CA Embedded Entitlements Manager

Guida introduttiva

r8.4 SP3

Riferimenti ai prodotti CA

Questo documento fa riferimento ai seguenti prodotti CA:

- CA® Embedded Entitlements Manager (CA EEM)
- Directory CA®
- CA® SiteMinder® Web Access Manager (CA SiteMinder)
- CA® Identity Manager
- CA® Security Command Center
- CA® Integrated Threat Management
- CA® Enterprise Log Manager

Contattare il servizio di Supporto tecnico

Per l'assistenza tecnica in linea e un elenco completo delle sedi, degli orari del servizio di assistenza e dei numeri di telefono, contattare il Supporto tecnico visitando il sito Web all'indirizzo http://www.ca.com/worldwide.

Sommario

Capitolo 1: Introduzione

Questa sezione contiene i seguenti argomenti:

Panoramica

CA Embedded Entitlements Manager (CA EEM) consente alle applicazioni di condividere i comuni servizi di gestione, autenticazione e autorizzazione dei criteri di accesso.

Funzioni

CA EEM fornisce un set di servizi di sicurezza. Sono disponibili i seguenti servizi di sicurezza:

- Servizi di configurazione:
  - Registrazione e annullamento della registrazione delle istanze dell'applicazione
  - Ambito amministrativo degli amministratori dell'applicazione
  - Delega dei diritti amministrativi
  - Gestione di utenti e gruppi
- Servizi di sicurezza dell'amministrazione:
  - Gestione dei criteri di accesso, di eventi e di obbligo
  - Gestione dei calendari
- Servizi di sicurezza Run-time:
  - Autenticazione utenti
  - Autorizzazione accesso
  - Registrazione degli eventi di sicurezza

Funzioni

CA EEM dispone delle seguenti funzioni:

Generale

- L'isolamento dei criteri consente a ogni istanza dell'applicazione registrata di utilizzare il relativo spazio per memorizzare i dati specifici dell'applicazione
- Run-time SDK disponibile per Java, C++ e C#
- SDK amministrativo disponibile per Java, C++ e C#
- Supporto dell'interfaccia della riga di comando per le funzioni amministrative (inserisci/modifica/rimuovi oggetti):
  - Esportazione/importazione XML
  - Controlli Run-time
  - Strumenti di migrazione
- Supporto dell'interfaccia Web per l'accesso indipendente e con avvio contestuale
- Comunicazioni HTTP protette
- Integrazione con CA Security Command Center e CA Audit per la gestione degli eventi di sicurezza
- Integrazione con CA SiteMinder per il recupero delle informazioni sugli utenti e sui gruppi dall'archivio dati di CA SiteMinder

Identity Management

- Utenti globali e attributi condivisi per tutte le applicazioni
- Supporto di modalità differenti per utenti globali
  - Utenti globali interni con gestione dei criteri password inclusa
  - Utenti globali esterni dai server di directory LDAP
  - Utenti globali esterni da CA Identity Manager
- Integrazione con CA Identity Manager per la gestione e il provisioning degli utenti in base al ruolo
- Supporto per l'esportazione e l'importazione delle sessioni portabili per il single sign-on

Gestione accessi

- Gestione accessi comprende sia gli elenchi di controllo accessi (ACL), sia i criteri aziendali
- La lingua dei criteri permette l'utilizzo degli attributi utente, sessione, ambiente e risorsa nelle decisioni relative ai criteri
- Ambito amministrativo incorporato di tutti gli oggetti

- Supporto incorporato per l'amministrazione delegata
- Supporto incorporato per le verifiche obbligo personalizzate che richiedono azioni specifiche dell'applicazione
  - Valutazione locale interna al processo delle verifiche permessi
  - SDK e interfaccia Web per la definizione dei criteri di accesso, degli ACL, dei criteri di ambito amministrativo e dell'autorità delegata

Accesso client

È possibile accedere al server CA EEM mediante interfacce Web standard e interfacce di servizi Web che forniscono integrazione di terze parti senza richiedere un modulo client. Le interfacce sono le seguenti:

- HTML e iTechnology per la configurazione e l'amministrazione
- iTechnology per la trasmissione degli eventi CA Audit

iTechnology è una tecnologia CA basata su standard Web quali HTTP, HTTPS, HTML, XML e SSL, che offre una struttura per la creazione e la distribuzione dei servizi Web su Internet.

Supporto dell'archivio dati

CA EEM supporta l'identificazione di una singola origine utente esterna, ad esempio Microsoft Active Directory. Indipendentemente dalla posizione di archiviazione degli oggetti utente, la configurazione e i criteri di CA EEM vengono memorizzi nel database di gestione CA Directory.

Capitolo 2: Installazione su Windows

Questa sezione contiene i seguenti argomenti:

Panoramica dell'installazione

L'installazione di CA EEM in ambienti operativi Windows avviene mediante l'installazione delle seguenti applicazioni:

Server CA EEM

È possibile utilizzare il server CA EEM per definire i criteri di autorizzazione relativi alle risorse dell'applicazione che utilizzano un'interfaccia Web. L'interfaccia amministrativa basata su Web consente di gestire le identità e i criteri di accesso. L'infrastruttura di protezione esistente viene utilizzata per implementare regole basate sulla logica aziendale, mediante attributi risorsa e utente definiti in archivi utenti centralizzati e in altri sistemi aziendali.

CA EEM SDK (Software Development Kit)

È possibile utilizzare CA EEM SDK per incorporare controlli di protezione basati sulle identità all'interno delle applicazioni. SDK comprende librerie, classi java, file di intestazione e un'esercitazione pratica e può essere utilizzato per implementare CA EEM in qualsiasi applicazione. Per ulteriori informazioni sulle modalità di implementazione di CA EEM mediante SDK, consultare la *Guida alla programmazione*.

Ogni applicazione viene installata separatamente e funziona in maniera indipendente.

Installazione del server

È possibile installare il server CA EEM mediante l'installazione guidata o la riga di comando. Utilizzare la riga di comando per installare CA EEM in modalità invisibile all'utente oppure l'installazione guidata per un'installazione interattiva.

Per installare e utilizzare CA EEM, JRE non rappresenta più un requisito minimo. È possibile installare e utilizzare CA EEM con o senza JRE. Se si desidera installare CA EEM senza JRE come requisito minimo, è necessario ignorare la schermata del percorso di selezione JRE nell'installazione guidata. Se si desidera installare il server CA EEM in modalità invisibile all'utente senza JRE, è necessario utilizzare il parametro javahome impostato su "None".

Nelle sezioni riportate di seguito vengono descritte le modalità di installazione del server CA EEM.

Ulteriori informazioni

Come ignorare la schermata di selezione del percorso JRE nell'installazione guidata (a pagina 15)
Elenco di controllo per la configurazione della procedura guidata (a pagina 14)
Installazione del server mediante l'installazione guidata (a pagina 16)
Installazione del server CA EEM in modalità invisibile all'utente (a pagina 23)

Elenco di controllo per la configurazione della procedura guidata

Durante l'installazione del server CA EEM su Windows, è necessario disporre delle seguenti informazioni:

Campo	Valore
Percorso di installazione di CA EEM	Posizione sul computer in cui si prevede di installare CA EEM.
Percorso di installazione di JRE	Posizione di installazione di JRE sul computer. **Nota**: se si desidera installare e utilizzare CA EEM senza JRE, è necessario impostare la variabile Javahome su "None" dalla riga di comando prima di eseguire l'installazione guidata di CA EEM.
Password EiamAdmin	Password associata all'amministratore EiamAdmin di CA EEM

Campo	Valore
Directory di backup	Il percorso sul computer in cui si prevede di eseguire il backup dei file da un'installazione precedente di CA EEM. **Nota:** tali informazioni saranno necessarie soltanto se si esegue l'aggiornamento da una versione precedente di CA EEM a quella corrente.

Come ignorare la schermata di selezione del percorso JRE nell'installazione guidata

Per installare e utilizzare CA EEM, JRE non rappresenta più un requisito minimo. Se si desidera installare CA EEM senza JRE, è necessario attenersi alla seguente procedura:

1. Impostare il parametro javahome su "None"

   Nota: se si imposta il parametro javahome su "None", non viene visualizzata la schermata di selezione del percorso Java nell'installazione guidata.

2. Installare CA EEM mediante l'installazione guidata.

Impostazione del parametro Javahome

È necessario impostare il parametro javahome sul valore None (nessuno) prima di utilizzare l'installazione guidata di CA EEM. Impostare il parametro javahome dalla riga di comando in base alla seguente procedura:

EEMServer_*[version number]*_win32.exe -s -a /z"javahome=None; "

Installazione del server mediante l'installazione guidata

L'installazione guidata del server CA EEM assiste l'utente durante il processo di installazione e fornisce opzioni che consentono di definire i parametri di installazione.

Per installare il server CA EEM

1. Eseguire una delle seguenti operazioni:
   - Avviare Windows Explorer, quindi fare doppio clic sul pacchetto di installazione EEMServer_[*numeroversione*].[*numero_build*]_win32.exe sul computer di destinazione.
   - Immettere il seguente comando al prompt dei comandi utilizzando i parametri di installazione:

     EEMServer_*[numeroversione].[numero_build]*_win32.exe -s -a /z "eiampath=<*Percorso di installazione personalizzato per CA EEM*>; etdirpath=<*Percorso di installazione personalizzato per CA Directory*>; igpath=<*Percorso di installazione personalizzato per iGateway*>;"

     È possibile specificare un percorso di installazione personalizzato utilizzando i parametri di installazione. Per ulteriori informazioni sui parametri di installazione, consultare Parametri di installazione del server.

     Viene visualizzata l'installazione guidata.
2. Seguire le istruzioni visualizzate sull'installazione guidata per completare l'installazione.

Ulteriori informazioni:

Come ignorare la schermata di selezione del percorso JRE nell'installazione guidata (a pagina 15)

Aggiornamento del server

È possibile aggiornare l'installazione del server CA EEM esistente alla versione corrente.

Per aggiornare un'installazione esistente del server CA EEM

1. Eseguire EEMServer_<version number>_win32.exe sul computer di destinazione.
2. In base alla versione del server CA EEM installata, si verifica quanto segue.
   - Se la versione esistente del server CA EEM è precedente a quella in corso di installazione, viene eseguito il backup della versione esistente e l'aggiornamento automatico alla nuova versione.
   - Se la versione del server CA EEM esistente è identica a quella in corso di installazione, viene richiesto se si desidera disinstallare il del server CA EEM. È possibile disinstallare e reinstallare il del server CA EEM.
   - Se la versione che si sta installando è precedente alla versione esistente, viene generato un errore e l'installazione si interrompe.

L'aggiornamento del server CA EEM comporta l'aggiornamento dei seguenti elementi:

- server CA EEM nella cartella \\CA\SharedComponents\iTechnology
- iGateway
- CA Directory

Viene inoltre eseguita la migrazione di tutti i certificati P12 nei certificati PEM.

Ulteriori informazioni:

Elenco di controllo per la configurazione della procedura guidata (a pagina 14)
Installazione del server mediante l'installazione guidata (a pagina 16)

Avvio del server

Per gestire le identità e i criteri di accesso delle applicazioni registrate, è necessario avviare il server CA EEM.

Per iniziare a utilizzare il server CA EEM

1. Eseguire una delle seguenti operazioni:
   - Immettere l'URL https://*nomehost* oppure *indirizzoip*:5250/spin/eiam nel browser. Se si utilizza il computer server CA EEM, specificare http://*hostlocale*:/5250/spin/eiam.
   - Selezionare Start, Programmi, CA, Embedded Entitlements Manager, EEM UI su sistemi operativi Windows.

     Viene visualizzata la pagina di accesso.
2. Immettere le seguenti informazioni nella finestra di dialogo di accesso:
   a. Selezionare un'istanza dell'applicazione registrata dall'elenco a discesa Applicazione. L'impostazione predefinita è <Globale>. Il nome utente predefinito dell'amministratore è EiamAdmin.

      Nota: è possibile aggiungere altri utenti globali per effettuare l'accesso, quindi impostare i relativi nomi utente in base alle preferenze.

   b. Immettere la password. Si tratta della stessa password specificata durante l'installazione del server CA EEM per EiamAdmin

   c. Selezionare la casella di controllo Ricorda impostazioni personali se in futuro si desidera eseguire l'accesso al server CA EEM con le stesse impostazioni.
3. Fare clic su Accedi.

   Viene visualizzata la pagina iniziale dell'interfaccia di CA EEM. Per ulteriori informazioni sull'utilizzo del server CA EEM, consultare la *Guida in linea*.

Attivazione dell'accessibilità nel server CA EEM

Le caratteristiche di accesso del server CA EEM consentono agli utenti, indipendentemente dalle loro abilità, di utilizzare appieno i prodotti e la documentazione di supporto per l'esecuzione di attività aziendali critiche. Quando si attiva l'accessibilità, gli utenti possono eseguire tali attività utilizzando solo la tastiera o un utilità di lettura dello schermo.

Per attivare l'accessibilità:

1. Eseguire una delle seguenti operazioni:
   - Immettere l'URL https://*nomehost* oppure *indirizzoip*:5250/spin/eiam nel browser. Se si utilizza il computer server CA EEM, specificare http://*hostlocale*:/5250/spin/eiam.
   - Selezionare Start, Programmi, CA, Embedded Entitlements Manager, EEM UI su sistemi operativi Windows.

     Viene visualizzata la pagina di accesso.
2. Immettere le seguenti informazioni nella finestra di dialogo di accesso:
   a. Selezionare un'istanza dell'applicazione registrata dall'elenco a discesa Applicazione. L'impostazione predefinita è <Globale>. Il nome utente predefinito dell'amministratore è EiamAdmin.

      Nota: è possibile aggiungere altri utenti globali per effettuare l'accesso, quindi impostare i relativi nomi utente in base alle preferenze.
   b. Inserire la password. Si tratta della stessa password specificata durante l'installazione del server CA EEM per EiamAdmin
   c. Selezionare la casella di controllo Ricorda impostazioni personali se in futuro si desidera eseguire l'accesso al server CA EEM con le stesse impostazioni.
3. Fare clic su Attiva accessibilità.

   L'accessibilità verrà attivata nell'interfaccia utente di CA EEM.
4. Fare clic su Accedi.

   Viene visualizzata la pagina iniziale dell'interfaccia di CA EEM.

Rimozione del server

È possibile disinstallare il server CA EEM utilizzando la funzione Installazione applicazioni del Pannello di controllo.

Nota: non è possibile rimuovere il server CA EEM se sono state registrate applicazioni in CA EEM. Prima di disinstallare il server CA EEM, è necessario annullare la registrazione delle applicazioni. Per ulteriori informazioni sull'annullamento della registrazione di un'applicazione, consultare la *Guida in linea*.

Installazione dell'SDK

L'installazione guidata di CA EEM SDK assiste l'utente durante il processo di installazione.

Per installare CA EEM SDK

1. Aprire Esplora risorse e fare doppio clic sul pacchetto di installazione EEMSDK_<version number>_win32.exe, oppure eseguire il file di installazione dal prompt dei comandi.

   Viene visualizzata l'installazione guidata.

2. Fare clic sul pulsante Accetto per accettare i termini e le condizioni.

   Nota: il pulsante Accetto diventa attivo solamente dopo aver letto o scorso il testo relativo ai termini e alle condizioni.

   Viene visualizzata la finestra di dialogo Scegli percorso di destinazione. Per impostazione predefinita, la procedura guidata installa CA EEM SDK nella seguente posizione: C:\Programmi\CA\Embedded IAM SDK

3. Fare clic su Avanti.

   Oppure

   Fare clic su Sfoglia per selezionare una directory nel computer in cui si desidera installare CA EEM SDK, quindi fare clic su Avanti.

   Il processo di installazione di CA EEM SDK viene avviato.

4. Fare clic su Fine.

   A questo punto, CA EEM SDK viene installato.

   Nota: durante l'installazione viene creata una variabile di ambiente %EIAM_SDK% per puntare a un percorso di installazione. Utilizzare questa variabile nel percorso di esplorazione per aprire la cartella di installazione.

Avvio di SDK

Per avviare CA EEM SDK, fare clic su Start, Programmi, CA, Embedded Entitlements Manager, EEM SDK.

Viene visualizzata la finestra di dialogo relativa alla documentazione di CA EEM SDK.

Rimozione di SDK

È possibile disinstallare CA EEM SDK utilizzando la funzione Installazione applicazioni del Pannello di controllo.

Parametri di installazione del server

Durante l'installazione di CA EEM su Windows, è necessario raccogliere informazioni sui seguenti parametri della riga di comando:

-eiampath

Specifica il percorso di installazione del server CA EEM. Il percorso predefinito è C:\Program Files\CA\SharedComponents\Embedded IAM.

-etdirpath [percorso]

Specifica il percorso di installazione di CA Directory. Il percorso predefinito è C:\Programmi\CA\Directory.

-igpath [path]

Specifica il percorso di installazione di iGateway. Il percorso predefinito è C:\Program Files\CA\SharedComponents\iTechnology.

backupdir

Specifica la posizione in cui eseguire il backup dei dati provenienti dall'installazione esistente.

-capkiinstalldir

Specifica il percorso della cartella di installazione per il modulo CAPKI. Il percorso predefinito è C:\Program Files\CA\SC\CAPKI.

