CA Identity Manager™

Configuration Guide

12.6.4

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.

Riferimenti ai prodotti CA Technologies

Questo documento fa riferimento ai seguenti prodotti CA:

- CA Identity Manager
- CA Siteminder®
- Directory CA
- CA User Activity Reporting
- CA Identity Governance

Sommario

Capitolo 4: Gestione del database relazionale 103

Capitolo 5: Directory di CA Identity Manager 155

Capitolo 1: Introduzione agli ambienti di CA Identity Manager

Questa sezione contiene i seguenti argomenti:

Componenti dell'ambiente di CA Identity Manager

Un *ambiente* di CA Identity Manager è una visualizzazione di uno spazio dei nomi di gestione che consente agli amministratori di CA Identity Manager di gestire oggetti quali utenti, gruppi e organizzazioni. Questi oggetti vengono assegnati con un set di ruoli e attività associati. L'ambiente di CA Identity Manager controlla la gestione e la presentazione grafica di una directory.

Un archivio utenti singolo può associare più ambienti di CA Identity Manager (a pagina 15) per definire visualizzazioni diverse della directory. Tuttavia, un ambiente di CA Identity Manager viene associato a un solo archivio utenti.

Gli ambienti di CA Identity Manager contengono gli elementi seguenti:

Directory

Descrive un archivio utenti a CA Identity Manager. L'elemento directory include:

- Un puntatore a un archivio utenti, che archivia oggetti gestiti, quali utenti, gruppi e organizzazioni.
- Metadati che descrivono come gli oggetti gestiti vengono archiviati nella directory e nella sua rappresentazione in CA Identity Manager.

Directory di provisioning (facoltativo)

Archivia i dati relativi al server di provisioning per la gestione di account aggiuntivi negli endpoint gestiti. È possibile associare una sola directory di provisioning a un ambiente.

Nota: per ulteriori informazioni sul server di provisioning o sulla directory di provisioning, consultare la *Guida all'installazione*.

Console utente

Consente agli amministratori di CA Identity Manager di eseguire attività in un ambiente di CA Identity Manager.

Definizioni di ruoli e attività

Consentono di determinare i privilegi dell'utente in CA Identity Manager e in altre applicazioni. Queste definizioni di attività e ruoli sono inizialmente disponibili nell'ambiente di CA Identity Manager in cui è possibile assegnarle agli utenti.

È possibile personalizzare i ruoli e le attività predefinite mediante la console utente.

Self-service

Consente agli utenti di creare e mantenere i propri account per accedere alle risorse, come ad esempio il sito Web di un cliente. L'opzione self-service consente inoltre agli utenti di richiedere una password temporanea nel caso si dimentichi la password corrente.

Definizioni del flusso di lavoro

CA Identity Manager include definizioni del flusso di lavoro predefinite che consentono di automatizzare l'approvazione e le notifiche relative alle attività di gestione degli utenti, come ad esempio la creazione di profili utente o l'assegnazione di utenti a ruoli o gruppi. È possibile modificare i processi del flusso di lavoro predefiniti in CA Identity Manager per supportare tutti i requisiti aziendali.

Interfacce

Consentono di determinare l'aspetto dell'interfaccia utente di CA Identity Manager.

Funzionalità personalizzate

È possibile modificare CA Identity Manager per soddisfare i requisiti aziendali mediante le API di CA Identity Manager. Per ulteriori informazioni, consultare la guida *Programming Guide for Java.*

Ciascun ambiente di CA Identity Manager richiede uno o più manager di sistema per personalizzare i ruoli e le attività iniziali mediante la console utente. Una volta che un manager di sistema ha creato i ruoli e le attività iniziali, tale manager potrà concedere privilegi amministrativi agli utenti in quell'ambiente. Questi utenti diventano amministratori che gestiscono utenti, gruppi e organizzazioni. Consultare la *Guida per l'amministratore*.

