server.

File di registro

- ▶ Starting aggiornamento 'CCM_DISCOVERY_DESTS' table
- ▶ Upgrade 'CCM_DISCOVERY_DESTS' table was successfully finished!
- ▶ Failed to aggiornamento 'CCM_DISCOVERY_DESTS' table
- ▶ Ci type [tipo CI precedente] has been upgraded to [nuovo tipo CI]. Indica che la classe [tipo CI precedente] è stata rinominata in [nuovo tipo CI].
- ▶ failed to update [tipo CI precedente], skipped. Indica che non è stato possibile cambiare un tipo CI in base al nuovo schema, probabilmente a causa di incoerenza di dati nel CMDB o di tipo CI non corretto definito dall'utente. Non influisce sulla funzionalità di destinazione ma influisce sulla visualizzazione della destinazione nell'interfaccia utente.

Modificare la modellazione di dati nel database

Nota: solo aggiornamento delle risorse.

Modificare la struttura del CMDB nella nuova struttura della versione 9.00.

È critico (S/N)	Può essere rieseguito (S/N)
S	N

Implicazioni in caso di errore

L'errore indica che gli schemi del database non sono nel formato corretto per il nuovo UCMDb. Il processo di aggiornamento non può continuare senza questo passaggio. Per cercare di eseguire di nuovo questo passaggio, ripristinare gli schemi del CMDB dal backup, eliminare la cartella **C:\hp\UCMDB\UCMDBServer\runtime** ed eseguire lo strumento di aggiornamento dall'inizio.

File di registro

Nessuno

Copiare informazioni sui destinatari dell'e-mail

Nota: solo aggiornamento delle risorse.

Copia le informazioni sui destinatari dalla tabella di dati **EmailRecipient** nella tabella di gestione **EN_UI_RECIPIENTS** nel CMDB. (In UCMDb 8.x i dati dei destinatari sono stati modellati come CI). **EmailRecipient** viene poi rimosso nell'ambito dell'aggiornamento dei dati.

È critico (S/N)	Può essere rieseguito (S/N)
N	Sì se l'aggiornamento del modello di classe non è stato ancora eseguito

Implicazioni in caso di errore

I report pianificati non vengono inviati. Gli utenti devono aggiungere i destinatari mediante Gestione destinatari o gli stessi processi pianificati aggiornati.

File di registro

- Number of EmailRecipients in the CMDB is x. Numero di destinatari esistenti.
- Failed to handle Recipient. Nel caso in cui l'aggiornamento non riesce.
- RecipientUpgrader is complete. Nel caso in cui l'aggiornamento riesce.

Copiare informazioni sulla pianificazione dei report

Nota: solo aggiornamento delle risorse.

Copia la configurazione dei report pianificati dal database Foundation nella nuova tabella di gestione nel CMDB.

È critico (S/N)	Può essere rieseguito (S/N)
N	S

Implicazioni in caso di errore

I report pianificati non sono stati aggiornati quindi si devono ripianificare.

File di registro

- Upgrade of scheduled report finished successfully.
- failed to upgrade scheduled reports. For an overall failure.
- failed to upgrade scheduled report of job name <nome processo>. Per un errore su un processo specifico.

Copiare le risorse su disco

Nota: solo aggiornamento delle risorse.

Estrae le query, le viste, i report, gli accrescimenti e le correlazioni dal database e li memorizza su disco. Le risorse vengono memorizzate in una sottocartella **C:\hp\UCMDB\UCMDBServer\runtime\1\\. I tipi di risorsa possono essere di uno dei tipi seguenti:**

- ▶ **bacviews.** Tipo di risorsa precedente, non esiste nella versione 9.0.
- ▶ **bundles.** Utilizzato per definire un gruppo di risorse. Consente la relazione many to many.
- ▶ **cmdbview.** Nuova definizione di vista, si sottopone soltanto ad aggiornamento del modello di classe.
- ▶ **Correlations.** Regole di correlazione, si sottopongono soltanto ad aggiornamento del modello di classe.
- ▶ **Accrescimento.** Regole di accrescimento, si sottopongono soltanto ad aggiornamento del modello di classe.
- ▶ **goldmaster.** Definizione di report goldmaster, si sottopone soltanto ad aggiornamento del modello di classe.
- ▶ **Patterns.** Query (TQL), si sottopone ad aggiornamento della struttura e del modello di classe.
- ▶ **reports.** Report Topologia, si sottopongono ad aggiornamento della struttura per diventare cmdbview e, successivamente, ad aggiornamento del modello di classe.
- ▶ **singlepatternref.** Query basata su prospettiva, si sottopone soltanto ad aggiornamento del modello di classe.
- ▶ **viewrefs.** Vista basata su prospettiva, si sottopone soltanto ad aggiornamento del modello di classe.
- ▶ **views.** Definizione vista precedente, si sottopone ad aggiornamento della struttura per diventare cmdbview.

Le sottocartelle possono essere di uno dei tipi seguenti:

- **db**. Risorse originali.
- **structure**. Risorse dopo aggiornamento della struttura.
- **classmodel**. Risorse dopo aggiornamento del modello di classe.

Le risorse vengono aggiornate in due fasi:

- **Aggiornamento della struttura**. Aggiornamento delle risorse dal formato precedente al nuovo. Questo passaggio viene eseguito per le sequenze, le viste e i report topologici. Le risorse aggiornate vengono collocate nella cartella **structure** a eccezione delle viste e dei report che dopo l'aggiornamento passano alla cartella **cmdbview\structure**. Le risorse senza un aggiornamento della struttura vengono copiate dalla sottocartella **db** a **structure**.
- **Aggiornamento del modello di classe**. Aggiornamento delle risorse in base alle trasformazioni del modello di classe. Riguarda tutte le risorse. Le risorse aggiornate vengono salvate nella cartella **classmodel**.

Oltre alle risorse, vengono copiati alcuni altri dati: **bundles** (raggruppamento di risorse) e **bacviews** (punta alle viste). Questi vengono conservati inalterati durante l'aggiornamento.

È critico (S/N)	Può essere rieseguito (S/N)
S	S

Implicazioni in caso di errore

Non è possibile aggiornare le risorse poiché non è presente alcun dato sul disco per l'aggiornamento. Non cercare continuare prima di aver completato questo passaggio.

File di registro

- Recuperare le risorse dai messaggi del database:
 - got <numero> < tipo risorsa> from database. Specifica il numero di risorse sono state recuperate dal database per ciascun tipo di risorsa. Il messaggio è seguito dall'elenco dei nomi delle risorse.
 - did not succeed to read <tipo risorsa> from database . Consultare l'eccezione associata al messaggio per la descrizione del problema.
 - did not success to write <tipo risorsa> to disk! Verificare l'eccezione collegata per verificare il motivo. Verificare che esistano le autorizzazioni di scrittura e spazio sufficiente su disco.
 - Could not write resource <nome>. Verificare l'eccezione collegata per verificare il motivo. Verificare che esistano le autorizzazioni di scrittura e spazio sufficiente su disco.
 - did not success to write resource bundles to disk! Verificare l'eccezione collegata per verificare il motivo. Verificare che esistano le autorizzazioni di scrittura e spazio sufficiente su disco.
- Rimuovere le risorse dai messaggi del database:
 - did not success to remove all <tipo risorsa> from database. Consultare l'eccezione associata al messaggio per la descrizione del problema.
 - did not success to remove from database all <tipo risorsa> additional data for <tipo risorsa>. Consultare l'eccezione associata al messaggio per la descrizione del problema.

Troncare le tabelle dei dati

Nota: solo aggiornamento delle risorse.

Rimuove tutti i dati non rilevanti dal CMDB e dagli schemi Cronologia. Tutti i dati che non sono di configurazione e che non sono necessari per l'aggiornamento solo delle risorse vengono eliminati in questo passaggio.

È critico (S/N)	Può essere rieseguito (S/N)
S	S

Implicazioni in caso di errore

I dati non aggiornati restano nel CMDB e negli schemi Cronologia. Poiché parte dei dati non è aggiornata nei passaggi successivi, il comportamento del sistema al termine dell'aggiornamento non è prevedibile.

File di registro

- ▶ Truncating table <nome>. Rimozione di tutti i dati dalla tabella specificata.
- ▶ Table <nome> will not be truncated (data is needed for resources upgrade).
La tabella contiene i dati di configurazione che non è necessario eliminare.
- ▶ Query to delete unrelevant data from root table: <istruzione SQL>.
L'istruzione che rimuove tutti i dati rilevanti dalla tabella radice.

Rinominare le tabelle dei dati originali

Nota: solo aggiornamento delle risorse.

Rinominare le tabelle dei dati precedenti aggiungendo il prefisso **TEMP_** ai nomi di tutte le tabelle CDM.

È critico (S/N)	Può essere rieseguito (S/N)
S	N

Implicazioni in caso di errore

Il processo di aggiornamento deve essere eseguito di nuovo dall'inizio dopo aver corretto il problema. Ripristinare gli schemi del database, eliminare la cartella **C:\hp\UCMDB\UCMDBServer\runtime** e avviare l'aggiornamento dall'inizio.

File di registro

Nessuno

Aggiornare il modello di classe nel database

Nota: solo aggiornamento delle risorse.

Tronca le tabelle del modello di classe nel CMDB rimuovendo le definizioni di modello di classe precedenti, utilizza il file

C:\hp\UCMDB\UCMDBServer\runtime\upgraded-class-model.xml per popolare le tabelle del modello di classe con i dati del modello di classe aggiornato e crea le nuove tabelle di dati (tabelle CDM) nella struttura aggiornata.

È critico (S/N)	Può essere rieseguito (S/N)
S	S

Implicazioni in caso di errore

L'errore implica che il nuovo modello di classe non è stato caricato nel database. L'aggiornamento non può continuare senza il nuovo modello di classes.

File di registro

Nessuno

Aggiornamento delle risorse su disco

Nota: solo aggiornamento delle risorse.

Legge le query originali, le viste, i report, gli accrescimenti e le correlazioni dal disco e li memorizza aggiornate su disco. È importante sapere che le risorse che utilizzano le classi rimosse durante l'aggiornamento non vengono aggiornate e non saranno caricate in UC MDB aggiornato. Allo stesso modo le query che utilizzano gli attributi rimossi durante l'aggiornamento come condizione di proprietà vengono anch'esse rimosse. A prescindere dalle trasformazioni del modello di classe applicate a queste risorse, vengono apportati i cambiamenti seguenti:

- ▶ Le viste vengono ridefinite per corrispondere alla nuova definizione di vista.
- ▶ I report Topologia vengono ridefiniti come viste. UC MDB 9.0 introduce il nuovo concetto che considera i report e le viste come una visualizzazione diversa degli stessi dati.
- ▶ Le query vengono salvate in un nuovo formato XML di maggiore leggibilità.

È critico (S/N)	Può essere rieseguito (S/N)
S	S

Implicazioni in caso di errore

L'errore in tutto il passaggio si riflette nell'errore dell'intero aggiornamento. In questo caso, dopo aver eseguito le correzioni necessarie, è possibile rieseguire l'aggiornamento a partire da questo passaggio.

L'errore nell'aggiornamento di singole risorse può essere gestito eseguendo di nuovo questo passaggio oppure al termine dell'aggiornamento. Le risorse non riuscite devono essere aggiornate manualmente per correggere il problema che ha causato errore nell'aggiornamento.

File di registro

- Messaggi di registro generali:
 - Removing all the following resources: [<elenco di nomi di risorse>] of type <nome> due to filter_resources.xml configuration file. Il file di configurazione **filter_resources.xml** contiene tutti i nomi e i tipi di risorse precedenti della versione UC MDB 8.0x che non esistono in UC MDB 9.0x. Tutte queste risorse vengono rimosse nel processo di aggiornamento. Questo messaggio di registro specifica tutte queste risorse.
- Aggiornamento delle sequenze:
 - About to upgrade pattern structure for the following patterns (<numero di sequenze>) <elenco di nomi di sequenze>. Elenco dei nomi delle sequenze che si stanno aggiornando.
 - About to check if pattern <nome> should be removed. Notifica prima di verificare se l'aggiornamento per questa sequenza è necessario o meno. Se la sequenza viene rimossa, il messaggio successivo informa di questa azione.
 - Pattern <nome> should be removed - has template instance group id. Tutte le sequenze con l'istanza dell'esemplare del gruppo vengono rimosse nell'aggiornamento.
 - About to remove unneeded pattern <nome>. Le sequenze non aggiornate come la sequenza <nome> si possono collocare nel percorso **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<ID cliente>\patterns\unupgradeable\<nome sequenza>.xml**. La sequenza non è aggiornata e quindi non esiste nelle risorse post-aggiornamento.
 - About to check if pattern <nome> should be upgraded. Notifica prima di verificare se questa sequenza deve essere aggiornata. I messaggi seguenti specificano i motivi dell'aggiornamento di una sequenza.
 - Pattern <nome> should be upgraded, about to upgrade. Sta per iniziare l'aggiornamento della sequenza. I messaggi seguenti specificano le parti della sequenza che vengono aggiornate.

- About to write patterns to disk after structure upgrade (<numero di sequenze>){<elenco di nomi di sequenze>}. Queste sequenze si possono trovare in **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<ID cliente>\patterns\structure**.
- About to upgrade pattern <nome>. Avvio dell'aggiornamento del modello di classe nella sequenza.
- Pattern <nome> was upgraded. La sequenza è stata aggiornata e si trova in **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<ID cliente>\patterns\classmodel**.
- Pattern <nome> did not need upgrade. Tutte le entità del modello di classe nella sequenza sono già compatibili con la versione 9.0. La sequenza si trova in **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<ID cliente>\patterns\classmodel**.
- Pattern <nome> is not valid after upgrade. La sequenza è stata rimossa e non è stata aggiornata. Ciò è dovuto probabilmente al fatto che almeno un'entità del modello di classe non esiste più nel modello di classe.
- Could not upgrade pattern <nome>. Verificare l'eccezione seguente per la descrizione del problema.
- Riferimento di sequenza singolo:
 - About to upgrade single pattern reference <nome>. Le risorse del risultato si possono collocare in **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<ID cliente>\singlepatternref\classmodel**.
- Aggiornamento dell'accrescimento:
 - About to upgrade enrichment <nome>. L'accrescimento non necessita di aggiornamento della struttura quindi si inizia direttamente con l'aggiornamento del modello di classe.
 - Couldn't obtain pattern <nome> for enrichment definition<nome>. La sequenza non esiste per l'accrescimento corrente.
 - Enrichment <nome> was upgraded. L'accrescimento è stato aggiornato e si trova in **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<ID cliente>\enrichments\classmodel**.

- Enrichment <nome> did not need upgrade. Tutte le entità del modello di classe nell'accrescimento sono già compatibili con la versione 9.0. L'accrescimento si trova in **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<ID cliente>\enrichments\classmodel.**
- Enrichment <nome> is not valid after upgrade. L'accrescimento è stato rimosso e non è stato aggiornato. Ciò è dovuto probabilmente al fatto che almeno un'entità del modello di classe non esiste più nel modello di classe.
- Aggiornamento della correlazione:
 - About to upgrade correlation <nome>. La correlazione non necessita di aggiornamento della struttura quindi si inizia direttamente con l'aggiornamento del modello di classe.
 - Correlation <nome> was upgraded. La correlazione è stata aggiornata e si trova in **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<ID cliente>\correlations\classmodel.**
- Aggiornamento del report Gold Master:
 - About to upgrade gold master definitions for class model changes. Gold master non necessita di aggiornamento della struttura quindi si inizia direttamente con l'aggiornamento del modello di classe.
 - Got <numero> gold master definitions. Numero di gold master nel sistema.
 - Gold master report <nome> was upgraded for class model changes. Il report è stato aggiornato e si trova in **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<ID cliente>\goldmaster\classmodel.**
 - Gold master report <nome> was not changed. Tutte le entità del modello di classe nel report sono già compatibili con la versione 9.0. Il report si trova in **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<ID cliente>\goldmaster\classmodel.**

- Aggiornamento delle viste:
 - About to upgrade view <nome> structure.
 - Could not upgrade template view [nome vista bac: [<nome>], mam name: [<nome>]] - <motivo>. Un motivo comune è Pattern by name [<nome>] not found. Ciò si verifica dopo che la sequenza è stata rimossa nella fase di aggiornamento della sequenza. L'elenco delle sequenze rimosse è nel messaggio di registro Removing all the following resources: [<elenco di nomi di risorse>] of type <nome> due to filter_resources.xml configuration file.
 - View <nome> structure was upgraded by a previous depending view. La vista è stata aggiornata in precedenza. Non è necessario riaggiornarla.
 - View <nome> structure was upgraded. La vista si trova in **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<ID cliente>\cmdbview\classmodel** oppure **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<ID cliente>\bacviews\classmodel** in base al tipo di vista.
 - Could not upgrade view <nome>. L'eccezione collegata può eseguire l'elaborazione sul motivo dell'errore. La vista non è stata aggiornata e si trova in una delle cartelle seguenti:
C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<ID cliente>\cmdbview\unupgradeable oppure
C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<ID cliente>\bacviews\unupgradeable in base al tipo di vista.
 - About to upgrade view <nome>. Avvio dell'aggiornamento delle entità del modello di classe nella vista.
 - Class model transformation for view <nome> finished. La vista si trova in **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<ID cliente>\cmdbview\classmodel**.
 - Could not upgrade view <nome>. Le viste si trovano in **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<ID cliente>\cmdbview\unupgradeable**.
 - About to copy unchanged BacViews. Le viste si trovano in **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<ID cliente>\bacviews\classmodel**.

- Aggiornamento dei report:
 - About to upgrade report <nome> structure.
 - Upgrading report <nome> with tql name <nome>.
 - Report pattern <nome> for report <nome> was not found. La sequenza aggiornata non si trova sul disco per il report corrente. Se la sequenza non viene aggiornata alla versione 9.0x (dopo l'aggiornamento oppure nello stato in cui si trova) si trova in **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\
<ID-cliente>\patterns\unupgradeable** e viene generato questo messaggio. Il report si trova in **C:\hp\UCMDB\
UCMDBServer\runtime\upgrade\
<ID cliente>\reports\structure.**
 - Report <nome> was upgraded to view <nome>. Aggiornamento del report terminato. Il report si trova in **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\
<ID
cliente>\cmdbview\structure.** L'aggiornamento del modello di classe viene eseguito dall'aggiornamento della vista.
 - Could not upgrade report structure <nome>. Cercare il motivo dell'errore nell'eccezione. Il report si trova in **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\
<ID
cliente>\reports\unupgradeable\.**

Dati di aggiornamento

Nota: solo aggiornamento delle risorse.

Esegue le istruzioni SQL da **C:\hp\UCMDB\UCMDBServer\runtime\data-upgrade-script.sql**, legge i dati dalle tabelle di dati precedenti e le tabelle **TEMP**, esegue la trasformazione richiesta e popola le nuove tabelle di dati (tabelle CDM) con i dati aggiornati.

Nota: questo passaggio raddoppia lo spazio utilizzato dal CMDB. Al termine dell'aggiornamento, questo spazio viene rilasciato.

È critico (S/N)	Può essere rieseguito (S/N)
S	N

Implicazioni in caso di errore

I dati del database non sono stati aggiornati.

File di registro

Nessuno.

Creare tabella temporanea dei CI rimossi

Crea una nuova tabella nel database del CDDB denominato **UPGRADE_REMOVED_ELEMENTS** per contenere gli ID e i tipi di tutti gli oggetti rimossi durante l'aggiornamento (non copiati dalle tabelle di dati precedenti nelle nuove) per utilizzarli in passaggi successivi.

È critico (S/N)	Può essere rieseguito (S/N)
S	S

Implicazioni in caso di errore

L'errore indica che non è possibile eseguire i passaggi per l'aggiornamento della tabella degli attributi di elenco e la gestione dei dati non coerenti.

File di registro

Nessuno.

Popolare la tabella radice

Nota: solo aggiornamento delle risorse.

Copia i valori rilevanti degli attributi aggiornati dalle tabelle dei dati foglia nella tabella radice (CDM ROOT).

È critico (S/N)	Può essere rieseguito (S/N)
S	N

Implicazioni in caso di errore

La tabella radice non è stata popolata e tutti i CI non esistono in UC MDB. L'errore equivale all'eliminazione di tutti i dati da UC MDB. Per recuperare, avviare la procedura di aggiornamento dall'inizio.

File di registro

Nessuno.

Aggiornamento della tabella degli attributi List

Nota: solo aggiornamento delle risorse.

Aggiornamento degli attributi di tipo list memorizzati in una tabella separata.

È critico (S/N)	Può essere rieseguito (S/N)
S	N

Implicazioni in caso di errore

Tutti gli attributi di tipo list hanno valori errati.

File di registro

Nessuno.

Eliminare le tabelle di configurazione precedenti

Nota: solo aggiornamento delle risorse.

Rimuove le tabelle non più necessarie nel CMDB.

È critico (S/N)	Può essere rieseguito (S/N)
N	S

Implicazioni in caso di errore

Le tabelle da eliminare restano nello schema del CMDB ma non interrompono il comportamento normale di UCMDB. È possibile rimuovere manualmente queste tabelle.

File di registro

Nessuno.

Aggiornamento del database cronologia

Aggiornamento del database cronologia. Il database Cronologia può contenere un'enorme quantità di dati. Durante questo passaggio si fa riferimento ai dati dell'ultimo aggiornamento in modo che in caso di errore l'aggiornamento continua dal punto in cui si è arrestato.

È critico (S/N)	Può essere rieseguito (S/N)
S	S

Implicazioni in caso di errore

Questo passaggio può essere rieseguito più volte e si può recuperare l'errore utilizzando gli appositi file di ripristino che si trovano nella cartella **C:\hp\UCMDB\UCMDBServer\runtime\upgrade**. Ogni file contiene lo stato di un passaggio secondario; tutti insieme contengono lo stato dell'intero aggiornamento della cronologia. I nome di file sono:

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

Se si salta questo passaggio si possono perdere i dati cronologici ed è necessario creare un nuovo schema cronologia mediante la procedura guidata di configurazione.

File di registro

- Messaggi di registro generali:
 - History DB upgrader failed, but is not failing upgrade process... In caso di errore.
 - INFO - <nome passaggio> is upgrading chunk <numero di blocco corrente> out of <numero totale di blocchi>. Messaggio del report sull'avanzamento.
 - No upgrade is needed. Upgrade was finished in the previous upgrade. Questa non è la prima volta che viene eseguito il database Cronologia. La volta precedente l'aggiornamento è terminato correttamente.
 - <nome passaggio> is upgrading chunk <numero> out of <numero>. Indica l'avanzamento di ciascun passaggio dell'aggiornamento.
 - Executing SQL statement on attributes between event id <numero> and <numero>. Statement: <istruzione SQL>. Esegue l'update oppure rimuove gli attributi di un determinato tipo (specificato nell'istruzione SQL).

- ▶ old Class <nome> has history attributes of types <elenco di nomi>. Per ciascuna classe da rimuovere/aggiornare, vengono elencati i tipi di attributo da gestire.
- ▶ Create auxiliary tables for History DB upgrade. Questo è un passaggio pre-aggiornamento per la raccolta dei dati rilevanti:
 - ▶ The history DB has <numero> events. Messaggio informativo con il numero di eventi di cronologia al momento contenuti nel database Cronologia.
 - ▶ The Chunk between rows <numero> and <numero>, translate to events IDs between <numero> and <numero>. Ciascun blocco funziona su un intervallo di righe del database Cronologia che viene tradotto in un'istruzione SQL per un intervallo di ID di eventi cronologia.
- ▶ Collect non-history data from the history DB. Si eseguono operazioni di pulizia sul database Cronologia per eliminare gli elementi del modello di classe che non esistono o non sono cronologici. Questo passaggio raccoglie i dati rilevanti da gestire in un secondo momento.
 - ▶ Recover cleanup data from file <nome>. L'aggiornamento è stato eseguito prima. I dati rilevanti per pulire lo schema sono stati raccolti prima e sono disponibili nel file.
 - ▶ Collect data from table for type <nome>. I dati da pulire vengono raccolti separatamente per ciascuno dei tipi di attributo.
 - ▶ Class <nome>, attribute <nome> is monitored in history DB. Elenco di tutti gli attributi per ciascuna classe nel modello di classe con voci nel database Cronologia.
 - ▶ Summary of all collect data from History DB. I messaggi di registro seguenti contengono i dati raccolti raggruppati per nome di classe.
 - ▶ Class <nome>, attributes [<elenco di nomi>] are monitored in history DB. Nuovo elenco di tutti gli attributi per tutte le classi con voci nel database Cronologia raggruppati per nome di classe.

- Cleanup problems found in the history DB. I messaggi di registro seguenti specificano tutti i dati da rimuovere dal database Cronologia poiché non sono coerenti con il modello di classe.
 - Class <nome> exists in history DB but not in class model. The class will be removed from the history DB.
 - Link Class <nome> is not marked as monitored for change. The class will be removed from the history DB. (Link classes must have the qualifier TRACK_LINK_CHANGES to be monitored)
 - Attribute <nome> in Class <name> exists in history DB but not in class model. The attribute will be removed from the history DB.
 - Attribute <nome> in Class <nome> exists in history DB but not marked as monitored for change. The attribute will be removed from the history DB.
 - Class <nome> has no attributes marked as monitored for change. The class will be removed from the history DB.
- Get colliding rules. In caso di unione di attributi da eseguire nell'ambito dei cambiamenti nel modello di classe è necessario identificare tali attributi per gestirli.
 - Skipped - Attribute name: <nome> Class name: <nome> was not found in old ClassModel. Messaggio di registro non significativo.
 - Classes <elenco di nomi> have history qualifiers. Queste classi hanno attributi che si possono unire. Il passaggio successivo verifica questa situazione.
 - Classes <elenco di nomi> has renamed attributes with CopyAttributeFromAttribute. Queste classi hanno attributi che erano l'origine dei dati per i dati degli attributi uniti.
 - Add remove data to configuration for merge rules:
 - Attribute <nome> in Class <nome> has colliding renaming rules. Questo attributo ha almeno due attributi nel precedente modello di classe che sono mappati a esso stesso.
 - Attribute <nome> in Class <nome> will receive its value from <nome attributo precedente>. Stabilisce l'origine dati dell'attributo.

Attribute <nome> in Class <nome> has more than one rename (including alias) without copyAttributeFromAttribute rule. Tutti gli attributi uniti non sono definiti come origine dati per il nuovo attributo. Selezionare un attributo precedente in modo arbitrario come origine dati.

In class <nome> the following attributes will be removed because of merging: <elenco nomi attributi precedenti>. Riepilogo di tutti gli attributi per classe da rimuovere in seguito all'unione.

- Removes history events that contain removed class model classes. Questo passaggio trova tutte le classi da rimuovere dal database Cronologia.
 - Class remove rule: oldClassName (object) = <nome>
 - Class remove rule: oldClassName (link) = <nome>
 - Class remove rule: oldClassName (cleanup) = <nome>. La regola è stata creata nella fase di pulizia.
 - Executing SQL statement for remove class between event id <numero> and <numero>. Statement: <istruzione SQL>. Eseguire la rimozione delle classi nel blocco corrente.
- Removes history events that contain removed class model attributes. Questo passaggio trova tutti gli attributi da rimuovere dal database Cronologia.
 - Attribute remove rule: oldClassName = <nome>, oldAttributeName <nome>, attribute type = <nome>
 - Attribute remove rule (cleanup): oldClassName = <nome>, oldAttributeName <nome>, attribute type = <nome>. La regola è stata creata nella fase di pulizia.
- Upgrades records that contain renamed class model attributes. Questo passaggio trova tutti gli attributi da rinominare nel database Cronologia.
 - Attribute rename rule: oldClassName = <nome>, oldAttributeName <nome>, new attribute name = <nome>, attribute type = <nome>

- Upgrades records that contain renamed class model classes. Questo passaggio trova tutte le classe da rinominare nel database Cronologia.
 - Class rename rule: oldClassName (object) = <nome> new class name = <nome>
 - Class rename rule: oldClassName (object) = <nome> new class name = <nome>
 - Executing SQL statement for rename class between event id <numero> and <numero>. Statement: <istruzione SQL>
- Upgrades records that contain snapshot result. Questo passaggio trova tutte le istantanee da aggiornare nel database Cronologia.
 - Executing SQL statement on snapshots between event id <numero>
 - ExecuteBatch for snapshot is done in seconds

Gestione dei dati non coerenti

Esegue le operazioni riportate di seguito:

- Rimuove i collegamenti dove uno degli oggetti dell'estremità viene rimosso durante l'aggiornamento.
- Esegue eliminazioni ricorsive se necessario.
- Ricalcola il valore degli attributi definiti come attributi calcolati per tutti gli oggetti e i collegamenti.