-javahome [directory]

Imposta la variabile JAVA_HOME a [directory] quando si richiama il programma di installazione iGateway. Il programma di installazione di CA EEM consente di impostare la variabile anche se è già impostata. Questo parametro non ha un valore predefinito.

Nota: se si desidera installare CA EEM senza Java, è necessario impostare javahome su "nessuno".

Durante l'installazione di CA Directory, vengono utilizzati i seguenti parametri. È possibile configurare i parametri secondo necessità.

Importante: prima di personalizzare i numeri di porta predefiniti, verificare l'assenza di altri servizi configurati per l'utilizzo delle stesse porte.

-dxadminport

Specifica la porta su cui DXadmind resta in attesa delle richieste da DXmanager. Tale porta viene utilizzata per la comunicazione LDAP tra DXadmind e DXmanager. *DXadmind* è un processo in background eseguito per ogni host contenente un DSA. DXmanager utilizza DXadmind per comunicare con i DSA.

Impostazione predefinita: 2123

-dsaport

Specifica la porta utilizzata dal dsa per l'ascolto delle eventuali richieste dirette a questa porta.

Predefinito: 509

-ssldport

Specifica la porta utilizzata da CA Directory per l'ascolto del server SSLD. Il server SSLD è un processo eseguito in background per la gestione dell'autenticazione, della crittografia e della decrittografia SSL e TLS di CA Directory.

Predefinito: 21847

RouterPort

Specifica la porta utilizzata dal dsa per il collegamento al dsa del router. Il DSA di un router non dispone di dati locali e archivio dati ed è in grado di instradare soltanto il traffico ad altri DSA.

Predefinito: 1684

-dxdbsize

Specifica le dimensioni massime dell'archivio dati di CA EEM.

Predefinito: 500 MB

-dxuser

Specifica un utente non dsa in grado di installare, amministrare e disinstallare CA Directory. L'utente dxuser può appartenere a un sistema locale o a una rete.

Nota: se CA Directory è stato installato mediante un utente del sistema locale come dxuser, è possibile che tale utente venga eliminato durante l'installazione. Quindi, se si utilizza un utente del sistema locale come dxuser per installare CA Directory, verificare che l'utente non sia impostato per l'esecuzione di eventuali altri programmi.

Nota: sui computer con Windows Server 2003, la lunghezza massima della stringa consentita nel prompt dei comandi è di 8191 caratteri. Con Microsoft Windows 2000, la lunghezza massima della stringa consentita nel prompt dei comandi è di 2.047 caratteri. Per ulteriori informazioni sulla lunghezza del comando di InstallShield, consultare le *Note di rilascio*.

Installazione del server CA EEM in modalità invisibile all'utente

L'installazione del server CA EEM in modalità invisibile all'utente richiede due operazioni:

1. Creazione del file di risposta.
2. Esecuzione del comando mediante specifica del file di risposta.

   Durante l'installazione in modalità invisibile all'utente, viene creato un file di registro eiaminstall.log per la registrazione di eventuali errori di installazione.

Nota: se si installa il server CA EEM in modalità invisibile all'utente è possibile rimuovere il prodotto utilizzando la stessa modalità.

Creazione del file di risposta

È possibile registrare gli input dell'installazione in un file di risposta, che viene utilizzato per installare il server CA EEM in modalità invisibile all'utente. È necessario creare un nuovo file di risposta per ogni build che si desidera installare.

Per creare un file di risposta

1. Eseguire il pacchetto di installazione del server CA EEM nel computer di destinazione.
2. Quando viene visualizzato il prompt dei comandi, immettere il comando riportato di seguito per creare un file di risposta nella directory specificata:

   EEMServer_[*numeroversione*].[*numero_build*]_win32.exe -s -a /r /f1"*nome del percorso del file di risposta*"

   Esempio:

   EEMServer_8.4.0.55_win32.exe -s -a /r /f1"c:\resp.iss"
3. Immettere i valori per i parametri di installazione che vengono memorizzati nel file di risposta.

Esecuzione del comando mediante specifica del file di risposta

Negli esempi riportati di seguito vengono illustrate le opzioni per l'esecuzione di un'installazione invisibile all'utente:

- Per installare il server CA EEM in modalità invisibile all'utente, è necessario immettere il comando riportato di seguito al prompt dei comandi:

  EEMServer_[*numeroversione*].[*numero_build*]_win32.exe -s -a /s /f1"*nome del percorso del file di risposta*"

  Esempio:

  EEMServer_8.4.0.55_win32.exe -s -a /s /f1"c:\resp.iss"
- Per creare un file di registro relativo all'installazione durante l'installazione invisibile all'utente, eseguire il comando riportato di seguito:

  EEMServer_[*numeroversione*].[*numero_build*]_win32.exe -s -a /s /v"/qn /L*v <percorso per la creazione del file di registro>" /f1"*nome del percorso del file di risposta*"

  Esempio:

  EEMServer_8.4.0.55_win32.exe -s -a /s /v"/qn /L*v c:\install.txt" /f1"c:\resp.iss"

In questo modo, il server CA EEM viene installato in modalità invisibile all'utente mediante il file di risposta specificato.

Nota: è possibile specificare i parametri di installazione insieme allo script di installazione. Per ulteriori informazioni sui parametri, consultare Parametri di installazione del server.

Rimozione del server CA EEM in modalità invisibile all'utente

È necessario utilizzare un file di risposta creato dalla stessa build del server CA EEM al fine di rimuovere il prodotto in maniera corretta. Per installare il server CA EEM in modalità invisibile all'utente, è necessario immettere il comando riportato di seguito al prompt dei comandi:

EEMServer_[*numeroversione*].[*numero_build*]_win32.exe -s -a /s /f1"*nome del percorso del file di risposta*" /z"uninstall"

Esempio:

EEMServer_8.4.0.55_win32.exe -s -a /s /f1"c:\resp.iss" /z"uninstall"

In questo modo, è possibile rimuovere il server CA EEM in modalità invisibile all'utente.

Nota: non è possibile rimuovere il server CA EEM se sono state registrate applicazioni in CA EEM. Prima di disinstallare il server CA EEM, è necessario annullare la registrazione delle applicazioni. Per ulteriori informazioni sull'annullamento della registrazione di un'applicazione, consultare la *Guida in linea*.

Capitolo 3: Installazione in Linux e UNIX

Questa sezione contiene i seguenti argomenti:

Panoramica dell'installazione

L'installazione di CA EEM in ambienti operativi Linux e UNIX avviene mediante l'installazione delle seguenti applicazioni:

Server CA EEM

È possibile utilizzare il server CA EEM per definire i criteri di autorizzazione relativi alle risorse dell'applicazione che utilizzano un'interfaccia Web. L'interfaccia amministrativa basata su Web consente di gestire le identità e i criteri di accesso. L'infrastruttura di protezione esistente viene utilizzata per implementare regole basate sulla logica aziendale, mediante attributi risorsa e utente definiti in archivi utenti centralizzati e in altri sistemi aziendali.

CA EEM SDK (Software Development Kit)

È possibile utilizzare CA EEM SDK per incorporare controlli di protezione basati sulle identità all'interno delle applicazioni. SDK comprende librerie, classi java, file di intestazione e un'esercitazione pratica e può essere utilizzato per implementare CA EEM in qualsiasi applicazione. Per ulteriori informazioni sulle modalità di implementazione di CA EEM mediante SDK, consultare la *Guida alla programmazione*.

Ogni applicazione viene installata separatamente e funziona in maniera indipendente.

Installazione del server

Server CA EEM per Linux e UNIX utilizza uno script con shell ad estrazione automatica che assiste l'utente durante il processo di installazione. Durante il processo di installazione, viene visualizzato un file di licenza e vengono richiesti i parametri di installazione. Dopo l'immissione dei parametri di installazione, viene avviata l'installazione.

Per installare il del server CA EEM per Linux e UNIX

1. Eseguire lo script di installazione EEMServer_[*numeroversione*].[*numero_build*]_[*nome del sistema operativo*].sh nel computer di destinazione.

   Esempio:

   EEMServer_8.4.0.55_sunos.sh

   Il file viene decompresso e l'installazione viene avviata.

2. Immettere Y per accettare i termini e le condizioni del contratto di licenza (oppure N per rifiutare e interrompere l'installazione).

   Vengono richiesti i parametri di installazione.

3. Immettere i parametri di installazione.

   Nota: per ulteriori informazioni sui parametri di installazione disponibili, consultare la sezione Parametri dello script di installazione del server.

   Esempio:

   a. Immettere il percorso di installazione del server CA EEM (oppure mantenere l'impostazione predefinita).

   Viene visualizzata una schermata di conferma contenente i valori dei parametri di installazione immessi.

4. Se le informazioni visualizzate nella schermata di conferma sono corrette, immettere Y per continuare l'installazione (se si immette N, si uscirà dal programma di installazione).

5. Immettere la password EiamAdmin.

   Nota: il nome utente predefinito dell'amministratore è EiamAdmin.

   La procedura di installazione varia in base ai parametri della riga di comando e al tipo di pacchetto del server CA EEM in corso di installazione.

   L'installazione del server CA EEM nel computer in uso viene completata mediante lo script del programma di installazione.

Aggiornamento del server

È possibile aggiornare l'installazione del server CA EEM esistente alla versione corrente.

Per aggiornare un'installazione esistente del server CA EEM

1. Eseguire EEMServer_[*numeroversione*].[*numero_build*]_[*nome del sistema operativo*] nel computer di destinazione.
2. In base alla versione del server CA EEM installata, si verifica quanto segue.
   - Se la versione esistente del server CA EEM è precedente a quella in corso di installazione, viene eseguito il backup della versione esistente e l'aggiornamento automatico alla nuova versione.
   - Se la versione del server CA EEM esistente è identica a quella in corso di installazione, viene richiesto se si desidera disinstallare il del server CA EEM. È possibile disinstallare e reinstallare il del server CA EEM.
   - Se la versione in corso di installazione è precedente a quella esistente, viene generato un errore e l'installazione viene interrotta.

   Per ulteriori informazioni sull'installazione del server CA EEM, consultare Installazione del server (a pagina 28).

L'aggiornamento del server CA EEM comporta l'aggiornamento dei seguenti elementi:

- server CA EEM nella cartella \\CA\SharedComponents\iTechnology
- iGateway
- CA Directory

Rimozione del server

Per rimuovere il del server CA EEM, eseguire lo script eiamuninstall.sh dalla directory di installazione.

Nota: non è possibile rimuovere il server CA EEM se sono state registrate applicazioni in CA EEM. Prima di disinstallare il server CA EEM, è necessario annullare la registrazione delle applicazioni. Per ulteriori informazioni sull'annullamento della registrazione di un'applicazione, consultare la *Guida in linea*.

Installazione di SDK

CA EEM SDK per Linux e UNIX utilizza uno script con shell ad estrazione automatica che assiste l'utente durante il processo di installazione. Durante il processo di installazione, viene visualizzato un file di licenza e vengono richiesti i parametri di installazione. Dopo l'immissione dei parametri di installazione, viene avviata l'installazione.

Per installare CA EEM SDK per Linux e UNIX

1. Eseguire lo script di installazione EEMSDK_[*numeroversione*].[*numero_build*]_[*nome del sistema operativo*].sh nel computer di destinazione.

   Esempio:

   EEM_8.4.0.55_sunos.sh

   Il file viene decompresso e viene avviata l'installazione.

2. Immettere Y per accettare i termini e le condizioni del contratto di licenza (oppure N per rifiutare e interrompere l'installazione).
3. Immettere il percorso di installazione di CA EEM SDK (oppure mantenere l'impostazione predefinita).
4. Selezionare Installa prodotto.

   CA EEM SDK viene installato nel computer in uso.

Avvio di CA EEM SDK

Per avviare CA EEM SDK, puntare il browser Web su /opt/CA/eIAMSDK/Doc/index.html (o nel punto in cui è stato installato CA EEM SDK).

Rimozione di SDK

È possibile rimuovere CA EEM SDK dai sistemi operativi Linux e UNIX:

Per rimuovere CA EEM SDK

1. Eseguire lo script di installazione EEMSDK_[*numeroversione*].[*numero_build*]_[*nome del sistema operativo*].sh nel computer di destinazione.

   Esempio:

   EEM_8.4.0.55_sunos_linux.sh

   Il file viene decompresso.

2. Selezionare Disinstalla/Rimuovi prodotto.

   CA EEM SDK viene rimosso dal computer.

Parametri dello script di installazione del server

Durante l'installazione di CA EEM, è necessario raccogliere informazioni sui seguenti parametri della riga di comando richiesti dallo script.

Lo script accetta i seguenti parametri della riga di comando:

backupdir

Specifica la posizione in cui eseguire il backup dei dati provenienti dall'installazione esistente.

-capkiinstalldir

Specifica il percorso della cartella di installazione per il modulo CAPKI.

Impostazione predefinita: /opt/CA/SharedComponents/capki

Durante l'installazione di CA Directory, vengono utilizzati i seguenti parametri. È possibile configurare i parametri secondo necessità.

Importante: prima di personalizzare i numeri di porta predefiniti, verificare l'assenza di altri servizi configurati per l'utilizzo delle stesse porte.

-dxadminport

Specifica la porta su cui DXadmind resta in attesa delle richieste da DXmanager. Tale porta viene utilizzata per la comunicazione LDAP tra DXadmind e DXmanager. *DXadmind* è un processo in background eseguito per ogni host contenente un DSA. DXmanager utilizza DXadmind per comunicare con i DSA.

Impostazione predefinita: 2123

-dsaport

Specifica la porta utilizzata dal dsa per l'ascolto delle eventuali richieste dirette a questa porta.

Predefinito: 509

-ssldport

Specifica la porta utilizzata da CA Directory per l'ascolto del server SSLD. Il server SSLD è un processo eseguito in background per la gestione dell'autenticazione, della crittografia e della decrittografia SSL e TLS di CA Directory.

Predefinito: 21847

RouterPort

Specifica la porta utilizzata dal dsa per il collegamento al dsa del router. Il DSA di un router non dispone di dati locali e archivio dati ed è in grado di instradare soltanto il traffico ad altri DSA.

Predefinito: 1684

-dxdbsize

Specifica le dimensioni massime dell'archivio dati di CA EEM.

Predefinito: 500 MB

-dxuser

Specifica un utente non dsa in grado di installare, amministrare e disinstallare CA Directory. L'utente dxuser può appartenere a un sistema locale o a una rete.

Nota: se CA Directory è stato installato mediante un utente del sistema locale come dxuser, è possibile che tale utente venga eliminato durante l'installazione. Quindi, se si utilizza un utente del sistema locale come dxuser per installare CA Directory, verificare che l'utente non sia impostato per l'esecuzione di eventuali altri programmi.

-eiamadminpw [password]

Imposta la password EiamAdmin su [password]

-eiampath

Specifica il percorso di installazione del server CA EEM. L'impostazione predefinita è /opt/CA/SharedComponents/EmbeddedIAM.

-etdirpath [percorso]

Imposta il percorso di installazione di CA Directory.

-igpath [directory]

Imposta il percorso di iGateway. Tale percorso deve essere completamente qualificato, ad esempio –iisystem. Il percorso predefinito è /opt/CA/SharedComponents/iTechnology.

-javahome [directory]

Imposta JAVA_HOME. Tale parametro è impostato in modo predefinito sui contenuti della variabile di ambiente JAVA_HOME e viene richiesto solo nel caso in cui il parametro $JAVA_HOME non sia impostato.

Nota: Se si desidera installare CA EEM senza Java, è necessario impostare javahome=nessuno. Questa opzione non è applicabile per HP-UX.

-logfile [nome file]

Consente al programma di installazione di scrivere le informazioni di accesso su [nomefile], impostate in maniera predefinita su /tmp/eiam-install.log.

-silent

Esegue l'installazione in modalità invisibile all'utente. Se non si specifica un parametro richiesto nella riga di comando, l'installazione si interrompe e avvia la stampa di un messaggio appropriato. Non esegue alcuna modifica al sistema a meno che non siano stati specificati tutti i parametri necessari.

-tempdir [directory]

Specifica la directory da utilizzare per l'archiviazione dei file temporanei. L'impostazione predefinita è /tmp/eiam_temp. Tale percorso deve essere completamente qualificato e trovarsi all'interno della relativa sottodirectory. Questo script utilizza rm -rf per rimuovere la directory che si specifica al completamento dello script.

Installazione del server in modalità invisibile all'utente

Per installare il del server CA EEM in modalità invisibile all'utente, è necessario immettere il comando riportato di seguito al prompt dei comandi:

EEMServer_[*numeroversione*].[*numero_build*]_[*nome del sistema operativo*].sh -silent -eiamadminpw *password* -*javahome directory*

Ad esempio, il comando riportato di seguito per ambienti operativi Sun comprende i parametri minimi richiesti:

EEMServer_8.4.0.55_sunos.sh -silent -eiamadminpw *password -javahome directory*

È possibile specificare ulteriori parametri di installazione. La maggior parte dei parametri di installazione ha valori predefiniti. Per ulteriori informazioni sui parametri dello script, consultare Parametri dello script di installazione del server.

Il file viene decompresso e l'installazione viene avviata.

Rimozione del server CA EEM in modalità invisibile all'utente

Per rimuovere il del server CA EEM, eseguire lo script eiamuninstall.sh dalla directory di installazione.