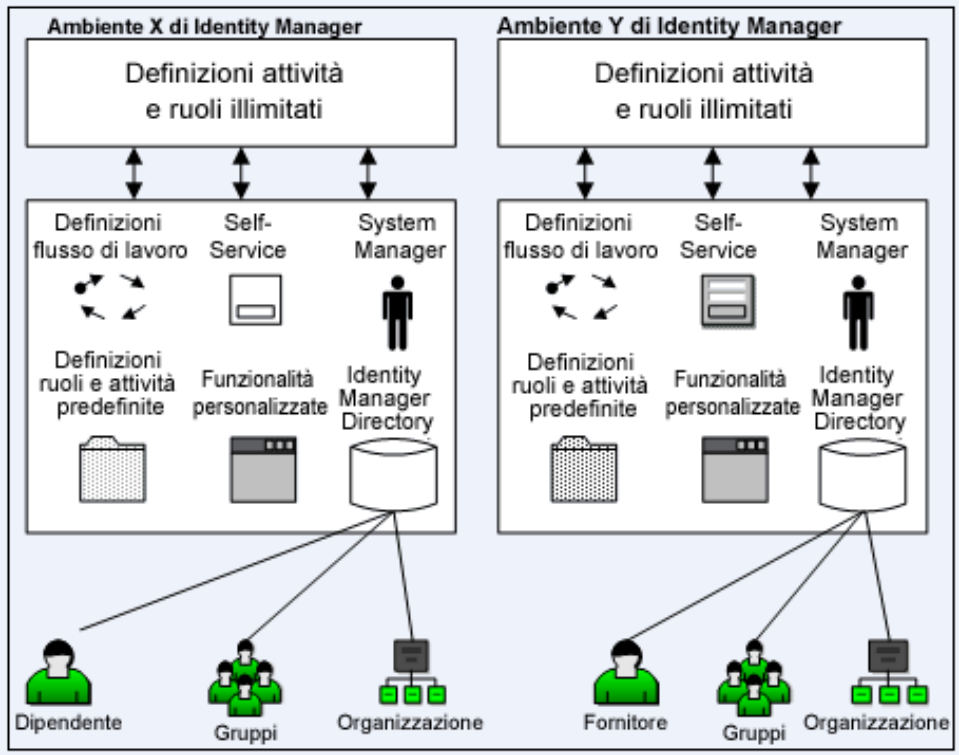
Più ambienti di CA Identity Manager

Creare più ambienti di CA Identity Manager quando si desidera:

Gestire archivi utenti aggiuntivi: è possibile gestire utenti in diversi tipi di archivi utenti. Ad esempio, l'azienda archivia tutti i profili utente in una directory LDAP di un sistema Sun Java. Si intraprende un'iniziativa commerciale congiunta con un partner che utilizza un database Oracle per archiviare le informazioni degli utenti. Si desidera un ambiente di CA Identity Manager diverso per ciascun set di utenti.

- Gestire oggetti con classi oggetto LDAP diverse: considerare che CA Identity Manager gestisca una directory LDAP. All'interno della stessa directory, è possibile gestire oggetti dello stesso tipo insieme a classi oggetto e attributi diversi. Ad esempio, l'illustrazione seguente mostra una directory che contiene due tipi di utenti:
  - Dipendenti, che hanno un numero ID di dipendente.
  - Fornitori, identificati da un numero di fornitore.

Equation 1: Diagramma che mostra un esempio di due ambienti di Identity Manager con directory contenenti dipendenti e fornitori.



Console di gestione di CA Identity Manager

Le responsabilità di un amministratore di sistema di CA Identity Manager includono:

- Creazione di una directory CA Identity Manager
- Configurazione di un directory di provisioning
- Configurazione di un ambiente di CA Identity Manager
- Assegnazione di un manager di sistema
- Abilitazione di funzionalità personalizzate per uso iniziale

Per configurare un ambiente di CA Identity Manager, utilizzare la console di gestione, un'applicazione basata sul Web.

La console di gestione è divisa nelle due sezioni seguenti:

- Directory: utilizzare questa sezione per creare e gestire le directory di CA Identity Manager e la directory di provisioning, che descrivono gli archivi utenti a CA Identity Manager.
- Ambienti: utilizzare questa sezione per creare e gestire ambienti di CA Identity Manager, che controllano la presentazione di gestione e grafica di una directory.

Accesso alla console di gestione di CA Identity Manager

Per accedere alla console di gestione, immettere il seguente URL in un browser:

http://*hostname:port*/iam/immanage

nomehost

Consente di definire il nome di dominio completo o l'indirizzo IP del server su cui è installato CA Identity Manager.

Nota: se si accede alla console di gestione mediante Internet Explorer 7 e il nome host include un indirizzo IPv6, la console di gestione non sarà visualizzata correttamente. Per prevenire questo problema, utilizzare il nome host completo o un indirizzo IPv4.

porta

Definisce la porta del server applicazioni.

Nota: se si utilizza un agente Web per fornire l'autenticazione avanzata per CA Identity Manager, non è necessario specificare il numero di porta.

Nota: abilitare JavaScript nel browser che si utilizza per accedere alla console di gestione.

Percorsi di esempio alla console di gestione:

- Per Geologic Weblogs:

  http://myserver.mycompany.org:7001/iam/immanage

- Per JBoss:

  http://myserver.mycompany.org:8080/iam/immanage

- Per WebSphere:

  http://myserver.mycompany.org:9080/iam/immanage

Modalità di creazione di un ambiente di CA Identity Manager

Per creare un ambiente di CA Identity Manager, completare i passaggi seguenti nella console di gestione:

1. Utilizzare la procedura di configurazione guidata di directory (a pagina 157) per creare una directory di CA Identity Manager.
2. Se l'ambiente include il provisioning, utilizzare la procedura di configurazione guidata di directory per creare una directory di provisioning (a pagina 172).
3. Creare un ambiente di CA Identity Manager.
4. Accedere all'ambiente (a pagina 194) per verificare che sia in esecuzione.

Capitolo 2: Ambiente di CA Identity Manager di esempio

Questa sezione contiene i seguenti argomenti:

Panoramica di un ambiente di CA Identity Manager di esempio

CA Identity Manager include un ambiente di esempio che è possibile utilizzare per apprendere il funzionamento di CA Identity Manager ed eseguire verifiche.

L'ambiente di esempio viene basato su un'azienda commerciale di automobili chiamata NeteAuto. Gli amministratori di NeteAuto utilizzano CA Identity Manager per gestire dipendenti, fornitori e rivenditori regionali.

Le configurazioni dell'archivio utenti per utilizzare ambienti di esempio di NeteAuto sono:

- Archivi utenti LDAP che supportano organizzazioni
- Archivi utenti LDAP che non supportano organizzazioni.
- Archivi utenti di database relazionale che supportano organizzazioni
- Archivi utenti di database relazionale che non supportano organizzazioni.

Nota: le capacità di provisioning non sono disponibili poiché questo ambiente non dispone di nessuna directory di provisioning.