È critico (S/N)	Può essere rieseguito (S/N)
N	S

Implicazioni in caso di errore

I dati sono incoerenti quindi possono influire sui valori degli attributi che vengono calcolati. L'esecuzione dello strumento di coerenza del database al termine dell'aggiornamento rimuove i collegamenti solo se manca uno degli oggetti dell'estremità.

File di registro

I messaggi di registro seguenti vengono visualizzati nel registro breve dell'aggiornamento:

- Found x objects/links that were removed during upgrade. Numero di oggetti e collegamenti rimossi durante l'aggiornamento.
- Found x dangling links. Numero di collegamenti tralasciati in fase di rimozione.
- Found x recursive-delete objects. Numero di oggetti rimossi a causa di eliminazione ricorsiva.
- Updating calculated attributes for type CLASS_NAME (x instances, y bulks). Riga di ciascun tipo di oggetto/collegamento per il ricalcolo dell'attributo in fase di esecuzione.

Ricalcolare gli ID generati non casualmente

Nota: solo aggiornamento delle risorse.

Ricalcola gli ID per tutti gli oggetti per i quali gli ID non sono casuali ma vengono calcolati in funzione del tipo e delle proprietà chiave.

È critico (S/N)	Può essere rieseguito (S/N)
S	S

File di registro

Nessuno

Popolare ID globali

Nota: solo aggiornamento delle risorse.

UCMDB standalone funziona come un CMS e richiede per ciascun CI un ID globale. Questo passaggio popola la colonna degli ID globali in una tabella di dati radice.

È critico (S/N)	Può essere rieseguito (S/N)
N	S

Implicazioni in caso di errore

Potrebbe causare CI privi di ID globale. Ciò potrebbe essere un problema significativo quando si utilizzano integrazioni o distribuzioni complesse di UCMDB.

Soluzione alternativa. Si possono utilizzare i servizi di istanze multiple del CMDB dopo l'aggiornamento per risolvere questo problema:

- ▶ Se si rende necessario un server generatore di ID globali, si dovrà fare in modo che sia un generatore di ID non globali e poi un generatore di ID globali.
- ▶ Se si rende necessario un server generatore di ID non globali, si dovrà fare in modo che sia un generatore di ID globali e poi un generatore di ID non globali.

File di registro

Nessuno.

Individuazione - Configurazione dell'aggiornamento

Nota: solo aggiornamento delle risorse.

Ricalcola gli ID per i CI di configurazione di GFD.

È critico (S/N)	Può essere rieseguito (S/N)
S	N

Implicazioni in caso di errore

L'individuazione potrebbe non funzionare affatto. Se si salta questo passaggio, è necessario eseguire le operazioni riportate di seguito:

- 1** Disabilitare i tre strumenti di aggiornamento
- 2** Esportare i pacchetti utenti dal CMDB precedente.
- 3** Aggiornare tutti i pacchetti manualmente mediante lo strumento di migrazione pacchetto. Per i dettagli consultare "Aggiornamento dei pacchetti dalla versione 8.04 alla 9.02" a pag. 257.
- 4** Prima del processo di aggiornamento rimuovere le istanze seguenti dei CI di configurazione di individuazione dal CMDB:
 - domain
 - discoveryjob
 - discoverymodule
 - cmdbclass
 - discoverypattern
 - discoverywizard
 - discoveryprobegateway
 - discoveryprobemanager
 - discoveryresource
 - discoverytql
 - triggers
 - management
- 5** Dopo il processo di aggiornamento importare i pacchetti aggiornati.

File di registro

- Starting upgrade Discovery Configuration CIs.
- Upgrade Discovery Configuration CIs was successfully finished!
- Failed to upgrade some Discovery Configuration CIs.

- About to get discovery configuration CIs and links from server.
- Finish getting discovery configuration CIs and links from server. Carica le istanze dei CI di configurazione di individuazione dal CMDB.
- About to remove old Discovery Configuration CIs.
- Finish removing old Discovery Configuration CIs. Rimuove i CI precedenti dal CMDB. I CI ora esistono solo nella cache. Un errore in questo passaggio potrebbe causare perdita di dati.
- About to update discovery configuration CIs.
- Finish updating [amount of CIs] discovery configuration CIs. Aggiorna i CI e li salva nel CMDB.
- Failed to add CI [new CI id, CI type], (old CI [old CI id]) skipped. Non è stato possibile aggiornare un determinato CI nello schema. Per maggiori dettagli, verificare il registro degli errori.
- About to update links related to discovery configuration CIs.
- Finish updating links related to discovery configuration CIs. Nuova creazione dei collegamenti tra CI. Un errore in questo passaggio potrebbe causare incoerenza dei dati.

Federazione - Rimuovere la configurazione precedente

Rimuove i dati della configurazione di federazione precedente (nuova configurazione in fase di distribuzione).

È critico (S/N)	Può essere rieseguito (S/N)
S	S

Implicazioni in caso di errore

Potrebbe causare il mancato funzionamento della federazione o della replica.

Soluzione alternativa. Utilizzare l'operazione JMX **deleteByClassType** (in Model Services) per rimuovere tutte le istanze del CIT **fcmdb_configuration**. Per i dettagli sull'utilizzo della console JMX consultare .

File di registro

Per i messaggi di registro consultare i file di registro `cmdb.model.audit.short.log` e `cmdb.model.audit.detailed.appended`.

Ridistribuire i pacchetti di base

Nota: solo aggiornamento delle risorse.

Distribuisce i pacchetti predefiniti del CMDB. Gli aggiornamenti del modello di classe in questo passaggio sono limitati alle aggiunte soltanto quindi i pacchetti predefiniti non rimuovono attributi aggiunti dall'utente.

È critico (S/N)	Può essere rieseguito (S/N)
N	S

Implicazioni in caso di errore

In caso di errore è possibile ridistribuire questi pacchetti da UCMDB stesso. Eventuali aggiunte eseguite dall'utente a queste classi potrebbero andare perse nella ridistribuzione.

File di registro

Per i messaggi di registro consultare il file di registro `mam.packaging.log`.

Convalidare il modello di classe aggiornato

Nota: solo aggiornamento delle risorse.

Fornisce la convalida che il modello di classe aggiornato sia compatibile con BDM e CMS rispetto a un modello di classe della classe predefinita della versione 9.02. Le entità del modello di classe mancanti vengono aggiunte.

Il modello di classe esistente nel database prima di questo passaggio (aggiornamento + pacchetti) viene scritto nel file

C:\hp\UCMDB\UCMDBServer\runtime\upgraded-after-packages-class-model.xml. Il modello di classe aggiornato viene scritto nel file

C:\hp\UCMDB\UCMDBServer\runtime\upgraded-fixed-after-packages-class-model.xml.

Se il modello di classe viene cambiato durante questo passaggio, viene riaggiornato nel database.

È critico (S/N)	Può essere rieseguito (S/N)
N	S

Implicazioni in caso di errore

Un errore in questa fase non causa errore nell'intero processo di aggiornamento. È comunque necessario tenerlo in seria considerazione poiché l'errore indica che il modello di classe utente non è completo e non è compatibile con CMS e Business Service Management.

File di registro

Per i dettagli consultare "Convalidare il modello di classe" a pag. 189.

Individuazione - Statistiche dell'aggiornamento

Rinomina i tipi CI nella tabella **CCM_DISCOVERY_STATS** nel CMDB (informazioni sulla cronologia di individuazione).

È critico (S/N)	Può essere rieseguito (S/N)
N	S

Implicazioni in caso di errore

Le informazioni sulle statistiche di esecuzioni di individuazione precedenti sono andate perdute. Se si salta questo passaggio sarà necessario troncane la tabella **CCM_DISCOVERY_STATS** nel CMDB.

File di registro

- Starting upgrade CCM_DISCOVERY_STATS table.
- Upgrade 'CCM_DISCOVERY_STATS' table was successfully finished!
- Failed to upgrade 'CCM_DISCOVERY_STATS' table.
- Ci type [tipo CI precedente] has been upgraded to [nuovo tipo CI]. Indica che un tipo CI precedente è stato rinominato nel nuovo tipo CI.
- failed to update [tipo CI precedente], skipped. Indica che non è stato possibile cambiare un tipo CI in base al nuovo schema. Potrebbe essere dovuto a incoerenza dei dati nel CMDB o che il tipo CI errato è stato definito dall'utente. Non influenza l'individuazione ma la riga nel pannello delle statistiche relative a questo CI viene visualizzata in rosso.

Individuazione - Aggiornamento delle risorse

Nota: solo aggiornamento delle risorse.

Aggiorna le risorse di individuazione: sequenze, processi e moduli (dati di configurazione dell'individuazione).

È critico (S/N)	Può essere rieseguito (S/N)
S	S

Implicazioni in caso di errore

Stesso passaggio di "Individuazione - Configurazione dell'aggiornamento" a pag. 237.

File di registro

- Starting upgrade discovery resources.
- Upgrade discovery resources have been successfully finished!
- Upgrade discovery resources have been finished. Failed to upgrade the following resources: [nome risorsa1], [nome risorsa2], ...

- File containing resources to filter, upgrade/filtered_resources.xml, not found. Impossibile trovare il file che contiene l'elenco delle risorse da rimuovere durante l'aggiornamento, nessuna risorsa è stata rimossa.
- Resource [nome risorsa] of type [sottosistema] was successfully updated. Indica che la risorsa è stata aggiornata correttamente.
- Failed to upgrade res [nome risorsa] of type [sottosistema]/ The resource might be already compatible with new schema. Please check resource manually. La risorsa non è stata aggiornata. Verificare la risorsa manualmente dopo l'avvio del CMDB. Nella maggior parte dei casi questi errori seguono dopo un altro messaggio di registro con maggiori dettagli.

Caricare risorse aggiornate

Nota: solo aggiornamento delle risorse.

Carica le risorse aggiornate create nel passaggio precedente "Individuazione - Aggiornamento delle risorse" a pag. 242 dal disco nel database.

Nota: le risorse aggiornate dei pacchetti predefiniti hanno la precedenza sulle risorse utente. Ciò significa che se la stessa risorsa (nome e tipo) esiste nei pacchetti predefiniti e nella cartella delle risorse aggiornate, la versione finale è quella dei pacchetti predefiniti.

È critico (S/N)	Può essere rieseguito (S/N)
S	S

Implicazioni in caso di errore

Le risorse aggiornate non vengono caricate nel database. Le risorse predefinite sono già nel database dopo il passaggio "Ridistribuire i pacchetti di base" a pag. 240. Solo le risorse utente mancano dal database.

File di registro

- got <conteggio> <tipo> from disk. Specifica il numero di risorse per ciascun tipo recuperato dal disco. Il messaggio è seguito dall'elenco delle risorse.
- Could not get resources map - all resources will be deployed from disk. I pacchetti predefiniti distribuiti nel database non possono essere recuperati. Le risorse predefinite non possono avere la precedenza sulle risorse utente quindi tutte le risorse utente vengono caricate nel database e sovrascrivono le risorse predefinite con lo stesso nome e tipo.
- did not success to add business view enrichment <nome>. Verificare la descrizione del problema nell'eccezione allegata.
- did not success to add gold master definition <nome>. Verificare la descrizione del problema nell'eccezione allegata.
- Resource <nome> does not exist in CMDB and should be added. La risorsa è una risorsa utente e viene caricata nel database.
- Resource <nome> could not be loaded because of missing dependencies: <elenco nomi>. La risorsa non può essere caricata nel database poiché altre risorse necessarie non esistono nel database. Al termine dell'aggiornamento è possibile rieseguire questo passaggio per caricare le risorse.
- Upgraded resource <nome> and out-of-the-box resource are the same, not loading upgraded resource. La risorsa predefinita non è stata cambiata dall'utente.
- Upgraded resource <nome> is not loaded since a different out-of-the-box resource with the same type and name already exists. L'utente ha cambiato la risorsa predefinita e sta perdendo i cambiamenti apportati.
- Failed to add <tipo> <nome>. La risorsa del tipo specifico non è stata caricata.

Aggiornamento delle istantanee

I dati delle istantanee vengono memorizzati nel CMDB.

È critico (S/N)	Può essere rieseguito (S/N)
N	S

File di registro

Nessuno.

Individuazione - Ricrittografare il documento dell'ambito del dominio

Nota: solo aggiornamento delle risorse.

Ricrittografa il file **domainScopeDocument** dalla crittografia DES (utilizzata nella versione 8.0x) alla crittografia AES.

È critico (S/N)	Può essere rieseguito (S/N)
N	S

Implicazioni in caso di errore

L'individuazione potrebbe non funzionare affatto. Se si salta questo passaggio è necessario eseguire le operazioni seguenti:

- 1** Esportare il file **domainScopeDocument** dal CMDB precedente.
- 2** Dopo il processo di aggiornamento importare il file **domainScopeDocument**. Per i dettagli consultare "Esportare e importare le informazioni sulle credenziali e sull'intervallo in formato crittografato" a pag. 332.

File di registro

- Upgrade process of DomainScopeDocument re-encryption to AES had been started.
- Upgrade process of DomainScopeDocument re-encryption to AES had been finished successfully.
- Upgrade process of DomainScopeDocument re-encryption to AES had been failed.
- DSD is empty - doing nothing... Indica che il file **domainScopeDocument** è vuoto e quindi questo passaggio è ridondante e non eseguirà alcuna operazione.
- The DSD already encrypted by AES - doing nothing... Indica che il file **domainScopeDocument** è già crittografato in base a AES; il passaggio è ridondante e non eseguirà alcuna operazione.
- The DSD is encrypted by 3DES... Indica che il file **domainScopeDocument** è già crittografato in base a 3DES quindi viene ricrittografato in base a AES.
- Failed to decrypt DSD by 3DES. Indica che il processo di crittografia del file **domainScopeDocument** non è riuscito (questo passaggio non ha ricrittografato il file **domainScopeDocument** in base ad AES); è necessario importare il file **domainScopeDocument** nel sistema UCMDB dopo il processo di aggiornamento.
- Failed to decrypt DSD by AES. Il passaggio non è riuscito. È necessario importare il file **domainScopeDocument** nel sistema UCMDB dopo il processo di aggiornamento.
- Got empty DSD after AES encryption. Il passaggio non è riuscito. È necessario importare il file **domainScopeDocument** nel sistema UCMDB dopo il processo di aggiornamento.
- Got empty DSD after 3DES decryption. Il passaggio non è riuscito. È necessario importare il file **domainScopeDocument** nel sistema UCMDB dopo il processo di aggiornamento.
- Failed to decrypt the DSD by AES and 3DES. Il passaggio non è riuscito. È necessario importare il file **domainScopeDocument** nel sistema UCMDB dopo il processo di aggiornamento.

Individuazione - Aggiornamento del documento dell'ambito del dominio

Nota: solo aggiornamento delle risorse.

Rinomina i tipi CI e gli attributi nel file **domainScopeDocument**.

È critico (S/N)	Può essere rieseguito (S/N)
N	S

Implicazioni in caso di errore

Consultare "Individuazione - Ricrittografare il documento dell'ambito del dominio" a pag. 245.

File di registro

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

Individuazione - Copiare le credenziali in Confidential Manager

Nota: solo aggiornamento delle risorse.

Estrae le informazioni sulle credenziali dal file **domainScopeDocument** in Confidential Manager. Le informazioni sulle credenziali del file **domainScopeDocument** sono sostituite dagli identificatori di Confidential Manager. Per i dettagli consultare "Confidential Manager" a pag. 387.

È critico (S/N)	Può essere rieseguito (S/N)
N	S

Implicazioni in caso di errore

Stesso procedimento del passaggio "Individuazione - Ricrittografare il documento dell'ambito del dominio" a pag. 245.

File di registro

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

Individuazione - Aggiornamento degli identificatori delle credenziali

Nota: solo aggiornamento delle risorse.

Aggiornamento dell'attributo **credential_id** sui CI nel CMDB in modo che corrispondano agli identificatori di Confidential Manager.

È critico (S/N)	Può essere rieseguito (S/N)
N	S

Implicazioni in caso di errore

L'attributo delle credenziali di CI esistenti contiene dati errati. Se si salta questo passaggio è necessario eseguire un'individuazione massiccia per ricostruire i dati.

File di registro

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

- Upgrade process of credentials_id's update had been failed.
- Failed to get layout (and update credentials id) for object of type <tipo>. Indica che il processo di aggiornamento per il tipo <tipo> non è riuscita, quindi i CI di tipo <tipo> potrebbero contenere ID delle credenziali obsoleti. Al termine del processo di aggiornamento è necessario rieseguire un'individuazione massiccia sul sistema.

Copiare la configurazione dei report

Nota: solo aggiornamento delle risorse.

Copia la configurazione dei report dal database Foundation nel nuovo database Management.

È critico (S/N)	Può essere rieseguito (S/N)
N	S

Implicazioni in caso di errore

I filtri preferiti della versione 8.0x non sono supportati e la relativa pianificazione non è disponibile.

File di registro

- failed to upgrade report: <nome report>.

Copiare informazioni sulla pianificazione delle istantanee

Nota: solo aggiornamento delle risorse.

Copia i dati di pianificazione delle istantanee dal database Foundation nelle nuove tabelle di gestione nel CMDB. Rimuove anche i processi pianificati dei tipi non più rilevanti (esecuzione TQL, ricostruzione viste e distribuzione pacchetti).

È critico (S/N)	Può essere rieseguito (S/N)
N	S

Implicazioni in caso di errore

Le istantanee pianificate non sono state aggiornate quindi si devono ridefinire.

File di registro

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

Impostazioni di aggiornamento

Nota: solo aggiornamento delle risorse.

Rinomina i tipi CI nelle impostazioni selezionate.

È critico (S/N)	Può essere rieseguito (S/N)
N	S

Implicazioni in caso di errore

Se i nomi di classe esistevano in Gestione impostazioni ed è stato cambiato il nome dallo strumento di aggiornamento del modello di classe, è possibile rilevare un comportamento strano dell'applicazione a seconda dell'impostazione.

Esempio: il CIT radice e la relazione sono definiti. L'impostazione aggiuntiva è l'URL frontend. Se è definito un bilanciamento del carico, è possibile che sia necessario ridefinire l'URL frontend. Le impostazioni del proxy inverso non sono interessate.

File di registro

- SettingsClassModelUpgrader failed o uno specifico con il prefisso non è riuscito nell'aggiornamento.

Aggiornamento del modello di protezione

Nota: solo aggiornamento delle risorse.

Aggiornamento delle autorizzazioni in base al nuovo modello ACL.

È critico (S/N)	Può essere rieseguito (S/N)
N	S

Implicazioni in caso di errore

Alcune autorizzazioni sono allineate con il nuovo modello ACL ma alcune non lo sono. Gli amministratori devono accedere a Gestione protezione e verificare che tutte le autorizzazioni sono come richiesto e, in caso contrario, impostarle di conseguenza.

File di registro

- Role [<role name>] failed to get permissions due to the following error:...

Eliminare dati precedenti

Nota: solo aggiornamento delle risorse.

Rimuove le tabelle di dati precedenti (tabelle TEMP).

È critico (S/N)	Può essere rieseguito (S/N)
N	S

Implicazioni in caso di errore

UCMDB funziona correttamente ma potrebbe essere più lento a causa di garbage presente nelle tabelle. È possibile rimuovere manualmente tutte le tabelle con prefisso **TEMP**.

File di registro

Nessuno.

Utente rispetto a valori predefiniti

Nota: solo aggiornamento delle risorse.

Mettere a confronto il modello di classe con il modello di classe predefinito per decidere per ognuna delle entità del modello di classe se si tratta di un'entità utente o di un'entità predefinita.

È critico (S/N)	Può essere rieseguito (S/N)
N	S

Implicazioni in caso di errore

Tutte le entità del modello di classe sono contrassegnate come entità predefinite. Talune operazioni sul modello di classe sono chiuse all'utente per le entità predefinite.

File di registro

I messaggi seguenti indicano problemi nel modello di dati. L'entità specificata nel messaggio è un'entità predefinita che manca nel modello di classe utente. Si potrebbe trattare di un problema precedente nella distribuzione del Content Pack 6.00 oppure nel processo di aggiornamento.

I passaggi interessati potrebbero essere uno o più di uno dei seguenti:

- "Convalidare il modello di classe" a pag. 189.
- "Aggiornamento del modello di classe su disco" a pag. 195.
- "Aggiornare il modello di classe nel database" a pag. 221.
- "Ridistribuire i pacchetti di base" a pag. 240.
- "Convalidare il modello di classe aggiornato" a pag. 240.
- !!! Class <nome> doesn't exist in the upgraded class model.
- !!! Class <nome> is missing qualifiers in the upgraded class model. The qualifiers are: <elenco nomi>.
- !!! Attribute <nome> in Class <nome> is missing from the upgraded class model.
- !!! Attribute <nome> in Class <nome> is missing qualifiers in the upgraded class model. The qualifiers are: <elenco nomi>.
- !!! Attribute Override <nome> was removed in Class <nome> and is missing qualifiers in the upgraded class model. The qualifiers are: <elenco nomi>.
- !!! Attribute Override <nome> in Class <nome> is missing qualifiers in the upgraded class model. The qualifiers are: <elenco nomi>.
- !!! Class <nome> is missing method <nome> in the upgraded class model.
- !!! Method <nome> in Class <nome> is missing qualifiers in the upgraded class model. The qualifiers are: <elenco nomi>.
- !!! Valid Link <nome> is missing in the upgraded class model.
- !!! Valid Link <nome> is missing qualifiers in the upgraded class model. The qualifiers are <elenco nomi>.
- !!! Calculated Link <nome> with Class <nome> is missing in the upgraded class model.

- !!! Calculated Link <nome> with Class <nome> is missing triplet in the upgraded class model. The triplet is <terna>.
- !!! Enum <nome> doesn't exist in the upgraded class model.
- !!! List <nome> doesn't exist in the upgraded class model.
- !!! Enum entry with key <numero> and value <valore> in Enum <nome> doesn't exist in the upgraded class model.
- !!! List entry <valore> in List <nome> doesn't exist in the upgraded class model.

Popolare l'attributo IPv6

Copia il valore IP dall'attributo del nome nel nuovo attributo IPAddressValue nella classe IPAddress nella forma normalizzata IPv6.

È critico (S/N)	Può essere rieseguito (S/N)
S	S

Implicazioni in caso di errore

L'individuazione potrebbe non funzionare.

Soluzione alternativa. L'update deve essere eseguito su IP e sottoreti IP nel CMDB. L'update può essere eseguito manualmente dall'interfaccia utente (uno alla volta).

File di registro

Per i messaggi di registro consultare il file di registro **cmdb.reconciliation.log**.

Aggiornamento guidato dell'accrescimento

Chiama accrescimenti predefiniti per aggiornare i dati nell'ambito del processo di aggiornamento.

1. Aggiorna l'attributo del nome nel dominio J2EE per rimuovere il suffisso (tutti i caratteri dopo '@').

2. Aggiorna l'attributo di nome nel gruppo di risorse cluster, lo fornisce di suffisso dal valore del rispettivo attributo di chiave host (tutti i caratteri dopo ':').
3. Rimuove i CI di archivio del report precedenti che non vengono aggiornati.

È critico (S/N)	Può essere rieseguito (S/N)
N	S

Definire le regole di riconciliazione degli attributi chiave

Nota: solo aggiornamento delle risorse.

Aggiunge una regola di riconciliazione di tipo 'attributi chiave' a un tipo CI dell'utente con gli attributi chiave.

È critico (S/N)	Può essere rieseguito (S/N)
N	S

Implicazioni in caso di errore

Un CIT definito dall'utente identificato dagli attributi chiave nella versione 8.00 utilizza la rispettiva regola di riconciliazione padre.

La regola di identificazione dell'attributo chiave può essere aggiunta in un secondo momento da un JMX del pacchetto/riconciliazione.

File di registro

Nessuno.

Aggiornamento Gestione pacchetti

Nota: solo aggiornamento delle risorse.

Aggiorna le informazioni sui pacchetti memorizzate nel modello del server UCMDB.

Il file di configurazione dell'aggiornamento di Gestione pacchetti si trova in **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\PackageManagerUpgrade\config.xml (cmdb.jar)**. La configurazione elenca i sottosistemi obsoleti e le regole di ridenominazione del sottosistema.

Lo strumento di aggiornamento di Gestione pacchetti esegue i passaggi seguenti:

- 1** Rimuove le risorse dei sottosistemi obsoleti dai pacchetti
- 2** Rinomina i nomi dei sottosistemi precedenti con i nuovi
- 3** Aggiorna i nomi delle risorse del modello di classe utilizzati da Gestione pacchetti
 - a** Cambia i nomi delle classi nelle definizioni di classe
 - b** Cambia i nomi delle classi nelle definizioni dei collegamenti validi
 - c** Cambia i nomi delle classi nelle terne delle definizioni dei collegamenti calcolati
- 4** Rimuove le risorse inesistenti dai pacchetti

È critico (S/N)	Può essere rieseguito (S/N)
N	S

Implicazioni in caso di errore

Informazioni non corrette sui pacchetti possono causare la creazione di file di pacchetto non corretti durante l'esportazione dei pacchetti e possono causare errore durante il ritiro di un pacchetto.

File di registro

Nessuno.

15

Aggiornamento dei pacchetti dalla versione 8.04 alla 9.02

Questo capitolo comprende:

Concetti

- Utilità di migrazione pacchetto - Panoramica a pag. 258

Compiti

- Migrare un pacchetto personalizzato a pag. 259

Riferimenti

Risoluzione dei problemi e limitazioni a pag. 262

Concetti

Utilità di migrazione pacchetto - Panoramica

In questo capitolo viene spiegato come utilizzare l'utilità di migrazione pacchetto per la migrazione dei pacchetti personalizzati in HP Universal CMDB (UCMDB) dalla versione 8.04 a 9.02.

I pacchetti personalizzati creati prima di eseguire l'aggiornamento del sistema alla versione 9.02 possono contenere le risorse che non sono supportate nella nuova versione. Per ridurre il rischio di problemi in questi pacchetti personalizzati, si consiglia di migrare i pacchetti offline utilizzando l'utilità di migrazione pacchetto fornita prima di distribuire i pacchetti nel sistema UCMDB versione 9.02.

L'utilizzo dell'utilità di migrazione pacchetto per la migrazione di pacchetti personalizzati offline offre i vantaggi seguenti:

- ▶ Non è richiesto alcun tempo di inattività.
- ▶ La migrazione dei pacchetti personalizzati può essere completata prima della distribuzione nel sistema, con conseguente riduzione dei rischi.
- ▶ È possibile migrare i pacchetti, distribuirli subito e procedere poi alla reindividuazione dei dati.
- ▶ I pacchetti con contenuto HP possono essere migrati in un solo processo, riducendo il rischio di contenuto danneggiato.

L'utilità di migrazione pacchetto consente di eseguire offline la migrazione su pacchetti personalizzati senza dover ricorrere al server.

Compiti

Migrare un pacchetto personalizzato

La procedura seguente spiega come migrare i pacchetti personalizzati a HP Universal CMDB versione 9.02.

Per migrare i pacchetti personalizzati:

- 1 Collocare i pacchetti personalizzati da migrare in una directory separata insieme ai pacchetti dai quali dipendono le risorse sottoposte ad aggiornamento. Ad esempio:
 - Se un pacchetto personalizzato contiene una vista o una regola di accrescimento che dipende da una definizione TQL che risiede in un altro pacchetto, collocare il pacchetto che contiene la definizione TQL in una directory con il pacchetto personalizzato.
 - Se un pacchetto personalizzato ha un riferimento a una definizione di classe personalizzata non fornita da nessuno dei pacchetti predefiniti, collocare il pacchetto con la definizione di classe personalizzata nella directory con il pacchetto personalizzato.
- 2 Accertarsi di disporre dei file XML della definizione di modello di classe precedente, ovvero il modello di classe della versione di UCMDDB (7.0 o 7.5) con la quale è stato creato il pacchetto.

Per creare il modello di classe, accedere alla console JMX, passare a **CMDB Class Model Services** ed eseguire il metodo **exportClassModelToXML**.