Nota: non è possibile rimuovere il del server CA EEM se sono state registrate applicazioni in CA EEM. È necessario annullare la registrazione di tutte le applicazioni per terminare il processo di disinstallazione in maniera corretta. Per ulteriori informazioni sull'annullamento della registrazione di un'applicazione, consultare la *Guida in linea*.

Capitolo 4: Configurazione di CA EEM SDK

I nuovi binari hanno richiesto la creazione di applicazioni tramite CA EEM SDK

Per incorporare CA EEM SDK r8,4 SR02 nelle applicazioni, i nuovi binari riportati di seguito devono essere utilizzati in aggiunta alle DLL di CA EEM SDK delle versioni precedenti:

Java

- xml-apis.jar

C++

Copiare i file seguenti dalla cartella EIAMSDK/lib/$OS a seconda del sistema operativo in uso:

Windows

- log4cxx.dll
- log4cxx.lib
- libexpat-2,0.1.dll
- libexpat-2,0.1.dll

HP-UX

- *log4cxx* come liblog4cxx.sl, liblog4cxx.sl.10, liblog4cxx.sl.10,0
- libapr* come libapr-1.sl.3, libaprutil-1.sl.3, libapr-1.sl.3,3, libaprutil-1.sl.3,4
- libexpat-2,0.1.dll

UNIX HP-UX 11i

- *log4cxx* come liblog4cxx.so, liblog4cxx.so.10, liblog4cxx.so.10,0
- libexpat*

Come creare applicazioni utilizzando i nuovi binari Java

1. Aggiornare il ClassPath con riferimenti a xml-apis.jar.
2. Aggiornare il programma di installazione per inserire i nuovi binari ed il file di configurazione del registratore.
3. Distribuire i nuovi binare ed il file di configurazione del registratore con i binari di CA EEM SDK.

File necessari per l'esecuzione di applicazioni che utilizzano SDK C++ di CA EEM

I seguenti file binari sono necessari per incorporare ed eseguire l'applicazione utilizzando l'SDK C++ di CA EEM:

Windows

- ipthread.dll
- libcurl_7_18_2.dll
- libexpat-2,0.1.dll
- log4cxx.dll
- Msvcm80.dll
- Msvcm90.dll
- Msvcp71.dll
- Msvcp80.dll
- Msvcp90.dll
- Msvcr70.dll
- Msvcr71.dll
- Msvcr80.dll
- Msvcr90.dll
- pcre.dll
- pthread.dll
- pthreadVCE.dll
- xerces-c_2_8.dll
- zlib.dll
- Microsoft.VC80.CRT.manifest
- Microsoft.VC90.CRT.manifest

HP-UX

- liblog4cxx.sl, liblog4cxx.sl.10, liblog4cxx.sl.10,0
- libapr-1.sl.3, libapr-1.sl.3,3, libaprutil-1.sl.3,4
- libexpat-2,0.1.sl, libxerces-c.sl.28 , libcurl.sl.4, libpcre.sl.0, libexpat.sl.2 libz.sl, liblog4cxx.sl.10,0

Linux

- libxerces-c.so.28
- libcurl.so.4
- libexpat.so.2 per linux_k24 e libexpat-2,0.1.so per linux_26
- libpcre.so.0
- libz.so.1
- liblog4cxx.so.10,0.0

AIX

- libxerces-c28.a libcurl.4.so libexpat-2,0.1.a libpcre.a libz.so
- liblog4cxx.a

Sun Solaris

- libxerces-c.so.28
- libcurl.so.4 libpcre.so
- libexpat.so.2 libz.so
- liblog4cxx.so.10,0.0

Come creare applicazioni utilizzando i nuovi binari C++

1. Includere le nuove librerie fornite con CA EEM SDK aggiungendo le righe seguenti al makefile:

   ```
   -llog4cxx -llibexpat
   ```

2. Aggiornare il programma per inserire i nuovi binari, il file eiam.config ed il file eiam.log4cxx.config.
3. Distribuire i nuovi binari ed i file eiam.config ed eiam.log4cxx.config con i binari di CA EEM SDK.

Nota: è necessario includere nel codice sorgente i file header del registratore.

File necessari per creare ed eseguire applicazioni che utilizzano SDK C# di CA EEM:

I seguenti file binari sono necessari per incorporare ed eseguire applicazione utilizzando l'SDK C# di CA EEM:

- log4net.dll
- CPoz.dll
- iclient.dll
- CsharpSDK.dll

Nota: CAPICOM.dll e InterOP.CAPICOM.dll non sono necessari per generare applicazioni utilizzando SDK C#. Rimuovere tali DLL dal pacchetto.

Modalità di integrazione di SDK C# di CA EEM con le proprie applicazioni

1. Aggiungere le DLL dalla cartella seguente come assembly di riferimento durante la creazione dell'applicazione:

   %EIAM_SDK%\lib\csharp

2. Aggiornare il programma di installazione per integrare le DLL di riferimento, il file eiam.config e il file eiam.log4net.config.

   Nota: il file eiam.config e i file eiam.lognet.config si trovano nella cartella %EIAM_SDK%\bin.

3. Distribuire le DLL di riferimento, il file eiam.config e il file eiam.log4net.config sui computer client.

Configurazione di CA EEM SDK

Gli argomenti seguenti spiegano come configurare CA EEM SDK usando la classe Safe::Configurator.

Ulteriori informazioni:

Informazioni sul file eiam.config (a pagina 40)
Registrazione di CA EEM SDK (a pagina 89)
Configurare CA EEM SDK C++ (a pagina 47)
Configurare CA EEM SDK Java utilizzando SafeConfigurator (a pagina 46)

Informazioni sul file eiam.config

È necessario utilizzare il file CA EEM SDK per verificare i dati di configurazione, ad esempio:

- Buffer ciclico
- File di configurazione del registratore
- Cartella SAF per l'archiviazione dei file di controllo
- Modalità compatibile con FIPS

Il file eiam.config è costituito dai seguenti parametri configurabili:

Dimensione CyclicBuffer

Specifica il numero di messaggi di registro contenuti in un buffer ciclico. Il buffer ciclico consente di archiviare nella memoria il numero specificato di messaggi di registro più recenti. Quando il buffer raggiunge la dimensione specificata, il precedente messaggio di registro verrà sostituito da uno nuovo. In caso di arresto dell'applicazione, è possibile recuperare i messaggi di registro più recenti.

Impostazione predefinita: 500

Minimo: 0

Massimo: 1000

abilita

Specifica se il buffer ciclico è abilitato. Se è abilitato ma impostato su false, il buffer ciclico è disabilitato. Pertanto, è necessario specificare i valori dei parametri relativi a dimensioni, dump e file di CyclicBuffer.

Valore: [*true*|*false*]

Valore predefinito: true

Importante: Per impostazione predefinita, il buffer ciclico è abilitato sia che la registrazione sia attivata, sia che non lo sia. L'abilitazione del buffer ciclico inciderà sulle prestazioni di CA EEM.

dump

Specifica se, nel caso di modifiche o aggiornamenti apportati al file eiam.config, i contenuti del buffer ciclico vengono scritti in un file.

Valore: [*true*|*false*]

Valore predefinito: false

file

Specifica il nome del file dump. Se il dump è impostato su false, i messaggi di registro non vengono scritti in un file dump. L'estensione del file è .log.

File LoggerConfiguration

Specifica il percorso assoluto dei file di configurazione del registratore per gli SDK Java e C++ di CA EEM. Le informazioni sulla registrazione di CA EEM vengono memorizzate nei file di configurazione del registratore. eiam.log4cxx.config e eiam.log4j.config sono i file di configurazione del registratore per l'SDK C++ di CA EEM e per l'SDK Java di CA EEM.

Directory Saf

SAF è la cartella nella quale vengono archiviati i file di controllo per l'elaborazione.

Network sockettimeout

Specifica il timeout del socket in millisecondi.

Impostazione predefinita: 120000 (2 secondi).

Ulteriori informazioni:

Registrazione di CA EEM SDK (a pagina 89)

Esempio di file eiam.config

Di seguito viene riportato un esempio di file eiam.config:

```
<EiamConfiguration>
 <!-- EIAM Interno: Configura buffer ciclico -->
 <CyclicBuffer size="500" dump="false" file="dump.log" enable="true" />
 <!-- Percorso assoluto del file per la configurazione del registratore, per Java:-  file="eiam.log4j.config" -->
 <LoggerConfiguration file="eiam.log4cxx.config"/>
 <!-- Percorso assoluto della cartella SAF nella quale vengono archiviati i file di controllo per l'elaborazione-->
 <Saf directory="audit"/>
  <!-- Timeout del socket in millisecondi. Il valore predefinito è 2 minuti -->
 <Network sockettimeout="120000"/>
 <SDK type="Java">
        <iTechSDK>
            <FIPSMode>true</FIPSMode>
            <JCEProvider>JsafeJCE</JCEProvider>
            <Security>
                <digestAlgorithm>SHA1</digestAlgorithm>
            </Security>
            <Debug>
                <logLevel>trace</logLevel>
            </Debug>
        </iTechSDK>
 </SDK>
 <SDK type="C++">
        <iTechSDK>
            <FIPSMode></FIPSMode>
            <Commons>
                <etpkiCryptoLib></etpkiCryptoLib>
            </Commons>
            <TransportConfig>
                <!--i valori possibili sono SSLV23 / SSLV3 / TLSV1-->
                <secureProtocol></secureProtocol>
            </TransportConfig>
            <Security>
                <!--i valori possibili sono MD5/SHA1/SHA256/SHA384/SHA512-->
                <digestAlgorithm></digestAlgorithm>
            </Security>
            <Debug>
                <!--i valori possibili sono ERROR/WARNING/TRACE/NOLEVEL-->
                <logLevel></logLevel>

                <!--i valori possibili sono true/false -->
                <logToFile></logToFile>

                <!--nome file di registro-->
                <logFile></logFile>

                <!--dimensioni file di registro in MB(numero intero positivo)-->
```

```
                    <maxLogSize></maxLogSize>
                </Debug>
            <iTechSDK>
 </SDK>
</EiamConfiguration>
```

Attivazione della registrazione SDK iTechnology

È possibile abilitare la registrazione SDK iTechnology solo per SDK C++ e Java di CA EEM. Per SDK C# di CA EEM, utilizzare il file di configurazione di registrazione.

Per abilitare la registrazione SDK iTechnology, aprire il file eiam.config e modificare i seguenti tag:

- logLevel
- logToFile
- logFile
- maxLogSize

Per SDK Java di CA EEM modificare i tag menzionati nella sezione <SDK type ="Java">. Per SDK C++ di CA EEM, modificare i tag menzionati nella sezione <SDK type ="C++">.

Operazioni preliminari alla configurazione di SDK Java di CA EEM in modalità Solo FIPS

Per configurare SDK Java di CA EEM in modalità Solo FIPS, eseguire le seguenti operazioni:

1. Configurare JRE per utilizzare le librerie di terze parti Java Cryptography Extension (JCE).
2. Aggiungere le librerie Crypto-J come provider JCE nel file di protezione di Java.

   Nota: per ulteriori informazioni sulle modalità di configurazione di JRE con JCE, si rimanda alla documentazione JCE specifica.
3. Attivazione della modalità Solo FIPS nel file eiam.config.

Configurazione di SDK Java di CA EEM in modalità Solo FIPS

Se si configurano SDK di CA EEM in modalità Solo FIPS, CA EEM utilizza librerie di crittografia conformi con gli standard FIPS 140-2 per crittografare e decrittografare dati sensibili.

Per configurare SDK Java di CA EEM in modalità Solo FIPS:

1. Aprire il file eiam.config e modificare i tag riportati di seguito nella sezione <SDK type="Java">:
   - FIPSMode
   - JCEProvider
   - digestAlgorithm
2. Salvare e chiudere il file eiam.config.
3. Riavviare l'applicazione.

   L'SDK Java di CA EEM sarà, così, configurato in modalità Solo FIPS.

Configurazione di SDK C++ di CA EEM in modalità Solo FIPS

Se si configurano SDK di CA EEM in modalità Solo FIPS, CA EEM utilizza librerie di crittografia conformi con gli standard FIPS 140-2 per crittografare e decrittografare dati sensibili.

Per configurare SDK C++ di CA EEM in modalità Solo FIPS:

1. Aprire il file eiam.config e modificare i tag riportati di seguito nella sezione <SDK type="C++">:
   - FIPSMode
   - etpkiCryptoLib
   - secureProtocol
   - digestAlgorithm
2. Salvare e chiudere il file eiam.config.
3. Riavviare l'applicazione.

   L'SDK C++ di CA EEM sarà, così, configurato in modalità Solo FIPS.

Configurazione di SDK C# di CA EEM in modalità Solo FIPS

Se si configurano SDK C# di CA EEM in modalità Solo FIPS, CA EEM utilizza solo librerie di crittografia conformi con gli standard FIPS 140-2 per crittografare e decrittografare dati sensibili.

Nota: i certificati P11 non sono supportati su SDK C#.

Per configurare SDK C# di CA EEM in modalità Solo FIPS:

1. Aprire il file eiam.config e modificare i tag riportati di seguito nella sezione <SDK type="C#">:
   - FIPSMode
   - digestAlgorithm
2. Salvare e chiudere il file eiam.config.
3. Riavviare l'applicazione.

   L'SDK C# di CA EEM sarà, così, configurato in modalità Solo FIPS.

Impostazione di informazioni SafeContext

La tag <safecontext> nel file eiam.config contiene le informazioni necessarie per la generazione di un SafeContext utilizzando la classe SafeContextFactory. Tutte le tag SafeContext nel file eiam.config vengono identificate con un unico tag di riferimento ID refID. Per generare SafeContext, occorre trasmettere l'ID di riferimento refID a SafeContextFactory. Di seguito vengono riportati i vantaggi di specificare le informazioni relative a SafeContext nel file eiam.config:

Per impostare le informazioni relative a SafeContext:

1. Aprire il eiam.config e modificare la sezione <SafeContext> per impostare i tag seguenti:
   - refID
   - Back-end
   - Applicazione
   - Impostazioni locali
   - autenticazione
2. Salvare e chiudere il file eiam.config.

Configurare CA EEM SDK Java utilizzando SafeConfigurator

È necessario configurare CA EEM SDK utilizzando la classe Safe::Configurator. Per configurare un CA EEM SDK, procedere come segue:

Nota: è necessario configurare eiam.config prima di configurare CA EEM SDK.

1. Durante la fase di avvio dell'applicazione, includere nel codice le API seguenti per inizializzare CA EEM SDK:

   ```
   SafeConfigurator.getInstance().init(filename);
   ```

   Dove

   nome file

   Specifica il percorso assoluto del file eiam.config definito nell'applicazione.

   Nota: dopo questa riga, tutte le operazioni di CA EEM SDK vengono registrate in base ai livelli di tracciamento della registrazione nella configurazione del registratore.

2. Durante la fase di chiusura dell'applicazione, includere nel codice le API seguenti:

   ```
   m_config.term();
   ```

   Nota: per ogni chiamata di inzializzazione eseguita con m_config.init(*filename*), è necessario terminare la chiamata con un g m_config.term() corrispondente. I metodi di inizializzazione e di termine sono thread-safe e comprendono il conteggio dei riferimenti. La libreria Safe viene inizializzata durante la prima chiamata init() e terminata quando il conteggio dei riferimenti diviene zero.

Ulteriori informazioni:

Informazioni sul file eiam.config (a pagina 40)
Informazioni sui file di configurazione del registratore (a pagina 90)

Configurare CA EEM SDK C++

È necessario configurare CA EEM SDK utilizzando la classe Safe::Configurator. Per configurare un CA EEM SDK, procedere come segue:

Nota: è necessario configurare eiam.config prima di configurare CA EEM SDK.

1. Durante la fase di avvio dell'applicazione, includere nel codice le API seguenti per inizializzare CA EEM SDK:

   Safe::Configurator::getInstance()->init(*filename*);

   Dove

   nome file

   Specifica il percorso assoluto del file eiam.config definito nell'applicazione.

2. Durante la fase di chiusura dell'applicazione, includere nel codice le API seguenti:

   Safe::Configurator::getInstance()->term();

   Nota: per ogni chiamata di avvio eseguita con Safe::Configurator::getInstance()->init(filename), è necessario terminare la chiamata con un Safe::Configurator::getInstance()->term() corrispondente. I metodi di inizializzazione e di termine sono thread-safe e comprendono il conteggio dei riferimenti. La libreria Safe viene inizializzata durante la prima chiamata init() e terminata quando il conteggio dei riferimenti diventa zero.

Ulteriori informazioni:

Informazioni sul file eiam.config (a pagina 40)
Informazioni sui file di configurazione del registratore (a pagina 90)

Inizializzazione di SDK C# di CA EEM

Configurazione di SDK CA EEM mediante la classe SafeConfigurator. Per configurare SDK di CA EEM, procedere come segue.

Nota: configurare il file eiam.config prima di configurare SDK di CA EEM. Se non si configura il file eiam.config, l'SDK di CA EEM verrà inizializzato con la seguente configurazione predefinita:

- Modalità Non FIPS
- Registrazione impostata su errore e attivazione della registrazione della console
- Posizione SAF disattivata

Per inizializzare SDK di CA EEM, procedere come segue:

1. Includere l'API riportata di seguito nel proprio codice per l'inizializzazione dell'SDK di CA EEM durante l'avvio dell'applicazione:

   SafeConfigurator.getInstance().Init(*filename*);

   Dove

   filename

   Specifica il percorso assoluto del file eiam.config definito per l'applicazione.