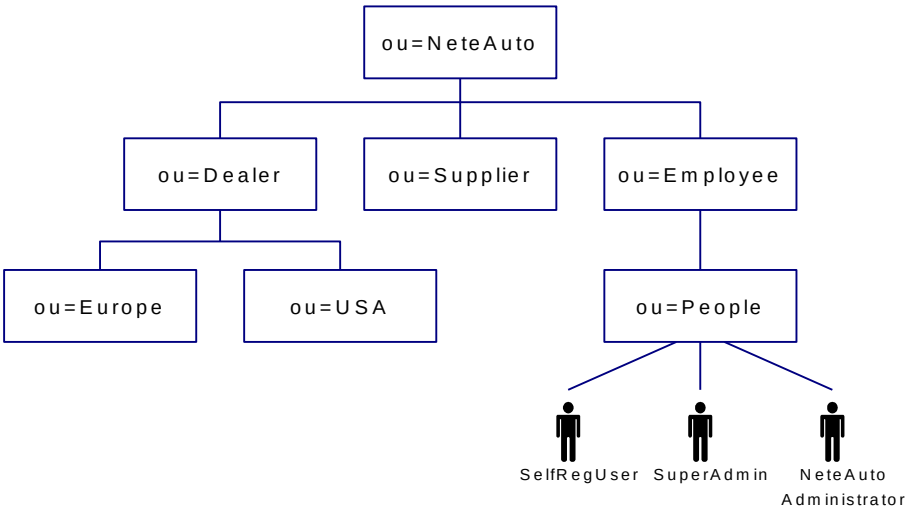
Configurazione dell'ambiente di esempio di NeteAuto con supporto per l'organizzazione

La configurazione dell'ambiente di esempio di NeteAuto con supporto per l'organizzazione comprende i passaggi seguenti:

- Installazione dei prerequisiti software
- Installazione dell'ambiente di CA Identity Manager di esempio
- Configurazione di una directory utente LDAP
- Configurazione di un database relazionale
- Creazione della directory di CA Identity Manager
- Creazione dell'ambiente CA Identity Manager di NeteAuto

Struttura di directory LDAP per NeteAuto

L'illustrazione seguente descrive l'ambiente di esempio di NeteAuto per directory LDAP:



L'ambiente di CA Identity Manager di esempio include gli utenti seguenti:

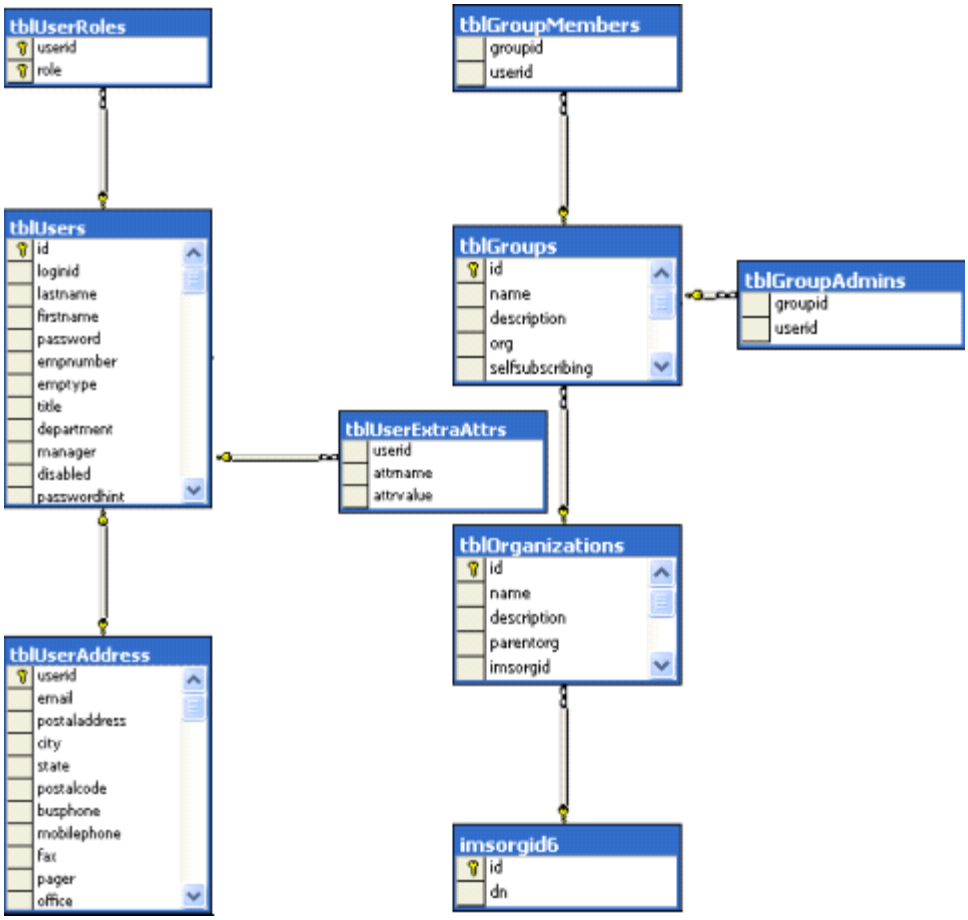
- Superadmin è l'account di amministratore con il ruolo di manager di Sistema per questo ambiente di CA Identity Manager. Come Superadmin, è possibile eseguire tutte le attività di amministrazione predefinite.

  Nota: per una descrizione delle attività di amministrazione predefinite, consultare la *Guida per l'amministratore*.