- 3 Eseguire lo script:
 - Windows: `C:\hp\UCMDB\UCMDBServer\tools\packupgrade.bat`
 - Solaris:
`C:/hp/UCMDB/UCMDBServer/2f/packupgrade/bin/packupgrade.sh`

La sintassi per eseguire lo script è indicata di seguito. (Questa informazione può essere visualizzata eseguendo lo script senza argomenti.)

```
packupgrade -cm {CLASS_MODEL_DEF_FILE} [-u {UPGRADE_CONFIG_FILE}] [-  
exclude <package(s)>] -out {OUTPUT_DIR} {INPUT_DIR}
```

-i. Accedere alla console JMX.

-cm {CLASS_MODEL_DEF_FILE}. Nome file della definizione di modello di classe precedente; questo file può essere creato tramite JMX: passare a **Class Model Services** nella console JMX e chiamare il metodo **exportClassModelToXml**.

-u {UPGRADE_CONFIG_FILE}. File di configurazione di aggiornamento.

-exclude {package(s)}. Pacchetto da escludere o elenco di nomi di pacchetti da escludere separati da virgola.

-filterResources {file path of filtered resources list}. Esclude le risorse elencate nel file XML fornito (il file XML deve essere conforme al file **schema\filtered_resources.xsd**).

-fullCM. Cambia l'aggiornamento del modello di classe in **full mode**. Nella modalità completa (full mode), vengono creati i pacchetti nuovi e il modello di classe viene trattato nella sua interezza, consentendo più convalide e correzioni. Nella modalità completa, i pacchetti si riferiscono all'intero modello di classe predefinito (almeno). Per impostazione predefinita, l'aggiornamento viene eseguito in **partial mode (modalità parziale)** che non prevede un trattamento completo.

-analyzeDataActions {DATA_ACTIONS_FILE}. Analizza i cambiamenti e genera il file di analisi delle azioni dei dati con il nome del file indicato. Implica **-fullCM**.

-outputFullCM {OUTPUT_FULL_CM_FILE}. Genera il nuovo modello di classe completo in un file. Implica **-fullCM**.

-out {OUTPUT_DIR}. Percorso della directory dei pacchetti aggiornati.

-doNotCreateNewPackages. Se questa opzione non è presente, il programma di aggiornamento non crea alcun file del nuovo pacchetto.

{INPUT_DIR}. Percorso della directory dei pacchetti da sottoporre ad aggiornamento.

Variabili di ambiente. **ucmdb.home**. Deve puntare alla directory del prodotto (di norma **C:\hp\UCMDB\UCMDBServer** per UCMDB standalone).

- 4 Individuare i pacchetti migrati nella directory di output fornita.
Distribuire i pacchetti migrati nel sistema UCMDB versione 9.02.

Riferimenti

Risoluzione dei problemi e limitazioni

- ▶ L'utilità di migrazione pacchetto è stata verificata solo per i pacchetti compatibili con UCMDB 8.04.
- ▶ I pacchetti di definizione di accrescimento che fanno riferimento a tipi CI eliminati o aggiornati non possono essere aggiornati utilizzando l'utilità di migrazione pacchetto.
- ▶ La migrazione parziale non è supportata. L'utilità di migrazione pacchetto non crea un nuovo pacchetto se una o più risorse non possono essere migrate correttamente.

Parte V

Disponibilità elevata e pianificazione della capacità

16

Installazione della modalità disponibilità elevata

Questo capitolo comprende:

Concetti

- Procedure consigliate per la disponibilità elevata di HP Universal CMDB a pag. 266
- Transizione tra server attivo e passivo a pag. 267

Transizione tra server attivo e passivo

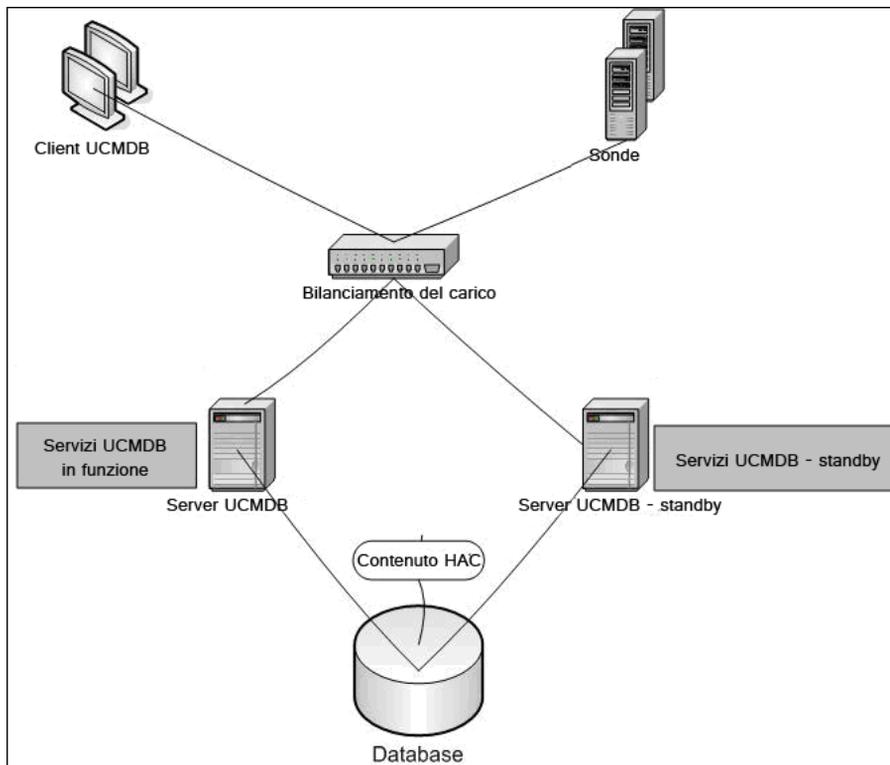
- Installare HP Universal CMDB in modalità disponibilità elevata a pag. 268
- Configurare la disponibilità elevata della rete a pag. 273
- Configurare il sito completo a pag. 274

Concetti

Procedure consigliate per la disponibilità elevata di HP Universal CMDB

In questa sezione vengono descritte le procedure consigliate per l'implementazione su campo della disponibilità elevata di HP Universal CMDB.

Diagramma della soluzione:



- Qualsiasi accesso esterno all'applicazione HP Universal CMDB viene eseguito tramite il bilanciamento del carico.

- Due o più server sono configurati.
- I servizi HP Universal CMDB vengono eseguiti su tutti i server del cluster ma i componenti del cliente sono attivi solo sul server attivo.
- Bilanciamento del carico con:
 - Mantenimento attivo su **http://<UCMDB-Server:port>/ping?clusterId=<clusterId>**.
 - Criterio round robin per i server.
 - La persistenza della sessione viene mantenuta.
 - L'IP virtuale viene configurato per cluster.
- Ciascun server è connesso a due reti separate:
 - Front-end (per l'accesso del bilanciamento del carico)
 - Back-end (per la comunicazione del database e del Controller disponibilità elevata)

Transizione tra server attivo e passivo

Per migliorare i tempi di avvio per i computer passivi durante una transizione dal computer attivo HP Universal CMDB avvia i computer passivi in modalità parziale.

In questo caso il componente topologia modello sui computer passivi viene avviato in modalità di sola lettura. Successivamente viene sincronizzato con i cambiamenti che si verificano sul server attivo, dal database di UCMDB, a distanza di secondi.

Quando entra in funzione il computer passivo si avvia rapidamente poiché la maggior parte del modello è già caricato in memoria.

Compiti

Installare HP Universal CMDB in modalità disponibilità elevata

In questa sezione viene descritto l'avvio dell'installazione e le procedure di configurazione quando HP Universal CMDB viene eseguito in modalità disponibilità elevata.

Nota: la modalità disponibilità elevata non è supportata in un ambiente con più clienti.

In questa sezione vengono trattati i seguenti argomenti:

- “Installare i server” a pag. 268
- “Completare l'avvio del server” a pag. 269
- “Configurare il server” a pag. 271
- “Configurare il bilanciamento del carico” a pag. 272
- “Configurare la sonda” a pag. 272

1 Installare i server

- a** Installare il server UCMDB su due o più computer senza eseguire la procedura guidata di configurazione (selezionare **No** quando richiesto dalla procedura guidata). La configurazione tipica è un server **attivo** e un server **passivo**.

Per i dettagli consultare “HP Universal CMDB Installazione su una piattaforma Windows” a pag. 71 o “HP Universal CMDB Installazione su una piattaforma Linux” a pag. 87

Nota: i computer utilizzati per i server UCMDB attivi e passivi devono disporre di hardware simile (in particolare la stessa quantità di memoria) e devono eseguire lo stesso sistema operativo.

- b** Eseguire la procedura guidata di configurazione sul server che deve fungere da server attivo. Selezionare **Crea un nuovo schema**. Per i dettagli consultare “Configurazione del server UCMDB” a pag. 101.
- c** Eseguire la procedura guidata di configurazione sul server passivo. Selezionare **Connettersi a un nuovo schema** e fornire i dettagli dello schema creato per il server attivo.
 - Per eseguire la procedura guidata dalla piattaforma Windows selezionare **Start > Tutti i programmi > HP UCMDB > Avvio della procedura guidata di configurazione di HP Universal CMDDB Server**.
 - Per eseguire la procedura guidata da una piattaforma Linux:

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

2 Completare l'avvio del server

- a** Avviare il server attivo. Attendere il completamento del processo di avvio.
- b** **Per Windows:** Accedere a **server_management.bat** (strumento Server Management) che si trova nella cartella seguente:
C:\hp\UCMDB\UCMDBServer\tools\.
Per Linux: eseguire **server_management.sh** che si trova nella cartella seguente: **/opt/hp/UCMDB/UCMDBServer/tools/.**
 - Nella pagina di accesso immettere il nome del server e le credenziali.
Se viene utilizzata la porta predefinita SSL (porta **8443**), immettere solo il nome del server (ad esempio **localhost**).
 - Se viene la porta SSL è stata cambiata, immettere il nome del server e la nuova porta (ad esempio **localhost:443**).

- Immettere il nome utente e la password dell'utente di sistema (i parametri predefiniti sono **sysadmin** e **sysadmin**).

Nota: la connessione dallo strumento a HP Universal CMDB viene eseguita tramite HTTPS. In caso di problemi di connessione, accertarsi che sia configurata la modalità **SSL (Abilita connessioni HTTP(S))** deve essere impostata su **true**.

- c** Nello strumento Server Management selezionare **Cluster** nel menu a sinistra. Fare clic sul pulsante **Nuovo cluster** per creare un nuovo cluster.
- d** Nella casella **Aggiungi server** immettere il nome del computer di uno dei server installati. Fare clic su **Aggiungi**. Ripetere i passaggi per gli altri server.
- e** Nell'elenco dei server selezionare il server che deve fungere da server attivo. Fare clic su **Imposta attivo**.
- f** Fare clic su **OK**.
- g** Rispondere **Sì** alla domanda sul passaggio di tutti i clienti esistenti a questo server attivo.

Nota: per cambiare utente o server fare clic sul collegamento **Disconnetti** per disconnettere lo strumento Server Management.

- h** Avviare il server passivo ed eseguire il file **server_management.bat** su quel server.

Nota: si può verificare un'incongruenza del server quando si utilizza lo strumento Server Management per convertire UCMDB Server da attivo a passivo. Per evitare questa evenienza, sul computer attivo, arrestare UCMDB Server. Dopo un breve periodo (circa un minuto), il server passivo diventa server attivo.

Tutti i server di un cluster devono utilizzare la stessa porta per HTTP, HTTPS e così via. Non è possibile configurare i due server per utilizzare porte diverse.

3 Configurare il server

- a** Selezionare **Amministrazione > Impostazioni infrastruttura categoria> Impostazioni generali**.
- b** Individuare e cambiare le impostazioni seguenti:
 - **L'URL front-end è abilitato dalle impostazioni?** deve essere impostato su **true**.
 - **URL front-end** deve essere impostato sull'URL del bilanciamento del carico. Il formato necessario è **URI://<nome server>:<porta>**.

4 Configurare il bilanciamento del carico

Definire l'IP virtuale per i due server HP Universal CMDB con la configurazione seguente:

- ▶ Selezionare la porta definita in Impostazioni infrastruttura.
- ▶ Verificare che non sia presente un criterio round robin per i server.
- ▶ Verificare che sia mantenuta la persistenza della sessione.
- ▶ Verificare che l'IP virtuale sia configurato per cluster.
- ▶ L'indirizzo di mantenimento per la sessione è: **http://<UCMDB-Server:port>/ping?clusterId=<clusterId>**. Un server attivo nel cluster restituisce la risposta HTTP 200 (OK). Un server passivo restituisce la risposta HTTP 503 (servizio non disponibile).

Nota: per il bilanciamento del carico è importante fornire l'ID cluster nella richiesta di mantenimento poiché un server può appartenere a diversi cluster ed essere attivo in uno e passivo in un altro.

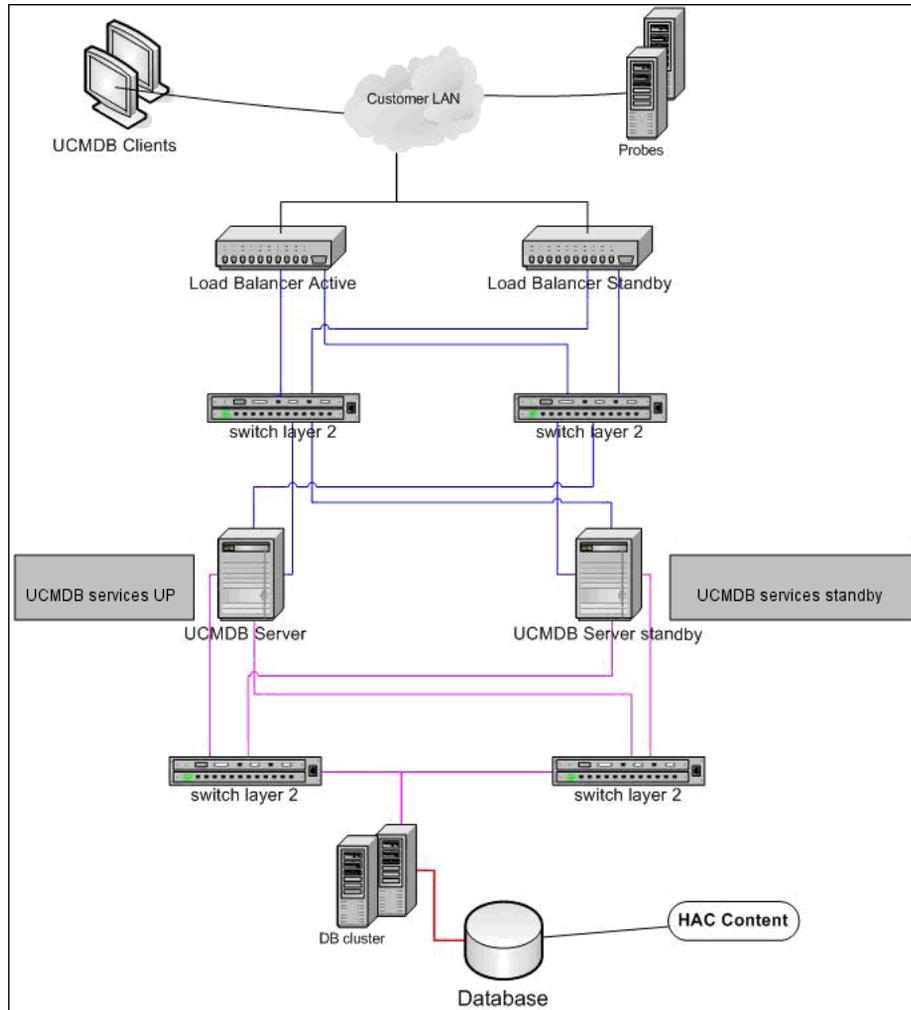
5 Configurare la sonda

- a** Eseguire l'installazione della sonda sul computer della sonda con l'indirizzo IP virtuale del bilanciamento del carico come nome di HP Universal CMDB Server.
- b** Avviare la sonda.

Configurare la disponibilità elevata della rete

Per distribuire la disponibilità elevata della rete connettere ai server i bilanciamenti del carico e i database tramite switch utilizzando la modalità Intel NIC con protocollo spanning tree (per Windows).

Diagramma della soluzione di configurazione della ridondanza di rete completa:



Configurare il sito completo

- ▶ La rete back-end deve essere definita sull'interfaccia principale (l'interfaccia collegata al nome del server). Se non è definita in questo modo, modificare il file `etc/hosts` per definire l'interfaccia back-end come collegata al nome del server.
- ▶ Durante l'installazione del server, l'hostname/IP back-end devono essere definiti come IP/HP Universal CMDB Server.

17

Pianificazione della grande capacità di HP Universal CMDB

Questo capitolo comprende:

Concetti

- Pianificazione della grande capacità - Panoramica a pag. 276
- Nodi gestiti e CI correlati ai nodi a pag. 277

Compiti

- Configurazione del server UCMDB a pag. 278
- Configurazione del database Oracle a pag. 278

Riferimenti

- Configurazione del test di sistema a pag. 279
- Risultati del test di sistema a pag. 280

Concetti

Pianificazione della grande capacità - Panoramica

La configurazione predefinita consente a HP Universal CMDB di utilizzare una distribuzione di oltre 25 milioni di oggetti e collegamenti. Per utilizzare una grande distribuzione, è necessario implementare la configurazione seguente:

- ▶ Aumentare il segmento di memoria (heap) del CMDB a 8 GB. Per i dettagli consultare "Configurazione del server UCMDB" a pag. 278.
- ▶ Se si utilizza un database Oracle, installare Oracle Database SGA come segue: 4 GB supportati, 8 GB consigliati. Per i dettagli consultare "Configurazione del database Oracle" a pag. 278.

Nella tabella seguente viene visualizzato il numero massimo supportato di CI e collegamenti per una distribuzione di UCMDB:

Database/Sistema operativo	Windows	Linux
MS SQL Server	40 milioni di CI e collegamenti	12,5 milioni di CI e collegamenti
Oracle	40 milioni di CI e collegamenti (configurazione richiesta come descritto in questa sezione)	40 milioni di CI e collegamenti (configurazione richiesta come descritto in questa sezione)

Per maggiori dettagli su:

- ▶ I cambiamenti da apportare alla configurazione di sistema per supportare questa capacità, consultare "Configurazione del server UCMDB" a pag. 278.
- ▶ Come migliorare le prestazioni, consultare "Configurazione del database Oracle" a pag. 278.

- ▶ La configurazione utilizzata per la verifica della capacità, consultare "Configurazione del test di sistema" a pag. 279.
- ▶ I risultati delle prestazioni dell'esecuzione del test del sistema su UCMDB 9.02, consultare "Risultati del test di sistema" a pag. 280.

Nodi gestiti e CI correlati ai nodi

Quando si pianifica la capacità, tra le altre problematiche, è necessario tenere presente il rapporto dei nodi gestiti nel CMDB e i CI correlati ai nodi. I CI correlati ai nodi devono includere tutti i CI dei tipi che sono sottoclassi di risorsa di applicazione, elemento di nodo o software.

Nella tabella seguente viene elencato il numero di CI correlati ai nodi che si possono individuare per ciascun nodo gestito nel proprio ambiente. Questo numero dipende dalla dimensione della distribuzione e dal numero di nodi gestiti, maggiori sono i nodi gestiti da mantenere nel CMDB, minori sono i CI correlati ai nodi che si possono individuare per ciascun nodo gestito.

Ad esempio, in una distribuzione Enterprise se si eseguono 89.600 nodi gestiti, è possibile individuare 160 CI correlati agli host per ciascun host gestito. Se si stanno eseguendo soltanto 28.000 host gestiti, è possibile individuare 500 CI risorsa per ciascun host gestito.

Distribuzione	Numero di host gestiti/CI correlati agli host
Enterprise	89.600/160 - 28.800/500
Standard	9.000/160 – 3.000/500
Piccola	4.500/160 – 1.000/500

Nota: i numeri della tabella includono soltanto i CI e non i collegamenti.

Compiti

Configurazione del server UCMDB

Per ottenere che il sistema supporti 40 milioni di CI e collegamenti, è necessario aggiornare i parametri seguenti sul server UCMDB:

Windows:

- **C:\hp\UCMDB\UCMDBServer\bin\wrapper-platform.conf**
wrapper.java.initmemory=2048
wrapper.java.maxmemory=8192
- **C:\hp\UCMDB\UCMDBServer\conf\settings.override.properties**
dal.object.condition.max.result.size=50000000
dal.use.memory.instead.temp.table.high.threshold.oracle=6000000
dal.joinf.max.result.size=4000000

Linux:

- **opt/hp/UCMDB/UCMDBServer/bin/wrapper-platform.conf**
wrapper.java.initmemory=2048
wrapper.java.maxmemory=8192
- **opt/hp/UCMDB/UCMDBServer/bin/settings.override.properties**
dal.object.condition.max.result.size=50000000
dal.use.memory.instead.temp.table.high.threshold.oracle=6000000
dal.joinf.max.result.size=4000000

Configurazione del database Oracle

Quando si lavora su un sistema che contiene 40 milioni di oggetti e collegamenti, è possibile migliorare le prestazioni migliorando le dimensioni di Oracle SGA da 6 a 8 GB (configurazione consigliata). Ciò migliora le prestazioni del calcolo TQL di diversi tipi di TQL e delle operazioni di data-in eseguite sul sistema.

Riferimenti

Configurazione del test di sistema

La capacità di sistema del test di sistema era di 40 milioni di CI e collegamenti.

Per il test è stato utilizzato l'hardware seguente:

Ruolo	Tipo di computer	CPU	Memoria	VM/ SWAP	SO + SW di terze parti
CMDB	HP ProLiant BL460c G6	2 x Intel Xeon Processor 2.533 GHz Quad core	16 GB	Windows: 24 GB Linux: 16 GB	Win2008R2 64-bit Red Hat Enterprise Linux Server release 5.5
Sonda del flusso di dati	HP ProLiant DL 140 G2	2 * 3.0 GHz CPU	2 MB	3 MB	Windows 2003 Server EE
Database	HP ProLiant BL460c G6	2 x Intel Xeon Processor 2.933 GHz Quad core	32 GB	51 GB	Win2008R2 64-bit REHL 5.4

Per il test è stata utilizzata la versione di software seguente:

- Oracle Database 11g, Release 11.2.0.1.0

Nell'ambito del test di sistema sono stati sottoposti a test i flussi aziendali seguenti:

► **Calcolo TQL**

Le TQL sono state divise in sottogruppi in base alle dimensioni dei risultati (<100, <1.000 e <10.000), a seconda del set di dati recuperati dalla TQL e in base alla configurazione della TQL:

- Condizione Simile a
- Simile a, Ignora maiusc/minusc
- Prospettiva
- Diversi numeri di gerarchia nei risultati della TQL (1-5)
- Compound
- Sottografico
- JoinF

► **Data-in**

Nello scenario dei data-in nel test di sistema sono stati inclusi inserimento, aggiornamento ed eliminazione.

► **Accrescimenti**

Negli scenari di accrescimento sono stati inclusi inserimento, aggiornamento ed eliminazione.

Risultati del test di sistema

Dopo un test di carico di 24 ore, con uno scenario che comprendeva l'esecuzione di query, data-in e l'esecuzione dell'accrescimento, i risultati raggiunti sono stati i seguenti:

- Il sistema è rimasto stabile per tutta la durata dell'esecuzione. Non sono stati osservati riavvii, perdite di memoria o alcuna diminuzione delle prestazioni nel tempo.
- Le prestazioni del sistema sono accettabili. Per la maggior parte delle TQL, il percentile 90% è inferiore a 1 secondo del tempo di calcolo.

Parte VI

Protezione avanzata di HP Universal CMDB

18

Introduzione alla protezione avanzata

Questo capitolo comprende:

Concetti

- Protezione avanzata - Panoramica a pag. 284
- Preparazione della protezione avanzata a pag. 286

Compiti

- Distribuire HP Universal CMDB in un'architettura protetta a pag. 287
- Cambiare il nome utente o la password di sistema per la console JMX a pag. 288
- Cambiare l'utente del servizio HP Universal CMDB Server a pag. 289

Concetti

Protezione avanzata - Panoramica

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

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

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

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

Si consiglia di utilizzare un proxy inverso con HP Universal CMDB per ottenere un'architettura sicura. Per i dettagli sulla configurazione di un proxy inverso da utilizzare con HP Universal CMDB, consultare “Utilizzo di un proxy inverso” a pag. 307.

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

Per i dettagli sulla protezione avanzata della sonda del flusso di dati, consultare “Protezione avanzata della sonda del flusso di dati” a pag. 345.

Importante:

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

Preparazione della protezione avanzata

- ▶ Valutare il rischio di protezione/stato della protezione per le reti generiche, e utilizzare le conclusioni quando si decide come integrare al meglio HP Universal CMDB nella rete.
- ▶ Sviluppare una buona conoscenza del framework tecnico di HP Universal CMDB e delle funzionalità di protezione di HP Universal CMDB.
- ▶ Riesaminare tutte le linee guida relative alla protezione avanzata.
- ▶ Verificare che HP Universal CMDB sia completamente funzionante prima di avviare le procedure di protezione avanzata.
- ▶ Seguire in ordine cronologico i passaggi delle procedure relative alla protezione avanzata in ciascun capitolo. Se si decide ad esempio di configurare il server HP Universal CMDB per supportare il protocollo SSL, leggere “Abilitazione della comunicazione Secure Sockets Layer (SSL)” a pag. 291 e poi seguire tutte le istruzioni in ordine cronologico.
- ▶ HP Universal CMDB non supporta l'autenticazione di base con password vuote. Non utilizzare una password vuota quando si impostano i parametri di connessione con autenticazione di base.

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

Compiti

Distribuire HP Universal CMDB in un'architettura protetta

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

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

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

➤ **Browser sicuro**

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

➤ **Protocollo di comunicazione SSL**

Il protocollo Secure Sockets Layer protegge la connessione tra il client e il server. Gli URL che richiedono una connessione SSL utilizzano una versione protetta (HTTPS) di Hypertext Transfer Protocol. Per i dettagli consultare "Abilitazione della comunicazione Secure Sockets Layer (SSL)" a pag. 291.

➤ **Architettura del proxy inverso**

Una delle soluzioni più protette e consigliate suggerisce la distribuzione di HP Universal CMDB utilizzando un proxy inverso. HP Universal CMDB supporta completamente l'architettura del proxy inverso protetta. Per i dettagli consultare "Utilizzo di un proxy inverso" a pag. 307.

Nota: quando il server UCMDB viene configurato per la connessione con il proxy inverso, l'autenticazione reciproca mediante il protocollo SSL tra il server proxy inverso e la sonda del flusso di dati non viene supportata. Per i dettagli consultare "Abilitare il protocollo SSL tra il server UCMDB e la sonda del flusso di dati con l'autenticazione reciproca" a pag. 350.

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

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

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

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

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

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

- 1** Per **Windows** eseguire il file seguente:
`C:\hp\UCMDB\UCMDBServer\tools\server_management.bat.`
Per Linux: eseguire **server_management.sh** che si trova nella cartella seguente: `/opt/hp/UCMDB/UCMDBServer/tools/.`
- 2** Accedere allo strumento con le credenziali di autenticazione:
sysadmin/sysadmin.

- 3 Fare clic sul collegamento **Utenti**.
- 4 Selezionare l'utente di sistema e fare clic su **Cambiare la password per l'utente connesso**.
- 5 Selezionare la password precedente e la nuova, quindi fare clic su **OK**.

Cambiare l'utente del servizio HP Universal CMDB Server

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

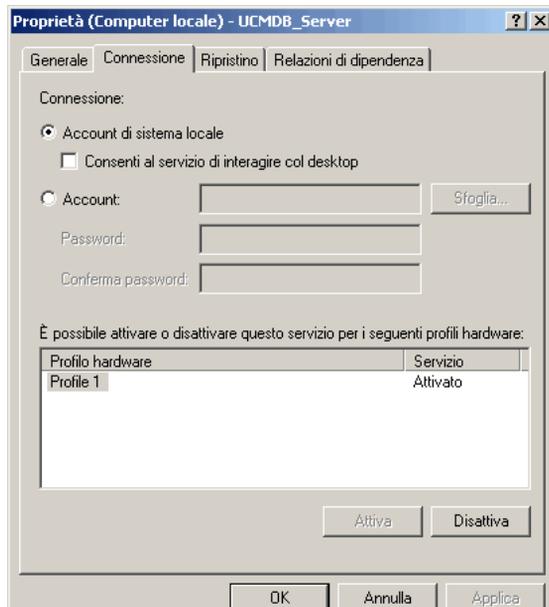
L'utente assegnato per eseguire il servizio deve disporre delle autorizzazioni seguenti:

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

Per cambiare l'utente del servizio.