   Nota: se non si specifica il nome file, l'SDK verrà inizializzato con i valori predefiniti.

2. Includere l'API seguente nel codice durante l'arresto dell'applicazione:

   SafeConfigurator.getInstance().term();

   Nota: per ulteriori informazioni sulla classe SafeConfigurator, consultare la *Guida alla programmazione*.

Capitolo 5: Supporto FIPS 140-2

Questa sezione contiene i seguenti argomenti:

Panoramica FIPS 140-2

La pubblicazione sul Federal information Processing Standard (FIPS) 140-2 specifica i requisiti per l'utilizzo di algoritmi di crittografia in un sistema di sicurezza per la protezione di dati sensibili non classificati. Il server CA EEM incorpora la libreria crittografica RSA Crypto-C ME v2.0, ritenuta conforme ai *requisiti FIPS 140-2 per la sicurezza dei moduli crittografici (Security Requirements for Cryptographic Modules).* Il numero del certificato di convalida per questo modulo è 608.

L'SDK Java di CA EEM utilizza una versione compatibile con FIPS della libreria crittografica RSA BSAFE Crypto-J 4.0. L'SDK C++ di CA EEM incorpora ETPKI 4.1.x, che utilizza librerie di crittografia RSA.

CA EEM può operare in modalità NON FIPS o Solo FIPS. I limiti di crittografia, ovvero il modo in cui viene applicata la crittografia, sono gli stessi in entrambe le modalità, ma gli algoritmi sono differenti.

Computer che utilizzano moduli crittografici FIPS 140-2 come modalità FIPS accreditata possono utilizzare solo funzioni di protezione FIPS, quali AES (Advanced Encryption Algorithm), SHA-1 (Secure Hash Algorithm) e protocolli di livello superiore, quali TLS v1.0 come esplicitamente consentito negli standard FIPS 140-2 e nelle guide all'implementazione.

In modalità Solo FIPS, CA EEM utilizza i seguenti algoritmi:

- SHA1 come algoritmo digest predefinito per crittografare le password e firmare le richieste al server. In modalità Solo FIPS, è possibile utilizzare uno dei seguenti algoritmi:
  - SHA1
  - SHA256
  - SHA384
  - SHA512
- TLS v1.0 per la comunicazione directory LDAP esterne se la connessione LDAP è su TLS.

Modalità di protezione supportate in CA EEM

CA EEM supporta due modalità operative: la modalità Non FIPS e la modalità Solo FIPS. La funzionalità di CA EEM è la stessa in entrambe le modalità. La differenza tra le due consiste negli algoritmi di crittografia utilizzati per l'archiviazione e la verifica delle password, per la comunicazione dei dati sensibili tra CA EEM e altri prodotti come directory LDAP, CA SiteMinder, e così via.

Non FIPS

È la modalità che utilizza tecniche Non FIPS per la crittografia. in questa modalità l'algoritmo MD5 è l'algoritmo predefinito utilizzato per crittografare e decrittografare dati sensibili. Nuove installazioni o aggiornamenti vengono sempre eseguiti in modalità Non FIPS. In questa modalità, il server CA EEM è compatibile con le versioni precedenti dei client di CA EEM. Ad esempio, è possibile utilizzare l'SDK CA EEM r8.4 SDK per la connessione al server CA EEM r8.4 SP3.

Solo FIPS

È la modalità che utilizza tecniche Solo FIPS per la crittografia. Questa modalità non è compatibile con client in esecuzione in modalità Non FIPS. Se i server CA EEM r8.4 SP3 sono in esecuzione in modalità Solo FIPS, è possibile utilizzare esclusivamente client dell'SDK di CA EEM r8.4 SP3 in modalità Solo FIPS.

Modalità di configurazione del server CA EEM in modalità Solo FIPS

In modalità Solo FIPS, è necessario configurare CA EEM per l'utilizzo di algoritmi compatibili con FIPS. I client dei server e degli SDK CA EEM possono comunicare solo se entrambi sono configurati in modalità Solo FIPS. Allo stesso modo, il server CA EEM in modalità Solo FIPS può comunicare solo con una directory LDAP configurata per utilizzare algoritmi compatibili con FIPS. Per configurare l'ambiente CA EEM in modalità Solo FIPS, eseguire le seguenti operazioni:

- Verificare i prerequisiti per la configurazione del server CA EEM in modalità Solo FIPS
- Configurazione del server CA EEM in modalità Solo FIPS

Prerequisiti di configurazione del server CA EEM in modalità Solo FIPS

Di seguito vengono riportati i prerequisiti per la configurazione del server CA EEM in modalità Solo FIPS:

- Verificare che gli altri prodotti CA che utilizzano iGateway (es. CA ITM, CA ELM, ecc.) siano in modalità Solo FIPS. iGateway non può essere inizializzato sia in modalità Solo FIPS che in modalità Non FIPS. Quando iGateway viene inizializzato in modalità Solo-FIPS, tutti i prodotti che utilizzano iGateway devono essere in modalità Solo FIPS. Aprire il file iGateway.conf e verificare il valore per il tag:

  FIPSMode

  Se il valore di questo tag è impostato su false, significa che il prodotto che utilizza iGateway è in modalità Non FIPS. Decidere, quindi, se si desidera abilitare CA EEM in modalità Solo FIPS a seconda della propria configurazione iGateway.

- Verificare le versioni spindle utilizzate da altri prodotti CA. Aprire il file spin.conf e annotare il valore del tag <Spindle Name> e <version>. Verificare nella relative documentazione di prodotto se le versioni siano compatibili con FIPS.

  Nota: i file iGateway.conf e spin.conf sono archiviati nel percorso seguente:

  - **Windows**: %IGW_LOC%
  - **Linux e UNIX**: /opt/CA/SharedComponents/iTechnology

Prima di configurare CA EEM in modalità Solo FIPS:

Assicurarsi che il proprio ambiente soddisfi i requisiti minimi prima di eseguire la migrazione per utilizzare la modalità Solo FIPS. Stampare il seguente elenco per utilizzarlo come elenco di controllo:

- ☐ Aggiornare il server CA EEM a CA EEM r8.4 SP3.
- ☐ Verificare che i prodotti integrati o connessi con CA EEM siano configurati per l'utilizzo della modalità Solo FIPS.

Configurazione del server CA EEM in modalità Solo FIPS

Se i configurano server CA EEM vengono configurati in modalità Solo FIPS, CA EEM utilizza solo librerie di crittografia conformi con gli standard FIPS 140-2 per crittografare e decrittografare dati sensibili.

Note:

- In modalità Solo FIPS, utilizzare IE7 (o versioni successive) oppure Firefox 3.0 (o versioni successive) per visualizzare la GUI dell'amministratore di CA EEM. Per ulteriori informazioni sulla configurazione di Firefox in modalità FIPS 140-2 Firefox, consultare il sito Web del supporto tecnico di Firefox.
- La procedura riportata di seguito è valida anche per la modifica della modalità di protezione del server CA EEM da Solo FIPS a Non FIPS oppure da Non FIPS a Solo FIPS.

Per configurare il server CA EEM in modalità Solo FIPS:

1. Interrompere il servizio iGateway.
2. Interrompere i servizi CA Directory utilizzando i seguenti comandi:

   Windows

   ```
   dxserver stop all
   ssld stop
   ```

   Linux e UNIX

   ```
   su - dsa -c "dxserver stop all"
   su - dsa -c "ssld stop"
   ```

3. Aprire il file iGateway.conf e attivare il seguente tag:

   ```
   <FIPSMode>ON<FIPSMode>
   ```

   Nota: per modificare la modalità da Solo FIPS a Non FIPS, impostare il tag FIPSMode su OFF.

4. Eseguire i seguenti comandi dal prompt dei comandi:

   Windows

   ssld remove iTechPoz-Server
   ssld install iTechPoz-Server -certfiles "%DXHOME%/config/ssld/personalities" -ca "%DXHOME%/config/ssld/iTechPoz-trusted.pem" -port 21847 -fips

   Linux e UNIX

   su - dsa
   ssld remove iTechPoz-Server
   ssld install iTechPoz-Server -certfiles $DXHOME/config/ssld/personalities -ca $DXHOME/config/ssld/iTechPoz-trusted.pem -port 21847 -fips

   Nota: l'opzione -port specifica la porta ssld. Se è stata configurata un'altra porta ssld, sostituire 21847 nel comando precedente con il numero di porta corretto. Inoltre, se si modifica la modalità di protezione da Solo FIPS a Non FIPS, utilizzare i comandi senza l'opzione -fips.

5. Avviare i servizi CA Directory utilizzando i seguenti comandi:

   Windows

   ssld start
   dxserver start all

   Linux e UNIX

   su - dsa -c "ssld start"
   su - dsa -c "dxserver start all"

6. Avviare il servizio iGateway.

   CA EEM verrà, così, configurato in modalità Solo FIPS.

Verificare che il server CA EEM sia in modalità Solo FIPS

Per verificare che il server CA EEM sia in modalità Solo FIPS, eseguire le seguenti operazioni:

1. Immettere l'URL https://*nomehost* oppure *indirizzo IP*:5250/spin/eiam/about.csp nel browser.

   Viene visualizzata la pagina Informazioni su.

2. Assicurarsi che l'etichetta FIPS: sia impostata su Abilitato.

   Se l'etichetta è impostata su Abilitato, il server CA EEM è in modalità Solo FIPS.

Comunicazione tra server CA EEM e directory LDAP esterne

La comunicazione tra server CA EEM e directory esterne dipende dal tipo di connessione LDAP tra i due: crittografata o non crittografata. Di seguito vengono riportate le modalità operative supportate del server CA EEM e dalle directory esterne in base alla crittografia:

Crittografia abilitata sul server CA EEM per la comunicazione LDAP

Quando il server CA EEM è configurato per l'utilizzo di un canale di comunicazione crittografato con una directory LDAP esterna, se il server CA EEM è in modalità FIPS, la directory LDAP deve essere configurata per utilizzare una modalità compatibile con FIPS.

Configurazione di CA EEM per l'utilizzo di certificati del server in una periferica PKCS#11

Per utilizzare periferiche nCipher PKCS#11 con server o SDK di CA EEM, configurare la periferica nCipher e impostare la seguente proprietà:

CKNFAST_OVERRIDE_SECURITY_ASSURANCES=all

Nota: per ulteriori informazioni sulle modalità di configurazione della periferica nCipher con un token di autenticazione, consultare la documentazione di nCIPHER.

Per configurare il server CA EEM per l'utilizzo di certificati archiviati in una periferica PKCS# 11, eseguire le seguenti operazioni:

1. Arrestare il servizio iGateway.
2. Aprire il file di configurazione iGateway.conf e modificare i tag <Connector name="defaultport"> CA Portal5250</port> per impostare i seguenti valori:

   certType

   Definisce il tipo di interfaccia da utilizzare. I tipi di certificato supportati sono p12, pem e p11.

   Impostazione predefinita:pem

   Tipo: childnode

Utilizzo del certificato P11

<pkcs11Lib/>—Percorso alla libreria PKCS11 fornito dal token

<token/>—ID del token

<userpin/>—PIN dell'utente crittografato

<id/>—ID del certificato e della chiave privata

<sensitive/>—La chiave privata è sensibile. Le chiavi sensibili non vengono convertite come le chiavi software e le operazioni di crittografia vengono eseguite mediante hardware cryptopki (le chiavi non sensibili possono essere considerato come sensibili, ma le chiavi sensibili non possono essere convertite o considerate come le chiavi non sensibili)

Impostazione predefinita: falso

3. Salvare e chiudere il file iGateway.conf.
4. Avviare i servizi iGateway.

Configurazione di CA EEM per l'archiviazione dei certificati del server in una periferica PKCS#11

Per archiviare i certificati di CA EEM in una periferica PKCS# 11, eseguire le seguenti operazioni:

1. Arrestare il servizio iGateway.
2. Aprire il file iGateway.conf e modificare il tag <certificatemanager> impostando i seguenti valori:

   certType

   Definisce il tipo di interfaccia da utilizzare. I tipi di certificato supportati sono p12, pem e p11.

   Impostazione predefinita:pem

   Tipo: childnode

Utilizzo del certificato P11

<pkcs11Lib><pkcs11Lib/>—Percorso alla libreria PKCS11 fornito dal token

<token><token/>—ID del token

<userpin/><userpin/>—PIN dell'utente crittografato

<id><id/>—ID del certificato e della chiave privata

<sensitive/><sensitive/>—La chiave privata è sensibile. Le chiavi sensibili non vengono convertite come le chiavi software e le operazioni di crittografia vengono eseguite mediante hardware cryptoki (le chiavi non sensibili possono essere considerate anche come chiavi sensibili mentre le chiavi sensibili non possono essere convertite/considerate come chiavi non sensibili). Facoltativo: impostato in modo predefinito su false.

3. Salvare e chiudere il file iGateway.conf.
4. Avviare i servizi iGateway.

Configurazione dell'applicazione in modalità Solo FIPS

Per configurare l'applicazione in modalità Solo FIPS, verificare che l'SDK di CA EEM sia in modalità Solo FIPS. L'SDK di CA EEM utilizza solo tecniche compatibili con FIPS per la crittografia. Il file di configurazione eiam.config dell'SDK di CA EEM determina la modalità operativa di protezione dell'SDK di CA EEM. Prima di configurare l'SDK di CA EEM in modalità Solo FIPS, verificare quanto segue:

- Assicurarsi che la versione dell'SDK di CA EEM sia la r8.4 SP3.
- Eseguire la migrazione dei certificati P12 esistenti utilizzati da CA EEM nei certificati PEM.
- Inizializzare l'SDK di CA EEM in modalità Solo FIPS.

Migrazione dei certificati P12 certificati utilizzati dall'applicazione nei certificati PEM.

CA EEM supporta certificati P12, PEM e PKCS# 11 con i seguenti presupposti:

- il supporto P12 è disabilitato (non disponibile) in modalità Solo FIPS. In alternativa, in modalità Solo FIPS, è stato aggiunto il supporto per i certificati PEM e PKCS#11.

Nota: l'SDK C# di CA EEM supporta solo certificati PEM in modalità Solo FIPS e certificati P12 e PEM in modalità Non FIPS.

In tal modo, se si utilizzano certificati P12, eseguire la migrazione di tali certificati in uno dei formati di certificato supportati in modalità Solo FIPS. Utilizzare l'utilità igwCertUtil per convertire certificati P12 in certificati PEM. igwCertUtil è un'utilità per convertire, creare o eliminare certificati. igwCertUtil si trova nella seguente cartella:

Windows

%IGW_LOC%

UNIX e LINUX

$IGW_LOC

Utilità igwcertutil-Creazione, copia, conversione ed eliminazione dei certificati

Valida per Windows, UNIX e Linux

Il formato del comando di creazione è il seguente:

igwCertUtil -version *version* -create -cert *inputcert*-params -issuer issuercert -params [-debug] [-silent]

Il formato del comando di conversione è il seguente:

igwCertUtil -version version -conv -cert *inputcert*-params -target newcert-params [-debug] [-silent]

Il formato del comando di copia è il seguente:

igwCertUtil -version version -copy -cert *inputcert*-params -target newcert-params [-debug] [-silent]

Il formato del comando di eliminazione è il seguente:

igwCertUtil -version version -delete -cert *cert*-params [-debug] [-silent]

-version *version*

Specifica la versione di igwCertUtil utilizzata durante la creazione, la conversione, la copia o l'eliminazione dei certificati. La versione viene utilizzata per la compatibilità con le versioni precedenti. Se l'utilità igwCertUtil viene modificata, il tag della versione assume il comportamento precedente.

-cert *inputcert*-parms

Specifica il certificato come stringa XML per la creazione, la conversione o la copia dei certificati.

-issuer *issuercert*-parms

Specifica il certificato utilizzato per firmare il nuovo certificato generato durante la creazione di un certificato. Se non viene specificato nessun certificato, verrà creato un certificato autofirmato.

-target *newcert*-parms

Specifica la configurazione del nuovo certificato durante la conversione (o la copia) di un certificato esistente.

-cert *cert*-parms

-debug

(Facoltativo) Attiva il debug per igwCertUtil.

-silent

(Facoltativo) Attiva modalità invisibile all'utente per igwCertUtil.

L'utilità igwCertUtil restituisce i seguenti codici di errore:

- CERTUTIL_ERROR_UNKNOWN (-1): unknown or undefined error happened (CERTUTIL_ERROR_UNKNOWN (-1): si è verificato un errore sconosciuto o non definito)
- CERTUTIL_SUCCESS (0): successful operation (CERTUTIL_SUCCESS (0): operazione completata con successo)
- CERTUTIL_ERROR_USAGE (1): wrong command line arguments passed (CERTUTIL_ERROR_USAGE (1): argomenti della riga di comando errati)
- CERTUTIL_ERROR_READCERT (2): unable to read certificate (CERTUTIL_ERROR_READCERT (2): impossibile leggere il certificato)
- CERTUTIL_ERROR_WRITECERT (3): unable to write certificate (CERTUTIL_ERROR_READCERT (3): impossibile scrivere il certificato)
- CERTUTIL_ERROR_DELETECERT (4): unable to delete certificate (CERTUTIL_ERROR_READCERT (3): impossibile eliminare il certificato)

Esempio: conversione di certificati P12 in certificati PEM

l'esempio seguente descrive l'utilizzo della conversione di un certificato P12 in un certificato PEM:

```
igwCertUtil -version 4,6.0,0 -conv  -cert
"<Certificate><certType>p12</certType><certURI>testCert.p12</certURI><certPW>password</certPW></Certificate>" -target "<Certificate><certType>pem</certType>
<certURI>testCert.cer</certURI><keyURI>testCert.key</keyURI></Certificate>"
```

Esempio: conversione di certificati P12 in certificati PKCS#11:

```
igwCertUtil -version 4,6.0,0 -conv  -cert
"<Certificate><certType>p12</certType><certURI>testCert.p12</certURI><certPW>password</certPW></Certificate>" -target "<Certificate><certType>p11</certTyp
><pkcs11Lib>pathto-pkcs11Lib</pkcs11Lib><token>pkcs11token</token><userpin>user
in</userpin><id>certid</id></Certificate>"
```

Inizializzazione dell'SDK di CA EEM in modalità Solo FIPS

L'SDK di CA EEM può essere inizializzato in modalità Solo FIPS configurando il file eiam.config. Per configurare il file eiam.config, consultare il capitolo relativo alla configurazione dell'SDK di CA EEM (a pagina 35).