- SelfRegUser è l'account di amministratore che CA Identity Manager utilizza per abilitare la registrazione automatica per questo ambiente di CA Identity Manager.
- L'amministratore di NeteAuto non ha nessun privilegio quando si installa l'ambiente di NeteAuto. Tuttavia, è possibile assegnare Manager gruppi come ruolo utente, secondo quanto descritto nella sezione Assegnazione del ruolo Manager gruppi.

Database relazionale per NeteAuto

L'illustrazione seguente descrive il database relazionale per l'ambiente di esempio di NeteAuto, inclusa una tabella di organizzazione:



Prerequisiti software per NeteAuto

L'ambiente CA Identity Manager di NeteAuto ha i prerequisiti seguenti:

- Installare CA Identity Manager secondo quanto descritto nella *Guida all'installazione*. Assicurarsi di installare gli strumenti di amministrazione di CA Identity Manager.
- È necessario disporre dell'accesso a un server di directory di un sistema Sun Java (Sun One o iPlanet) o a un database Microsoft SQL Server.

File di installazione per l'ambiente di NeteAuto

CA Identity Manager include un insieme di file che è possibile utilizzare per impostare un ambiente di CA Identity Manager di esempio. L'ambiente di CA Identity Manager è una visualizzazione di uno spazio dei nomi di gestione che abilita gli amministratori di CA Identity Manager alla gestione di oggetti quali utenti, gruppi e organizzazioni. Questi oggetti vengono gestiti insieme a un set di ruoli e attività associate. L'ambiente di CA Identity Manager controlla la gestione e la presentazione grafica di una directory.

L'ambiente di CA Identity Manager di esempio include:

- Oggetti di esempio, quali utenti e organizzazioni
- Definizioni di ruoli, attività e schermate

  Le attività vengono visualizzate nella console utente quando si fa clic su una scheda, come ad esempio Utenti o Gruppi. In base ai ruoli assegnati, le attività associate vengono visualizzate quando l'utente esegue l'accesso.

  Nota: per ulteriori informazioni su ruoli e attività, consultare la *Guida per l'amministratore*.
- Un'interfaccia di esempio che personalizza la console utente per gli utenti di NeteAuto.
- Un file di configurazione di directory che si utilizza per creare una directory CA Identity Manager.

I file per creare l'ambiente di CA Identity Manager di esempio vengono installati nella posizione seguente:

admin_tools\samples\NeteAuto

In questo percorso, *admin_tools* fa riferimento agli strumenti di amministrazione. Gli Strumenti di amministrazione sono ora installati nelle seguenti posizioni predefinite:

- **Windows:** C:\Programmi\CA\Identity Manager\IAM Suite\Identity Manager\tools
- **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

Installazione dell'ambiente di NeteAuto

Eseguire la procedura seguente per installare l'ambiente di NeteAuto.

Procedere come descritto di seguito:

1. Assicurarsi che i prerequisiti software siano installati (a pagina 22).
2. Configurare l'archivio utenti e importare i dati di esempio.
   - Per gli utenti LDAP: configurare una directory utente LDAP (a pagina 23)
   - Per utenti del database relazionale: configurare un database relazionale
3. Creare la directory CA Identity Manager di NeteAuto.
4. Creare l'ambiente CA Identity Manager di NeteAuto.
5. Configurare l'aspetto dell'interfaccia utente di CA Identity Manager per gli utenti di NeteAuto (a pagina 38).

Configurazione di una directory utente LDAP

La directory LDAP è disponibile in base all'installazione effettuata. È possibile utilizzare la procedura seguente per verificare se la directory esiste o per crearla.

Procedere come descritto di seguito:

1. Nella console del server di directory, creare un'istanza LDAP con la radice seguente:

   ```
   dc=security,dc=com
   ```

   Prendere nota del numero di porta per riferimento futuro.
2. Importare il file NeteAuto.ldif nel server di directory da samples\NeteAuto negli strumenti di amministrazione.

   Gli strumenti di amministrazione sono installati nelle seguenti posizioni predefinite:
   - **Windows**: C:\Programmi\CA\Identity Manager\IAM Suite\Identity Manager\tools
   - **UNIX**: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

Nota: se si verificano dei problemi durante l'importazione del file LDIF o la creazione della directory di CA Identity Manager, aggiungere il testo seguente all'inizio del file LDIF:

```
dn: dc=security, dc=com
objectClass: top
objectClass: domain
dc: security
```

Salvare il file e ripetere i passaggi 1 e 2.

Configurazione di un database relazionale

Eseguire la procedura seguente per configurare un database relazionale.

Procedere come descritto di seguito:

1. Creare un'istanza di database denominata NeteAuto.
2. Creare un utente chiamato neteautoadmin con il test di password. Concedere i diritti a neteautoadmin (ad esempio i diritti Public e db_owner) a NeteAuto modificando le proprietà dell'utente.

   Nota: per creare un database di NeteAuto, il ruolo di neteautoadmin deve avere almeno autorizzazioni minime (selezione, inserimento, aggiornamento ed eliminazione) per tutte le tabelle create dallo script by.sql. Inoltre, neteautoadmin deve essere in grado di eseguire tutte le procedure archiviate, se ve ne sono, definite in questi script.
3. Quando si modificano le proprietà dell'utente, selezionare NeteAuto come database predefinito per neteautoadmin.
4. Eseguire gli script seguenti nell'ordine in cui sono elencati:
   - *db_type*-rdbuserdirectory.sql: configura le tabelle per l'ambiente NeteAuto di esempio e crea le voci utente.
   - ims_*db_type*_rdb.sql: configura il supporto per le organizzazioni

     db_type

     Definisce Microsoft SQL o Oracle a seconda del tipo di database che si sta configurando.