- 1 Disabilitare HP Universal CMDB dal menu Start (**Start > Programmi > HP UCMDb > Arresta server HP Universal CMDB**) oppure arrestando il servizio HP Universal CMDB Server. Per i dettagli consultare “Avviare e arrestare il servizio del server HP Universal CMDB” a pag. 119.
- 2 Nella finestra **Servizi** di Windows, fare doppio clic su **UCMDb_Server**. Si apre la finestra di dialogo **Proprietà (computer locale) - UCMDb_Server**.

3 Fare clic sulla scheda **Connessione**.



- 4** Selezionare **Account** quindi **Sfoglia** per selezionare un altro utente dall'elenco degli utenti validi sul computer.
- 5** Immettere la password di Windows per l'utente selezionato e confermare la password.
- 6** Fare clic su **Applica** per salvare le impostazioni quindi su **OK** per chiudere la finestra di dialogo.
- 7** Abilitare HP Universal CMDB dal menu Start (**Start > Tutti i programmi > HP UCMDB > Avvio di HP Universal CMDB Server**) oppure avviando il servizio HP Universal CMDB Server. Per i dettagli consultare “Avviare e arrestare il servizio del server HP Universal CMDB” a pag. 119.

19

Abilitazione della comunicazione Secure Sockets Layer (SSL)

Questo capitolo comprende:

Compiti

- Attivare SSL sul computer server con certificato autofirmato a pag. 292
- Abilitare SSL sul computer server con un certificato dall'Autorità di certificazione a pag. 295
- Abilitare SSL sui computer client a pag. 297
- Abilitare SSL sull'SDK del client a pag. 298
- Abilitare l'autenticazione reciproca del certificato per SDK a pag. 298
- Cambiare le password del keystore del server a pag. 301
- Abilitare o disabilitare le porte HTTP/HTTPS a pag. 302
- Mappare i componenti Web di UCMDB alle porte a pag. 304

Compiti

Attivare SSL sul computer server con certificato autofirmato

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

HP Universal CMDB utilizza 6.1 come server Web predefinito.

1 Prerequisiti

- a** Prima di avviare la procedura seguente, rimuovere il **server.keystore** precedente che si trova in
C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore.
- b** Collocare il keystore di HP Universal CMDB (tipo JKS) nella cartella
C:\hp\UCMDB\UCMDBServer\conf\security.

2 Generare un keystore per il server

- a** Creare un keystore (tipo JKS) con un certificato autofirmato e corrispondente alla chiave privata:
 - Da **C:\hp\UCMDB\UCMDBServer\bin\jre\bin** eseguire il comando seguente:

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

Si apre la finestra di dialogo della console.

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

- Rispondere alla domanda **Qual è il suo nome e cognome?** Immettere il nome server Web HP Universal CMDB. Immettere gli altri parametri in relazione alla propria organizzazione.
- Immettere la password della chiave. La password della chiave DEVE essere la stessa della password keystore.

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

b Esportare il certificato autofirmato in un file.

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

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

3 Collocare il certificato nell'archivio dati attendibile del client

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

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

4 Disabilitare la porta 8080 HTTP

Per i dettagli consultare “Abilitare o disabilitare le porte HTTP/HTTPS” a pag. 302.

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

5 Riavviare il server

6 Display HP Universal CMDB

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

Abilitare SSL sul computer server con 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 **server.keystore** precedente che si trova in

C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore.

2 Generare un keystore per il server

- a** Generare un certificato CA firmato e installarlo in Windows.
- b** Esportare il certificato in un file ***.pfx** (incluse le chiavi private) utilizzando Microsoft Management Console (**mmc.exe**).
 - Immettere qualsiasi stringa come la password per il file **pfx**. (Questa password viene chiesta quando si converte il tipo keystore in un keystore JAVA.)
Il file **.pfx** ora contiene un certificato pubblico e una chiave privata e la password è protetta.
- c** Copiare il file **.pfx** creato nella seguente cartella:
C:\hp\UCMDB\UCMDBServer\conf\security.
- d** Aprire il prompt dei comandi e cambiare la directory in
C:\hp\UCMDB\UCMDBServer\bin\jre\bin.
 - Cambiare il tipo di keystore da **PKCS12** a un keystroke **JAVA** eseguendo il seguente comando:

```
keytool -importkeystore -srckeystore
c:\hp\UCMDB\UCMDBServer\conf\security\

```

Viene chiesta la password keystore originale (**.pfx**). (È la password fornita durante la creazione del file pfx nel passaggio b.)

- e** Immettere la password del keystore di destinazione. Deve essere la stessa password definita in precedenza nel metodo JMX **changeKeystorePassword** in Security Services. Se la password non è stata cambiata, utilizzare la password predefinita **hppass**.
- f** Dopo aver generato il certificato, disabilitare la porta 8080 HTTP. Per i dettagli consultare “Abilitare o disabilitare le porte HTTP/HTTPS” a pag. 302.
- g** Se è stata utilizzata una password diversa da **hppass** oppure la password utilizzata per il file .pfx, eseguire il metodo JMX **changeKeystorePassword** e accertarsi che la chiave abbia la stessa password.

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

3 Riavviare il server

4 Verificare la protezione del server

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

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

Abilitare SSL sui computer client

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

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

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

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

- 1** Individuare e rinominare il certificato **hpcert** in **hpcert.cer**.
In Esplora risorse, l'icona mostra che il file è un certificato di protezione.
- 2** Fare doppio clic su **hpcert.cer** per aprire la finestra di dialogo Certificato Internet Explorer.
- 3** Seguire le istruzioni per abilitare l'affidabilità installando il certificato con la procedura guidata per l'importazione del certificato.

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

Abilitare SSL sull'SDK del client

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

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

Utilizzare il comando seguente:

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

Abilitare l'autenticazione reciproca del certificato per SDK

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

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

- 1 Protezione avanzata del connettore del client UCMDB-API in UCMDB:
 - a Per accedere alla console JMX di UCMDB: Avviare un browser Web e specificare il seguente indirizzo: **http://<nome del computer UCMDB oppure IP>:8080/jmx-console**. È necessario accedere con nome utente e password (il valore predefinito è sysadmin/sysadmin).

- b** Individuare **UCMDB:service=Ports Management Services** e fare clic sul collegamento per aprire la pagina Operazioni.
- c** Individuare l'operazione **PortsDetails** e fare clic su **Invoke**. Prendere nota dell'HTTPS con il numero di porta di autenticazione del client. Il valore predefinito è 8444 e deve essere abilitato.
- d** Tornare alla pagina Operazioni.
- e** Per mappare il connettore di ucmdb-api alla modalità di autenticazione reciproca, richiamare il metodo **mapComponentToConnectors** con i parametri seguenti:
 - **componentName:** ucmdb-api
 - **isHTTPSWithClientAuth:** true
 - Tutti gli altri flag: false

Viene visualizzato il messaggio seguente:

```
Operazione riuscita. Il componente ucmdb-api è ora mappato a: porte
HTTPS_CLIENT_AUTH.
```

- f** Tornare alla pagina Operazioni.
- 2** Accertarsi che JRE che esegue il client UCMDB-api abbia un keystore contenente un certificato del client.
 - 3** Esportare il certificato di UCMDB-api dal rispettivo keystore.
 - 4** Importare il certificato del client UCMDB-api esportato nel truststore del server UCMDB.
 - a** Nel computer di UCMDB copiare il file creato del certificato del client UCMDB-api nella directory seguente su UCMDB:
C:\HP\UCMDB\UCMDBServer\conf\security
 - b** Eseguire il comando seguente:

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

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

- d** Quando viene chiesto **Il certificato è attendibile?** premere **s** quindi INVIO.
 - e** Accertarsi che l'output sia Il certificato è stato aggiunto al keystore.
- 5** Esportare il certificato del server UCMDB dal keystore del server.
- a** Nel computer di UCMDB eseguire il comando seguente:

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

- b** Immettere la password del truststore del server UCMDB (valore predefinito **hppass**).
 - c** Verificare che il certificato venga creato nella directory seguente:
C:\HP\UCMDB\UCMDBServer\conf\security\server.cert
- 6** Importare il certificato di UCMDB esportato nel JRE del truststore del client UCMDB-API.
- 7** Riavviare il server UCMDB e il client UCMDB-API.
- 8** Per la connessione dal client UCMDB-API al server UCMDB-API utilizzare il codice seguente:

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

Cambiare le password del keystore del server

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

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

Nota: è necessario eseguire ogni passaggio della procedura.

- 1** Avviare il server UCMDB.
- 2** Eseguire il cambiamento della password nella console JMX.
 - a** Avviare il browser Web e specificare l'indirizzo del server come segue: **http://<nome host del server UCMDB oppure IP>:8080/jmx-console**.
Potrebbe essere necessario effettuare l'accesso con nome utente e password.
 - b** In UCMDB fare clic su **UCMDB:service=Security Services** per aprire la pagina Operazioni.
 - c** Individuare ed eseguire l'operazione **changeKeystorePassword**.
Questo campo non può essere vuoto e deve essere lungo almeno sei caratteri. La password viene cambiata soltanto nel database.
- 3** Arrestare il server UCMDB.
- 4** Eseguire i comandi.
Da **C:\hp\UCMDB\UCMDBServer\bin\jre\bin** eseguire i comandi seguenti:
 - a** Cambiare le password dell'archivio:

```
keytool -storepasswd -new <nuova_pass_keystore> -keystore
C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore -storepass
<pass_corrente_keystore>
```

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

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

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

```
keytool -keypasswd -alias <alias> -keypass <passcorrente> -new <nuovapass> -  
keystore C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore
```

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

Abilitare o disabilitare le porte HTTP/HTTPS

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

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

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

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

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

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

Mappare i componenti Web di UCMDB alle porte

È possibile configurare la mappatura di ciascun componente di UCMDB alle porte disponibili dalla console JMX.

Per visualizzare le configurazioni del componente corrente:

- 1** Avviare un browser Web e specificare il seguente indirizzo:
`http://localhost.<nome_dominio>:8080/jmx-console.`
- 2** Immettere le credenziali di autenticazione della console JMX, che per impostazione predefinita sono:
 - Nome di accesso = **sysadmin**
 - Password = **sysadmin**
- 3** Individuare **UCMDB:service=Ports Management Services** e fare clic sul collegamento per aprire la pagina Operazioni.
- 4** Individuare il metodo **ComponentsConfigurations** e fare clic su **Invoke**.
- 5** Per ogni componente vengono visualizzate le porte valide e le porte al momento mappate.

Per mappare i componenti:

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

Nota:

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

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

Per impostare i valori delle porte:

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

20

Utilizzo di un proxy inverso

Questo capitolo comprende:

Concetti

- Proxy inverso - Panoramica a pag. 308
- Aspetti di protezione nell'utilizzo di un server proxy inverso a pag. 310

Compiti

- Configurare un proxy inverso utilizzando le impostazioni dell'infrastruttura a pag. 311
- Configurare un proxy inverso utilizzando la console JMX a pag. 312
- Apache 2.0.x - Configurazione di esempio a pag. 313

Concetti

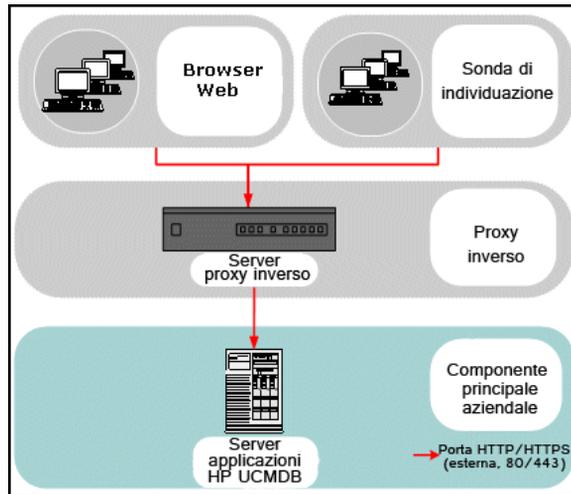
Proxy inverso - Panoramica

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

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

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

HP Universal CMDB supporta un proxy inverso nell'architettura DMZ. Il proxy inverso è un mediatore HTTP tra la sonda del flusso di dati, il client Web e il server HP Universal CMDB.



Nota: diversi tipi di proxy inversi richiedono sintassi diverse di configurazione. Per un esempio di configurazione di proxy inverso Apache 2.0.x, consultare "Apache 2.0.x - Configurazione di esempio" a pag. 313.

Aspetti di protezione nell'utilizzo di un server proxy inverso

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

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

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

- ▶ Nessuna conversione di protocollo DMZ. Il protocollo in entrata e il protocollo in uscita sono identici (cambia soltanto l'intestazione).
- ▶ È ammesso soltanto l'accesso HTTP al proxy inverso, ovvero i firewall di ispezione del pacchetto con stato sono in grado di proteggere meglio la comunicazione.
- ▶ Sul proxy inverso si può definire un set statico e limitato di richieste.
- ▶ La maggior parte delle funzioni di protezione del server Web sono disponibili sul proxy server (metodi di autenticazione, crittografia e così via).
- ▶ Il proxy inverso visualizza gli indirizzi IP dei server reali nonché l'architettura della rete interna.
- ▶ L'unico client accessibile del server Web è il proxy inverso.
- ▶ Questa configurazione supporta i firewall NAT (contrariamente ad altre soluzioni).
- ▶ Il proxy inverso richiede un numero minimo di porte aperte nel firewall.
- ▶ Il proxy inverso fornisce buone prestazioni rispetto ad altre soluzioni bastioni.

Compiti

Configurare un proxy inverso utilizzando le impostazioni dell'infrastruttura

La procedura seguente spiega come accedere alle impostazioni dell'infrastruttura per consentire la configurazione del proxy:

Per consentire la configurazione del proxy inverso:

- 1** Selezionare **Amministrazione > Impostazioni infrastruttura categoria> Impostazioni generali**.
- 2** Cambiare l'impostazione **URL front-end**. Immettere l'indirizzo, ad esempio **https://my_proxy_server:443/**.
- 3** Cambiare **L'URL front-end è abilitato dalle impostazioni?** in **true**.

Importante: dopo questo cambiamento non è possibile accedere direttamente al server HP Universal CMDB da un client. È comunque possibile cambiare la configurazione del proxy inverso utilizzando la console JMX sul server. Per i dettagli consultare “Configurare un proxy inverso utilizzando la console JMX” a pag. 312.

Configurare un proxy inverso utilizzando la console JMX

La procedura seguente spiega come cambiare la configurazione del proxy inverso utilizzando la console JMX sul server HP Universal CMDB.

Per cambiare la configurazione del proxy inverso:

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

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

dove **<nome del computer o indirizzo IP>** è il computer su cui è installato HP Universal CMDB. Potrebbe essere necessario effettuare l'accesso con nome utente e password.

- 2** Fare clic sul collegamento **UCMDB-UI > UCMDB-UI:name=UI Server frontend settings**.
- 3** Nel campo **setUseFrontendURLBySettings** immettere l'URL del server proxy ad esempio **https://mio_server_proxy:443/**.
- 4** Fare clic su **Invoke**.
- 5** Per disabilitare/abilitare questa impostazione, utilizzare il metodo **enableUseFrontendURLBySettings** oppure **disableUseFrontendURLBySettings**.
- 6** Per visualizzare il valore di questa impostazione, utilizzare il metodo **showFrontendURLInSettings**.

Apache 2.0.x - Configurazione di esempio

Di seguito viene riportato un esempio di file di configurazione che supporta l'utilizzo di un proxy inverso Apache 2.0.x in un caso in cui le sonde del flusso di dati e gli utenti dell'applicazione si connettono a HP Universal CMDB.

Nota:

- Nell'esempio seguente il nome DNS del computer di HP Universal CMDB è **UCMDB_server**.
- Soltanto gli utenti che conoscono l'amministrazione di Apache possono eseguire questo cambiamento.

1 Aprire il file <directory principale del computer Apache>\Webserver\conf\httpd.conf.

2 Abilitare i moduli seguenti:

- LoadModule proxy_module modules/mod_proxy.so
- LoadModule proxy_http_module modules/mod_proxy_http.so

3 Aggiungere le righe seguenti al file `httpd.conf`:

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

4 Salvare i cambiamenti.

21

Gestione credenziali del flusso di dati

Questo capitolo comprende:

Concetti

- Gestione credenziali del flusso di dati - Panoramica a pag. 316
- Metodi dei dati delle credenziali (Direzione dei dati: verso HP Universal CMDB) a pag. 320
- Metodi dei dati delle credenziali (Direzione dei dati: verso HP Universal CMDB) a pag. 321

Compiti

- Configurare le impostazioni dell'autenticazione e della crittografia del client CM sul server UCMDB a pag. 322
- Configurare manualmente le impostazioni dell'autenticazione e della crittografia del client CM sulla sonda a pag. 324
- Configurare la cache del client Confidential Manager (CM) a pag. 329
- Esportare e importare le informazioni sulle credenziali e sull'intervallo in formato crittografato a pag. 332
- Cambiare il livello di messaggi del file di registro del client CM a pag. 334
- Generare o aggiornare la chiave di crittografia a pag. 336

Riferimenti

- Impostazioni della crittografia di CM a pag. 342

Concetti

Gestione credenziali del flusso di dati - Panoramica

Per eseguire l'individuazione o l'integrazione è necessario impostare le credenziali di accesso al sistema remoto. Le credenziali sono configurate nella finestra Impostazione della sonda del flusso di dati nel server UCMDB. Per i dettagli consultare “Finestra Impostazione della sonda del flusso di dati” a pag. 58.

L'archiviazione delle credenziali viene gestita dal componente Confidential Manager (CM). Per i dettagli consultare “Confidential Manager” a pag. 387.

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

L'autenticazione del client CM sul server CM si basa su un componente LW-SSO. Prima della connessione al server CM, il client CM invia prima un cookie LW-SSO. Il server CM verifica il cookie e dopo l'esito positivo viene avviata la comunicazione con il client CM. Per i dettagli sul LW-SSO consultare “Configurare le impostazioni LW-SSO sul server UCMDB” a pag. 322.

La comunicazione tra il client CM e il server CM viene crittografata. Per i dettagli sull'aggiornamento della configurazione della crittografia consultare “Configurare la crittografia della comunicazione di CM sul server UCMDB” a pag. 323.

Il client CM gestisce una cache locale delle credenziali. Il client CM è configurato per il download di tutte le credenziali dal server CM e la memorizzazione in una cache. I cambiamenti delle credenziali vengono automaticamente sincronizzati dal server CM su base continua. La cache può essere un file-system o una cache in memoria a seconda delle impostazioni preconfigurate. Inoltre la cache viene crittografata e non vi si può accedere dall'esterno. Per i dettagli sull'aggiornamento delle impostazioni della cache consultare “Configurare la modalità della cache del client CM sulla sonda” a pag. 329. Per i dettagli sull'aggiornamento della crittografia della cache consultare “Configurare le impostazioni della crittografia della cache del client CM sulla sonda” a pag. 330.

Per i dettagli sulla risoluzione dei problemi consultare “Cambiare il livello di messaggi del file di registro del client CM” a pag. 334.

Le informazioni sulle credenziali si possono copiare da un server UCMDDB a un altro. Per i dettagli consultare “Esportare e importare le informazioni sulle credenziali e sull'intervallo in formato crittografato” a pag. 332.

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

In questa sezione vengono trattati i seguenti argomenti:

- “Ipotesi di protezione di base” a pag. 318
- “Sonda del flusso di dati in esecuzione in modalità separata” a pag. 318
- “Tenere aggiornata la cache delle credenziali” a pag. 318
- “Sincronizzazione di tutte le sonde con i cambiamenti di configurazione” a pag. 319
- “Archiviazione protetta sulla sonda” a pag. 320

Ipotesi di protezione di base

Tenere presente l'ipotesi di protezione seguente:

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

Sonda del flusso di dati in esecuzione in modalità separata

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

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

Tenere aggiornata la cache delle credenziali

Alla prima connessione riuscita al server CM, il client CM scarica tutte le credenziali rilevanti (tutte le credenziali configurate nel dominio della sonda). Dopo la prima comunicazione riuscita, il client CM mantiene la sincronizzazione continua con il server CM. La sincronizzazione differenziale viene eseguita a intervalli di un minuto durante i quali vengono sincronizzate soltanto le differenze tra il server CM e il client CM. Se le credenziali vengono cambiate lato server UCMDB (ad esempio aggiunta di nuove credenziali o aggiornamento o eliminazione di credenziali esistenti), il client CM riceve la notifica immediata dal server UCMDB ed esegue la sincronizzazione aggiuntiva.

Sincronizzazione di tutte le sonde con i cambiamenti di configurazione

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

Il server UCMDB controlla costantemente i cambiamenti nella configurazione della crittografia di comunicazione di CM e la configurazione dell'autenticazione di CM. Questo controllo viene eseguito ogni 15 secondi; in caso di cambiamento la configurazione aggiornata viene inviata alle sonde. La configurazione viene passata alle sonde in forma crittografata e memorizzata lato sonda nell'archiviazione protetta. La crittografia della configurazione inviata viene eseguita utilizzando una chiave di crittografia simmetrica. Per impostazione predefinita il server UCMDB e la sonda del flusso di dati vengono installati con la stessa chiave di crittografia simmetrica predefinita. Per una protezione ottimale si consiglia di cambiare questa chiave prima di aggiungere credenziali al sistema. Per i dettagli consultare “Generare o aggiornare la chiave di crittografia” a pag. 336.

Nota:

- A causa dell'intervallo di controllo di 15 secondi, è possibile che il client CM la sonda non venga aggiornato con l'ultima configurazione per un periodo di 15 secondi.
 - Se si sceglie di disabilitare la sincronizzazione automatica della configurazione dell'autenticazione e della comunicazione di CM tra il server UCMDB e la sonda del flusso di dati, ogni volta che si aggiorna la configurazione dell'autenticazione e della comunicazione lato server UCMDB è necessario aggiornare anche tutte le sonde con la nuova configurazione. Per i dettagli consultare “Disabilitare la sincronizzazione automatica delle impostazioni dell'autenticazione e della crittografia del client CM tra il server UCMDB e le sonde” a pag. 325.
-

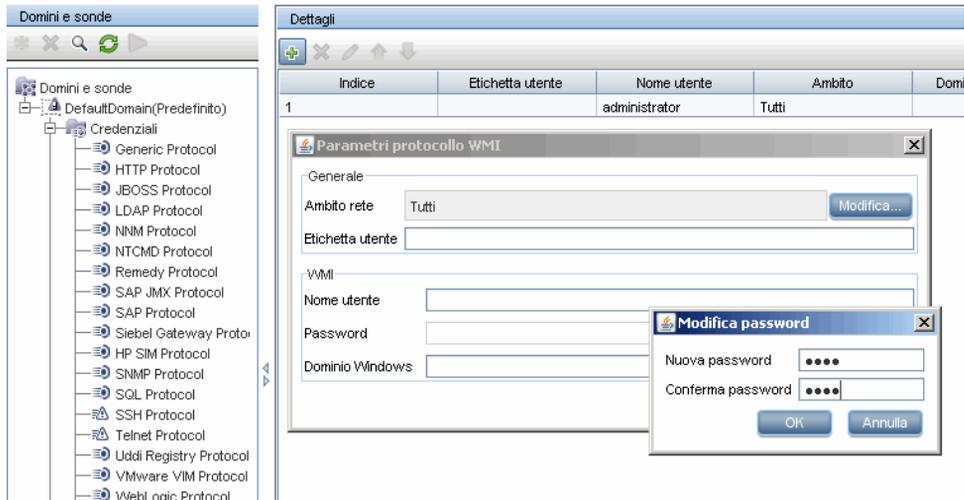
Archiviazione protetta sulla sonda

Tutte le informazioni sensibili (ad esempio la configurazione dell'autenticazione e della comunicazione di CM e la chiave di crittografia) vengono memorizzate sulla sonda in archiviazione protetta nel file **secured_storage.bin** che si trova nella directory

C:\hp\UCMDB\DataFlowProbe\conf\security. Questa archiviazione protetta viene crittografata utilizzando il metodo DPAPI che si basa sulla password utente di Windows nel processo di crittografia. DPAPI è un metodo standard utilizzato per proteggere i dati riservati come ad esempio i certificati e le chiavi private sui sistemi Windows. La sonda deve essere sempre eseguita con lo stesso utente di Windows in modo che, anche se viene cambiata la password, la sonda può continuare a leggere le informazioni memorizzate nell'archiviazione protetta.

Metodi dei dati delle credenziali (Direzione dei dati: verso HP Universal CMDB)

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



Metodi dei dati delle credenziali (Direzione dei dati: verso HP Universal CMDB)

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

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

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

Compiti

Configurare le impostazioni dell'autenticazione e della crittografia del client CM sul server UCMDB

Questo compito include i passaggi seguenti:

- “Configurare le impostazioni LW-SSO sul server UCMDB” a pag. 322
- “Configurare la crittografia della comunicazione di CM sul server UCMDB” a pag. 323

Configurare le impostazioni LW-SSO sul server UCMDB

Questa procedura descrive come cambiare la stringa init di LW-SSO sul server UCMDB. Questo cambiamento viene automaticamente inviato alle sonde (come stringa crittografata) a meno che il server UCMDB non sia configurato in tal senso. Per i dettagli consultare “Disabilitare la sincronizzazione automatica delle impostazioni dell'autenticazione e della crittografia del client CM tra il server UCMDB e le sonde” a pag. 325.

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

Configurare la crittografia della comunicazione di CM sul server UCMDB

Questa procedura descrive come cambiare le impostazioni della crittografia della comunicazione di CM. Queste impostazioni specificano come viene crittografata la comunicazione tra il client CM e il server CM. Questo cambiamento viene automaticamente inviato alle sonde (come stringa crittografata) a meno che il server UCMDB non sia configurato in tal senso. Per i dettagli consultare “Disabilitare la sincronizzazione automatica delle impostazioni dell'autenticazione e della crittografia del client CM tra il server UCMDB e le sonde” a pag. 325.

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

Viene visualizzato l'XML della configurazione corrente di CM.

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

Per i dettagli sui valori che si possono aggiornare consultare “Impostazioni della crittografia di CM” a pag. 342.

Esempio:

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

10 Fare clic su **Invoke**.

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

Questo compito include i passaggi seguenti:

- ▶ “Disabilitare la sincronizzazione automatica delle impostazioni dell'autenticazione e della crittografia del client CM tra il server UCMDDB e le sonde” a pag. 325
- ▶ “Configurare le impostazioni dell'autenticazione e della crittografia del client CM sulla sonda” a pag. 326
- ▶ “Configurare la crittografia della comunicazione di CM sulla sonda” a pag. 327

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

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

Per disabilitare la sincronizzazione automatica delle impostazioni di CM/LW-SSO:

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



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

Questa procedura è rilevante se il server UCMDB è stato configurato per non inviare la configurazione e le impostazioni di LW-SSO/CM alle sonde. Per i dettagli consultare “Disabilitare la sincronizzazione automatica delle impostazioni dell'autenticazione e della crittografia del client CM tra il server UCMDB e le sonde” a pag. 325.

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

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

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

Configurare la crittografia della comunicazione di CM sulla sonda

Questa procedura è rilevante se il server UCMDB è stato configurato per non inviare la configurazione e le impostazioni di LW-SSO/CM alle sonde. Per i dettagli consultare “Disabilitare la sincronizzazione automatica delle impostazioni dell'autenticazione e della crittografia del client CM tra il server UCMDB e le sonde” a pag. 325.

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

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

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

Nota: è necessario aggiornare le stesse impostazioni aggiornate sul server UCMDB. Per eseguire questa operazione alcuni metodi che si aggiornano sulla sonda possono richiedere più di un parametro. Per visualizzare la configurazione corrente della sonda fare clic su **displayTransportConfiguration** nella pagina JMX MBEAN View. Per i dettagli consultare “Configurare la crittografia della comunicazione di CM sul server UCMDB” a pag. 323. Per i dettagli sui valori che si possono aggiornare consultare “Impostazioni della crittografia di CM” a pag. 342.