Capitolo 6: Backup e ripristino del server CA EEM

Questa sezione contiene i seguenti argomenti:

Backup del file system

Si consiglia di eseguire il backup dei server CA EEM periodicamente o dopo aver apportato modifiche negli ambienti server CA EEM. È possibile utilizzare i backup del server CA EEM per ripristinare il del server CA EEM qualora fosse danneggiato.

È necessario eseguire il backup dei seguenti file e cartelle di CA EEM:

Descrizione dei dati	Nomi dei file su Windows	Nomi dei file su Linux
File di configurazione	■ iPoz.conf ■ Eiam.conf ■ iPoz.map ■ Spin.conf ■ iPozDsa.pem ■ iPozRouterDsa.pem ■ logDepot.conf ■ calmReporter.conf	■ iPoz.conf ■ Eiam.conf ■ iPoz.map ■ Spin.conf ■ iPozDsa.pem ■ iPozRouterDsa.pem ■ eiam-type ■ Sponsorfiles ■ logDepot.conf ■ calmReporter.conf

Descrizione dei dati	Nomi dei file su Windows	Nomi dei file su Linux
Informazioni sugli eventi	■ logdepotdb ■ cartella calm_catalog ■ cartella calm_archive	■ logdepotdb ■ cartella calm_catalog ■ cartella calm_archive
Cartelle	■ Registro di sistema ■ Cartella iTechnology	■ Cartella iTechnology ■ Impostazioni di ambiente

Backup dei file e delle cartelle del server CA EEM

Si consiglia di eseguire il backup dei server CA EEM periodicamente o dopo aver apportato modifiche negli ambienti server CA EEM. È possibile utilizzare i backup del server CA EEM per ripristinare il del server CA EEM qualora fosse danneggiato.

Per eseguire il backup dei file e delle cartelle del server CA EEM

1. Arrestare iGateway.
2. Eseguire il backup dei file di configurazione, delle informazioni sugli eventi e delle cartelle di CA EEM.
3. Eseguire il backup dei dati di CA EEM memorizzati in CA Directory.

   A questo punto, viene eseguito il backup dei file di configurazione, degli eventi e delle cartelle del server CA EEM.

Ulteriori informazioni:

Backup del file system (a pagina 61)
Backup dei dati di CA EEM memorizzati in CA Directory (a pagina 65)

Procedure di ripristino

È necessario ripristinare i dati di CA EEM affinché sia possibile:

- Recuperare un'installazione di CA EEM danneggiata
- Recuperare un ambiente server CA EEM con funzionamento non appropriato

Per recuperare i file di configurazione e i dati di CA EEM

1. Arrestare iGateway.
2. Rinominare tutti i file di backup .conf di CA EEM in .conf.merge, quindi copiare i file di configurazione rinominati nella cartella iTechnology. I file .conf.merge sono necessari per unire i file di configurazione sottoposti a backup con quelli nuovi.
3. Ripristinare i dati di CA EEM.
4. Avviare iGateway.

Ulteriori informazioni:

Backup dei dati di CA EEM memorizzati in CA Directory (a pagina 65)

Avvio del servizio iGateway

È necessario immettere i seguenti comandi per avviare il servizio iGateway:

Windows

net start igateway

Linux e UNIX

$IGW_LOC/S99igateway start

Arresto del servizio iGateway

È necessario immettere i seguenti comandi per arrestare il servizio iGateway:

Windows

net stop igateway

Linux e UNIX

$IGW_LOC/S99igateway stop

Capitolo 7: Backup dei dati di CA EEM memorizzati in CA Directory

Questa sezione contiene i seguenti argomenti:

Introduzione alla terminologia di CA Directory

In questa sezione viene descritta la terminologia di CA Directory utilizzata nel presente documento:

DSA

Un *DSA* è un processo che gestisce tutti gli spazi dei nomi di una directory o parte di questi.

This also needs to be expanded to make it accessible to readers new to CA Directory. Durante l'installazione del server CA EEM, è possibile configurare i seguenti parametri correlati a CA Directory:

DXmanager

DXmanager è un'applicazione Web che consente di creare, configurare, gestire e controllare la dorsale di directory.

Console DSA

La *console DSA* consente il collegamento a un DSA per fornire comandi DXserver, ricevere informazioni di traccia e fungere da agente utente.

DXtools

Gli strumenti *DXtools* sono un set di utilità della riga di comando disponibili in CA Directory che consentono di gestire directory, operare con dati LDIF, caricare e scaricare dati da una directory, nonché estrarre e convertire schemi da utilizzare con CA Directory.

LDIF (Formato interscambio dati LDAP, LDAP Data Interchange Format)

I *file LDIF* sono file di testo che consentono di memorizzare le informazioni sulla directory in formato LDIF. È possibile utilizzare i file LDIF per trasferire le informazioni sulla directory tra i server directory LDAP oppure per descrivere un insieme di modifiche da applicare a una directory.

Modalità di utilizzo degli strumenti DXtools

È possibile eseguire gli strumenti DXtools in base alle seguenti procedure:

- Eseguire i comandi DXtools sull'host, mediante la console DSA.
- Eseguire i comandi DXtools su un host remoto, mediante la console DSA su una rete TCP/IP.
- Includere i comandi DXtools negli script.

In caso di operazione completata correttamente, tutti gli strumenti restituiscono zero, in caso contrario non zero.

Variabile d'ambiente DXHOME

Alcuni strumenti richiedono che la variabile d'ambiente DXHOME sia impostata sul percorso della home directory di DXserver. Tale operazione viene eseguita automaticamente quando CA Directory è installato.

Alcuni strumenti prevedono che i file di configurazione DSA siano ubicati nella cartella *config* nel percorso in DXHOME.

Codici di stato di uscita per gli strumenti DXtools

Gli strumenti DXtools condividono codici di uscita comuni, sebbene non tutti i codici di uscita siano applicabili a tutti gli strumenti. Di seguito vengono riportati i codici di uscita:

0

Operazione riuscita

1

Il DSA associato è in esecuzione.

2

Sono già presenti uno o più file dell'archivio dati.

3

La posizione della directory specificata non esiste oppure non è una directory.

4

Il tipo di file specificato non è valido, ad esempio si tratta di una directory.

5

Si sono verificati problemi di autorizzazione con il file specificato.

6

Il nome del percorso completo del file dell'archivio dati è troppo lungo. Ad esempio, è possibile che si verifichi tale situazione quando la posizione specificata per la directory dell'archivio dati è troppo lunga.

7

Si è verificato un errore durante il tentativo di rimozione dei file precedenti dell'archivio dati.

8

Si è verificato un errore durante il tentativo di ridenominazione dei file precedenti dell'archivio dati.

9

Si è verificato un errore durante il tentativo di creazione o modifica di uno dei file.

10

Le dimensioni dell'archivio dati sono inferiori o pari a zero.

11

Spazio insufficiente sul dispositivo oppure mancanza di memoria durante il tentativo di creazione del file.

12

Accesso insufficiente (probabilmente a causa di diritti insufficienti) per la creazione del file o per l'impostazione dell'accesso al file.

13

Variabile di ambiente DXHOME non impostata.

14

Variabile di ambiente DXHOME non valida.

15

DSA associato già esistente.

16

Impossibile avviare il DSA creato. Per dettagli, consultare i relativi file di registro.

17

Sono stati immessi parametri della riga di comando non validi o sconosciuti.

18

DSA associato inesistente.

Modalità di backup dei dati di CA Directory

Per eseguire il backup dei dati di CA Directory, attenersi alla seguente procedura:

1. Eseguire la connessione a un DSA locale.
2. Creare un'istantanea dell'archivio dati del DSA predefinito in esecuzione. Tale processo viene definito dump in linea. Per creare l'istantanea, utilizzare il seguente comando:

   dump *dxgrid-db*

   Nota: sostituire dxgrid-db con il nome dsa iTechPoz-Servern per il backup di CA EEM.
3. Utilizzare lo strumento DXdumpdb per eseguire il backup del dump in linea (file .ZDB), ovvero l'istantanea dell'archivio dati in un file LDIF.

Ulteriori informazioni:

Eseguire la connessione a una console DSA locale. (a pagina 68)
Dump in linea dell'archivio dati (a pagina 69)
Comando dump dxgrid-db: creazione di un'istantanea coerente di un archivio dati (a pagina 70)

Eseguire la connessione a una console DSA locale.

È possibile eseguire la connessione a un DSA in locale su UNIX o Windows se è stata impostata una porta della console per tale DSA.

Per eseguire la connessione a una console DSA locale

1. Aprire un prompt dei comandi sull'host in cui viene eseguito il DSA.
2. Immettere il seguente comando:

   telnet localhost *local-port-number*

   local-port-number

   Specifica il numero di porta della console del DSA a cui si desidera eseguire la connessione.

Dump in linea dell'archivio dati

È possibile creare un'istantanea coerente dell'archivio dati di un DSA in esecuzione (un dump in linea). Il DSA completa eventuali aggiornamenti prima di eseguire il dump in linea e non vengono avviati ulteriori aggiornamenti fino al termine della copia.

Il file dell'archivio dati viene copiato in un file la cui estensione inizia con .z: il file del database è, quindi, *dxgrid-db*.zdb.

Nota: ciascun dump comporta la sovrascrittura dei file di backup precedenti. Se si desidera salvare i file di backup, copiarli in una diversa posizione prima di eseguire il dump successivo.

Comando dump dxgrid-db: creazione di un'istantanea coerente di un archivio dati

Il comando *dump dxgrid-db* consente di creare un'istantanea coerente dell'archivio dati di un DSA in esecuzione (un dump in linea). Il DSA completa eventuali aggiornamenti prima di eseguire tale comando e non vengono avviati ulteriori aggiornamenti fino al termine della copia.

Il file dell'archivio dati viene copiato in un file la cui estensione inizia con .z: il file del database è, quindi, *dxgrid-db*.zdb.

Nota: ciascun dump comporta la sovrascrittura dei file di backup precedenti. Se si desidera salvare i file di backup, copiarli in una diversa posizione prima di eseguire il dump successivo.

Lo strumento DXdumpdb è in grado di esportare dati da un archivio dati creato dal comando dump.

Il formato del comando è il seguente:

dump *dxgrid-db* [period *start period*];

period *start period*

(Facoltativo) Specifica che il dump in linea viene eseguito a intervalli periodici.

start

Definisce il numero di secondi a partire da domenica 00:00:00 GMT.

Nota: l'ora di avvio viene definita mediante il fuso orario GMT anziché quello locale.

period

Definisce il numero di secondi tra i dump in linea.

Esempio: esecuzione di un dump in linea ogni ora

Il seguente comando consente di creare un'istantanea dell'archivio dati ogni ora:

dump *dxgrid-db* 0 3600

Nota: accertarsi di creare un processo cron su UNIX o un'attività pianificata su Windows per copiare i file sottoposti a backup in una posizione protetta. Ciascun dump comporta la sovrascrittura dei file di backup precedenti.

Utilizzo di un file LDIF per il backup e il caricamento dei dati

I *file LDIF* sono file di testo che consentono di memorizzare le informazioni sulla directory in formato LDIF. È possibile utilizzare i file LDIF per trasferire le informazioni sulla directory tra i server directory LDAP oppure per descrivere un insieme di modifiche da applicare a una directory.

CA Directory è dotato dello strumento DXdumpdb, che consente di scaricare dati da un archivio dati in un file LDIF. Successivamente, è possibile caricare i dati dal file LDIF in un archivio dati per recuperare il contenuto della directory.

Backup di una directory in un file LDIF

Per eseguire il backup di una directory in un file LDIF

1. Eseguire l'accesso come *dsa* utente (su UNIX) o amministratore DXserver (su Windows).
2. Utilizzare il seguente comando per eseguire il backup dell'archivio dati nel file LDIF:

   dxdumpdb -f *nomefile* -z *nomedsa*

   -f *nomefile*

   Specifica il percorso e il nome file in cui viene eseguito il dump dei dati.

   -z

   Specifica che il dump di DXdumpdb viene eseguito dall'archivio dati creato dal dump del comando di console dxgrid-db.

   dsaname

   Specifica il nome del DSA.

Strumento DXdumpdb: esportazione dei dati da un archivio dati in un file LDIF

Utilizzare lo strumento DXdumpdb per esportare dati da un archivio dati in un file LDIF.

Nota: per un elenco dei codici di stato restituiti da tutti i comandi DXtools, incluso il comando specificato sopra, consultare Codici di stato per gli strumenti DXtools (a pagina 66).

Il formato del comando è il seguente:

dxdumpdb *options DSA*

opzioni

Denota una o più delle seguenti opzioni:

-f *nomefile*

Specifica il file in cui ricevere i dati esportati. Se non si specifica tale opzione, l'output diventa output standard o viene visualizzato nella schermata.

-v

Viene eseguito in modalità dettagliata. L'opzione passa a errore e tracing di stato. Affinché l'opzione -v funzioni correttamente, è necessario specificare anche l'opzione -f.

-z

Specifica che il dump di DXdumpdb viene eseguito dall'archivio dati creato dal dump del comando di console *dxgrid-db*.

DSA

Definisce il DSA. Viene eseguita la ricerca nei file di configurazione del DSA per individuare l'archivio dati da esportare in un file LDIF.

Esempio: estrazione di dati democorp sulla schermata

Nell'esempio riportato di seguito, i dati in formato LDIF vengono stampati dall'archivio dati del DSA *democorp* nella schermata:

dxdumpdb democorp

Backup di un dump in linea dell'archivio dati

Nell'esempio riportato di seguito, un dump in linea dell'archivio dati viene esportato in un file LDIF.

dxdumpdb -f eembackup -z iTechPoz-Servern

Modalità di ripristino dei dati di CA Directory

Per ripristinare CA Directory, attenersi alla seguente procedura:

1. Arrestare il DSA.
2. Utilizzare lo strumento DXloaddb in un archivio dati da un file LDIF.

Strumento DXloaddb: caricamento di un archivio dati da un file LDIF

Utilizzare lo strumento DXloaddb per caricare un archivio dati da un file LDIF. È necessario che l'archivio dati sia già esistente. Tutte le informazioni precedenti nell'archivio dati vengono eliminate.

Note di utilizzo:

- Non è necessario ordinare il file LDIF.
- Viene eseguito l'hashing di eventuali voci di password nel file LDIF non crittografato.

  Se viene specificato un algoritmo hash nella configurazione DSA, viene utilizzato tale algoritmo. In caso contrario, viene utilizzato SHA-1.
- Per impostazione predefinita, viene utilizzata la configurazione del DSA per la gestione degli attributi operativi:
  - In caso di *op-attrs* = *true*, nell'archivio dati vengono caricati gli eventuali attributi operativi nel file LDIF.

    Viene aggiunto un createTimestamp al file LDIF qualora non ne fosse già presente uno.
  - In caso di *op-attrs* = *false*, gli attributi operativi nel file LDIF vengono ignorati e non ne vengono creati altri mediante lo strumento DXloaddb.

Il formato del comando è il seguente:

dxloaddb [*opzioni*] *dsa ldif-file*

opzioni

Denota una o più delle seguenti opzioni:

-n

Specifica che lo strumento DXloaddb non esegue alcuna azione.

-O

Specifica che lo strumento DXloaddb include gli attributi operativi standard, ad esempio il criterio di password (ad esempio il numero di tentativi di accesso) e gli attributi timestamp. Se si specifica tale opzione, vengono creati gli eventuali attributi operativi non definiti nel file LDIF.

-s

Specifica che lo strumento DXloaddb produce le seguenti statistiche relative all'archivio dati:

- Dimensioni totali dei dati in MB
- Numero di voci totali
- Numero di voci ignorate
- Quantità di riempimento nel file dell'archivio dati in KB
- Numero medio di voci per MB

-v

Specifica l'output dettagliato.

ldif-file

Nome del file LDIF da caricare nell'archivio dati.

DSA

Definisce il DSA il cui archivio dati deve essere caricato.