   Questi file di script si trovano nella cartella *admin_tools*\samples\NeteAutoRDB\Organization. In questo esempio, *admin_tools* fa riferimento agli strumenti di amministrazione, che vengono installati nelle posizioni predefinite seguenti:
   - **Windows:** C:\Programmi\CA\Identity Manager\IAM Suite\Identity Manager\tools
   - **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools
5. Definire un'origine dati JDBC denominata neteautoDS che punti al database di NeteAuto.

   La procedura per configurare un'origine dati dipende dal tipo di server applicazioni in cui CA Identity Manager è installato. La sezione Creazione di un'origine dati JDBC (a pagina 107) include istruzioni specifiche del server applicazioni per la creazione di un'origine dati JDBC.

Creazione di una directory CA Identity Manager

Eseguire la procedura seguente per creare una directory CA Identity Manager.

Procedere come descritto di seguito:

1. Aprire la console di gestione immettendo il seguente URL in un browser:

   http://*im_server:port*/iam/immanage

   im_server

   Definisce il nome di dominio completo del server su cui è installato CA Identity Manager.

   porta

   Definisce il numero di porta del server applicazioni.

2. Fare clic su Directory.
3. Fare clic su Create from Wizard (Creazione guidata) per avviare la procedura guidata di creazione della directory di CA Identity Manager.
4. Accedere al file .xml di configurazione directory appropriato e fare clic su Avanti.

   Il file di configurazione di directory è disponibile nelle cartelle seguenti:

   - Per le directory utente del server di directory del sistema Sun Java:

     admin_tools\samples\NeteAuto\Organization\directory.xml

   - Per i database relazionali:

     admin_tools\samples\NeteAutoRDB\Organization*db_type* directory.xml

     admin_tools

     Definisce la posizione di installazione degli strumenti di amministrazione.

     Gli strumenti di amministrazione sono installati nelle seguenti posizioni predefinite:

     Windows: C:\Programmi\CA\Identity Manager\IAM Suite\Identity Manager\tools

     UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

     db_type

     Specifica il tipo di database che si sta configurando: Microsoft SQL o Oracle.

   Le informazioni di stato vengono visualizzate nella schermata Directory Configuration Output (Output di configurazione directory).

5. Nella seconda pagina della procedura guidata, fornire i valori seguenti:
   - Server di directory del sistema Sun Java

     Nome

     Directory NeteAuto

     Descrizione

     Directory di esempio di NeteAuto

     Connection Object Name (Nome oggetto di connessione)

     Utenti di NeteAuto

     Host

     Specifica il nome o l'indirizzo IP del sistema su cui è installato l'archivio utenti.

     Porta

     Numero di porta per l'archivio utenti

     Cerca in principale

     dc=security, dc=com

     Nome utente

     Nome utente di un account che può accedere all'archivio utenti.

     Password e Conferma password

     Password per l'account utente

   - Database Microsoft SQL Server e Oracle

     Nome

     Directory NeteAutoRDB

     Descrizione

     Directory di esempio di NeteAuto

     Connection Object Name (Nome oggetto di connessione)

     NeteAutoRDB

     JDBC Data Source (Origine dati JDBC)

     neteautoDS

     Nome utente

     Neteautoadmin

     Password

     Test

6. Fare clic su Avanti.
7. Per uscire dalla procedura guidata, fare clic su Fine.

Creazione dell'ambiente CA Identity Manager di NeteAuto

Eseguire la procedura seguente per creare l'ambiente CA Identity Manager di NeteAuto.

Procedere come descritto di seguito:

1. Nella Console di gestione, fare clic su Environments (Ambienti).
2. Nella schermata Environments (Ambienti) di CA Identity Manager, fare clic su Nuovo.

   Viene visualizzata la procedura guidata di creazione dell'ambiente di CA Identity Manager.
3. Nella prima pagina della procedura guidata, immettere i valori seguenti:

   Nome dell'ambiente

   Ambiente NeteAuto

   Descrizione

   Ambiente di esempio

   Alias

   Neteauto

   L'alias viene aggiunto all'URL per accedere all'ambiente di CA Identity Manager. Ad esempio, l'URL per accedere all'ambiente di neteauto è:

   http://*server_name*/iam/im/neteauto

   server_name

   Consente di definire il nome di dominio completo del server in cui CA Identity Manager è installato, ad esempio:

   http://myserver.mycompany.org/iam/im/neteauto

   Nota: l'alias distingue tra maiuscole e minuscole.

   Fare clic su Avanti.
4. Selezionare la directory di CA Identity Manager da associare all'ambiente che si sta creando:
   - Per il server di directory del sistema Sun Java, utilizzare la directory NeteAuto.
   - Per il database Microsoft SQL Server o Oracle, utilizzare la directory NeteAutoRDB.

   Fare clic su Avanti.

5. Configurare il supporto per le attività pubbliche, come la registrazione automatica e le attività relative alle password dimenticate, nel modo seguente:
   a. Digitare l'alias seguente per le attività pubbliche:

      Neteautopublic

   b. Immettere SelfRegUser come account utente anonimo.
   c. Fare clic su Convalida per visualizzare l'ID univoco dell'utente.