- a** `setTransportInitString` cambia l'impostazione `encryptDecryptInitString`.
 - b** `setTransportEncryptionAlgorithm` cambia le impostazioni di CM sulla sonda in base alla mappa seguente:
 - **Engine name** si riferisce alla voce `<engineName>`
 - **Key size** si riferisce alla voce `<keySize>`
 - **Algorithm padding name** si riferisce alla voce `<algorithmPaddingName>`
 - **PBE count** si riferisce alla voce `<pbeCount>`
 - **PBE digest algorithm** si riferisce alla voce `<pbeDigestAlgorithm>`
 - c** `setTransportEncryptionLibrary` cambia le impostazioni sulla sonda in base alla mappa seguente:
 - **Encryption Library name** si riferisce alla voce `<cryptoSource>`
 - **Support previous lightweight cryptography versions** si riferisce alla voce `<lwJCEPBCompatibilityMode>`
 - d** `setTransportMacDetails` cambia le impostazioni sulla sonda in base alla mappa seguente:
 - **Use MAC with cryptography** si riferisce alla voce `<useMacWithCrypto>`
 - **MAC key size** si riferisce alla voce `<macKeySize>`
- 4** Fare clic sul pulsante `reloadTransportConfiguration` per rendere effettivi i cambiamenti sulla sonda.

Per i dettagli sulle diverse impostazioni e i possibili valori consultare “Impostazioni della crittografia di CM” a pag. 342.

Configurare la cache del client Confidential Manager (CM)

Questo compito include i passaggi seguenti:

- “Configurare la modalità della cache del client CM sulla sonda” a pag. 329
- “Configurare le impostazioni della crittografia della cache del client CM sulla sonda” a pag. 330

Configurare la modalità della cache del client CM sulla sonda

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

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

Per cambiare questa impostazione:

- 1** Aprire il file **DiscoveryProbe.properties** in un editor di testo. Il file si trova nella directory `c:\hp\UCMDB\DataFlowProbe\conf`.
- 2** Individuare l'attributo seguente:
`com.hp.ucmdb.discovery.common.security.storeCMDData=true`
 - Per memorizzare le informazioni sul file system, lasciare il valore predefinito (**true**).
 - Per memorizzare le informazioni in memoria, immettere **false**.
- 3** Salvare il file **DiscoveryProbe.properties**.
- 4** Riavviare la sonda.

Configurare le impostazioni della crittografia della cache del client CM sulla sonda

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

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

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

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

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

- a **setCacheInitString** cambia la cache del file system <encryptDecryptInitString> setting.
- b **setCacheEncryptionAlgorithm** cambia le impostazioni della cache del file system in base alla mappa seguente:
 - **Engine name** si riferisce alla voce <engineName>
 - **Key size** si riferisce alla voce <keySize>

- ▶ **Algorithm padding name** si riferisce alla voce <algorithmPaddingName>
 - ▶ **PBE count** si riferisce alla voce <pbeCount>
 - ▶ **PBE digest algorithm** si riferisce alla voce <pbeDigestAlgorithm>
 - c setCacheEncryptionAlgorithm** cambia le impostazioni della cache del file system in base alla mappa seguente:
 - ▶ **Encryption Library name** si riferisce alla voce <cryptoSource>
 - ▶ **Support previous lightweight cryptography versions** si riferisce alla voce <lwJCEPBCompatibilityMode>
 - d setCacheMacDetails** cambia le impostazioni della cache del file system in base alla mappa seguente:
 - ▶ **Use MAC with cryptography** si riferisce alla voce <useMacWithCrypto>
 - ▶ **MAC key size** si riferisce alla voce <macKeySize>
- 4** Fare clic sul pulsante **reloadCacheConfiguration** per rendere effettivi i cambiamenti sulla sonda. Ciò comporta il riavvio della sonda.

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

Per i dettagli sulle diverse impostazioni e i possibili valori consultare “Impostazioni della crittografia di CM” a pag. 342.

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

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

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

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

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

Per esportare le informazioni sulle credenziali dal server UCMDB:

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

3 Individuare l'operazione **exportCredentialsAndRangesInformation**.

Eseguire l'operazione seguente:

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

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

Quando il processo di esportazione viene completato correttamente, il file viene salvato nella posizione seguente:

c:\hp\UCMDB\UCMDBServer\conf\discovery\<customer_dir> directory.

Per importare le informazioni sulle credenziali dal server UCMDB:

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

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

2 Fare clic su **UCMDB:service=DiscoveryManager** per aprire la pagina JMX MBEAN View.

3 Individuare una delle operazioni seguenti:

- Individuare l'operazione **importCredentialsAndRangesInformation** se il file che si sta importando è stato esportato da un server UCMDB successivo alla versione 8.02.
- Individuare l'operazione **importCredentialsAndRangesWithKey** se il file che si sta importando è stato esportato da un server UCMDB versione 8.02.

4 Immettere l'ID del cliente (l'impostazione predefinita è 1).

5 Immettere il nome del file da importare. Questo file deve essere individuato nella directory

c:\hp\UCMDB\UCMDBServer\conf\discovery\<customer_dir>.

- 6 Immettere la password. Deve essere la stessa password utilizzata al momento dell'esportazione del file.
- 7 Se il file è stato esportato da un sistema UCMDB versione 8.02, immettere il nome file **key.bin**. Questo file deve essere individuato nella directory **c:\hp\UCMDB\UCMDBServer\conf\discovery\<customer_dir>** insieme al file da importare.
- 8 Fare clic su **Invoke** per importare le credenziali.

Cambiare il livello di messaggi del file di registro del client CM

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

- “File di registro del client CM” a pag. 334
- “File di registro LW-SSO” a pag. 335

File di registro del client CM

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

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

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

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

3 Cambiare la riga:

```
loglevel.cm=INFO
```

in:

```
loglevel.cm=DEBUG
```

4 Salvare il file.

File di registro LW-SSO

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

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

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

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

```
loglevel.lwssolog=INFO
```

in:

```
loglevel.lwssolog=DEBUG
```

4 Salvare il file.

Generare o aggiornare la chiave di crittografia

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

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

Nota:

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

Questo compito include i passaggi seguenti:

- ▶ “Generare una nuova chiave di crittografia” a pag. 337
- ▶ “Aggiornare una chiave di crittografia su un server UC MDB” a pag. 338
- ▶ “Aggiornare una chiave di crittografia su una sonda” a pag. 340
- ▶ “Cambiare manualmente la chiave di crittografia quando Probe Manager e Probe Gateway sono installati su computer diversi” a pag. 341
- ▶ “Generare una nuova chiave di crittografia” a pag. 337

Generare una nuova chiave di crittografia

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

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

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

Potrebbe essere necessario effettuare l'accesso con nome utente e password.
- 2** Fare clic su **UCMDB:service=DiscoveryManager** per aprire la pagina JMX MBEAN View.
- 3** Individuare l'operazione `generateEncryptionKey`.
 - a** Nella casella del parametro **customerId** immettere **1** (valore predefinito).
 - b** Per **keySize** indicare la lunghezza della chiave di crittografia. Valori validi sono 128, 192 o 256.
 - c** Per **usePBE** specificare **True** o **False**:
 - **True**: utilizzare ulteriori cicli hash PBE.
 - **False**: non utilizzare ulteriori cicli hash PBE.
 - d** Per **jceVendor** è possibile scegliere di utilizzare un provider JCE non predefinito. Se la casella è vuota, viene utilizzato il valore predefinito.
 - e** Per **autoUpdateProbe** specificare **True** o **False**:
 - **True**: il server distribuisce automaticamente la nuova chiave alle sonde.
 - **False**: la nuova chiave deve essere posizionata manualmente nelle sonde.

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

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

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

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

Aggiornare una chiave di crittografia su un server UCMDB

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

Per aggiornare una chiave di crittografia mediante la console JMX:

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

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

2 Fare clic su **UCMDB:service=DiscoveryManager** per aprire la pagina JMX MBEAN View.

3 Individuare l'operazione **changeEncryptionKey**.

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

- b** Per **newKeyFileName** immettere il nome della nuova chiave.
- c** Per **keySizeInBits** indicare la lunghezza della chiave di crittografia. Valori validi sono 128, 192 o 256.
- d** Per **usePBE** specificare **True** o **False**:
 - **True**: utilizzare ulteriori cicli hash PBE.
 - **False**: non utilizzare ulteriori cicli hash PBE.
- e** Per **jceVendor** è possibile scegliere di utilizzare un provider JCE non predefinito. Se la casella è vuota, viene utilizzato il valore predefinito.
- f** Per **autoUpdateProbe** specificare **True** o **False**:
 - **True**: il server distribuisce automaticamente la nuova chiave alle sonde.
 - **False**: la nuova chiave deve essere distribuita manualmente utilizzando la console JMX della sonda.

Importante: accertarsi che la sonda sia in funzione e connessa al server. Se la sonda non è in funzione la chiave non può arrivare alla sonda.

Se si cambia la chiave prima che la sonda si arresti, quando la sonda torna di nuovo in funzione la chiave viene inviata di nuovo alla sonda. Tuttavia, se la chiave viene cambiata più di una volta prima che la sonda si arresti, è necessario cambiare la chiave manualmente mediante la console JMX. (Selezionare **False** per **autoUpdateProbe**).

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

Aggiornare una chiave di crittografia su una sonda

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

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

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

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

- 3 Nel dominio della sonda fare clic su `type=MainProbe` per aprire la pagina JMX MBEAN View.
- 4 Individuare il metodo `importEncryptionKey`.
- 5 Immettere il nome del file della chiave di crittografia che si trova nella directory `C:\hp\UCMDB\DataFlowProbe\conf\security\`. Questo file contiene la chiave da importare.
- 6 Fare clic sul pulsante `importEncryptionKey`.

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

- 1 Sul computer di Probe Manager avviare il servizio Probe Gateway (**Start > Programmi > HP UCMDB > Probe Gateway**).
- 2 Importare la chiave dal server utilizzando JMX di Probe Gateway. Per i dettagli consultare “Generare una nuova chiave di crittografia” a pag. 337.
- 3 Dopo l'importazione corretta della chiave di crittografia arrestare il servizio Probe Gateway.

Definire diversi provider JCE

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

Per cambiare il provider JCE predefinito:

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

Riferimenti

Impostazioni della crittografia di CM

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

Nome impostazione di CM di UCMDB	Nome impostazione di CM della sonda	Descrizione impostazione	Valori possibili	Valore predefinito
cryptoSource	Nome libreria di crittografia	Questa impostazione definisce la libreria di crittografia da utilizzare.	lw, jce, windowsDPAPI, lwJCECompatible	lw
lwJCEPBCompatibilityMode	Supporta le versioni precedenti della crittografia semplificata	Questa impostazione definisce se supportare o meno la crittografia precedente semplificata.	true, false	true
engineName	Nome motore	Nome meccanismo di crittografia	AES, DES, 3DES, Blowfish	AES

Nome impostazione di CM di UC MDB	Nome impostazione di CM della sonda	Descrizione impostazione	Valori possibili	Valore predefinito
keySize	Dimensione chiave	lunghezza chiave di crittografia in bit	Per AES - 128, 192 o 256; Per DES - 64; Per 3DES - 192; Per Blowfish - qualsiasi numero compreso tra 32 e 448	256
algorithmPadding Name	Nome spaziatura algoritmo	Standard spaziatura	PKCS7Padding, PKCS5Padding	PKCS7Padding
pbeCount	Conteggio PBE	Numero di esecuzioni della funzione hash per creare la chiave dalla password (stringa init)	Qualsiasi numero positivo	20
pbeDigestAlgorithm	Algoritmo digest PBE	Tipo di hash	SHA1, SHA256, MD5	SHA1
useMacWithCrypto	Utilizzo MAC con crittografia	Indica se utilizzare il codice MAC con la crittografia	true, false	false
macKeySize	Dimensione chiave MAC	Dipende dall'algoritmo MAC	256	256

22

Protezione avanzata della sonda del flusso di dati

Questo capitolo comprende:

Compiti

- Impostare la password crittografata del database MySQL a pag. 346
- Impostare la password crittografata della console JMX a pag. 348
- Abilitare il protocollo SSL tra il server UCMDB e la sonda del flusso di dati con l'autenticazione reciproca a pag. 350
- Abilitare l'autenticazione nella sonda del flusso di dati con autenticazione HTTP di base a pag. 358
- Connettere la sonda del flusso di dati mediante il proxy inverso a pag. 359
- Controllo della posizione del file domainScopeDocument a pag. 361
- Creare un keystore per la sonda del flusso di dati a pag. 362
- Crittografare le password del keystore e del truststore della sonda a pag. 362

Riferimenti

- Keystore e truststore predefiniti della sonda del flusso di dati a pag. 364

Compiti

Impostare la password crittografata del database MySQL

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

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

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

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

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

- b** Individuare il servizio **Type=MainProbe** e fare clic sul collegamento per aprire la pagina Operazioni.
- c** Individuare l'operazione **getEncryptedDBPassword**.
- d** Nel campo **DB Password** immettere la password da crittografare.
- e** Chiamare l'operazione facendo clic sul pulsante **getEncryptedDBPassword**.

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

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

2 Arrestare la sonda del flusso di dati

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

3 Eseguire lo script `set_dbuser_password.cmd`

Lo script si trova nella cartella seguente:

```
C:\hp\UCMDB\DataFlowProbe\tools\dbscripts  
\set_dbuser_password.cmd
```

Eseguire lo script `set_dbuser_password.cmd` con la nuova password come argomento, ad esempio `set_dbuser_password <mia_password>`.

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

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

- a La password deve risiedere crittografata nei file di configurazione. Per recuperare la forma crittografata della password utilizzare il metodo JMX `getEncryptedDBPassword` come spiegato a pagina 346.
- b Aggiungere la password crittografata alle proprietà seguenti nel file `C:\hp\UCMDB\DataFlowProbe\conf\DiscoveryProbe.properties`.

- `appilog.agent.probe.jdbc.pwd`

Ad esempio:

```
appilog.agent.probe.jdbc.user = mamprobe  
appilog.agent.probe.jdbc.pwd =  
66,85,54,78,69,117,56,65,99,90,86,117,97,75,50,112,65,53,67,114,112,65,6  
1,61
```

- `appilog.agent.local.jdbc.pwd`

5 Avviare la sonda del flusso di dati

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

Script `clearProbeData.bat`: Utilizzo

Lo script `clearProbeData.bat` ricrea l'utente del database con una password fornita come argomento allo script.

Dopo aver impostato una password, ogni volta che si esegue lo script `clearProbeData.bat` viene recuperata la password del database come argomento.

Dopo avere eseguito lo script:

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

Impostare la password crittografata della console JMX

In questa sezione viene spiegato come crittografare la password per l'utente JMX. La password crittografata è archiviata nel file

`DiscoveryProbe.properties`. Gli utenti devono registrarsi per accedere alla console JMX.

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

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

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

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

- b** Individuare il servizio **Type=MainProbe** e fare clic sul collegamento per aprire la pagina Operazioni.
- c** Individuare l'operazione **getEncryptedKeyPassword**.
- d** Nel campo **Key Password** immettere la password da crittografare.
- e** Chiamare l'operazione facendo clic sul pulsante **getEncryptedKeyPassword**.

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

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

2 Arrestare la sonda del flusso di dati

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

3 Aggiungere la password crittografata

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

appilog.agent.Probe.JMX.BasicAuth.Pwd

Ad esempio:

```
appilog.agent.Probe.JMX.BasicAuth.User=admin  
appilog.agent.Probe.JMX.BasicAuth.Pwd=-85,-9,-61,11,105,-93,-81,118
```

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

4 Avviare la sonda del flusso di dati

- a** Start > Tutti i programmi > HP UCMDB > Avvia sonda del flusso di dati
- b** Verificare il risultato in un browser Web.

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

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

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

In questa sezione vengono trattati i seguenti argomenti:

- “Panoramica” a pag. 350
- “Keystore e truststore” a pag. 351
- “Abilitare l'autenticazione reciproca del certificato” a pag. 351
- “Abilitare il protocollo SSL con autenticazione del server” a pag. 355

Panoramica

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

- **Autenticazione reciproca.** Questa modalità utilizza il protocollo SSL e consente l'autenticazione del server da parte della sonda e l'autenticazione del client da parte del server. Per i dettagli consultare “Abilitare l'autenticazione reciproca del certificato” a pag. 351.
- **Autenticazione del server.** Questa modalità utilizza il protocollo SSL e la sonda autentica il certificato del server UCMDB. Per i dettagli consultare “Abilitare il protocollo SSL con autenticazione del server” a pag. 355.
- **Standard HTTP.** Nessuna comunicazione SSL. Questa è la modalità predefinita e il componente Sonda del flusso di dati in UCMDB non richiede alcun certificato. La sonda del flusso di dati comunica con il server mediante il protocollo HTTP.

Keystore e truststore

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

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

Abilitare l'autenticazione reciproca del certificato

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

Nota: le istruzioni seguenti utilizzano il keystore **cKeyStoreFile** come keystore della sonda. Questo è un keystore del client predefinito che fa parte dell'installazione di UCMDB. Per i dettagli consultare “Keystore e truststore predefiniti della sonda del flusso di dati” a pag. 364. Si consiglia comunque di creare un nuovo keystore univoco contenente una chiave privata generata di nuovo. Per i dettagli consultare “Creare un keystore per la sonda del flusso di dati” a pag. 362.

- 1** Verificare che sia UCMDB sia la sonda del flusso di dati siano in esecuzione. Se la sonda è installata in modalità separata, queste istruzioni si riferiscono a Probe Gateway.
- 2** Protezione avanzata del connettore della sonda del flusso di dati in UCMDB:
 - a** Per accedere alla console JMX di UCMDB: Avviare un browser Web e specificare il seguente indirizzo: **http://<nome del computer UCMDB oppure IP>:8080/jmx-console.**

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

- b** Individuare **UCMDB:service=Ports Management Services** e fare clic sul collegamento per aprire la pagina Operazioni.
- c** Individuare l'operazione **PortsDetails** e fare clic su **Invoke**. Prendere nota dell'HTTPS con il numero di porta di autenticazione del client. Il valore predefinito è 8444 e deve essere abilitato.
- d** Tornare alla pagina Operazioni.
- e** Per mappare il connettore della sonda del flusso di dati alla modalità di autenticazione reciproca, richiamare il metodo **mapComponentToConnectors** con i parametri seguenti:
 - **componentName:** mam-collectors
 - **isHTTPSWithClientAuth:** true
 - Tutti gli altri flag: false

Viene visualizzato il messaggio seguente:

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

- f** Tornare alla pagina Operazioni.
- g** Per mappare il connettore di Confidential Manager alla modalità di autenticazione reciproca, richiamare il metodo **mapComponentToConnectors** con i parametri seguenti:
 - **componentName:** cm
 - **isHTTPSWithClientAuth:** true
 - Tutti gli altri flag: false

Viene visualizzato il messaggio seguente:

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

- 3** Copiare il keystore da utilizzare come keystore della sonda nel percorso seguente nel file system della sonda del flusso di dati:
C:\HP\UCMDB\DataFlowProbe\conf\security

Nota:

- Se si crea un nuovo keystore utilizzare il rispettivo nome, in caso contrario utilizzare **cKeyStoreFile**.
 - Se si sta utilizzando il keystore del client predefinito (**cKeyStoreFile**), passare al passaggio 6 a pag. 354.
-

4 Esportare il certificato della sonda dal rispettivo keystore.

- a** Nel computer della sonda eseguire il comando seguente:

```
C:\HP\UCMDB\DataFlowProbe\bin\jre\bin\keytool.exe -export -alias clientcert -
keystore <pKeyStoreFile> -file
C:\HP\UCMDB\DataFlowProbe\conf\security\probe.cert
```

- b** Immettere la password del keystore (**pKeyStorePass**).
- c** Verificare che il certificato venga creato nella directory seguente:
C:\HP\UCMDB\DataFlowProbe\conf\security\probe.cert

5 Importare il certificato della sonda esportato nel truststore di UCMDB.

- a** Nel computer di UCMDB copiare il file creato **probe.cert** nella directory seguente su UCMDB:
C:\HP\UCMDB\UCMDBServer\conf\security

- b** Eseguire il comando seguente:

```
C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -import -v -keystore
<sTrustStoreFile> -file C:\HP\UCMDB\UCMDBServer\conf\security\probe.cert -
alias probecert
```

- c** Immettere la password del truststore del server UCMDB (**sTrustStorePass**).
- d** Quando viene chiesto **Il certificato è attendibile?** premere **s** quindi INVIO.
- e** Accertarsi che l'output sia **Il certificato è stato aggiunto al keystore**.

6 Esportare il certificato di UC MDB dal rispettivo keystore.

- a** Nel computer di UC MDB eseguire il comando seguente:

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

- b** Immettere la password del keystore (**sKeyStorePass**).

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

7 Importare il certificato di UC MDB esportato nel truststore della sonda.

- a** Nel computer della sonda copiare il file creato **server.cert** nella sonda del flusso di dati nel percorso seguente:
C:\HP\UCMDB\DataFlowProbe\conf\security

- b** Eseguire il comando seguente:

```
C:\HP\UCMDB\DataFlowProbe\bin\jre\bin\keytool.exe -import -v -keystore  
<pTrustStoreFile> -file C:\HP\UCMDB\DataFlowProbe\conf\security\server.cert -  
alias ucmbcert
```

- c** Immettere la password del truststore della sonda del flusso di dati (**pTrustStorePass**).

- d** Quando viene chiesto **Il certificato è attendibile?** premere **s** quindi INVIO.

- e** Accertarsi che l'output sia Il certificato è stato aggiunto al keystore.

8 Aggiornare il file della sonda **ssl.properties** che si trova nella directory seguente: **C:\HP\UCMDB\DataFlowProbe\conf\security**

- a** Definire il percorso del keystore nella proprietà **javax.net.ssl.keyStore** (**pKeyStoreFile**). Per la limitazione consultare “Limiti dell'autenticazione reciproca” a pag. 355.

- b** Definire la password del keystore nella proprietà **javax.net.ssl.keyStorePassword** (**pKeyStorePass** crittografata).

- c** Definire il percorso del truststore in **javax.net.ssl.trustStore** property (**pTrustStoreFile**).

- d Definire la password del truststore nella proprietà `javax.net.ssl.trustStorePassword` (`pTrustStorePass` crittografata).

Nota: le proprietà della password del keystore e della password del truststore sono crittografate. Per le istruzioni sulla crittografia consultare “Crittografare le password del keystore e del truststore della sonda” a pag. 362.

- 9 Aggiornare il file `DiscoveryProbe.properties` che si trova nella directory seguente: `C:\HP\UCMDB\DataFlowProbe\conf`.
 - a Aggiornare la proprietà `appilog.agent.probe.protocol` in `HTTPS`.
 - b Aggiornare la proprietà `serverPortHttps` con il numero di porta rilevante come annotato nel passaggio 2 a pag. 351.
- 10 Riavviare il server UCMDB e la sonda del flusso di dati.

Limiti dell'autenticazione reciproca

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

Abilitare il protocollo SSL con autenticazione del server

Per abilitare l'autenticazione del server:

- 1 Verificare che sia UCMDB sia la sonda del flusso di dati siano in esecuzione. Se la sonda è installata in modalità separata, queste istruzioni si riferiscono a Probe Gateway.
- 2 Protezione avanzata del connettore della sonda del flusso di dati in UCMDB:
 - a Per accedere alla console JMX di UCMDB: Avviare un browser Web e specificare il seguente indirizzo: `http://<nome del computer UCMDB oppure IP>:8080/jmx-console`.

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

- b** Individuare **UCMDB:service=Ports Management Services** e fare clic sul collegamento per aprire la pagina Operazioni.
- c** Individuare l'operazione **PortsDetails** e fare clic su **Invoke**. Prendere nota del numero della porta dell'HTTPS. Il valore predefinito è 8443 e deve essere abilitato.
- d** Tornare alla pagina Operazioni.
- e** Per mappare il connettore della sonda del flusso di dati alla modalità di autenticazione reciproca, richiamare il metodo **mapComponentToConnectors** con i parametri seguenti:
 - **componentName:** mam-collectors
 - **isHTTPS:** true
 - Tutti gli altri flag: false

Viene visualizzato il messaggio seguente:

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

- f** Tornare alla pagina Operazioni.
- g** Per mappare il connettore di Confidential Manager alla modalità di autenticazione reciproca, richiamare il metodo **mapComponentToConnectors** con i parametri seguenti:
 - **componentName:** cm
 - **isHTTPS:** true
 - Tutti gli altri flag: false

Viene visualizzato il messaggio seguente:

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

3 Esportare il certificato di UCMDB dal rispettivo keystore.

- a** Nel computer di UCMDB eseguire il comando seguente:

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

- b** Immettere la password del keystore (**sKeyStorePass**).

- c** Verificare che il certificato venga creato in

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

4 Importare il certificato di UCMDB esportato nel truststore della sonda.

- a** Nel computer della sonda copiare il file creato **server.cert** nella sonda del flusso di dati nel percorso seguente:

```
C:\HP\UCMDB\DataFlowProbe\conf\security
```

- b** Eseguire il comando seguente:

```
C:\HP\UCMDB\DataFlowProbe\bin\jre\bin\keytool.exe -import -v -keystore  
<pTrustStoreFile> -file C:\HP\UCMDB\DataFlowProbe\conf\security\server.cert -  
alias ucmbcert
```

- c** Immettere la password del truststore della sonda del flusso di dati (**pTrustStorePass**).

- d** Quando viene chiesto **Il certificato è attendibile?** premere **s** quindi INVIO.

- e** Accertarsi che l'output sia **Il certificato è stato aggiunto al keystore**.

5 Aggiornare il file della sonda **ssl.properties** che si trova nella directory seguente: **C:\HP\UCMDB\DataFlowProbe\conf\security**

- a** Definire il percorso del truststore nella proprietà **javax.net.ssl.trustStore** (**pTrustStoreFile**).

- b** Definire la password del truststore nella proprietà **javax.net.ssl.trustStorePassword** (**pTrustStorePass** crittografata).

Nota: la proprietà della password del truststore è crittografata. Per le istruzioni sulla crittografia consultare “Crittografare le password del keystore e del truststore della sonda” a pag. 362.

- 6** Aggiornare il file **DiscoveryProbe.properties** che si trova nella directory seguente: **C:\HP\UCMDB\DataFlowProbe\conf**
 - a** Aggiornare la proprietà **appilog.agent.probe.protocol** in **HTTPS**.
 - b** Aggiornare la proprietà **serverPortHttps** con il numero di porta rilevante come annotato nel passaggio 2 a pag. 355.
- 7** Riavviare il server UCMDB e la sonda del flusso di dati.

Abilitare l'autenticazione nella sonda del flusso di dati con autenticazione HTTP di base

Importante:

- Il metodo dell'autenticazione di base per l'abilitazione dell'autenticazione sulla sonda del flusso di dati è il metodo meno preferito. Si consiglia di utilizzare la protezione dell'autenticazione reciproca poiché è un metodo di protezione molto più efficace (combina la crittografia dei dati e l'autenticazione del certificato). Per i dettagli consultare “Abilitare il protocollo SSL tra il server UCMDB e la sonda del flusso di dati con l'autenticazione reciproca” a pag. 350.
- Se il protocollo SSL non è abilitato, le credenziali vengono trasmesse a UCMDB come testo normale.

Per impostare l'autenticazione di base:

- 1** Individuare il file seguente: **C:\hp\UCMDB\DataFlowProbe\conf\DiscoveryProbe.properties**.

- 2 Rimuovere i contrassegni dei commenti (#) dalle proprietà seguenti e immettere le rispettive credenziali:

```
appilog.agent.Probe.BasicAuth.Realm=  
appilog.agent.Probe.BasicAuth.User=  
appilog.agent.Probe.BasicAuth.Pwd=
```

Le credenziali devono corrispondere a quelle definite sul server UCMDB.

Connettere la sonda del flusso di dati mediante il proxy inverso

Eeguire la procedura seguente per connettere la sonda del flusso di dati mediante il proxy inverso.

Nota: l'abilitazione dell'autenticazione reciproca quando si utilizza il protocollo SSL tra il server UCMDB e la sonda del flusso di dati non è supportata quando la connessione viene eseguita mediante il proxy inverso.