Esempio: creazione e caricamento di un archivio dati

Di seguito viene riportata la sequenza appropriata di creazione e caricamento di un archivio dati:

```
dxnewdb
dxloaddb
```

Esempio: caricamento dei dati LDIF nell'archivio dati

Nel seguente esempio i dati vengono caricati dal file democorp.ldif al democorp dell'archivio dati:

```
dxloaddb democorp democorp.ldif
```

Di seguito viene riportata una porzione possibile del file democorp.ldif:

```
dn: o=Democorp, c=US
oc: organization
dn: ou=Administration, o=Democorp, c=US
oc: organizationalUnit
dn: cn=Fred Jones, ou=Administration, o=Democorp, c=US
oc: organizationalPerson
postalAddress: 11 Main Street $ Newtown
surname: Mario
title: Manager
telephonenumber: +1 (123) 456 7890
telephonenumber: +1 (987) 654 3210
dn: ou=Sales, o=democorp, c=US
oc: organizationalUnit
```

Telephonenumber viene visualizzato due volte poiché si tratta di un attributo multivalutato

Capitolo 8: Configurazione del failover

Questa sezione contiene i seguenti argomenti:

Failover

Il failover è la capacità di garantire flusso dei dati e funzionamento ininterrotti anche quando i dati non sono disponibili.

Affinché il failover di CA EEM funzioni correttamente, è necessario associare un'applicazione a CA EEM installato su un server per ottenere le informazioni relative ad altri server. Le informazioni sulla configurazione di altri server sono disponibili nel file iPoz.conf utilizzato per il failover.

È possibile configurare CA EEM per il supporto di due scenari di failover:

- Failover dell'archivio dati
- Failover del server (a pagina 82)

Nota: in questo scenario si presuppone che i nomi degli host siano Server1, Server2 e ServerN.

Failover dell'archivio dati applicazioni

Il server CA EEM utilizza CA Directory come archivio dati applicazioni. Questo archivio dati applicazioni fornisce supporto incorporato per il failover e il ripristino. Sincronizzare quanto segue su tutti i server nella configurazione di failover:

1. Ora di sistema
2. Modalità di protezione (Non FIPS o Solo FIPS)
3. Archivio dati applicazioni
4. Verificare che la ricerca DNS sia corretta

Importante: Eseguire il backup degli archivi applicazione dati prima di eseguire la sincronizzazione. Per ulteriori informazioni sulle modalità di backup dell'archivio dati, consultare la sezione relativa al backup dei dati CA EEM archiviati in CA Directory (a pagina 65).

Configurazione del failover dell'archivio dati applicazioni

Nota: eseguire i passaggi della seguente procedura sul server primario. Eventuali passaggi da eseguire sui server secondari vengono indicati esplicitamente.

Nella procedura riportata, si considera che il server CA EEM sia stato installato con i seguenti valori predefiniti:

- dsa user: dsa
- data dsa port: 509
- group membership: etrdir

Se alcuni dei suddetti parametri sono stati personalizzati, sostituire i valori predefiniti con i valori personalizzati.

Per configurare il failover dell'archivio dati applicazioni:

1. Interrompere i servizi di CA EEM utilizzando i comandi seguenti su tutti i server presenti nella configurazione di failover:

   Windows

   net stop igateway
   dxserver stop all
   ssld stop

   Linux e UNIX

   $IGW_LOC/S99igateway stop
   su - dsa -c "dxserver stop all"
   su - dsa -c "ssld stop"

2. Copiare i file riportati di seguito dai server secondari di CA EEM al server primario (ad es. Server1) nelle rispettive cartelle:

   Windows

   %DXHOME%\config\knowledge\iTechPoz-*HostnameOfServerN*.dxc
   %DXHOME%\config\knowledge\iTechPoz-*HostnameOfServerN-Router*.dxc
   %DXHOME%\config\ssld\personalities\iTechPoz-*HostnameOfServerN*.pem
   %DXHOME%\config\ssld\personalities\iTechPoz-*HostnameOfServerN*-Router.pem

   Linux e UNIX

   $DXHOME/config/knowledge/iTechPoz-*HostnameOfServerN*.dxc
   $DXHOME/config/knowledge/iTechPoz-*HostnameOfServerN-Router*.dxc
   $DXHOME/config/ssld/personalities/iTechPoz-*HostnameOfServerN*.pem
   $DXHOME/config/ssld/personalities/iTechPoz-*HostnameOfServerN*-Router.pem

3. Copiare il file riportato di seguito dai server secondari in una cartella temporanea sul server primario Server1:

   UNIX e Linux

   $DXHOME/config/ssld/iTechPoz-trusted.pem

   Windows

   %DXHOME%\config\ssld\iTechPoz-trusted.pem

4. Modificare i file di configurazione (iTechPoz-*HostnameOfServerN*.dxc) di tutti i server in Server1, come indicato di seguito:

   Modificare la seguente riga:

   address = tcp localhost port 509

   #address = tcp HostnameOfServerN port 509, tcp localhost port 509

   #dsa-flags = multi-write

   In:

   #address = tcp localhost port 509

   address = tcp HostnameOfServerN port 509, tcp localhost port 509

   dsa-flags = multi-write

   Note:

   - CA EEM utilizza il numero di porta 509 come dato predefinito per la porta DSA. Se è stato configurato il server CA EEM per utilizzare una porta DSA personalizzata, sostituire 509 con il numero di porta personalizzato.
   - Per utilizzare indirizzi IP al posto del nome host, racchiudere l'indirizzo IP tra virgolette (" ").

5. Modificare iTechPoz.dxg del Server1 per includere i riferimenti al server secondario.

   Esempio:

   ```
   # iTechPoz - iTechnology Repozitory
   # Source the knowledge files of the iTechPozRouter and iTechPoz DSAs.
   source "iTechPoz-HostnameofServer1-Router.dxc";
   source "iTechPoz-HostnameofServer1.dxc";
   source "iTechPoz-HostnameOfServer2-Router.dxc";
   source "iTechPoz-HostnameOfServer2.dxc";
   source "iTechPoz-ServerN-Router.dxc";
   source "iTechPoz-ServerN.dxc";
   ```

6. Creare un nuovo file iTechPoz-trusted.pem concatenando i contenuti del file iTechPoz-trusted.pem di ciascun server secondario con il Server1.

   Windows

   type <absolute path to iTechPoz-trusted.pem of Server2> >> <absolute path to iTechPoz-trusted.pem of Server1>

   UNIX o Linux

   cat <absolute path to iTechPoz-trusted.pem of Server2> >> <absolute path to iTechPoz-trusted.pem of Server1>

   Example: type "C:\Program Files\CA\Directory\dxserver\config\ssld\iTechPoz-trusted_2.pem" >> "C:\Program Files\CA\Directory\dxserver\config\ssld\iTechPoz-trusted.pem

7. Concatenare il contenuto di iTechPoz-trusted.pem di ogni server secondario con il file iTechPoz-trusted.pem del Server1.

8. Copiare i file riportati dal server primario nelle rispettive cartelle su tutti i server secondari:

   Nota: eseguire il backup dei file iTechPoz-trusted.pem, dei file di dati DSA e dei file router (iTechPoz. *) dei server secondari prima di eseguire la copia.

   UNIX e Linux

   $DXHOME/config/ssld/iTechPoz-trusted.pem
   $DXHOME/config/ssld/personalities/iTechPoz-*.pem
   $DXHOME/config/knowledge/iTechPoz*

   Windows

   %DXHOME%\config\ssld\iTechPoz-trusted.pem
   %DXHOME%\config\ssld\personalities\iTechPoz-*.pem
   %DXHOME%\config\knowledge\iTechPoz*

9. Modificare il file iTechPoz.dxg su ciascun server secondario. Nel file iTechPoz.dxg deve risultare:

   # iTechPoz - iTechnology Repozitory
   # Source the knowledge files of the iTechPozRouter and iTechPoz DSAs.
   source "iTechPoz-HostnameOfServerN-Router.dxc";
   source "iTechPoz-HostnameOfServerN.dxc";
   source "iTechPoz-HostnameOfServer1-Router.dxc";
   source "iTechPoz-HostnameOfServer1.dxc";
   source "iTechPoz-HostnameOfServer2-Router.dxc";
   source "iTechPoz-HostnameOfServer2.dxc";
   source "iTechPoz-ServerKRouter.dxc";
   source "iTechPoz-ServerK.dxc";

   Nota: le voci per l'host locale devono trovarsi prima delle voci per gli altri server.

10. Modificare il proprietario e l'appartenenza al gruppo dei seguenti file rispettivamente a dsa e etrdir per tutti i server CA EEMin esecuzione su UNIX o Linux. Eseguire i seguenti comandi:

    chown dsa:etrdir /opt/CA/Directory/dxserver/config/ssld/iTechPoz-trusted.pem
    chown dsa:etrdir /opt/CA/Directory/dxserver/config/knowledge/iTechPoz*

11. Avviare i servizi CA EEM utilizzando i seguenti comandi su tutti i server:

    Windows

    ssld start
    dxserver start all
    net start igateway

    Linux e UNIX

    su - dsa -c "ssld start"
    su - dsa -c "dxserver start all"
    $IGW_LOC/S99igateway start

    La configurazione dell'archivio dati applicazioni viene salvata.

Failover del server CA EEM

Nota: assicurarsi di installare la stessa versione del server CA EEM su tutti i server nella configurazione di failover (Server1, Server2, ... e ServerN) e sincronizzarne l'orologio di sistema.

È possibile configurare il Server1 per considerare attendibili le sessioni e i certificati provenienti da tutti gli altri server nella configurazione di failover. Ripetere la seguente procedura per tutti i server impostati nella configurazione di failover.

Per configurare Server1 per il failover:

1. Immettere l'URL https://server1:5250/spin.
2. Selezionare iTech Administrator, quindi fare clic su Vai a.

   Viene visualizzata la schermata di accesso.
3. Immettere le credenziali di accesso nel modo seguente in base alla selezione dell'opzione Tipo nella schermata di accesso:

   Host

   Accedere come utente principale o amministratore.
4. Fare clic sulla scheda Configura, aggiungere ServerN come nome host al riquadro Host iAuthority attendibili e fare clic su Considera attendibile.

   Nel file iControl.conf viene aggiunta una voce e Server1 inizia a considerare attendibili le sessioni di ServerN.

   Nota: aggiungere tutti gli altri server nella configurazione di failover al riquadro Host iAuthority attendibili.
5. Fare clic sulla scheda iAuthority, immettere Etichetta come ServerN, accedere al percorso del file del certificato PEM nel riquadro Aggiungi root attendibile, quindi fare clic su Aggiungi root attendibile.

   Nota: il file del certificato PEM (rootcert.pem) si trova nella directory iTechnology di ServerN.

   Nel file iAuthority.conf viene aggiunta una voce e Server1 inizia a considerare attendibili i certificati di ServerN.

   Nota: aggiungere i certificati in tutti gli altri server nella configurazione di failover.

Configurazione dei file di CA EEM

È necessario configurare CA EEM Server1 per la ricezione dell'elenco dei server disponibili a cui fare riferimento, i quali rappresentano versioni replicate.

Per configurare CA EEM Server1

1. Aprire la directory iTechnology di Server1.
   - **Windows**: %IGW_LOC%
   - **Linux e UNIX**: /opt/CA/SharedComponents/iTechnology (posizione predefinita)
2. Aprire il file iPoz.conf e aggiungere il seguente tag:

   <BackboneMember>Server2</BackboneMember>
3. Arrestare e avviare iGateway.

   Windows

   net stop igateway
   net start igateway

   Linux e UNIX

   /opt/CA/SharedComponents/iTechnology/S99igateway stop
   /opt/CA/SharedComponents/iTechnology/S99igateway start

È inoltre necessario configurare CA EEM Server2 per la ricezione dell'elenco dei server disponibili a cui fare riferimento, i quali rappresentano versioni replicate.

Per configurare CA EEM Server2

1. Aprire la directory iTechnology di Server2.
   - **Windows**: %IGW_LOC%
   - **Linux e UNIX**: /opt/CA/SharedComponents/iTechnology (posizione predefinita)
2. Aprire il file iPoz.conf e aggiungere il seguente tag:

   ```
   <BackboneMember>Server1</BackboneMember>
   ```

3. Arrestare e avviare iGateway.

   Windows

   ```
   net stop igateway
   net start igateway
   ```

   Linux e UNIX

   ```
   /opt/CA/SharedComponents/iTechnology/S99igateway stop
   /opt/CA/SharedComponents/iTechnology/S99igateway start
   ```

Nota: ripetere la procedura precedente per tutti i server CA EEM impostati nella configurazione di failover.

Capitolo 9: Federazione elemento

Abilitazione della federazione elemento

Se si desidera utilizzare la federazione degli elementi, eseguire la procedura seguente su tutti i server CA EEM presenti nella configurazione di failover.

Abilitazione della federazione elemento

1. Arrestare il servizio iGateway.
2. Individuare e aprire il file iPoz.conf.
3. Modificare il seguente tag:

   <ArtifactManager SessionTimeout="10"
   RequestTimeout="30"ArtifactStore="local/federated"></ArtifactManager>

   Dove

   SessionTimeOut

   Indica il tempo in minuti per la scadenza di una sessione esportata.

   Impostazione predefinita: 10 minuti

   Intervallo:

   RequestTimeOut

   Indica il tempo in minuti per la scadenza di una richiesta di avvio.

   Impostazione predefinita: 30 minuti

   Intervallo:

   Store

   Indica la posizione di archiviazione degli elementi. Se viene specificato un valore locale, gli elementi di un server CA EEM non saranno disponibili su altri server CA EEM nella configurazione di failover. Affinché gli elementi siano disponibili su tutti i server, sarà necessario impostare il valore di questo parametro su Federato.

   Valore: [locale|federato]

   Impostazione predefinita: locale

   Nota: i parametri SessionTimeout e RequestTimeOut sono presenti anche nel file eiam.conf. Se si specificano tali parametri nel file eiam.conf, i valori provenienti da questo file avranno la precedenza.
4. Salvare e chiudere il file.
5. Riavviare i servizi iGateway.

   La federazione degli elementi verrà abilitata.

Capitolo 10: Integrazione con CA SiteMinder

Questa sezione contiene i seguenti argomenti:

Come integrare CA SiteMinder con CA EEM

Per integrare CA SiteMinder con CA EEM, eseguire quanto descritto di seguito in CA SiteMinder Administrator:

- Creare un agente in CA SiteMinder per la comunicazione fra CA EEM e il server dei criteri CA SiteMinder. Assicurarsi che l'agente supporti gli agenti 4.x.
- Creare un amministratore o utilizzare l'amministratore predefinito esistente "SiteMinder" con ambito a livello di sistema.
- Creare una directory utente CA SiteMinder per l'autorizzazione, che viene usata da CA EEM per recuperare gli attributi LDAP.
- Impostare il campo UniversalID per l'identificazione univoca di un utente nella directory, per esempio sAMAccountName o UID. È possibile impostare UniversalID dalla UI, dalle Directory utente, dalle Proprietà e dalla scheda Attributi utente di SiteMinder.
- Impostare su userPassword l'Attributo password (RW) nella scheda Attributo utente.
- Creare un archivio dati CA SiteMinder per l'autenticazione, che viene usato da CA EEM per autenticare gli utenti.

  Nota: se l'archivio utente di autenticazione e l'archivio utente di autorizzazione corrispondono, utilizzare l'archivio utente esistente per l'autorizzazione.
- Creare un'area di autenticazione con il filtro della risorsa "/iamt.html".
- Creare un dominio CA SiteMinder e aggiungervi le directory utente, l'amministratore e l'area di autenticazione.

Per ulteriori informazioni, consultare la documentazione di CA SiteMinder.

Configurazione della registrazione lato server di CA EEM per moduli CA SiteMinder

Per configurare il livello di log per l'integrazione CA SiteMinder:

1. Creare un file con i seguenti contenuti e salvarlo con nome sm_log.properties:

   ```
   #filename: sm_log.properties
   #set the default logging level for the root logger
   .level = INFO
   #set the default logging level for the logger name com.ca.eiam
   com.ca.eiam.level = ALL
   ```

2. Modificare il livello del log per il registratore com.ca.eiam nel file sm.properties a uno dei seguenti valori:

   SEVERE

   Specifica un livello per i messaggi che indicano un errori gravi.

   WARNING

   Specifica un livello per indicare gli avvisi.

   INFO

   Specifica un livello per i messaggi informativi.

   CONFIG

   Specifica un livello per i messaggi di configurazione statica.

   FINE

   Specifica un livello per le tracciare le informazioni.

   ALL

   Specifica che tutti i livelli dei messaggi vengono registrati.

3. Salvare il file nel percorso seguente:

   Windows

   %IGW_LOC%

   Linux e UNIX

   /opt/CA/SharedComponents/iTechnology

4. Arrestare il servizio iGateway.

5. Aprire il file iGateway.conf dal percorso specificato nel passaggio 3 e aggiungere i seguenti tag nel tag <JVMSettings></JVMSettings>:

   ```
   <Properties name="eiam.sm">
   <system-properties>java.util.logging.config.file=sm_log.properties</system-properties>
   </Properties>
   ```

6. Salvare e chiudere il file.

7. Avviare il servizio iGateway.

Capitolo 11: Registrazione di CA EEM SDK

Per quanto riguarda gli SDK Java e C ++, il nuovo processo di registrazione in CA EEM utilizza come framework registratore rispettivamente log4j e log4cxx. Il processo di registrazione precedente utilizzava un registratore dell'utilità safe::util. Questa nuova funzione offre i seguenti vantaggi:

- Se si aggiornano o si modificano i livelli di registro, non sarà necessario riavviare l'applicazione.
- È possibile gestire le proprietà di registrazione, come ad esempio nomi e dimensioni dei file, numero di file di registro di backup e così via, modificando i parametri nel file di configurazione del registratore.
- È possibile classificare i messaggi del registro di CA EEM SDK in chiamate di rete e statistiche delle prestazioni.