   Nota: non è necessario eseguire l'accesso per svolgere le attività pubbliche.
6. Selezionare le attività e i ruoli da creare per l'ambiente di NeteAuto:
   a. Selezionare Import roles from the file (Importa ruoli dal file).
   b. Accedere a una delle posizioni seguenti:
      - Per un archivio utenti del server di directory del sistema Sun Java:

        admin_tools\samples\NeteAuto\RoleDefinitions.xml
      - Per un archivio utenti di Server di Microsoft SQL:

        admin_tools\samples\NeteAutoRDB\Organization\mssqlRoleDefinitions.xml
      - Per un archivio utenti Oracle:

        admin_tools\samples\NeteAutoRDB\Organization\oracleRoleDefinitions.xml

      admin_tools fa riferimento agli strumenti di amministrazione, che sono installati per impostazione predefinita nella posizione seguente:

      Windows: C:\Programmi\CA\Identity Manager\IAM Suite\Identity Manager\tools

      UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

7. Specificare un utente che esegua le funzioni di Manager di sistema per questo ambiente e fare clic su Avanti:
   a. Digitare SuperAdmin nel campo Manager di sistema.
   b. Fare clic su Aggiungi.

      CA Identity Manager aggiunge l'ID univoco dell'utente Superadmin all'elenco degli utenti.
   c. Fare clic su Avanti.

8. Rivedere le impostazioni per l'ambiente ed eseguire le attività seguenti:
   - (Facoltativo) Fare clic su Precedente per apportare delle modifiche.
   - Fare clic su Fine per creare l'ambiente di CA Identity Manager con le impostazioni attuali.

     La schermata Environment Configuration Output (Output di configurazione ambiente) mostra l'avanzamento della creazione dell'ambiente.
9. Fare clic su Continua per uscire dalla procedura guidata di creazione dell'ambiente di CA Identity Manager.
10. Avviare l'ambiente di CA Identity Manager.

Una volta creato l'ambiente di NeteAuto, è possibile:

- Creare un'interfaccia per questo ambiente di CA Identity Manager (a pagina 38).
- Accedere all'ambiente (a pagina 36)

Configurazione dell'ambiente di NeteAuto di esempio senza il supporto per l'organizzazione

La configurazione dell'ambiente di NeteAuto di esempio senza il supporto per l'organizzazione comprende i passaggi seguenti:

- Installazione dei prerequisiti software (a pagina 22)
- Installazione dell'ambiente di CA Identity Manager di esempio
- Configurazione del database
- Creazione di un'origine dati JDBC
- Creazione della directory di CA Identity Manager
- Creazione dell'ambiente CA Identity Manager di NeteAuto

Descrizione di un ambiente CA Identity Manager di esempio

Per i database Microsoft SQL Server e Oracle, CA Identity Manager include una versione dell'ambiente di NeteAuto che non comprende le organizzazioni. Questo ambiente di CA Identity Manager include i tre utenti seguenti:

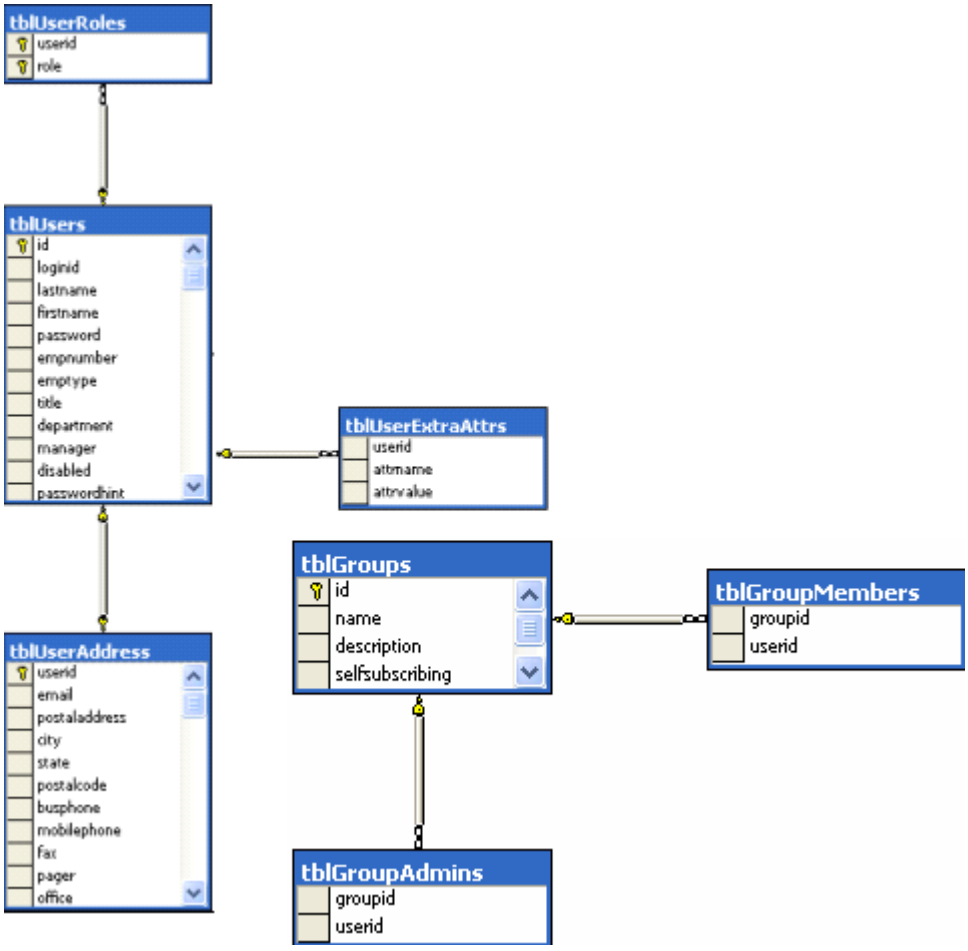
- Superadmin è l'account di amministratore con il ruolo di manager di sistema per questo ambiente di CA Identity Manager. Come Superadmin, è possibile eseguire tutte le attività di amministrazione predefinite.