Per configurare il funzionamento della sonda del flusso di dati rispetto al proxy inverso:

- 1 Modificare il file **discoveryProbe.properties** (in **C:\hp\UCMDB\DataFlowProbe\conf**).
- 2 Impostare la proprietà **serverName** sul nome DNS o IP del server proxy inverso.
- 3 Impostare le proprietà **serverPort** e **serverPortHttps** sulle porte del server proxy inverso.
- 4 Salvare il file.

La configurazione del server proxy seguente è richiesta se le sonde del flusso di dati sono connesse soltanto mediante un proxy inverso a HP Universal CMDB:

Richieste di ... sul server proxy inverso	Richiesta proxy deve essere eseguita da:
/mam-collectors	http://[HP Universal CMDB server]/mam-collectors

La configurazione seguente viene richiesta se un adattatore SOAP viene utilizzato per la replica tramite un server proxy per la protezione (avanzata) di HP Universal CMDB:

Richieste di ... sul server proxy inverso	Richiesta proxy deve essere eseguita da:
/axis2	http://[HP Universal CMDB server]/axis2

Connessione della sonda del flusso di dati e dei client web mediante un proxy inverso

La configurazione seguente è richiesta se le sonde del flusso di dati e gli utenti dell'applicazione sono entrambi connessi mediante un proxy inverso a HP Universal CMDB:

Richieste di ... sul server proxy inverso	Richiesta proxy deve essere eseguita da:
/mam	[HP Universal CMDB server]/mam
/mam_images	[HP Universal CMDB server]/mam_images
/mam-collectors	[HP Universal CMDB server]/mam-collectors
/ucmdb	[HP Universal CMDB server]/ucmdb
/site	[HP Universal CMDB server]/site

Controllo della posizione del file domainScopeDocument

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

Per controllare la posizione del file domainScopeDocument:

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

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

in:

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

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

Per i dettagli sull'utilizzo del file domainScopeDocument per la protezione avanzata di GFD, consultare “Gestione credenziali del flusso di dati” a pag. 315.

- 2 Riavviare la sonda.

Creare un keystore per la sonda del flusso di dati

- 1 Nel computer della sonda eseguire il comando seguente:

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

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

Crittografare le password del keystore e del truststore della sonda

Le password del keystore e del truststore della sonda sono archiviate crittografate in

C:\HP\UCMDB\DataFlowProbe\conf\security\ssl.properties. Questa procedura spiega come crittografare la password.

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

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

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

```
66,85,54,78,69,117,56,65,99,90,86,117,97,75,50,112,65,53,67,114,112,65,61,61
```
- 7** Copiare e incollare la password crittografata nella riga rilevante nel keystore o nel truststore nel file seguente:
C:\HP\UCMDB\DataFlowProbe\conf\security\ssl.properties.

Riferimenti

Keystore e truststore predefiniti della sonda del flusso di dati

In questa sezione vengono trattati i seguenti argomenti:

- “UCMDB” a pag. 364
- “Sonda del flusso di dati” a pag. 365

UCMDB

I file si trovano nella directory seguente:

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

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

Sonda del flusso di dati

I file si trovano nella directory seguente:

C:\HP\UCMDB\DataFlowProbe\conf\security.

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

23

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

Questo capitolo comprende:

Concetti

- Autenticazione LW-SSO - Panoramica a pag. 368

Riferimenti

- Requisiti di sistema di LW-SSO a pag. 370
- Avvisi di protezione LW-SSO a pag. 371

Risoluzione dei problemi e limitazioni a pag. 373

Concetti

Autenticazione LW-SSO - Panoramica

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.

In questa sezione vengono trattati i seguenti argomenti:

- “Scadenza del token LW-SSO” a pag. 368
- “Configurazione consigliata della scadenza del token LW-SSO” a pag. 368
- “Orario GMT” a pag. 369
- “Funzionalità multi-dominio” a pag. 369
- “Ottenerne il SecurityToken per la funzionalità URL” a pag. 369

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 **lwssso** 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 **lwssso** della configurazione.

Riferimenti

Requisiti di sistema di LW-SSO

Nella tabella seguente sono elencati i requisiti di configurazione di LW-SSO:

Applicazione	Versione	Commenti
Java	1.5 e superiore	
HTTP Sevlets API	2.1 e superiore	
Internet Explorer	6.0 e superiore	Il browser deve abilitare i cookie di sessione HTTP e la funzionalità HTTP 302.
FireFox	2.0 e superiore	Il browser deve abilitare i cookie di sessione HTTP e la funzionalità HTTP 302.
JBoss Authentications	JBoss 4.0.3 JBoss 4.3.0	
Tomcat Authentications	Standalone Tomcat 5.0.28 Standalone Tomcat 5.5.20	
Acegi Authentications	Acegi 0.9.0 Acegi 1.0.4	
Spring Security Authentication	Spring Security 2.0.4	
Web Services Engines	Axis 1 - 1.4 Axis 2 - 1.2 JAX-WS-RI 2.1.1	

Avvisi di protezione LW-SSO

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

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

Attenzione:

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

-
- ▶ **Abilita LW-SSO solo se 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 attendibile dalle altre applicazioni integrate determina il livello di protezione delle autenticazioni per tutte le altre applicazioni.

Si raccomanda che soltanto le applicazioni che utilizzano un framework di autenticazione protetto rilascino un token LW-SSO.

- ▶ **Implicazioni crittografia simmetrica.** LW-SSO utilizza la crittografia simmetrica per rilasciare e convalidare i token LW-SSO. Quindi, qualsiasi applicazione che utilizza LW-SSO può rilasciare un token da rendere attendibile per tutte le altre applicazioni che condividono lo stesso parametro **initString**. Questo rischio potenziale è importante quando un'applicazione condivide un `initString` sia residente su, o accessibile da una posizione non attendibile.
- ▶ **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.
- ▶ **Modalità Demo LW-SSO.**
 - ▶ La modalità Demo deve essere utilizzata solo a scopi dimostrativi.
 - ▶ La modalità Demo deve essere utilizzata solo su reti non protette.
 - ▶ La modalità Demo non può essere utilizzata in produzione. Non può essere utilizzata alcuna combinazione della modalità Demo con la modalità di produzione.

Risoluzione dei problemi e limitazioni

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>

► Comportamento di cookie di terze parti in Internet Explorer:

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

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

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

► **Token SAML2.**

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

Quindi, se il token SAML2 è utilizzato per accedere a una seconda applicazione, l'utente che si disconnette dalla prima applicazione non viene disconnesso dalla seconda applicazione.

- La scadenza del token SAML2 non viene presa dalla gestione della sessione dell'applicazione.

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

- **JAAS Realm.** Il JAAS Realm in Tomcat non è supportato.

- **Uso degli spazi nelle directory Tomcat.** L'uso degli spazi nelle directory Tomcat non è supportato.

Non è possibile utilizzare LW-SSO quando un percorso (cartelle) di installazione Tomcat include gli spazi (ad esempio, File di programma) e il file di configurazione LW-SSO è posizionato nella cartella Tomcat `common\classes`.

- **Configurazione del bilanciamento del carico.** Si deve configurare un bilanciamento del carico distribuito con LW-SSO per poter utilizzare sessioni sticky.
- **Modalità Demo.** In modalità Demo LW-SSO supporta pertanto collegamenti da un'applicazione all'altra e non supporta la digitazione di un URL in una finestra del browser a causa dell'assenza di un'intestazione del referrer HTTP in questo caso.

24

Autenticazione per l'accesso a HP Universal CMDB

Questo capitolo comprende:

Concetti

- Impostazione del metodo di autenticazione a pag. 378

Compiti

- Abilitare e definire il metodo di autenticazione LDAP a pag. 379
- Impostare una connessione protetta con il protocollo SSL (Secure Sockets Layer) a pag. 380
- Utilizzare la console JMX per verificare le connessioni LDAP a pag. 382
- Configurare le impostazioni LDAP utilizzando la console JMX a pag. 382
- Abilitare l'accesso a HP Universal CMDB con LW-SSO a pag. 383
- Ripristinare la configurazione LW-SSO corrente nell'ambiente distribuito a pag. 385

Concetti

Impostazione del metodo di autenticazione

Per eseguire l'autenticazione è necessario lavorare:

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

Per i dettagli sul protocollo LDAP consultare "Mapping LDAP" nella *Guida all'amministrazione di HP Universal CMDB*.

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

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

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

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

Compiti

Abilitare e definire il metodo di autenticazione LDAP

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

Per abilitare e definire il metodo di autenticazione LDAP:

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

```
ldap://<ldapHost>[:<porta>][<baseDN>][??scope]
```

Ad esempio:

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

- 3** Selezionare la categoria **Definizione gruppo LDAP**, individuare **DN di base dei gruppi** e immettere il nome distinto del gruppo generale.
- 4** Individuare **DN di base dei gruppi radice** e immettere il nome distinto del gruppo radice.
- 5** Selezionare la categoria **LDAP - Generale**, individuare **Abilita sincronizzazione utenti** e verificare che il valore sia impostato su **True**.
- 6** Selezionare la categoria **LDAP - Autenticazione generale**, individuare **Password per l'utente autorizzato alla ricerca** e immettere la password.
- 7** Salvare i nuovi valori. Per sostituire una voce con il valore predefinito, fare clic su **Ripristina predefinito**.
- 8** Mappare i gruppi utenti LDAP ai ruoli utente di UCMDB. Per i dettagli consultare "Autenticazione per l'accesso a HP Universal CMDB" a pag. 377.

Il protocollo predefinito utilizzato per comunicare con il server LDAP è TCP ma si può cambiare con il protocollo SSL. Per i dettagli consultare "Impostare una connessione protetta con il protocollo SSL (Secure Sockets Layer)" a pag. 380.

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

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

HP Universal CMDB supporta SSL con utilizzo di un certificato emesso da una Autorità di certificazione (AC) attendibile. Questa AC è compresa in Java Runtime Environment.

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

Per i dettagli sulla configurazione della piattaforma HP Universal CMDB per il supporto della comunicazione basata su SSL, consultare "Abilitazione della comunicazione Secure Sockets Layer (SSL)" a pag. 291.

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

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

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

Ad esempio:

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

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

Nota: queste impostazioni si possono configurare anche utilizzando la console JMX. Per i dettagli consultare "Configurare le impostazioni LDAP utilizzando la console JMX" a pag. 382.

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

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

Ad esempio:

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

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

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

Utilizzare la console JMX per verificare le connessioni LDAP

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

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

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

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

Configurare le impostazioni LDAP utilizzando la console JMX

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

Per configurare le impostazioni di autenticazione LDAP:

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

Potrebbe essere necessario accedere con nome utente e password.
- 2 In **UCMDB** fare clic su **UCMDB-UI:name=LDAP Settings** per aprire la pagina Operazioni.

- 3 Per visualizzare le impostazioni di autenticazione LDAP correnti, individuare il metodo **getLDAPSettings**. Fare clic su **Invoke**. Viene visualizzata una tabella con tutte le impostazioni LDAP e i rispettivi valori.
- 4 Per cambiare i valori delle impostazioni di autenticazione LDAP, individuare il metodo **configureLDAP**. Immettere i valori per le impostazioni rilevanti e fare clic su **Invoke**. Nella pagina Operation Result di JMX MBEAN viene indicato se le impostazioni di autenticazione LDAP sono state aggiornate correttamente.

Nota: se non viene immesso un valore per un'impostazione, viene mantenuto il valore corrente.

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

Abilitare l'accesso a HP Universal CMDB con LW-SSO

Per abilitare LW-SSO per HP Universal CMDB, utilizzare una delle procedure seguenti:

Abilitare LW-SSO mediante la console JMX

- 1 Per accedere alla console JMX immettere l'indirizzo seguente nel browser Web: **http://<nome_server>:8080/jmx-console**, dove **<nome_server>** è il nome del computer in cui è installato HP Universal CMDB.
- 2 In **UCMDB-UI** fare clic su **name=LW-SSO configuration** per aprire la pagina Operazioni.
- 3 Selezionare la stringa **init** utilizzando il metodo **setInitString**.

- 4 Impostare il nome di dominio del computer sul quale è installato UCMDDB utilizzando il metodo **setDomain**.
- 5 Chiamare il metodo **setEnabledForUI** con il parametro impostato su **True**.
- 6 **Facoltativo.** Impostare altri parametri di configurazione LW-SSO utilizzando i metodi pertinenti. Per i dettagli su altri parametri, consultare "Autenticazione LW-SSO - Panoramica" a pag. 368.
- 7 Per visualizzare la configurazione LW-SSO come è stata salvata nel meccanismo impostazioni, chiamare il metodo **retrieveConfigurationFromSettings**.
- 8 Per visualizzare la configurazione LW-SSO effettivamente caricata, chiamare il metodo **retrieveConfiguration**.

Abilitare LW-SSO mediante Impostazioni infrastruttura di UCMDDB.

- 1 Accedere a HP Universal CMDB.
- 2 Selezionare **Amministrazione > Impostazioni infrastruttura > categoria Impostazioni generali**.
- 3 Immettere il nome di dominio e i valori del parametro `initString` per le opzioni **Dominio LW-SSO** e **Stringa init LW-SSO**.
- 4 Cambiare **Stato di abilitazione di LW-SSO** in **True**.
- 5 **Facoltativo.** Impostare altri parametri di configurazione LW-SSO utilizzando le voci dei parametri pertinenti. Per i dettagli su altri parametri, consultare "Autenticazione LW-SSO - Panoramica" a pag. 368.
- 6 Riavviare il server.

Ripristinare la configurazione LW-SSO corrente nell'ambiente distribuito

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

Per ripristinare la configurazione LW-SSO corrente:

- 1** Avviare un browser Web e specificare il seguente indirizzo:
`http://localhost.<nome_dominio>:8080/jmx-console.`
Potrebbero essere richiesti nome utente e password.
- 2** Individuare **UCMDB:service=Security Services** e fare clic sul collegamento per aprire la pagina Operazioni.
- 3** Individuare l'operazione **retrieveLWSSOConfiguration**.
- 4** Fare clic su **Invoke** per ripristinare la configurazione.

25

Confidential Manager

Questo capitolo comprende:

Concetti

- Confidential Manager - Panoramica a pag. 388
- Considerazioni sulla protezione a pag. 389

Compiti

- Configurare il server HP Universal CMDB a pag. 390

Riferimenti

- Definizioni a pag. 392
- Proprietà di crittografia a pag. 393

Concetti

Confidential Manager - Panoramica

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

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

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

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

Per le linee guida dettagliate sulla gestione della crittografia delle credenziali sulla sonda del flusso di dati, consultare “Gestione credenziali del flusso di dati” a pag. 315.

Considerazioni sulla protezione

- È possibile utilizzare le dimensioni chiave seguenti per l'algoritmo di protezione: 128, 192 e 256 bit. L'algoritmo viene eseguito più velocemente con una chiave più piccola ma è meno sicuro. La dimensione 128-bit è abbastanza sicura nella maggior parte dei casi.
- Per rendere il sistema più sicuro, utilizzare il codice MAC: impostare **useMacWithCrypto** su **true**. Per i dettagli consultare “Proprietà di crittografia” a pag. 393. L'impostazione di questo parametro aumenta comunque le dimensioni del database.
- Per sfruttare i fornitori di una forte protezione dei clienti, è possibile utilizzare la modalità JCE.

Compiti

Configurare il server HP Universal CMDB

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

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

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

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

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

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

- 4** Per apportare cambiamenti alla configurazione, copiare il file XML chiamato nel passaggio precedente in un editor di testo. Apportare i cambiamenti in base alla tabella in "Proprietà di crittografia" a pag. 393.

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

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

- **username**. Nome utente.
- **customer**. Il valore predefinito è ALL_CUSTOMERS.
- **resource**. Nome della risorsa. Il valore predefinito è ROOT_FOLDER.

- **permission.** Scegliere tra ALL_PERMISSIONS, CREATE, READ, UPDATE e DELETE. Il valore predefinito è ALL_PERMISSIONS.

Fare clic su **Invoke**.

- 6 Se necessario riavviare HP Universal CMDB.

Nota:

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

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

Nota:

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

Riferimenti

Definizioni

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

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

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

Nota:

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

Proprietà di crittografia

Nella tabella seguente vengono descritte le proprietà di crittografia. Per i dettagli sull'utilizzo dei parametri, consultare “Configurare il server HP Universal CMDB” a pag. 390.

Parametro	Descrizione	Valore consigliato
encryptTransportMode	Crittografare i dati trasportati: <ul style="list-style-type: none"> ➤ true ➤ false 	true
encryptDecryptInitString	Password per la crittografia	Maggiore di 8 caratteri
cryptoSource	Libreria di implementazione della crittografia da utilizzare: <ul style="list-style-type: none"> ➤ lw ➤ jce ➤ windowsDPAPI ➤ lwJCECompatible 	lw
lwJCEPBCompatibilityMode	Supporta le versioni precedenti della crittografia semplificata: <ul style="list-style-type: none"> ➤ true ➤ false 	true
cipherType	Tipo di crittografia utilizzata da CM. CM supporta un solo valore: symmetricBlockCipher	symmetricBlockCipher
engineName	<ul style="list-style-type: none"> ➤ AES ➤ Blowfish ➤ DES ➤ 3DES ➤ Null (nessuna crittografia) 	AES
algorithmModeName	Modalità di algoritmo della crittografia a blocchi: <ul style="list-style-type: none"> ➤ CBC 	CBC

Parametro	Descrizione	Valore consigliato
algorithmPaddingName	Standard spaziatura interna: <ul style="list-style-type: none"> ▶ PKCS7Padding ▶ PKCS5Padding 	PKCS7Padding
keySize	Dipende dall'algoritmo (quale engineName supporta)	256
pbeCount	Numero di esecuzioni della funzione hash per creare la chiave da encryptDecryptInitString . Qualsiasi numero positivo.	1000
pbeDigestAlgorithm	Tipo di hash: <ul style="list-style-type: none"> ▶ SHA1 ▶ SHA256 ▶ MD5 	SHA256
encodingMode	Rappresentazione ASCII dell'oggetto crittografato: <ul style="list-style-type: none"> ▶ Base64 ▶ Base64Url 	Base64Url
useMacWithCrypto	Definisce se il codice MAC viene utilizzato con la crittografia: <ul style="list-style-type: none"> ▶ true ▶ false 	false
macType	Tipo di codice di autenticazione dei messaggi (message authentication code, MAC): <ul style="list-style-type: none"> ▶ hmac 	hmac
macKeySize	Dipende dall'algoritmo MAC	256
macHashName	Algoritmo MAC hash <ul style="list-style-type: none"> ▶ SHA256 	SHA256

Parte VII

Ripristino di emergenza

26

Impostazione del ripristino di emergenza

Questo capitolo comprende:

Concetti

- Ripristino di emergenza - Panoramica a pag. 398

Compiti

- Preparare l'ambiente del ripristino di emergenza a pag. 399
- Preparare l'istanza di failover di HP Universal CMDB per l'attivazione a pag. 402
- Eseguire la procedura di pulizia all'avvio a pag. 403

Concetti

Ripristino di emergenza - Panoramica

Questo capitolo descrive i principi e le linee guida di base su come impostare un sistema di ripristino di emergenza e i passaggi necessari per fare in modo che un sistema HP Universal CMDB secondario diventi il nuovo sistema primario. Il capitolo copre un ambiente HP Universal CMDB tipico di un server HP Universal CMDB e un server del database contenente gli schemi del database di HP Universal CMDB.

Nota:

- Questo capitolo è una guida di alto livello che introduce i concetti necessari per abilitare il ripristino di emergenza.
 - Il ripristino di emergenza prevede passaggi manuali per spostare i vari file di configurazione e gli aggiornamenti negli schemi del database di HP Universal CMDB. Questa procedura richiede almeno un amministratore di HP Universal CMDB e un amministratore di database che conosca i database e gli schemi di HP Universal CMDB.
 - Esistono distribuzioni e configurazioni diverse di HP Universal CMDB. Per convalidare che lo scenario di ripristino di emergenza funzioni in un determinato ambiente, è necessario che venga interamente testato e documentato. Rivolgersi a HP Professional Services per accertarsi che siano messe in atto le procedure consigliate nel design e nel workflow del failover per ogni scenario di ripristino di emergenza.
-

Compiti

Preparare l'ambiente del ripristino di emergenza

La preparazione dell'ambiente del ripristino di emergenza comprende i passaggi seguenti:

- ▶ “Installare il software di HP Universal CMDB nell'ambiente failover” a pag. 399
- ▶ “Configurare il backup del sistema e dei dati” a pag. 400

Installare il software di HP Universal CMDB nell'ambiente failover

Installare una seconda istanza di HP Universal CMDB che corrisponda all'ambiente di produzione corrente.

- ▶ Installare esattamente la stessa versione di HP Universal CMDB dell'ambiente di backup, come quella utilizzata nell'ambiente di produzione.
- ▶ Per semplificare le problematiche legate a diverse capacità e distribuzioni, l'ambiente di backup deve essere lo stesso dell'ambiente di produzione.
- ▶ Non eseguire l'utilità di configurazione del server e del database e non creare alcun database.
- ▶ Non avviare il sistema di backup.

Nota: l'ambiente di ripristino di emergenza deve ricordare molto da vicino l'ambiente di produzione di HP Universal CMDB. L'hardware, la distribuzione e le versioni devono essere messi tutti in corrispondenza per evitare l'eventuale perdita di funzionalità quando si passa al sistema di failover.

Configurare il backup del sistema e dei dati

Questo passaggio comprende la copia delle directory di configurazione nell'istanza di failover e la configurazione dell'invio del file di registro del database.

Copia delle directory di configurazione nell'istanza di failover

Copiare dall'istanza di produzione di HP Universal CMDB nello stesso tipo di server nell'istanza di failover eventuali file cambiati nelle directory seguenti:

- UCMDBServer\conf
- UCMDBServer\content\

Copiare anche eventuali altri file o directory nel sistema che sono stati personalizzati.

Nota: si consiglia di eseguire backup dei server HP Universal CMDB con frequenza almeno giornaliera. A seconda del numero e dell'intervallo di cambiamenti di configurazione potrebbe essere necessario adottare un intervallo più frequente per evitare perdite maggiori di cambiamenti di configurazione in caso di perdita dell'istanza di produzione.

Microsoft SQL Server - Configurare l'invio del file di registro del database

Per fornire i dati di monitoraggio e configurazione più aggiornati possibile è fondamentale abilitare l'invio del file di registro per ridurre il tempo delle interruzioni dei dati. L'utilizzo dell'invio del file di registro consente di creare un duplicato esatto del database originale che non comprende soltanto lo scarto legato al processo di copia e caricamento. Si ha la possibilità in tal modo di rendere il server del database di standby un nuovo server primario del database se il server del database originale non risulta disponibile. Quando il server primario originale è di nuovo disponibile, è possibile renderlo un nuovo server di standby, invertendo in modo efficace i ruoli dei server.

L'invio del file di registro deve essere configurato per i database di HP Universal CMDB seguenti:

- Database di HP Universal CMDB
- Database Cronologia di HP Universal CMDB

Questa sezione non contiene i passaggi specifici per configurare l'invio del file di registro. L'amministratore del database di HP Universal CMDB può utilizzare i collegamenti seguenti come guida alla configurazione dell'invio del file di registro per la versione appropriata del software del database utilizzato nell'ambiente di HP Universal CMDB:

Microsoft SQL Server 2000:

- support.microsoft.com/default.aspx?scid=http://support.microsoft.com/support/sq/content/2000papers/LogShippingFinal.asp
- www.microsoft.com/technet/prodtechnol/sql/2000/maintain/logship1.msp

Microsoft SQL Server 2005:

- msdn2.microsoft.com/en-us/library/ms188625.aspx
- msdn2.microsoft.com/en-us/library/ms190016.aspx
- msdn2.microsoft.com/en-us/library/ms187016.aspx

Oracle - Configurare il database di standby (Data Guard)

Oracle dispone di registri soltanto a livello di database, non per ciascuno schema. Ciò significa che non è possibile creare un database di standby a livello dello schema ed è necessario creare copie dei database del sistema di produzione sul sistema di backup.

Nota: se Oracle è la piattaforma del database, HP consiglia di utilizzare Oracle 11i per l'uso di Data Guard.

Questa sezione non contiene i passaggi specifici per configurare un database di standby. L'amministratore del database di HP Universal CMDB può utilizzare il collegamento seguente come guida alla configurazione del database di standby per Oracle 11i:

http://download.oracle.com/docs/cd/B19306_01/server.102/b14239/toc.htm

Al termine della configurazione del database di backup, è necessario sincronizzare il database di failover di HP Universal CMDB con il database di produzione di HP Universal CMDB.

Preparare l'istanza di failover di HP Universal CMDB per l'attivazione

Al momento dell'attivazione dell'istanza di failover, eseguire i passaggi seguenti nell'ambiente di failover:

- Attivare il sistema di backup, compreso il rispettivo database.
- Accertarsi che tutti i registri più recenti del database sono stati aggiornati nei database dell'ambiente di failover.
- Eseguire la procedura di pulizia all'avvio per rimuovere un'eventuale localizzazione nei database. Per i dettagli consultare “Eseguire la procedura di pulizia all'avvio” a pag. 403.

Eseguire la procedura di pulizia all'avvio

Questa procedura ripulisce tutti i riferimenti specifici del computer nelle configurazioni dall'istanza di produzione. È necessaria per reimpostare il database sul sistema di backup.

Nota:

- ▶ Prima di avviare le procedure di attivazione, l'amministratore di HP Universal CMDB deve accertarsi che sia stata applicata la licenza appropriata all'istanza di failover.
- ▶ HP consiglia di far eseguire a un amministratore esperto le istruzioni SQL previste da questa procedura.

1 Svuotare e aggiornare le tabelle:

```
update CUSTOMER_REGISTRATION set CLUSTER_ID=null;
truncate table CLUSTER_SERVER;
truncate table SERVER;
truncate table CLUSTERS;
```

2 Eseguire l'utilità di configurazione del server e del database.

Eseguire l'utilità di configurazione del server e del database su ciascun computer per reinizializzare le tabelle necessarie nel database. Per eseguire l'utilità di configurazione del server e del database selezionare **Start > Tutti i programmi > HP UCMDB > Avvio della procedura guidata di configurazione di HP Universal CMDB.**

Nota:

- ▶ Quando si esegue l'utilità di configurazione del server e del database, accertarsi di riconnettere gli stessi database creati per l'ambiente di failover (ovvero quello al quale sono stati inviati i dati di backup). Si potrebbe verificare la perdita totale dei dati di configurazione se l'utilità viene eseguita sull'istanza di produzione.
 - ▶ Quando richiesto per i database dall'utilità di configurazione del server e del database, accertarsi di immettere i nomi dei nuovi database nell'ambiente di failover.
-

3 Avviare i server.

Per eseguire il ripristino di emergenza da un sistema a elevata disponibilità, avviare uno dei server HP Universal CMDB, eseguire lo strumento di configurazione di sistema su quel server per la configurazione di un cluster e aggiungere nuovi server di failover a questo cluster.

4 Attivare l'ambiente di backup.

Avviare HP Universal CMDB nell'ambiente di failover.

Parte VIII

Introduzione a HP Universal CMDB

27

Accesso a HP Universal CMDB mediante il server Web IIS

Questo capitolo comprende:

Concetti

- Accesso a HP Universal CMDB mediante IIS - Panoramica a pag. 408

Compiti

- Impostazione di IIS per consentire l'accesso a UCMDDB - Windows 2003 a pag. 409
- Impostazione di IIS per consentire l'accesso a UCMDDB - Windows 2008 a pag. 413
- Configurare la sonda del flusso di dati a pag. 416

Concetti

Accesso a HP Universal CMDB mediante IIS - Panoramica

In questo capitolo viene descritto come accedere a HP Universal CMDB utilizzando il server Web Microsoft Internet Information Services (IIS).

È possibile impostare il server Web IIS per consentire agli utenti finali e ai client di HP Universal CMDB (ad esempio la sonda del flusso di dati) di accedere al sistema tramite il server Web IIS Web. Grazie a questa impostazione gli utenti finali e i client di HP Universal CMDB utilizzano l'URL del computer di IIS per accedere a UCMDB anziché utilizzare l'URL del computer di UCMDB.