Nota: la registrazione di SDK C# di CA EEM non è aggiornata. Occorre continuare ad utilizzare safe::util per registrare i messaggi nell'SDK C# di CA EEM.

La registrazione consente di registrare messaggi, errori e informazioni generate da CA EEM SDK. Nell'CA EEM SDK, la registrazione viene controllata dai seguenti file:

- eiam.log4cxx.config
- eiam.log4j.config

Questi due file sono parte del pacchetto CA EEM SDK e, per impostazione predefinita, vengono inseriti nella cartella Bin, come riportato di seguito.

UNIX

/opt/CA/eIAMSDK/bin

Windows

C:\Programmi\CA\Embedded IAM SDK\safetool

Informazioni sui file di configurazione del registratore

I file di configurazione del registratore, eiam.log4cxx.config ed eiam.log4j.config, vengono utilizzati per configurare la registrazione di CA EEM SDK. Essi contengono i seguenti componenti principali:

- Appender
- Registratore
- Registratore root

Questi componenti includono parametri configurabili che consentono di personalizzare il processo di registrazione in base ai propri requisiti aziendali.

Appender

Un appender include parametri che controllano la registrazione di ogni registratore. Per impostazione predefinita, i file di configurazione del registratore includono gli appender seguenti:

SDK

Consente di registrare i messaggi SDK in un file di registro. Specifica il percorso che include il nome del file di registro.

Impostazione predefinita: eiam.cppsdk.log

Nota: se si sta distribuendo l'applicazione server Tomcat su Windows, assicurarsi di utilizzare nel percorso la barra '/' anziché la barra '\'. Se si utilizza quest'ultima, il file di registro non viene creato nel percorso specificato ma nella cartella Apache Tomcat.

Rete

Consente di registrare i messaggi relativi alla chiamata di rete in un file di registro.

Impostazione predefinita:eiam.network.cpp.log

Prestazioni

Consente di registrare i messaggi relativi alla chiamata di rete in un file di registro.

Impostazione predefinita:eiam.network.cpp.log

Console

I messaggi di registro vengono visualizzati sulla console.

Per impostazione predefinita, l'appender SDK è disabilitato. Per abilitare gli altri appender, rimuovere le stringhe di commento (<!-- and -->) dal rispettivo codice.

Un appender è costituito dai seguenti parametri configurabili:

file

Specifica il nome file di registro dell'appender.

append

Specifica se viene aggiunto al file di registro un set di messaggi di registro. Se il valore è true, questo set viene aggiunto all'ultimo messaggio di registro nel file di registro.

BufferedIO

Specifica se è stato eseguito il buffer sul messaggio di registro più recente. Se il valore è true, i pochi messaggi di registro più recenti vengono conservati in memoria prima che vengano scritti sul file di registro. Ciò riduce al minimo l'operazione IO e risulta vantaggioso se il livello di registro è più elevato.

Valore: [*true*|*false*]

Valore predefinito*:* false

Nota: il valore predefinito per BufferedIO è 8.

MaxFileSize

Specifica la dimensione massima del file di registro. Se un file di registro supera le dimensioni massime, viene creato un nuovo nome del file di registro, log.1, nel quale vengono trasferiti i contenuti del file di registro. Adesso il file di registro contiene i messaggi di registro più recenti. Se questo file supera le dimensioni massime, viene creato un nuovo nome del file di registro, log.2. I contenuti di log.1 verranno trasferiti al file log.2 e quelli del file di registro al file log.1.

Predefinito: 10 MB

Dimensione minima: 10KB

Dimensione massima: 2GB

Nota: la dimensione minima del maxFileSize deve essere superiore o uguale alla dimensione di BufferedIO.

maxBackupIndex

Specifica il numero massimo dei file di registro di backup utilizzati per mantenere i registri datati. Se il numero di file di registro supera il valore massimo di indice di backup, il file contenente i messaggi di registro più datati viene eliminato.

Impostazione predefinita: 1

Minimo: 1

Massimo: 12

ConversionPattern

Specifica la formattazione di un messaggio di registro. Per definire il modello di conversione, configurare il modificatore di formato e i caratteri di conversione.

Nota: per ulteriori informazioni sui modelli di conversione, fare riferimento all'argomento log4j in www.apache.org.

Esempio: appender SDK

```
<appender name="SDK" class="org.apache.log4j.RollingFileAppender">
    <!-- File di registro sdk attivo -->
    <param name="file" value="eiam.cppsdk.log" />
    <param name="append" value="true" />
    <param name="BufferedIO" value="false"/>
    <param name="maxFileSize" value="10000KB" />
    <param name="maxBackupIndex" value="1" />
    <layout class="org.apache.log4j.PatternLayout">
    <!-- Modello file di registro -->
    <param name="ConversionPattern" value="%5p %d{ISO8601} [%t] [%c] %m%n"/>
    </layout>
</appender>
```

Appender in eiam.log4net.config

un appender contiene parametri che controllano la registrazione di ciascun registratore. Per impostazione predefinita, i file di configurazione del registratore contengono i seguenti appender:

SDK

Registra i messaggi dell'SDK in un file di log Specifica il percorso includendo il nome file del file di log

Impostazione predefinita: EIAM.C#SDK.log

Nota: se si distribuisce l'applicazione in un server Tomcat in Windows, assicurarsi di utilizzare la barra '/' nel percorso invece della barra rovesciata '\'. Se si utilizza la barra rovesciata, il file di registro non viene creato nel percorso specificato ma nella cartella Apache Tomcat.

Rete

Registra i messaggi relativi alle chiamate di rete in un file di log.

Impostazione predefinita:EIAM.NETWORK.C#SDK.log

Prestazioni

Registra i messaggi relativi alle chiamate inerenti alle prestazioni in un file di log.

Impostazione predefinita: EIAM.PERFORMANCE.C#SDK.log

Console

Visualizza i messaggi di log sulla console.

L'appender dell'SDK è attivo per impostazione predefinita. Per attivare altri appender, rimuovere le stringhe di commento (<!-- e -->) dai rispettivi codici.

Un appender comprende i seguenti parametri configurabili:

file

Specifica il nome del file di log dell'appender.

appendToFile

Specifica se un insieme di messaggi di log deve essere aggiunto al file di log. Se il valore è true, il set di messaggi di log viene aggiunto all'ultimo messaggio nel file di log.

maxSizeRollBackups

Specifica il numero massimo di file di log di backup da utilizzare per mantenere i registri precedenti. Se il numero di file di log supera il valore di indice massimo di backup, il file viene eliminato con i messaggi di log meno recenti.

Impostazione predefinita: 1

Minimo: 1

Massimo: 12

rollingStyle

Specifica se l'ultimo messaggio di log viene memorizzato nel buffer. Se il valore è true, gli ultimi messaggi di log vengono archiviati nella memoria prima di essere scritti nel file di log. Ciò consente di minimizzare le operazioni di I/O e risulta utile se il livello di log è alto.

Value: [*true*|*false*]

Impostazione predefinita*:* false

Nota: la dimensione predefinita per BufferedIO è 8 KB.

maximumFileSize

Specifica la dimensione massima del file di log Se un file di log supera la dimensione massima, viene creato un nuovo file di log denominato log.1 e i contenuti del file di log vengono trasferiti nel file log.1. Il file di log contiene, quindi, gli ultimi messaggi di log. Se anche questo file supera la dimensione massima, viene creato un nuovo file di log denominato nomefile log.2 e i contenuti del file log.1 vengono trasferiti al file log.2, mentre quelli del file di log continuano ad essere trasferiti al file log.1.

Impostazione predefinita: 10 MB

Minimo: 10 KB

Massimo: 2 GB

Nota: la dimensione minima del parametro maxFileSize deve essere maggiore o uguale alla dimensione del parametro rollingStyle.

ConversionPattern

Specifica la formattazione di un messaggio di log Configurare i modificatori di formato e i caratteri di conversione per definire il modello di conversione.

Nota: per ulteriori informazioni sui modelli di conversione, consultare l'a sezione log4net in www.apache.org.

Registratore

I registratori consentono di controllare la modalità in cui i messaggi di registro della rete e delle prestazioni vengono classificati in base a livelli e se vengono visualizzati in fase di esecuzione. Per impostazione predefinita, i registratori Rete e Prestazione sono disabilitati. Per abilitare un registratore, rimuovere le stringhe di commento dal rispettivo codice.

Un registratore contiene i seguenti parametri:

nome registratore

Indica il nome del registratore.

additivity

Specifica se i messaggi di registro della rete o delle prestazioni vengono duplicati nel file di registro SDK.

Valore: [*true*|*false*]

Valore predefinito: false

level value

Specifica il livello di registro di un registratore.

Valore:
[*Traccia*|*Debug*|*Informazioni*|*Warn*|*Errore*|*Irreversibile*|*Disattivata*]

Di seguito vengono riportati in ordine di priorità i livelli di registro:

Nota: più il livello di registro è alto, minori saranno le prestazioni di CA EEM.

Traccia

Indica il debug di livello basso. Esso include il flusso di controllo e passa gli argomenti.

Debug

Indica i messaggi utilizzati per diagnosticare il problema. Contiene informazioni contestuali.

Informazioni

Indica le informazioni contestuali che in un ambiente di produzione tengono traccia dell'esecuzione ad un livello coarse-grained.

Warn

Indica l'eventuale presenza di un problema nel sistema. Per esempio, se il messaggio fa parte della categoria protezione, un messaggio di avviso deve segnalare se sono stati rilevati attacchi al dizionario.

Errore

Indica la presenza di un problema grave nel sistema. Non è possibile eseguire un ripristino e si richiede l'intervento manuale.

Irreversibile

Indica un'eccezione irreversibile dell'applicazione.

Disattivata

Indica l'assenza di registrazione.

Nota: il livello di registro dell'appender SDK predefinito deve essere Errore.

Esempio: registratore delle prestazioni

```
<logger name="Perform" additivity="false">
    <level value="trace"/>
    <appender-ref ref="Performance" />
</logger>
```

Registratore root

Il registratore root controlla il livello di registro di tutti gli appender. Tuttavia, se il livello di registro dell'appender di riferimento nel registratore root risulta diverso da quello specificato nell'appender principale, il livello di registro con priorità più alta sostituirà quello con priorità più bassa.

Per esempio, se il livello di registro di un registratore root è Errore e quello dell'appender Rete è Traccia, quest'ultimo sostituirà il livello Errore ed il sistema considererà, in fase di esecuzione, i messaggi di registro con livello Traccia.

Esempio: registratore root

```
<root>
    <priority value="error" />
    <appender-ref ref="SDK" />
    <appender-ref ref="Console" />
</root>
```

Configurazione dei file del registratore

CA EEM consente di configurare i messaggi di registro correlati alla rete, alle prestazioni, alla console e alle classi SDK.

Per configurare i file del registratore

1. Aprire il file di configurazione del registratore, eiam.log4cxx.config o eiam.log4j.config, in un editor di testo.
2. Abilitare i registratori e gli appender.
3. Aggiornare i parametri dell'appender.
4. Salvare il file di configurazione del registratore.

Esempio di file eiam.log4cxx.config

Di seguito viene riportato un esempio del file eiam.log4cxx.config:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE log4j:configuration SYSTEM "log4j.dtd">
<!-- Il file viene letto dall'sdk ogni 60 secondi -->

<log4j:configuration xmlns:log4j="http://jakarta.apache.org/log4j/">

    <appender name="SDK" class="org.apache.log4j.RollingFileAppender">
        <!-- File di registro sdk attivo -->
        <param name="file" value="eiam.cppsdk.log" />
        <param name="append" value="true" />
        <param name="BufferedIO" value="false"/>
        <param name="maxFileSize" value="10000KB" />
        <param name="maxBackupIndex" value="1" />
        <layout class="org.apache.log4j.PatternLayout">
        <!-- Modello file di registro -->
        <param name="ConversionPattern" value="%5p %d{ISO8601} [%t] [%c] %m%n"/>
        </layout>
    </appender>

    <appender name="Network" class="org.apache.log4j.RollingFileAppender">
        <!-- File per registrare chiamate di rete -->
        <param name="file" value="eiam.network.cpp.log" />
        <param name="append" value="true" />
        <param name="BufferedIO" value="true"/>
        <param name="maxFileSize" value="10000KB" />
        <param name="maxBackupIndex" value="1" />
        <layout class="org.apache.log4j.PatternLayout">
        <!-- Modello file di registro -->
        <param name="ConversionPattern" value="%5p %d{ISO8601} [%t] [%c] %m%n"/>
        </layout>
    </appender>

    <appender name="Performance" class="org.apache.log4j.RollingFileAppender">
        <!-- File per registrare chiamate delle prestazioni -->
        <param name="file" value="eiam.performance.cpp.log" />
        <param name="append" value="true" />
        <param name="BufferedIO" value="true"/>
        <param name="maxFileSize" value="10000KB" />
        <param name="maxBackupIndex" value="1" />
        <layout class="org.apache.log4j.PatternLayout">
        <!-- Modello file di registro -->
        <param name="ConversionPattern" value="%5p %d{ISO8601} [%t] [%c] %m%n"/>
        </layout>
    </appender>

    <appender name="Console" class="org.apache.log4j.ConsoleAppender">
        <!-- Registri su console -->
        <layout class="org.apache.log4j.PatternLayout">
```

```
            <!-- Modello file di registro -->
            <param name="ConversionPattern" value="%5p %d{ISO8601} [%t] [%c] %m%n"/>
            </layout>
        </appender>

        <!-- Rimuovere commento per l'abilitazione della registrazione delle prestazioni -->
        <!--
        <logger name="Perform" additivity="false">
            <level value="trace"/>
            <appender-ref ref="Performance" />
        </logger>
        -->

        <!-- Rimuovere commento per l'abilitazione della registrazione di rete -->
        <!--
        <logger name="Network" additivity="false">
            <level value="trace"/>
            <appender-ref ref="Performance" />
        </logger>
        -->

        <root>
            <priority value="error" />
            <appender-ref ref="SDK" />
            <!-- <appender-ref ref="Console" /> -->
        </root>
</log4j:configuration>
```

Esempio di file eiam.log4net.config

Di seguito viene riportato un esempio di file eiam.log4net.config:

```
<?xml version="1.0" encoding="utf-8" ?>

<log4net>
	<appender name="SDK" type="log4net.Appender.RollingFileAppender">
		<file value="EIAM.C#SDK.log" />
		<appendToFile value="true" />
		<maxSizeRollBackups value="1" />
		<maximumFileSize value="10000KB" />
		<rollingStyle value="Size" />
		<layout type="log4net.Layout.PatternLayout">
			<conversionPattern value="%date [%thread] %-5level %logger -
%message%newline" />
		</layout>
	</appender>

	<appender name="Network" type="log4net.Appender.RollingFileAppender">
		<file value="EIAM.NETWORK.C#SDK.log" />
		<appendToFile value="true" />
		<maxSizeRollBackups value="1" />
		<maximumFileSize value="10000KB" />
		<rollingStyle value="Size" />
		<layout type="log4net.Layout.PatternLayout">
			<conversionPattern value="%date [%thread] %-5level %logger -
%message%newline" />
		</layout>
	</appender>

	<appender name="Performance" type="log4net.Appender.RollingFileAppender">
		<file value="EIAM.PERFORMANCE.C#SDK.log" />
		<appendToFile value="true" />
		<maxSizeRollBackups value="1" />
		<maximumFileSize value="10000KB" />
		<rollingStyle value="Size" />
		<layout type="log4net.Layout.PatternLayout">
			<conversionPattern value="%date [%thread] %-5level %logger -
%message%newline" />
		</layout>
	</appender>

	<appender name="ConsoleAppender" type="log4net.Appender.ConsoleAppender">
		<layout type="log4net.Layout.PatternLayout">
			<conversionPattern value="%date [%thread] %-5level %logger -
%message%newline" />
		</layout>
	</appender>
```

```
        <!-- Uncomment to enable Performance Logging -->
        <!--
        <logger name="Perform" additivity="false">
                <level value="ERROR"/>
                <appender-ref ref="Performance" />
        </logger>-->

        <!-- Uncomment to enable Network Logging -->
        <!--<logger name="Network" additivity="false">
                <level value="ERROR"/>
                <appender-ref ref="Network" />
        </logger>-->