  Nota: per una descrizione delle attività di amministrazione predefinite, consultare la *Guida per l'amministratore*.

- SelfRegUser è l'account di amministratore che CA Identity Manager utilizza per abilitare la registrazione automatica per questo ambiente di CA Identity Manager.
- L'amministratore di NeteAuto non ha nessun privilegio quando si installa l'ambiente di NeteAuto.

  Tuttavia, è possibile assegnare il ruolo di Manager gruppi all'account di amministratore di NeteAuto.

L'illustrazione seguente descrive l'ambiente NeteAuto di esempio per un database relazionale, senza organizzazioni:



File di installazione per l'ambiente di NeteAuto

CA Identity Manager include un insieme di file che è possibile utilizzare per impostare un ambiente di CA Identity Manager di esempio. Un ambiente di CA Identity Manager è una visualizzazione di uno spazio dei nomi di gestione che abilita gli amministratori di CA Identity Manager alla gestione di oggetti. Questi oggetti, quali utenti e gruppi, hanno un insieme di ruoli e attività associate. L'ambiente di CA Identity Manager controlla la gestione e la presentazione grafica di un archivio utenti.

L'ambiente di CA Identity Manager di esempio include:

- Utenti di esempio
- Definizioni di ruoli, attività e schermate

  Le attività vengono visualizzate nella console utente quando si fa clic su una categoria, come ad esempio Utenti o Gruppi. Le attività che vengono visualizzate sono basate sui ruoli che vengono assegnati all'utente.

  Nota: per ulteriori informazioni su ruoli e attività, consultare la *Guida per l'amministratore*.
- Un'interfaccia di esempio che personalizza la console utente per gli utenti di NeteAuto.
- Un file di configurazione di directory che si utilizza per creare una directory CA Identity Manager.

I file per creare l'ambiente di CA Identity Manager di esempio vengono installati nella posizione seguente:

admin_tools\samples\NeteAutoRDB\NoOrganization

In questo percorso, *admin_tools* fa riferimento agli strumenti di amministrazione.

Gli Strumenti di amministrazione sono ora installati nelle seguenti posizioni predefinite:

- **Windows:** C:\Programmi\CA\Identity Manager\IAM Suite\Identity Manager\tools
- **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

Installazione dell'ambiente NeteAuto (senza supporto per l'organizzazione)

Eseguire la procedura seguente per installare l'ambiente di NeteAuto.

Procedere come descritto di seguito:

1. Verificare che i prerequisiti software (a pagina 32) siano installati.
2. Configurare il database (a pagina 24).

3. Creare la directory CA Identity Manager. (a pagina 33)
4. Creare l'ambiente CA Identity Manager di NeteAuto (a pagina 35).
5. Configurare l'aspetto dell'interfaccia utente di CA Identity Manager (a pagina 38) per gli utenti di NeteAuto.

Prerequisiti software

L'ambiente CA Identity Manager di NeteAuto ha i prerequisiti seguenti:

- Installare CA Identity Manager secondo quanto descritto nella *Guida all'installazione*. Verificare di installare gli strumenti di amministrazione di CA Identity Manager.
- È necessario avere accesso a un database Microsoft SQL Server o Oracle.

Configurazione di un database relazionale

Eseguire la procedura seguente per configurare un database relazionale.

Procedere come descritto di seguito:

1. Creare un'istanza di database denominata NeteAuto.
2. Creare un utente chiamato neteautoadmin con il test di password. Concedere i diritti a neteautoadmin (ad esempio i diritti Public e db_owner) a NeteAuto modificando le proprietà dell'utente.

   Nota: per creare un database di NeteAuto, il ruolo di neteautoadmin deve avere almeno autorizzazioni minime (selezione, inserimento, aggiornamento ed eliminazione) per tutte le tabelle create dallo script by.sql. Inoltre, neteautoadmin deve essere in grado di eseguire tutte le procedure archiviate, se ve ne sono, definite in questi script.
3. Quando si modificano le proprietà dell'utente, selezionare NeteAuto come database predefinito per neteautoadmin.

4. Eseguire gli script seguenti nell'ordine in cui sono elencati:
   - *db_type*-rdbuserdirectory.sql: configura le tabelle per l'ambiente NeteAuto di esempio e crea le voci utente.
   - ims_*db_type*_rdb.sql: configura il supporto per le organizzazioni

     db_type

     Definisce Microsoft SQL o Oracle a seconda del tipo di database che si sta configurando.

   Questi file di script si trovano nella cartella *admin_tools*\samples\NeteAutoRDB\Organization. In questo esempio, *admin_tools* fa riferimento agli strumenti di amministrazione, che vengono installati nelle posizioni predefinite seguenti:
   - **Windows:** C:\Programmi\CA\Identity Manager\IAM Suite\Identity Manager\tools
   - **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools
5. Definire un'origine dati JDBC denominata neteautoDS che punti al database di NeteAuto.