In questa sezione vengono trattati i seguenti argomenti:

- ▶ “Software richiesto per l'integrazione” a pag. 408
- ▶ “Configurazioni supportate” a pag. 408

Software richiesto per l'integrazione

La tabella seguente illustra il software richiesto per l'integrazione:

IIS Web Server	Versione 6.0, 7.X
HP Universal CMDB Server	Versione 9.02 o successiva

Configurazioni supportate

Le configurazioni seguenti sono supportate per questa integrazione:

- ▶ Windows 2003/8 64-bit, HP Universal CMDB 9.02 o successiva e IIS 6 oppure 7.X sullo **stesso** server.
- ▶ Windows 2003/8 64-bit, HP Universal CMDB 9.02 o successiva e IIS 6 oppure 7.X su server **separati**.

Compiti

Impostazione di IIS per consentire l'accesso a UCMDDB - Windows 2003

In questa sezione viene descritta la procedura di integrazione di HP Universal CMDB e IIS per Windows 2003.

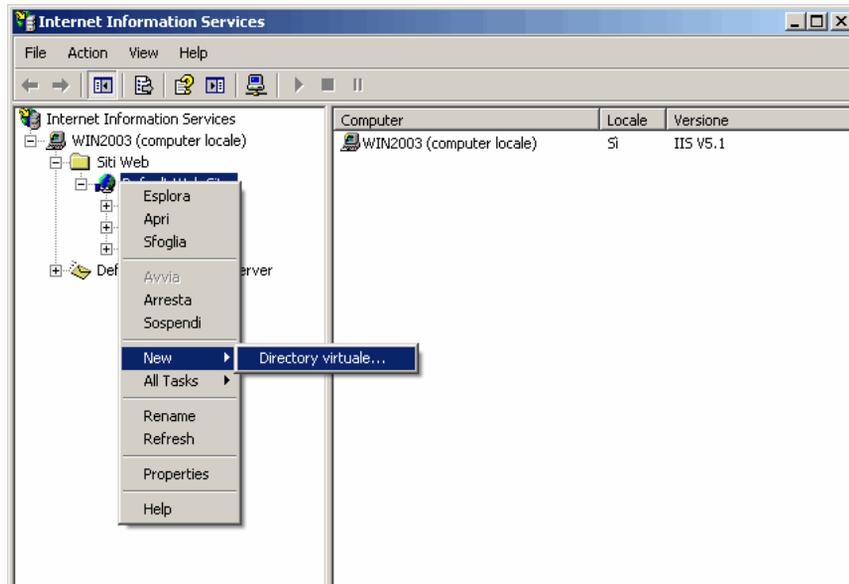
Per l'interazione manuale di HP Universal CMDB e IIS:

1 Se il server HP Universal CMDB non risiede nello stesso computer di IIS, copiare tutti i file dalla directory

C:\hp\UCMDDB\UCMDBServer\tools\iis_integration nella cartella **c:\ucmdb_iis** del computer di IIS. Nel computer di IIS modificare i file seguenti:

- a** Nel file **workers.properties.minimal** cambiare la stringa **worker.localAjp.host=localhost** con il nome host del server UCMDDB.
- b** Nel file **isapi_redirect.properties**:
 - Il **log_file** deve puntare a una cartella che contiene i registri di integrazione, ad esempio **c:\ucmdb_iis\isapi.log**.
 - Il **worker_file** deve contenere il percorso del file **workers.properties.minimal**, ad esempio **C:\ucmdb_iis\workers.properties.minimal**.
 - Il **worker_mount_file** deve contenere il percorso del file **uriworkermap.properties**, ad esempio **C:\ucmdb_iis\uriworkermap.properties**.

- 2 Se il server HP Universal CMDB risiede nello stesso computer di IIS, modificare il file **isapi_redirect.properties** nella directory **C:\hp\UCMDB\UCMDBServer\tools\iis_integration** come segue:
 - a Il **log_file** deve puntare a una cartella che contiene i registri di integrazione, ad esempio **C:\hp\UCMDB\UCMDBServer\runtime\log\isapi.log**.
 - b Il **worker_file** deve contenere il percorso del file **workers.properties.minimal**, ad esempio **C:\hp\UCMDB\UCMDBServer\tools\iis_integration\workers.properties.minimal**.
 - c Il **worker_mount_file** deve contenere il percorso del file **uriworkermap.properties**, ad esempio **C:\hp\UCMDB\UCMDBServer\tools\iis_integration\uriworkermap.properties**.
- 3 Cambiare la stringa **worker.localAjp.host=localhost** con il nome host del server UCMDB (se il server HP Universal CMDB non risiede nello stesso computer di IIS).
- 4 Aprire la console di gestione di IIS. Eseguire **inetmgr** dalla riga di comando.
- 5 Aggiungere una nuova directory virtuale al proprio sito Web IIS per **Windows 2003/IIS6**:

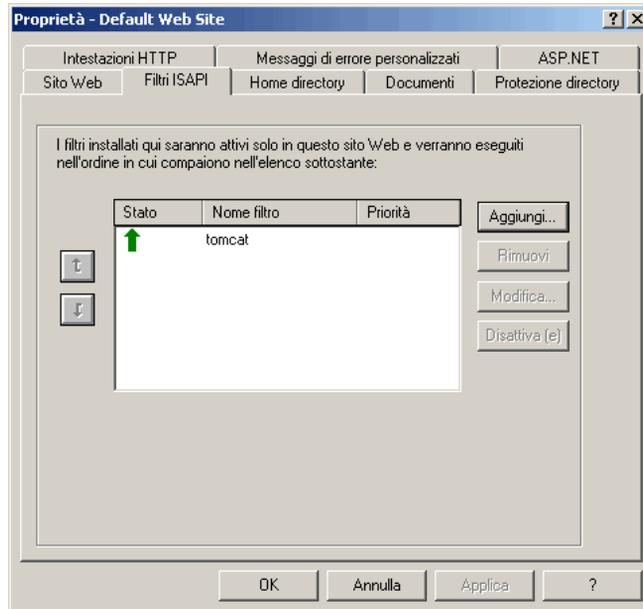


- 6 Viene visualizzata la finestra Creazione guidata Directory virtuale. L'alias della directory virtuale deve essere **jakarta**. Il percorso fisico deve essere **C:\hp\UCMDB\UCMDBServer\tools\iis_integration**. Se il server UCMDB e il server IIS sono in esecuzione su computer separati, il percorso deve essere la directory sul computer di IIS. Consentire l'accesso di tipo **Esecuzione** alla nuova directory virtuale:



- 7 Aprire la finestra di dialogo **Proprietà - Sito Web predefinito** e aggiungere **isapi_redirect.dll** come filtro ISAPI al proprio sito Web IIS. Il nome del filtro deve riflettere il rispettivo compito (ad esempio **tomcat**) e l'eseguibile deve essere **isapi_redirect.dll**. Se il server UCMDB e il server IIS sono in esecuzione su computer separati, l'eseguibile deve essere **isapi_redirect.dll** nella directory dove è stato copiato sul computer di IIS.
- 8 Aprire **Estensioni servizio Web**, selezionare **Tutte le estensioni ISAPI sconosciute** dall'elenco e fare clic su **Consenti**.

- 9 Riavviare IIS (arrestare e avviare il servizio IIS) e accertarsi che il filtro **tomcat** sia contrassegnato con una freccia verde verso l'alto:



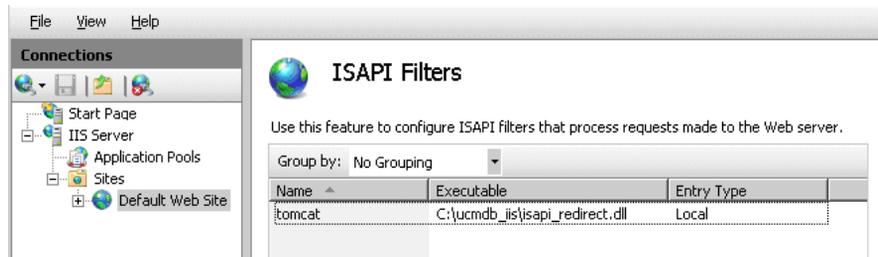
Impostazione di IIS per consentire l'accesso a UCMDDB - Windows 2008

In questa sezione viene descritta la procedura di integrazione di HP Universal CMDB e IIS per Windows 2008.

Per l'interazione manuale di HP Universal CMDB e IIS:

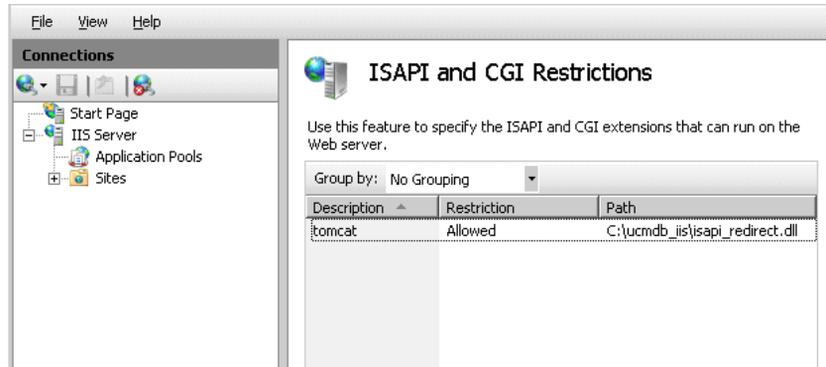
- 1** Se il server HP Universal CMDB non risiede nello stesso computer di IIS, copiare tutti i file dalla directory **C:\hp\UCMDDB\UCMDBServer\tools\iis_integration** nella cartella **c:\ucmdb_iis** del computer di IIS. Nel computer di IIS modificare i file seguenti:
 - a** Nel file **workers.properties.minimal** cambiare la stringa **worker.localAjp.host=localhost** con il nome host del server UCMDDB.
 - b** Nel file **isapi_redirect.properties**:
 - Il **log_file** deve puntare a una cartella che contiene i registri di integrazione, ad esempio **c:\ucmdb_iis\isapi.log**.
 - Il **worker_file** deve contenere il percorso del file **workers.properties.minimal**, ad esempio **C:\ucmdb_iis\workers.properties.minimal**.
 - Il **worker_mount_file** deve contenere il percorso del file **uriworkermap.properties**, ad esempio **C:\ucmdb_iis\uriworkermap.properties**.
- 2** Se il server HP Universal CMDB risiede nello stesso computer di IIS, modificare il file **isapi_redirect.properties** nella directory **C:\hp\UCMDDB\UCMDBServer\tools\iis_integration** come segue:
 - a** Il **log_file** deve puntare a una cartella che contiene i registri di integrazione, ad esempio **C:\hp\UCMDDB\UCMDBServer\runtime\log\isapi.log**.
 - b** Il **worker_file** deve contenere il percorso del file **workers.properties.minimal**, ad esempio **C:\hp\UCMDDB\UCMDBServer\tools\iis_integration\workers.properties.minimal**.

- c** Il **worker_mount_file** deve contenere il percorso del file **uriworkermap.properties**, ad esempio
C:\hp\UCMDB\UCMDBServer\tools\iis_integration\uriworkermap.properties.
- 3** Cambiare la stringa **worker.localAjp.host=localhost** con il nome host del server UCMDB (se il server HP Universal CMDB non risiede nello stesso computer di IIS).
- 4** Aprire la **console di gestione di IIS**. Eseguire **inetmgr** dalla riga di comando.
- 5** Fare doppio clic su **ISAPI**.
- 6** Fare clic con il pulsante destro del mouse sulla finestra principale nella **console di gestione di IIS** e selezionare **Aggiungi**.
- 7** Aggiungere **isapi_redirect.dll** come filtro ISAPI al proprio sito Web IIS. Il nome del filtro deve riflettere il rispettivo compito (ad esempio **tomcat**) e l'eseguibile deve essere **isapi_redirect.dll**. Se il server UCMDB e il server IIS sono in esecuzione su computer separati, l'eseguibile deve essere **isapi_redirect.dll** nella directory dove è stato copiato sul computer di IIS.



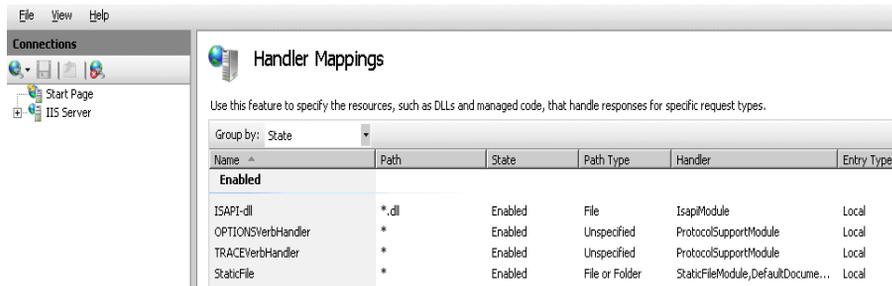
- 8** Aggiungere una nuova directory virtuale al proprio sito Web IIS. L'alias della directory virtuale deve essere **jakarta**. La directory virtuale deve puntare a **C:\hp\UCMDB\UCMDBServer\tools\iis_integration** (se la cartella risiede nello stesso server UCMDB) oppure alla directory dove è stato copiato **iis_integration** se risiede in un server diverso.
- 9** Selezionare il nome del server IIS nel riquadro **Connessioni**.
- 10** Fare doppio clic su **Restrizione ISAPI e CGI**.
- 11** Fare clic con il pulsante destro del mouse e immettere le stesse informazioni aggiunte nel passaggio 7 precedente.

12 Selezionare la casella per consentire l'esecuzione di **Percorso**.



13 Aprire **Mapping gestori**.

14 Selezionare **ISAPI-dll**. Fare clic on pulsante destro del mouse e selezionare **Modifica autorizzazioni funzionalità**. Fare clic su **Esegui**.



15 Riavviare IIS.

16 In UCMDB accedere a Impostazioni infrastruttura (**Amministrazione > Impostazioni infrastruttura > Impostazioni generali**). Cambiare l'opzione **Abilita connessioni AJP** in **True** e riavviare il server UCMDB.

Risoluzione dei problemi e limitazioni

Non è possibile aprire la console JMX da IIS. Ciò significa che l'autenticazione di base non può passare da Jetty.

Configurare la sonda del flusso di dati

Per la configurazione della sonda del flusso di dati, cambiare le stringhe seguenti nel file seguente: **C:\hp\UCMDB\DataFlowProbe\conf\DiscoveryProbe.properties**:

- `serverName = <nome host IIS>`
- `serverPort = <porta HTTP IIS>`, per impostazione predefinita 80

L'URL di IIS (ad esempio **http://<nome host IIS>/ucmdb**) può essere utilizzato ora per accedere a UCMDB, alla console JMX, a UCMDB SDK e così via.

28

Accesso a HP Universal CMDB

Questo capitolo comprende:

Concetti

- Accesso a HP Universal CMDB - Panoramica a pag. 418
- Modalità di installazione locale a pag. 419

Compiti

- Accesso a HP Universal CMDB e ai rispettivi componenti a pag. 420
- Abilitare l'accesso automatico a pag. 422
- Cambiare il limite di tempo predefinito per la disconnessione dell'utente a causa di inattività a pag. 423

Concetti

Accesso a HP Universal CMDB - Panoramica

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

Per i dettagli sui requisiti del browser Web e i requisiti minimi per visualizzare HP Universal CMDB, consultare "Matrice di supporto di HP Universal CMDB" a pag. 35.

Per i dettagli sull'accesso a HP Universal CMDB, consultare Parte VI, "Protezione avanzata di HP Universal CMDB".

Per i dettagli sulle strategie di autenticazione che si possono utilizzare in HP Universal CMDB consultare "Impostazione del metodo di autenticazione" a pag. 378.

Per informazioni sulla risoluzione dei problemi di accesso consultare "Login Troubleshooting" on page 175.

Suggerimento: per la guida completa all'accesso fare clic sul pulsante **Guida** nella pagina di accesso.

Modalità di installazione locale

La modalità di installazione locale è un metodo di caricamento di UCMDB che riduce notevolmente il tempo di caricamento dell'applet. Quando si utilizza il metodo di installazione locale, i file dell'applet (jars) vengono caricati in una directory locale denominata **UcldbAppletJars** che si trova nella directory temporanea dell'ambiente. Le classi vengono caricate utilizzando un caricatore di classe personalizzato che funziona più velocemente ma non verifica la firma dei jars firmati. La modalità di installazione locale viene quindi considerata una modalità non protetta.

Per selezionare la modalità di installazione locale, selezionare la casella di controllo **Abilita la modalità di installazione locale** nella schermata di accesso. Questa casella di controllo è visibile soltanto se il parametro **Autorizzazione della modalità di installazione locale** è stato impostato su **True** in Gestione impostazioni infrastruttura. È possibile impostare lo stato predefinito della casella di controllo utilizzando l'impostazione **Stato iniziale della modalità di installazione locale**. Quando il parametro è impostato su **True** la casella di controllo è selezionata per impostazione predefinita. Quando è impostata su **False** la casella di controllo è deselezionata per impostazione predefinita.

Nota: se all'accesso si seleziona la casella di controllo **Memorizza dati su questo computer** lo stato della casella di controllo **Abilita la modalità di installazione locale** resta invariata per l'accesso successivo, a prescindere dalle impostazioni dell'infrastruttura.

Per i clienti di HP Software-as-a-Service le impostazioni dell'installazione sono concepite per le esigenze del singolo cliente.

Compiti

Accesso a HP Universal CMDB e ai rispettivi componenti

Questa sezione spiega come accedere ai componenti di HP Universal CMDB.

- 1** Nel browser Web, immettere l'URL del server HP Universal CMDB, ad esempio `http://<nome server o indirizzo IP>.<nome dominio>:8080` dove `<nome server o indirizzo IP>.<nome dominio>` rappresenta il nome dominio completo (FQDN) del server HP Universal CMDB.

Se HP Universal CMDB è impostato per funzionare con un proxy inverso, immettere `https://<nome_server_proxy>:443` dove `nome_server_proxy` è il nome o indirizzo IP del server proxy.

Se sul computer non è installata la versione Java corretta, è possibile scegliere di scaricare la versione da sun.com oppure dal server UCMDB. (Se si accede senza installare Java, non sarà possibile visualizzare le pagine necessarie per la visualizzazione corretta dell'applet Java.) Per i dettagli consultare "Troubleshooting and Limitations" on page 175.

- 2** Fare clic su un collegamento per utilizzare HP Universal CMDB:

- a Applicazione UCMDB.** Apre la pagina di accesso. Per i dettagli consultare "Accedere a HP Universal CMDB" a pag. 421.

Nota: è possibile accedere alla pagina di accesso anche immettendo `http://<nome server o indirizzo IP>.<nome dominio>:8080/ucmdb`.

- b Server Status.** Apre la pagina di stato del server. Per i dettagli consultare "Servizi di HP Universal CMDB" a pag. 117.
- c JMX Console.** Consente di eseguire operazioni sul CMDB mediante l'interfaccia della console JMX.
- d API Connection Test.** Visualizza le informazioni sul server HP Universal CMDB da utilizzare quando si esegue un'API nel CMDB.
- e API Client Download.** Esegue il download del file jar dell'API UCMDB.
- f API Reference.** Apre la documentazione di riferimento dell'API HP UCMDB.

Accedere a HP Universal CMDB

- 1 Immettere i parametri di accesso dell'utente con privilegi avanzati predefinito.
 - **Accesso utente=admin, Password utente=admin.**
 - Se HP Universal CMDB è installato in un ambiente multiutente o multistato (ad esempio HP Software-as-a-Service o Amber), viene visualizzato il campo Cliente. Selezionare il nome del cliente dall'elenco.
 - Selezionare **Apri in una nuova finestra** per aprire l'applicazione in un'altra finestra del browser.
 - **Memorizza dati su questo computer:** Selezionare questa opzione per l'accesso automatico. Ciò significa che all'accesso successivo a UCMDDB non è necessario immettere nome utente e password.
 - **Abilita la modalità di installazione locale:** Selezionare questa opzione per caricare UCMDDB in modalità di installazione locale. Per i dettagli consultare "Modalità di installazione locale" a pag. 419.
- 2 Fare clic su **Accesso**. Una volta eseguito l'accesso, il nome utente viene visualizzato nella parte superiore destra dello schermo.
- 3 (Consigliato) Cambiare subito la password dell'utente con privilegi avanzati per impedire accessi non autorizzati. Per i dettagli sul cambio della password consultare "Finestra di dialogo Reimposta password" nella *Guida all'amministrazione di HP Universal CMDB*.
- 4 (Consigliato) Creare altri utenti amministrativi per abilitare gli amministratori di HP Universal CMDB ad accedere al sistema. Per i dettagli sulla creazione di utenti nel sistema HP Universal CMDB consultare "Procedura guidata Aggiunta di un nuovo utente" nella *Guida all'amministrazione di HP Universal CMDB*.

Disconnessione

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

Per disconnettere:

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

Abilitare l'accesso automatico

Le opzioni avanzate di accesso consentono l'accesso automatico, l'accesso limitato e forniscono funzioni di accesso diretto a determinate pagine di HP Universal CMDB.

Quando è abilitato l'accesso automatico dalla pagina di accesso, la volta successiva che l'utente immette l'URL per accedere a HP Universal CMDB, la pagina di accesso non si apre, non è necessario immettere nome e password e la pagina predefinita impostata per l'apertura si apre automaticamente.

Per abilitare l'accesso automatico:

- 1** Nella pagina di accesso a HP Universal CMDB selezionare l'opzione **Memorizza dati su questo computer**.
- 2** Al termine della sessione non fare clic su **Disconnessione** nella parte superiore della pagina ma chiudere la finestra del browser.

La disconnessione disabilita l'opzione di accesso automatico ed è necessario immettere il nome di accesso e la password la volta successiva che si accede a HP Universal CMDB.

Linee guida per l'utilizzo dell'accesso automatico

Quando si utilizza questa opzione tenere presente quanto segue:

- ▶ L'utilizzo dell'opzione **Disconnessione** nella parte superiore della pagina di HP Universal CMDB annulla l'opzione. Se un utente che si è disconnesso si riconnette, si apre la pagina di accesso e l'utente deve immettere nome di accesso e password. Ciò risulta utile se si deve connettere un altro utente sullo stesso computer con nome utente e password diversi.
- ▶ Questa opzione rappresenta un rischio per la sicurezza e deve essere utilizzata con prudenza.

Cambiare il limite di tempo predefinito per la disconnessione dell'utente a causa di inattività

HP Universal CMDB prevede la funzionalità di disconnessione automatica in caso di inattività del sistema per un determinato periodo di tempo. Il periodo predefinito è 1.440 minuti (24 ore). Dopo questo periodo viene visualizzato un messaggio con conteggio alla rovescia di trenta secondi fino alla disconnessione.

Questo compito descrive come regolare il limite di tempo durante il quale UCMDB resta in funzione senza alcun input da parte dell'utente prima della disconnessione automatica.

Per cambiare il tempo di disconnessione predefinito:

- 1** Selezionare **Amministrazione > Impostazioni infrastruttura**> categoria **Impostazioni generali** > impostazione **Tempo inattivo consentito**.
- 2** Immettere un valore dalla colonna **Valore**.
- 3** Immettere un nuovo intervallo di tempo in minuti. Tutti i valori del **Tempo inattivo consentito** si trovano nella finestra **Proprietà**. Fare clic con il pulsante destro del mouse su **Tempo inattivo consentito** **Proprietà** oppure fare clic con il pulsante destro del mouse sull'impostazione **Tempo inattivo consentito**.

29

Spostamento in HP Universal CMDB

Questo capitolo comprende:

Concetti

- Spostamento nell'interfaccia utente di HP Universal CMDB a pag. 426
- Utilizzo della documentazione di HP Universal CMDB a pag. 428

Riferimenti

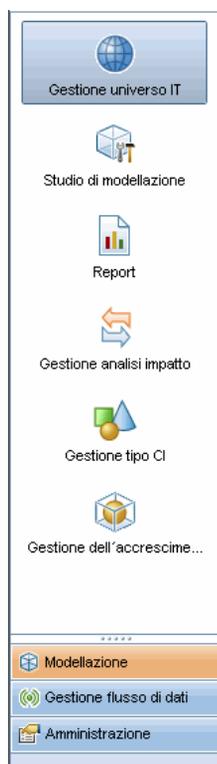
- Menu e opzioni a pag. 431

Concetti

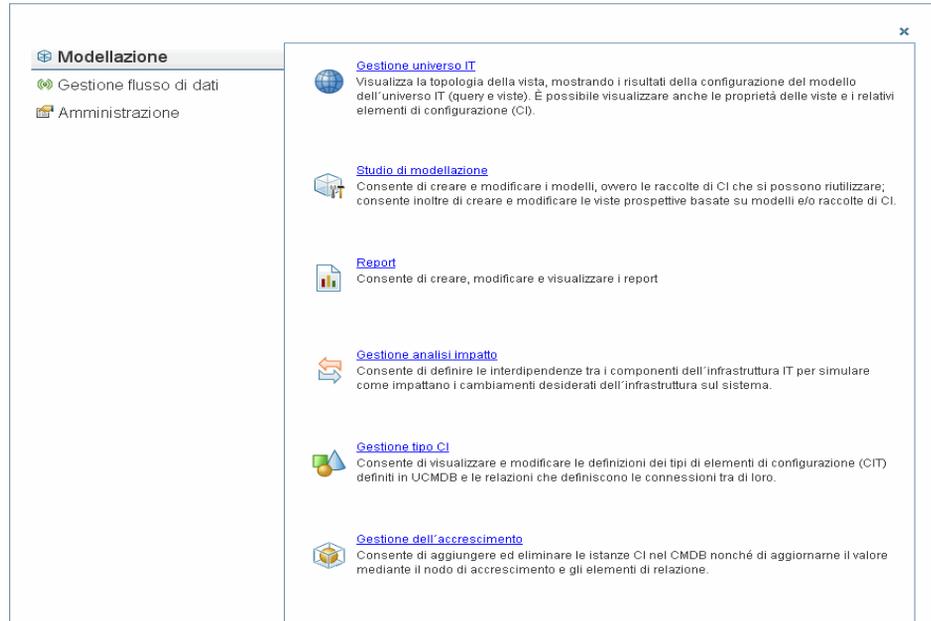
Spostamento nell'interfaccia utente di HP Universal CMDB

HP Universal CMDB viene eseguito in un browser Web. Per spostarsi in HP Universal CMDB utilizzare le funzioni di spostamento seguenti:

- **Barra di spostamento.** Consente lo spostamento veloce tra i moduli. Fare clic sulla categoria nella parte inferiore della barra e selezionare il modulo dalle icone nella parte superiore della barra.



- **Mapa di orientamento.** Per ciascuna categoria è possibile visualizzare una mappa con brevi descrizioni di ogni modulo selezionando **Gestioni> Mapa di orientamento.**



- **Barra di stato.** Fornisce informazioni sull'applicazione CMDB e consente di configurare alcuni aspetti dell'interfaccia.



- **Frecce Comprimi/Espandi.** Consentono di comprimere ed espandere i pannelli con un solo clic.



Nota: la funzione **Indietro** del browser Web non è supportata in HP Universal CMDB. L'utilizzo della funzione **Indietro** non sempre riporta il contesto corrente al contesto precedente. Per spostarsi a un contesto precedente utilizzare la funzione Fili di Arianna.

Utilizzo della documentazione di HP Universal CMDB

Nelle sezioni seguenti viene descritto come spostarsi e utilizzare la documentazione di HP Universal CMDB.

Spostamento nella Guida di UCMDB

La guida di UCMDB è un sistema integrato che può essere utilizzato nei modi seguenti:

- ▶ **Dalla pagina iniziale.** Per accedere alla pagina iniziale selezionare **Guida di UCMDB** nel menu della guida.

Nella pagina iniziale sono presenti i collegamenti alle varie guide contenute nella guida di UCMDB o in formato PDF.

- ▶ **Dal riquadro di spostamento.** Per accedere al riquadro di spostamento, se non è visualizzato, fare clic sul pulsante **Mostra navigazione** .



Il riquadro di spostamento è suddiviso nelle schede seguenti:

- ▶ **Scheda Contenuto.** Nella scheda Contenuto le varie guide sono organizzate in una struttura gerarchica che consente lo spostamento diretto in una guida o argomento specifico.
- ▶ **Scheda Indice.** La scheda Indice consente di selezionare un argomento specifico da visualizzare. Fare doppio clic sulla voce Indice per visualizzare la pagina corrispondente. Se la selezione ricorre in più documenti viene visualizzata una finestra di dialogo che consente di selezionare un contesto.
- ▶ **Scheda Cerca.** La scheda Cerca consente di cercare argomenti o termini specifici. I risultati vengono restituiti in ordine organizzato.
- ▶ **Scheda Preferiti.** La scheda Preferiti consente di contrassegnare determinate pagine per un riferimento rapido. Tenere presente che la scheda Preferiti è disponibile soltanto quando si utilizza l'implementazione Java della guida di UCMDB. Se il browser non supporta Java, l'implementazione JavaScript viene utilizzata automaticamente e la scheda Preferiti non viene visualizzata.