        <root>
                <level value="ERROR" />
                <appender-ref ref="SDK" />
                <!--        <appender-ref ref="ConsoleAppender" />      -->
        </root>
</log4net>
```

Esempio di file eiam.lo4j.config

Di seguito viene riportato un esempio di file eiam.log4cxx.config:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE log4j:configuration SYSTEM "log4j.dtd">

<!-- Note that this file is read by the sdk every 60 seconds -->

<log4j:configuration xmlns:log4j="http://jakarta.apache.org/log4j/">

        <appender name="SDK" class="com.ca.eiam.log4j.RollingFileAppender">
                <!-- The active sdk log file -->
                <param name="file" value="eiam.javasdk.log" />
                <param name="append" value="true" />
                <param name="BufferedIO" value="false"/>
                <param name="maxFileSize" value="10000KB" />
                <param name="maxBackupIndex" value="1" />
                <layout class="com.ca.eiam.log4j.PatternLayout">
                        <!-- The log message pattern -->
                        <param name="ConversionPattern" value="%5p %d{ISO8601} [%t] [%c]
%m%n"/>
                </layout>
        </appender>

        <appender name="Network" class="com.ca.eiam.log4j.RollingFileAppender">
                <!-- The file to log Network calls -->
                <param name="file" value="eiam.network.java.log" />
                <param name="append" value="true" />
                <param name="BufferedIO" value="false"/>
                <param name="maxFileSize" value="10000KB" />
                <param name="maxBackupIndex" value="1" />
                <layout class="com.ca.eiam.log4j.PatternLayout">
                        <!-- The log message pattern -->
                        <param name="ConversionPattern" value="%5p %d{ISO8601} [%t] [%c]
%m%n"/>
                </layout>
        </appender>

        <appender name="Performance" class="com.ca.eiam.log4j.RollingFileAppender">
                <!-- The file to log Performance calls -->
                <param name="file" value="eiam.performance.java.log" />
                <param name="append" value="true" />
                <param name="BufferedIO" value="false"/>
                <param name="maxFileSize" value="10000KB" />
                <param name="maxBackupIndex" value="1" />
                <layout class="com.ca.eiam.log4j.PatternLayout">
                        <!-- The log message pattern -->
                        <param name="ConversionPattern" value="%5p %d{ISO8601} [%t] [%c]
%m%n"/>
```

```
                </layout>
        </appender>

        <appender name="Console" class="com.ca.eiam.log4j.ConsoleAppender">
                <!-- Logs to Console -->
                <layout class="com.ca.eiam.log4j.PatternLayout">
                        <!-- The log message pattern -->
                        <param name="ConversionPattern" value="%5p %d{ISO8601} [%t] [%c]
%m%n"/>
                </layout>
        </appender>

        <!-- Uncomment to enable Performance Logging -->
        <!--
        <logger name="Perform" additivity="false">
                <level value="trace"/>
                <appender-ref ref="Performance" />
        </logger>
        -->

        <!-- Uncomment to enable Network Logging -->
        <!--
        <logger name="Network" additivity="false">
                <level value="trace"/>
                <appender-ref ref="Network" />
        </logger>
        -->

        <root>
                <priority value="error" />
                <appender-ref ref="SDK" />
                <!-- <appender-ref ref="Console" /> -->
        </root>

</log4j:configuration>
```

Capitolo 12: Configurazione per il supporto del server di directory esterne

Questa sezione contiene i seguenti argomenti:

Configurazione di una directory esterna con CA EEM

Se si utilizzano vari archivi di directory esterne per l'autenticazione e l'autorizzazione, configurare CA EEM come segue:

- Utilizzare il file iPoz.conf per configurare la directory di autenticazione esterna con CA EEM
- Utilizzare la GUI dell'amministratore di CA EEM per configurare il server CA EEM con la directory di autorizzazione esterna.

  Nota: per ulteriori informazioni sulle modalità di configurazione dei riferimenti alle directory esterne, consultare la Guida in linea.

Per configurare il server CA EEM per l'utilizzo di directory di autenticazione esterne, configurare le seguenti opzioni nel file iPoz.conf reperibile nella cartella /CA/SharedComponents/iTechnology dopo l'installazione.

Nota: interrompere iGateway prima di modificare il file iPoz.conf e riavviarlo in seguito.

UseExternalAuthDirectory

Specifica se si desidera utilizzare una directory esterna diversa per l'autenticazione. Digitare True per utilizzare una directory esterna diversa. Il valore predefinito è False.

ExternalAuthDirType:

Specifica il tipo di directory esterna. I tipi attualmente supportati comprendono CA Identity Manager, Custom Mapped Directory, Microsoft Active Directory, Novell eDirectory, Novell eDirectory-CN e Sun One Directory.

ExternalAuthDirUserDn

Specifica il userdn per il tipo di directory esterna specificato.

ExternalAuthDirPassword

Specifica la password utente nel formato crittografato.

Nota: è necessario crittografare la password utilizzando il comando riportato di seguito e incollarla nel file ipoz.conf.

/iTechnology/safex -munge <*password in testo non crittografato*>

ExternalAuthDirHost

Specifica il nome dell'host in cui è stata configurata la directory esterna.

ExternalAuthDirPort

Specifica la porta in cui la directory esterna sarà in ascolto.

ExternalAuthDirUserSearchPreFilter

Specifica il filtro di ricerca preliminare in base alla directory esterna. È possibile ricercare qualsiasi classe oggetto, ad esempio gli utenti.

ExternalAuthDirUserSearchPreFilter

Specifica il filtro di post-ricerca in base alla directory esterna. È possibile ricercare qualsiasi classe oggetto, ad esempio gli utenti.

ExternalDirCacheFolder

Specifica se il server CA EEM deve memorizzare nella cache cartelle della directory esterna. Se questo tag è impostato su True, il server CA EEM memorizza nella cache le cartelle esterne, per cui sarà possibile accedere a tali cartelle utilizzando la GUI dell'amministratore di CA EEM. Se questo tag è impostato su False, CA EEM non visualizza le cartelle della directory esterna nella GUI dell'amministratore di CA EEM.

Value: [True|False]

Valore predefinito: **True**

Configurazione del server CA EEM per aggirare le barre rovesciate in DN restituiti da directory esterne

Per configurare il server CA EEM per l'utilizzo di directory di autenticazione esterne, configurare la seguente opzione nel file iPoz.conf reperibile nella cartella /CA/SharedComponents/iTechnology dopo l'installazione.

Nota: interrompere iGateway prima di modificare il file iPoz.conf e riavviarlo in seguito.

ExternalDirEscapeSlash

Specifica se CA EEM deve aggirare la barra '/' nel DN restituito da direcotry esterne. Impostare questo tag su True se si desidera aggirare la barra.

Nota: è necessario configurare CA EEM per ignorare la barra nei DN, altrimenti potrebbe non essere possibile recuperare gli oggetti in modo corretto.

Value: [True|False]

Impostazione predefinita: **falso**

Configurazione per il supporto del failover per una directory esterna

È possibile estendere le funzionalità di CA EEM affinché faccia riferimento a un altro server di directory esterne, che rappresenta una versione replicata del server.

A questo scopo, è sufficiente fornire il mapping nel file iPoz.conf.

Nota: prima di apportare qualsiasi modifica al file iPoz.conf, è necessario arrestare iGateway, quindi riavviarlo dopo aver eseguito l'operazione.

ExternalDirHostBackup

Specifica il nome host del server di directory esterne replicato.

ExternalAuthDirHostBackup

Specifica il nome host del server di directory esterne alternativo da utilizzare per l'autenticazione utente.

Connessione ai server LDAP mediante TLS

Per stabilire una connessione TLS al server LDAP, è necessario configurare il server LDAP per accettare certificati anonimi. Per configurare EEM per la connessione LDAP mediante TLS, eseguire le seguenti operazioni:

Per configurare CA EEM per la connessione a LDAP mediante TLS:

1. Accedere alla GUI di CA EEM.
2. Fare clic su Configura, Server EEM.
3. Fare clic su Utenti globali/Gruppi globali.

   Viene visualizzato il pannello di configurazione del server EEM.
4. Selezionare l'opzione Riferimento da una directory esterna.
5. Immettere i dettagli di configurazione.

   Nota: per ulteriori informazioni sull'utilizzo dei dettagli di configurazione, consultare la Guida in linea.
6. (Facoltativo) Selezionare l'opzione Usa TLS (Transport Layer Security).
7. Fare clic su Salva.

Connessione ai server LDAP mediante SSL

Per stabilire una connessione SSL ai server LDAP, è necessario disporre dei seguenti certificati:

Certificato da autorità di certificazione

È possibile ottenere tale certificato da un'autorità di certificazione, ad esempio Verisign o Thwate. I certificati emessi dall'autorità di certificazione sono considerati validi e attendibili.

Certificato del server LDAP

È necessario ottenere tale certificato da un'autorità di certificazione attendibile. Tale certificato contiene informazioni sul server LDAP e identifica il server LDAP con il client.

Nota: CA EEM supporta unicamente certificati .pem per connessioni SSL.

Modalità di connessione di CA EEM al server LDAP mediante SSL

Di seguito vengono descritte le modalità di comunicazione del server CA EEM e del server LDAP mediante una connessione SSL.

1. Server CA EEM viene connesso al server LDAP mediante un certificato emesso da un'autorità di certificazione.
2. Il server LDAP verifica il certificato emesso dall'autorità di certificazione e, se il certificato risulta valido, viene stabilito un handshake con server CA EEM.
3. Durante l'handshake, la chiave pubblica del server LDAP viene inviata a server CA EEM. La chiave pubblica viene utilizzata per crittografare dati inviati al server LDAP.
4. Server CA EEM utilizza la chiave pubblica per crittografare i dati e inviarli al server LDAP.
5. Server CA EEM invia il nome utente e la password per l'autenticazione in base al server LDAP.

Modalità di configurazione delle connessioni SSL

Per configurare la comunicazione SSL tra il server LDAP e server CA EEM, è necessario attenersi alla seguente procedura:

1. Configurare il server LDAP per l'utilizzo dei certificati.
2. Configurare il del server CA EEM per la comunicazione mediante connessione SSL.

Configurazione del server LDAP per l'utilizzo dei certificati SSL.

Per configurare il server LDAP per l'utilizzo della connessione SSL, è necessario attenersi alla seguente procedura:

1. Ottenere un certificato dall'autorità di certificazione, quindi installarlo nell'archivio dei certificati attendibili sul server LDAP.
2. Ottenere un certificato del server dall'autorità di certificazione, quindi installarlo nell'archivio dei certificati del server sul server LDAP.
3. Attivare il server LDAP per l'accettazione delle connessioni SSL.

Attivazione della connessione SSL in server CA EEM

Per attivare la connessione SSL nel server

1. Copiare il certificato dell'autorità di certificazione dal server LDAP, quindi salvarlo nel computer su cui viene eseguito server CA EEM.
2. Aprire il file ipoz.conf e modificare i seguenti tag:

   <ExternalDirSSL>

   Specifica se la comunicazione SSL è attivata o disattivata. Per attivare la comunicazione SSL, è necessario impostare tale tag su "true".

   <ExternalDirCACertPath>

   Specifica il percorso di archiviazione del certificato emesso dall'autorità di certificazione sul computer in cui viene eseguito server CA EEM.
3. Riavviare igateway.

Capitolo 13: Configurazione del supporto per un numero elevato di criteri

Questa sezione contiene i seguenti argomenti:

Supporto di un elevato numero di criteri

Nota: CA EEM fornisce supporto per un elevato numero di criteri esclusivamente in ambienti client con C++ SDK attivato.

È necessario configurare il del server CA EEM e i client prima di registrare le applicazioni che utilizzano un elevato numero di criteri.

Nota: CA EEM supporta fino 20.000 criteri sulla piattaforma HP-UX.

Configurazione di ulteriori impostazioni del server CA EEM su AIX

È necessario attenersi alle seguenti procedure aggiuntive per configurare il del server CA EEM affinché supporti un elevato numero di criteri su AIX.

Per configurare il del server CA EEM su AIX

1. Modificare le impostazioni di rete mediante il seguente comando al prompt dei comandi di AIX:

   ```
   no -o tcp_nodelayack=1
   ```

2. Aumentare il limite di processi mediante il seguente comando al prompt dei comandi di AIX:

   ```
   ulimit -d unlimited
   ulimit -f unlimited
   ```

Configurazione del client

È necessario configurare il client affinché supporti un elevato numero di criteri.

Configurazione del client per tutti i sistemi operativi

Per supportare lo sviluppo di un elevato numero di criteri, è necessario configurare i client per tutti i sistemi operativi:

- Aumentare l'orario di aggiornamento cache delle applicazioni per evitare aggiornamenti della cache durante la registrazione delle applicazioni mediante Safex.

  Per ulteriori informazioni sull'aggiornamento della cache, consultare la *Guida alla programmazione.*

  Nota: si consiglia di impostare l'orario di aggiornamento cache su 3600 secondi durante la registrazione per evitare aggiornamenti della cache. Una volta completata la registrazione, modificare l'orario di aggiornamento cache in 30 secondi, ovvero l'impostazione predefinita.

- Attivare Recapito eventi affidabile.

  Per ulteriori informazioni su Recapito eventi affidabile, consultare la *Guida alla programmazione*.

Capitolo 14: Archiviazione degli eventi

Questa sezione contiene i seguenti argomenti:

Panoramica

CA EEM consente di creare e gestire rapporti per gli eventi generati da server CA EEM. Il sistema di archiviazione organizza i file archiviati nei seguenti tre stati:

File di database warm

Si riferisce ai file di archivio creati dopo che il numero di eventi ha superato le righe massime in un database di eventi. I file archiviati con stato warm sono disponibili per l'esecuzione di query e la creazione di rapporti da server CA EEM. Non è possibile inserire dati in un file di database warm. Tali file sono disponibili in server CA EEM esclusivamente per il numero di giorni specificato in Numero massimo di giorni per l'archiviazione in Impostazioni del registro eventi.

File di database cold

Si riferisce ai file di archivio in stato warm sottoposti a backup manuale in un'altra posizione. Non è possibile eseguire query o creare rapporti da un file di database cold. È necessario sbloccare i file di database cold affinché sia possibile utilizzarli per l'esecuzione di query o la creazione di rapporti.

File di database defrosted

Si riferisce ai file di archivio in stato cold ripristinati affinché gli utenti siano in grado di eseguire query o creare rapporti da server CA EEM. Tali file sono disponibili nella directory di archivio esclusivamente per il numero di ore specificato come criterio di eventi in Impostazioni del registro eventi.

Per modificare Impostazioni del registro eventi

1. Accedere a CA EEM.

   Viene visualizzata la pagina iniziale di CA EEM.

2. Fare clic su Gestisci rapporti, Configurazione, Servizi, Impostazioni del registro eventi.

   Vengono visualizzate le impostazioni del registro eventi.

Nota: per ulteriori informazioni sulla configurazione dei servizi per la gestione dei rapporti, consultare la *Guida in linea*.

Utilità per lo sblocco dei file di database cold

CA EEM è dotato di un'utilità che consente di sbloccare i file di database cold. È necessario ripristinare e sbloccare i file dallo stato cold a quello warm affinché sia possibile eseguire query in base ai file e visualizzare rapporti immediati. L'utilità sem fornisce questa funzionalità. È possibile scaricare l'utilità sem dal supporto tecnico all'indirizzo http://ca.com/support.

Per impostare l'utilità sem

1. Estrarre i file compressi dell'utilità sem.
2. Impostare le variabili di ambiente in base al sistema operativo in uso:

   Linux o Solaris

   Export LD_LIBRARY_PATH = <*cartella_estrazione_sem*>:$LD_LIBRARY_PATH

   AIX

   Export LIBPATH = <*cartella_estrazione_sem*> :$LIBPATH

   HP-UX

   Export SHLIB_PATH= <*cartella_estrazione_sem*> :$SHLIB_PATH

Nota: per impostare l'utilità sem in Windows, dalla riga di comando è necessario individuare la cartella estratta ed eseguire sem.exe.

Sintassi dell'utilità SEM

La sintassi dell'utilità sem è la seguente:

sem -h <hostname> -u <user> -p <password> -listcolddb | -defrost <archive>

-h

Specifica il nome host del computer in cui vengono memorizzati i file cold db.

-u

Specifica il nome utente utilizzato per eseguire l'autenticazione con server CA EEM.

-p

Specifica la password associata a un nome utente utilizzata per eseguire l'autenticazione con server CA EEM.

-listcolddb

Elenca tutti i file di database cold memorizzati sul computer host.

-defrost <archive>

Consente di sbloccare il file di archivio specificato.

-fips

Specifica se l'utilità sem utilizza algoritmi compatibili con FIPS.

Nota: l'utilità sem deve essere utilizzata con l'opzione -fips se il server CA EEM è configurato in modalità Solo FIPS.

Nella seguente tabella vengono riportati i valori restituiti dell'utilità sem:

Valore restituito	Descrizione
0	Riuscito
1	Argomenti non validi
2	Nome utente non valido
3	Autenticazione non riuscita
4	Impossibile elencare i file di database cold
5	Impossibile sbloccare un file di database cold
6	Errore di inizializzazione

Sblocco di file di database cold

È necessario ripristinare e sbloccare i file dallo stato cold a quello warm affinché sia possibile eseguire query in base ai file e visualizzare rapporti immediati.

Nota: prima di eseguire lo sblocco, è necessario copiare i file di database cold nella directory di archivio iTechnology\calm_archive.

Per ripristinare e sbloccare i file di database cold

1. Copiare la cartella calm _ archive di cui è stato eseguito il backup nella cartella calm_archive corrente.
2. Eseguire l'utilità sem dalla riga di comando per recuperare un elenco di tutti i file di database cold.

   sem -h <*hostname*> -u <*username*> -p <*password*> -listcolddb

   Server CA EEM in modalità Solo FIPS

   sem -h <*hostname*> -u <*username*> -p <*password*> -fips -listcolddb
3. Eseguire l'utilità sem per sbloccare i file di database cold.

   sem -h <*hostname*> -u <*username*> -p <*password*> -defrost <*archive*>

   Server CA EEM in modalità Solo FIPS

   sem -h <*hostname*> -u <*username*> -p <*password*> -fips -defrost <*archive*>

   I file di database cold vengono ripristinati e sbloccati.