Funzionalità di Libreria della documentazione

La funzionalità seguente è disponibile nel riquadro superiore del riquadro principale di Libreria della documentazione.



- **Pulsante Navigazione.** Fare clic per visualizzare il riquadro di spostamento che comprende le schede Contenuto, Indice, Cerca e Preferiti. Per i dettagli sul riquadro di spostamento consultare "Utilizzo della documentazione di HP Universal CMDB" a pag. 428. Tenere presente che questo pulsante viene visualizzato quando il riquadro di spostamento è chiuso.



- **Pulsante Mostra in Contenuto** Fare clic per evidenziare nella scheda Contenuto la voce corrispondente alla pagina visualizzata al momento. Tenere presente che questo pulsante viene visualizzato quando il riquadro di spostamento è aperto.



- **Pulsanti Precedente e Avanti.** Fare clic per spostarsi in avanti o indietro nella guida visualizzata al momento.



- **Pulsante E-mail.** Fare clic per aprire il client di posta e inviare un feedback a HP. Si apre un messaggio di posta elettronica con i campi **A** e **Oggetto** già completati e un collegamento alla pagina corrente nel corpo del messaggio. Accertarsi di completare l'e-mail immettendo il proprio feedback. Tenere presente che per il corretto funzionamento di questa funzione è necessario che sia configurato il client di posta nel computer.



- **Pulsante Stampa.** Fare clic per stampare la pagina visualizzata al momento.

Organizzazione delle informazioni in argomenti

Il materiale nella maggior parte delle guide Libreria della documentazione è organizzato in base ai tipi di argomento. Sono utilizzati tre tipi di argomenti principali: Concetti, Compiti e Riferimenti. I tipi di argomenti sono stati differenziati visivamente tramite l'uso di icone. Di seguito viene spiegato ogni tipo di argomento e la rispettiva icona:



► **Concetti.** Gli argomenti relativi ai concetti forniscono informazioni di background, descrittive o concettuali. Leggere gli argomenti sui concetti per ottenere informazioni generali su cosa esegue e come funziona una funzionalità.



► **Compiti.** Gli argomenti sui compiti forniscono una guida dettagliata su come completare i compiti specifici che vengono di norma richiesti per l'amministrazione o l'utilizzo del software. Gli argomenti sui compiti comprendono anche gli scenari per alcuni compiti. Leggere gli argomenti sui compiti e seguire i passaggi elencati per eseguire il compito.



► **Riferimenti.** Gli argomenti sui riferimenti forniscono elenchi e spiegazioni dettagliate dei parametri, degli elementi di interfaccia utente comuni e altro materiale di riferimento. Leggere gli argomenti sui riferimenti per cercare determinate informazioni di riferimento rilevanti per un particolare contesto.



► **Interfaccia utente.** Gli argomenti sull'interfaccia utente sono un tipo speciale di argomenti di riferimento utilizzati essenzialmente per la guida sensibile al contesto. I collegamenti della guida a partire dal software di norma aprono gli argomenti dell'interfaccia utente.



► **Risoluzione dei problemi e limitazioni.** Gli argomenti sulla risoluzione dei problemi e le limitazioni sono un tipo speciale di argomenti di riferimento che forniscono l'elenco delle limitazioni della funzione. Leggere gli argomenti sulla risoluzione dei problemi e le limitazioni in caso di comportamento imprevisto del software. Si consiglia di riesaminare le limitazioni di una funzione prima di utilizzarla.

Riferimenti

Menu e opzioni

Le categorie seguenti sono disponibili nella parte inferiore della barra di spostamento:

Categoria	Descrizione
Modellazione	Fare clic per aprire il menu Modellazione per creare e gestire un modello del proprio universo IT nel CMDB. Per i dettagli consultare "Modellazione" nella <i>Guida alla modellazione di HP Universal CMDB</i> .
Gestione flusso di dati	Fare clic per aprire il menu di Gestione flusso di dati (GFD) per impostare ed eseguire il processo di GFD, popolare il modello di universo IT con i CI (configuration item, CI) e utilizzare Studio di integrazione. Per i dettagli consultare <i>Guida alla gestione del flusso di dati di HP Universal CMDB</i> . Per i dettagli sul contenuto di GFD consultare la <i>HP Universal CMDB Discovery and Integration Content Guide</i> in PDF.
Amministrazione	Fare clic per aprire il menu Amministrazione per configurare le impostazioni dell'infrastruttura, gli utenti, i ruoli, le autorizzazione, le pianificazioni e l'utilizzo di Gestione pacchetti. Per i dettagli consultare la <i>Guida all'amministrazione di HP Universal CMDB</i> .

Menu della guida

Si accede alle risorse online seguenti dal menu della guida di HP Universal CMDB:

- **Guida per questa pagina.** Si apre la guida di UCMDB sull'argomento che descrive la pagina o il contesto corrente.
- **Guida di UCMDB.** Apre la pagina iniziale. La pagina iniziale fornisce collegamenti rapidi ai principali argomenti della guida.

- ▶ **Risoluzione dei problemi & Knowledge Base.** Apre il sito Web di HP Software Support direttamente alla pagina di destinazione di Knowledge base di HP Software con soluzioni implementabili dall'utente. L'URL del sito Web è <http://support.openview.hp.com>.
- ▶ **Assistenza software HP.** Apre il sito Web di HP Software Support. Questo sito consente di sfogliare la knowledge base e di aggiungere articoli propri, registrare un messaggio o cercare forum di discussione tra utenti, inoltrare richieste di assistenza, scaricare patch e documentazione aggiornata e così via. L'URL del sito Web è <http://support.openview.hp.com>.
- ▶ **Sito Web HP Software.** Apre il sito Web HP Software che contiene informazioni e risorse sui prodotti software e servizi di HP. L'URL del sito Web è <http://www.hp.com/managementsoftware>.
- ▶ **Novità** Apre il documento Novità che descrive le funzioni e gli ampliamenti nuovi della versione.
- ▶ **Guida di Content pack di integrazione e individuazione.** Descrive il contenuto predefinito: ciò che viene individuato, le credenziali richieste nell'individuazione, come risolvere i problemi relativi ai risultati di individuazione e come utilizzare gli adattatori di integrazione.
- ▶ **Informazioni su HP Universal CMDB.** Apre la finestra di dialogo HP Universal CMDB che contiene informazioni sulla versione, la licenza, la patch e terze parti.

Nota: per informazioni sulla disponibilità elevata consultare "Installazione della modalità disponibilità elevata" a pag. 265.

30

Risoluzione dei problemi delle risorse disponibili

Questo capitolo comprende:

Risoluzione dei problemi delle risorse a pag. 433

Risoluzione dei problemi delle risorse

- **Risoluzione dei problemi di installazione.** Utilizzare questo metodo di risoluzione dei problemi comuni che si possono incontrare durante l'installazione di HP Universal CMDB. Per i dettagli consultare "Troubleshooting and Limitations" on page 175.
- **Risoluzione dei problemi di accesso.** Utilizzare questo metodo per risolvere le possibili cause di errore di accesso a HP Universal CMDB. Per i dettagli consultare "Troubleshooting and Limitations" on page 175.
- **Knowledge base di HP Software con soluzioni implementabili dall'utente.** Utilizzarla per cercare informazioni specifiche per la risoluzione dei problemi su un'ampia gamma di argomenti. È disponibile nel sito Web HP Software Support; si accede alla knowledge base HP Software con soluzioni implementabili dall'utente selezionando **Risoluzione dei problemi & Knowledge Base** dal menu Guida di HP Universal CMDB.
Tenere presente che soltanto i clienti registrati possono accedere alle risorse sul sito Web HP Software Support. I clienti che non sono ancora registrati possono farlo da questo sito.
- **File di registro di HP Universal CMDB.** Utilizzarli per risolvere i problemi di runtime del CMDB. Per i dettagli consultare "File di registro del CMDB" nella *Guida all'amministrazione di HP Universal CMDB*.

- **File di registro di Gestione flusso di dati.** Utilizzarli per risolvere i problemi di runtime di GFD. Per i dettagli consultare "File di registro di Gestione flusso di dati" nella *Guida all'amministrazione di HP Universal CMDB*.
- **File di registro delle query.** Utilizzarli per visualizzare le definizioni per i file di registro dei parametri delle query. Per i dettagli consultare "File di registro del CMDB" nella *Guida all'amministrazione di HP Universal CMDB*.

31

Utilizzo di impostazioni internazionali non in lingua inglese

Questo capitolo comprende:

Riferimenti

- Problemi di installazione e distribuzione a pag. 436
- Problemi relativi all'ambiente del database a pag. 437
- Problemi relativi all'amministrazione a pag. 437
- Problemi relativi ai report a pag. 437
- Supporto per Multi-Lingual User (MLU) Interface a pag. 438

Riferimenti

Problemi di installazione e distribuzione

- ▶ Se si utilizza la lingua giapponese, cinese o coreana nel browser è necessario accertarsi che sul server HP Universal CMDB siano installate le lingue asiatiche. Sul computer su cui è installato il server HP Universal CMDB selezionare **Pannello di controllo > Opzioni internazionali e della lingua > Lingue > Installa i file delle lingue dell'Asia orientale**.
- ▶ L'installazione di HP Universal CMDB in un ambiente multilingue (I18N) è supportata per HP Universal CMDB installato su una piattaforma Windows. Altre piattaforme non sono supportate (ad esempio Solaris, UNIX, Linux e così via). Per i dettagli sull'installazione di HP Universal CMDB su una piattaforma Windows consultare "HP Universal CMDB Installazione su una piattaforma Windows" a pag. 71.
- ▶ Per l'accesso a HP Universal CMDB la password dell'utente non può includere caratteri giapponesi o cinesi se il server UCMDB è installato su un computer Windows 2003 con sistema operativo giapponese o cinese.
- ▶ Il percorso di installazione di tutti i componenti di HP Universal CMDB non deve contenere caratteri non in lingua inglese.
- ▶ La procedura guidata di aggiornamento delle versioni 9.00 e 9.01 non supporta l'interfaccia utente non in lingua inglese. (L'aggiornamento funziona correttamente)

Problemi relativi all'ambiente del database

- ▶ Per lavorare in un ambiente HP Universal CMDB non in lingua inglese, è possibile utilizzare un database Oracle Server oppure Microsoft SQL Server. La lingua delle impostazioni internazionali del sistema operativo Windows OS del database deve essere la stessa di quella del server UCMDb. Quando si utilizza un database Oracle Server la codifica del database può essere inoltre UTF-8 o AL32UTF-8 che supporta lingue che non sono inglese e più lingue.
- ▶ Quando si crea una nuova istanza Oracle in un database Oracle è necessario specificare il set di caratteri per l'istanza. Tutti i dati dei caratteri, compresi i dati del dizionario dei dati, è memorizzato nel set di caratteri dell'istanza. Per i dettagli sull'utilizzo dei database Oracle consultare "HP Universal CMDB Installation on a Solaris Platform" on page 107.
- ▶ Il monitor di query del database può connettersi a un database Oracle ma i nomi utenti e le password Oracle devono contenere caratteri non inglesi.

Problemi relativi all'amministrazione

- ▶ Per supportare caratteri non in lingua inglese la codifica per il database di HP Universal CMDB deve essere definita come UTF-8 o AL32UTF-8 oppure deve essere impostata sulla lingua specifica. Per ulteriori dettagli consultare "Problemi relativi all'ambiente del database" a pag. 437.

Problemi relativi ai report

- ▶ HP Universal CMDB non supporta i nomi dei report personalizzati che contengono più di 50 caratteri multibyte.
- ▶ I report scaricati da HP Universal CMDB in Excel non possono essere visualizzati correttamente su un sistema operativo con lingua diversa dalla lingua dei dati.

Quando si utilizza Microsoft Office versione 2007 o successiva con gli ultimi aggiornamenti installati, questo problema non è rilevante poiché i dati sono salvati in formato Unicode.

- ▶ Se un report viene creato in un'impostazione internazionale della lingua e viene inviato via e-mail da un'altra impostazione internazionale della lingua, il report contiene informazioni sul sistema nelle lingue del server e nell'impostazione internazionale originale.
- ▶ Se un nome di file contiene caratteri multibyte (ad esempio in giapponese, cinese o coreano) e il report viene inviato come allegato di un'e-mail, il nome diventa illeggibile.
- ▶ Per impostazione predefinita Excel non apre correttamente documenti CSV con codifica UTF-8. Dopo aver salvato un report come file .csv, per importarlo in Excel eseguire le operazioni seguenti in Excel:
 - a** Nel menu **Dati** selezionare **Importa dati esterni** e fare clic su **Importa dati**.
 - b** Nella casella Tipo file fare clic su **File di testo**.
 - c** Nella casella **Cerca in** individuare e fare clic sul file di testo da importare come intervallo di dati esterni.
 - d** Per specificare come dividere il testo in colonne seguire le istruzioni nella procedura guidata di importazione del testo e fare clic su **Fine**.
- ▶ Quando si esporta un'istanza CI in un file PDF i caratteri multibyte (ad esempio giapponese, cinese, coreano e così via) non vengono visualizzati nel file PDF.

Supporto per Multi-Lingual User (MLU) Interface

Nota: la matrice di supporto seguente è rilevante per la versione 9.00 (ma non per la versione 9.01 o altre patch minori).

L'interfaccia utente di HP Universal CMDB può essere visualizzata nelle lingue seguenti nel browser Web:

Lingua	Interfaccia utente localizzata	Materiali localizzati	Disponibilità
Inglese	Sì	Sì	Parte di release del prodotto iniziale
Francese	Sì		Parte di release del prodotto iniziale
Giapponese	Sì	Sì	Media pack B
Coreano	Sì		Parte di release del prodotto iniziale
Cinese semplificato	Sì		Parte di release del prodotto iniziale
Olandese	Sì		Media pack A
Tedesco	Sì		Parte di release del prodotto iniziale
Portoghese	Sì		Media pack A
Russo	Sì		Media pack A
Spagnolo	Sì		Parte di release del prodotto iniziale
Italiano	Sì		Media pack A

Nota: i media pack complementari vengono rilasciati entro 90 giorni dalla release del prodotto.

Utilizzare l'opzione di preferenza della lingua nel browser per selezionare come visualizzare HP Universal CMDB. La preferenza della lingua scelta riguarda soltanto il proprio computer (client) e non il server HP Universal CMDB o un qualsiasi altro utente che accede allo stesso computer HP Universal CMDB.

Per impostare e visualizzare HP Universal CMDB in una lingua specifica:

- 1** Installare i caratteri appropriati della lingua nel proprio computer se non sono stati già installati. Se si seleziona una lingua nel browser Web dove i caratteri non sono stati installati, HP Universal CMDB visualizza i caratteri come quadrati.
- 2** Se si è connessi a HP Universal CMDB è necessario disconnettersi. Fare clic su **DISCONNETTI** nella parte superiore della finestra di HP Universal CMDB.

Chiudere tutte le finestre aperte del browser o, in alternativa, cancellare la memoria.

- 3** Se HP Universal CMDB è in esecuzione su Internet Explorer, configurare il browser Web sul proprio computer per selezionare la lingua i cui si desidera visualizzare HP Universal CMDB (**Strumenti > Opzioni Internet**).
 - a** Fare clic sul pulsante **Lingue** e nella finestra di dialogo Preferenze lingua evidenziare la lingua in cui si desidera visualizzare HP Universal CMDB.
 - b** Se la lingua desiderata non è presente nell'elenco della finestra di dialogo fare clic su **Aggiungi** per visualizzare l'elenco delle lingue. Selezionare la lingua da aggiungere e fare clic su **OK**.
 - c** Fare clic su **Sposta su** per spostare la lingua selezionata alla prima riga.
 - d** Fare clic su **OK** per salvare le impostazioni.
 - e** Visualizzare la finestra di accesso aHP Universal CMDB.
 - f** Dal menu di Internet Explorer selezionare **Visualizza > Aggiorna**. HP Universal CMDB viene subito aggiornato e l'interfaccia utente viene visualizzata nella lingua selezionata.

Nota: per i dettagli sulla visualizzazione delle pagine Web in Internet Explorer scritte in una lingua diversa, consultare <http://support.microsoft.com/kb/306872/en-us>.

Note e limitazioni

- Non è presente alcuna installazione del language pack. Tutte le lingue tradotte incluse nella release iniziale sono integrate nella Multi-lingual User Interface (MLU) di HP Universal CMDB.
- I dati restano nella lingua in cui sono stati immessi anche se la lingua del browser Web cambia. Se si cambia la lingua del browser Web sul proprio computer locale non cambia la lingua delle definizioni di input dei dati e delle configurazioni.
- Non è possibile distribuire un pacchetto se le impostazioni internazionali del server sono diverse da quelle del client e il nome del pacchetto contiene caratteri non inglesi. Per i dettagli consultare "Gestione pacchetti" nella *Guida all'amministrazione di HP Universal CMDB*.
- Non è possibile creare un pacchetto che contiene risorse (ad esempio viste e query TQL) con caratteri non in lingua inglese nei nomi se le impostazioni internazionali del server sono diverse dalle impostazioni internazionali del client. Per i dettagli consultare "Gestione pacchetti" nella *Guida all'amministrazione di HP Universal CMDB*.
- Non è possibile creare un nuovo utente in Utenti e ruoli se il nome del nuovo utente contiene più di 20 caratteri asiatici. Per i dettagli consultare "Utenti e ruoli" nella *Guida all'amministrazione di HP Universal CMDB*.
- In Studio di modellazione non è possibile creare una nuova vista se il nome della vista contiene più di 18 caratteri giapponesi. Per i dettagli consultare "Studio di modellazione" nella *Guida alla modellazione di HP Universal CMDB*.
- Le pagine seguenti vengono visualizzate soltanto in inglese. Non sono tradotte in un'altra lingua. Per i dettagli consultare "Utilizzo di impostazioni internazionali non in lingua inglese" a pag. 435:
 - Pagina HTML sullo stato del server HP Universal CMDB
 - Pagina di accesso di HP Universal CMDB
 - Pagina della console JMX
 - Pagina di verifica di connessione API
- Se sul computer client si selezionano lingue che non sono supportate da UCMDDB MLU, HP Universal CMDB viene visualizzato con la stessa lingua delle impostazioni internazionali di sistema di quella del server UCMDDB.

Indice

A

- accesso
 - accesso automatico 422
- accesso a UCMDB
 - impostazione di IIS Web server 409, 413
 - mediate il server Web IIS 407
 - mediate il server Web IIS, panoramica 408
- aggiornamenti documentazione 22
- aggiornamenti, documentazione 22
- aggiornamento
 - alla versione 9.0x da 8.0x 163
- applet Java
 - cambiare allocazione di memoria 32
- architettura protetta
 - distribuzione 287
- autenticazione
 - LW-SSO, panoramica 368
 - Riferimenti generali LW-SSO 367
- autenticazione di accesso 377
- autenticazione di base
 - abilitazione sulla sonda del flusso di dati 358
- autenticazione reciproca
 - abilitazione sulla sonda del flusso di dati 350
 - SDK 298

C

- client UCMDB
 - browser supportati 45
 - requisiti software 44
- Confidential Manager 387
 - considerazioni sulla protezione 389
 - panoramica 388

- configuration management database (CMDB)
 - introduzione 29
- Configurazione database, procedura guidata
 - accesso su piattaforma Windows o Linux 123
- conflitto del modello classe 179
- console JMX
 - cambio nome utente o password 288
 - impostare password per crittografare 348
- credenziali
 - esportazione, importazione in formato crittografato 332
 - visualizzazione informazioni 320

D

- database
 - requisiti di installazione del sistema 40
- disconnessione
 - automatica per inattività utente 423
- disponibilità elevata
 - installazione 265
 - installazione di UCMDB 268
 - transizione tra server attivo e passivo 267
- distribuzione
 - in architettura protetta 287
 - installazione di Windows server 71, 87
- Documentazione online 17
- documentazione online 17
- documentazione, online 17
- domainScopeDocument
 - controllo posizione 361

Indice

dsinstallazione
su una piattaforma Windows 84

G

Gestione credenziali del flusso di dati 315
Guida in linea 18
guida UCMDB
spostamento 428

H

HP Universal CMDB
accesso 417, 418
accesso a UCMDB e componenti 420
architettura di sistema 28
avvio/arresto del server 119
distribuzione 28
esecuzione su piattaforma VMware 31
informazioni 26
introduzione 25, 59
matrice di supporto 35
panoramica 26
ripristino di emergenza 397
servizi 117, 120
stato del server 118
HP Universal CMDB Server
avvio e arresto 123
HP Universal CMDB server
avvio, arresto su una piattaforma
Linux 125

I

I18N
problemi ambiente del database 437
problemi di amministrazione 437
problemi di installazione e
distribuzione 436
problemi report 437
ID cliente
configurazione per sonda 142
configurazione per sonda in
esecuzione su Linux 158
IIS
configurazione per la sonda del flusso
di dati 416

impostazioni internazionali
non in lingua inglese 435
inattività utente
disconnessione automatica 423
Individuazione
panoramica 29
installazione
connessione a un database Microsoft
SQL Server esistente 115
connessione a uno schema Oracle
esistente 116
creazione database Microsoft SQL
Server 106
creazione schema Oracle 111
distribuzione di Microsoft SQL Server
103
modalità disponibilità elevata 265
panoramica 68
passaggi 69
prerequisiti per Windows 72, 88
procedura di distribuzione tipica con
Oracle Server 74, 90
scelta database o schema 102
su un computer 130
installazione database
configurazione del server UCMDB 101
impostazione dei parametri del
database 103
riavvio del server 116
installazione server
su Windows 71, 87
interfaccia utente
spostamento 425
supporto multilingue 438
intervalli di rete
esportazione, importazione in
formato crittografato 332
introduzione 63
compiti di amministrazione 64
pianificazione predistribuzione 60
istanza del sistema operativo 49

K

keystore
crittografia della password della sonda

- del flusso di dati 362
- percorsi sul server e sulla sonda del
flusso di dati 364
- Knowledge Base 21

L

LDAP

- configurazione impostazioni di
 - autenticazione 382
- definizione del metodo di
 - autenticazione 379
- verifica connessioni per
 - autenticazione 382

- Leggimi 17

- licenza 47

- aggiornamento a standard o advanced
 - 56
- DDM Advanced Edition 54
- panoramica 48
- risoluzione dei problemi e limitazioni
 - 57
- UCMDB Foundation 50
- UCMDB Integration 53

- licenza Advanced Edition 48

- licenza DDM Advanced Edition 54

- licenza di UCMDB Foundation 50

- licenza UCMDB Integration 53

- lingue

- impostazioni internazionali non in
 - lingua inglese 435

- LTU (license to use), licenza d'uso 54

- LW-SSO

- avvisi di protezione 371
- panoramica 368
- requisiti di sistema 370
- riferimenti generali 367
- ripristino configurazione corrente in
 - ambiente distribuito 385
- risoluzione dei problemi e limitazioni
 - 373

M

- metodi di autenticazione

- definizione per LDAP 379

- impostazione 378

- impostazione protezione SSL 380

- verifica connessione LDAP 382

- Microsoft SQL Server

- connessione a database esistente 115

- creazione database 106

- distribuzione 103

- requisiti di installazione 42

- migrazione da versioni precedenti 31

- modalità di installazione locale 419

- MySQL

- impostare password per crittografare
 - database 346

N

- Novità 17

O

- Oracle

- connessione a uno schema esistente
 - 116

- creazione schema 111

- parametri dello schema utente 104

- requisiti di installazione 40

P

- pacchetti

- aggiornamento a 9.02 257

- password

- crittografare database MySQL 346

- crittografia console JMX 348

- pianificazione capacità 275

- nodi gestiti e CI correlati ai nodi 277

- preferenze di lingua 438

- preferenze di lingua del browser 438

- Probe Gateway

- esecuzione su computer separato,
 - Probe Manager 140

- Probe Manager

- esecuzione su computer separato,
 - Probe Gateway 140

- protezione

- protezione avanzata 283

- protezione avanzata 283

- abilitare SSL su client Web 297
- abilitazione SSL dall'Autorità di certificazione 295
- abilitazione SSL sulla sonda del flusso di dati 350, 358
- attivazione SSL su computer server UCMDB 292
- distribuzione architettura protetta 287
- esempio di configurazione di Apache 2.0.x 313
- preparazioni 286
- proxy inverso, aspetti di protezione 310
- proxy inverso, panoramica 308
- proxy inverso, utilizzo 307
- SSL 291
- proxy inverso
 - aspetti protezione 310
 - connessione della sonda del flusso di dati al server UCMDB 359
 - panoramica 308
 - utilizzo 307

R

- requisiti
 - database di sistema 40
 - Microsoft SQL Server 42
 - Oracle 40
- requisiti di sistema
 - piattaforma VMware 31
- ripristino di emergenza
 - backup della configurazione del sistema, backup della configurazione dei dati 400
 - HP Universal CMDB 397
 - installazione software di HP Universal CMDB in ambiente failover 399
 - introduzione 398
 - preparazione dell'ambiente 399
 - preparazione dell'istanza di failover di HP Universal CMDB per l'attivazione 402
 - prima della procedura di pulizia all'avvio 403

- Risoluzione dei problemi & Knowledge Base 21
- risoluzione dei problemi delle risorse 433
- risorse online 21

S

- SDK
 - abilitazione SSL 298
- server gestito 49
- Server HP Universal CMDB
 - accedere ai comandi 123
- server HP Universal CMDB
 - avvio, arresto su una piattaforma Windows 124
- server UCMDB
 - ambienti virtuali 39
 - percorsi keystore e truststore 364
 - requisiti hardware 36
 - requisiti software 38
- servizi 117, 120
 - avvio/arresto del server 119
 - stato del server, visualizzazione 118
- servizi UCMDB
 - risoluzione dei problemi 122
- Sito Web HP Software 21
- Sito Web HP Software Support 21
- Sonda
 - esecuzione di Probe Manager e Probe Gateway su computer separati 140
- Sonda del flusso di dati
 - abilitazione SSL con autenticazione di base 358
 - abilitazione SSL con autenticazione reciproca 350
 - aggiornamento su computer Linux 158
 - arresto del server su un computer Linux 157
 - configurazione per IIS 416
 - connessione a un cliente non predefinito 142
 - connessione a un cliente non predefinito su Linux 158
 - connessione mediante proxy inverso al server UCMDB 359

- crittografia della password per keystore e truststore 362
- installazione su Linux 129, 147
- installazione, configurazione di Probe Manager e Probe Gateway come processi separati 141
- percorsi keystore e truststore 364
- procedura di installazione su Linux 148
- protezione avanzata 345
- requisiti ambiente virtuale 144
- requisiti di installazione 143
- requisiti hardware 143
- requisiti installazione su Linux 159
- requisiti software 143
- risoluzione dei problemi di installazione e limitazioni 145, 159
- spostamento 425
 - interfaccia utente 426
 - menu e opzioni 431
 - utilizzo della documentazione 428
- SSL 291
 - abilitare con Autorità di certificazione 295
 - abilitare su client Web 297
 - abilitazione su SDK del client 298
 - abilitazione su SDK del client con autenticazione reciproca 298
 - abilitazione sulla sonda del flusso di dati 350, 358
 - attivazione su computer server UCMDB 292
 - cambiamento delle password del keystore del server UCMDB 301
 - impostazione connessione protetta per autenticazione 380
- stato server UCMDB
 - accesso su piattaforma Windows o Linux 123
- supporto per multi-lingual user interface 438

T

- Topology Query Language (TQL)
 - introduzione 30
- truststore

- crittografia della password della sonda del flusso di dati 362
- percorsi sul server e sulla sonda del flusso di dati 364

U

- UCMDB
 - cambiare utente del servizio 289
- UCMDB Server
 - accesso ai comandi su Linux 125
 - avvio e arresto 123
- utente del servizio Windows
 - change 289
- Utilità di migrazione pacchetto 257

V

- VMware, esecuzione di HP Universal CMDB 31

W

- Windows
 - installazione server 71, 87