   La procedura per configurare un'origine dati dipende dal tipo di server applicazioni in cui CA Identity Manager è installato. La sezione Creazione di un'origine dati JDBC (a pagina 107) include istruzioni specifiche del server applicazioni per la creazione di un'origine dati JDBC.

Creazione di una directory CA Identity Manager

Eseguire la procedura seguente per creare la directory di CA Identity Manager.

Procedere come descritto di seguito:

1. Aprire la console di gestione immettendo il seguente URL in un browser:

   http://*im_server*:*port*/iam/immanage

   im_server

   Definisce il nome di dominio completo del server su cui è installato CA Identity Manager.

   porta

   Definisce il numero di porta del server applicazioni.
2. Fare clic su Directory.

   La schermata delle directory di CA Identity Manager viene visualizzata.
3. Fare clic su Nuovo per avviare la procedura guidata di directory di CA Identity Manager.

4. Accedere a uno dei file XML di configurazione di directory seguenti e fare clic su Avanti:
   - Sistemi Sun Java:

     admin_tools\samples\NeteAuto\NoOrganization\directory.xml
   - Database SQL Server:

     admin_tools\samples\NeteAuto\NoOrganization\mssql-directory.xml
   - Database Oracle:

     admin_tools\samples\NeteAuto\NoOrganization\oracle-directory.xml

   admin_tools fa riferimento agli strumenti di amministrazione, che sono installati per impostazione predefinita nella posizione seguente:
   - **Windows:** C:\Programmi\CA\Identity Manager\IAM Suite\Identity Manager\tools
   - **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

   Le informazioni di stato vengono visualizzate nella schermata Directory Configuration Output (Output di configurazione directory).
5. Nella seconda pagina della procedura guidata, fornire i valori seguenti:

   Nome

   Directory NeteAutoRDB

   Descrizione

   Directory di esempio di NeteAuto senza supporto per l'organizzazione

   Connection Object Name (Nome oggetto di connessione)

   NeteAutoRDB

   JDBC Data Source (Origine dati JDBC)

   neteautoDS

   Nome utente

   neteautoadmin

   Password

   test
6. Fare clic su Avanti.
7. Per uscire dalla procedura guidata, fare clic su Fine.

Creazione dell'ambiente CA Identity Manager di NeteAuto

Eseguire la procedura seguente per creare l'ambiente CA Identity Manager di NeteAuto.

Procedere come descritto di seguito:

1. Nella Console di gestione, fare clic su Environments (Ambienti).
2. Nella schermata Environments (Ambienti) di CA Identity Manager, fare clic su Nuovo.

   Si apre la procedura guidata di creazione ambiente di CA Identity Manager.
3. Nella prima pagina della procedura guidata, digitare i valori seguenti:
   - Environment Name (Nome ambiente): Ambiente NeteAuto
   - Descrizione: NeteAuto è un ambiente di esempio.
   - Alias: neteautoRDB

     L'alias viene aggiunto all'URL per accedere all'ambiente di CA Identity Manager. Ad esempio, l'URL per accedere all'ambiente di neteauto è:

     `http://domain/iam/im/neteautoRDB`

     In questo percorso, *domain* definisce il nome di dominio completo del server in cui CA Identity Manager è installato, come nell'esempio seguente:

     `http://myserver.mycompany.org/iam/im/neteautoRDB`

     Nota: l'alias distingue tra maiuscole e minuscole.

   Fare clic su Avanti.
4. Selezionare la directory di CA Identity Manager di NeteAutoRDB per associarla all'ambiente che si sta creando e fare clic su Avanti.
5. Configurare il supporto per le attività pubbliche, come la registrazione automatica e le attività relative alle password dimenticate.

   Nota: non è necessario che gli utenti eseguano l'accesso per svolgere le attività pubbliche.

   a. Digitare l'alias seguente per le attività pubbliche:

      neteautoRDBpublic

   b. Digitare SelfRegUser come account utente anonimo.

   c. Fare clic su Convalida per visualizzare l'ID univoco dell'utente (2, in questo caso).
6. Selezionare le attività e i ruoli da creare per l'ambiente di NeteAuto:
   - Selezionare Import roles from the file (Importa ruoli dal file).

- Accedere alla posizione seguente:

  im_admin_tools_dir\samples\NeteAutoRDB\NoOrganizations\RoleDefinitions.xml

  In questo percorso, *im_admin_tools_dir* definisce la posizione di installazione degli strumenti di amministrazione di CA Identity Manager.

7. Specificare un utente che esegua le funzioni di Manager di sistema per questo ambiente e fare clic su Avanti:
   a. Digitare SuperAdmin nel campo Manager di sistema.
   b. Fare clic su Aggiungi.
   c. Fare clic su Avanti.
8. Rivedere le impostazioni per l'ambiente.
   - Fare clic su Precedente per modificare.
   - Fare clic su Fine per creare l'ambiente di CA Identity Manager con le impostazioni attuali.

     La schermata Environment Configuration Output (Output di configurazione ambiente) mostra l'avanzamento della creazione dell'ambiente.
9. Fare clic su Fine per uscire dalla procedura guidata di creazione dell'ambiente di CA Identity Manager.
10. Avviare l'ambiente di CA Identity Manager.

Una volta creato l'ambiente di NeteAuto, è possibile:

- Creare un'interfaccia per questo ambiente di CA Identity Manager secondo quanto descritto nella sezione Impostazione dell'interfaccia di NeteAuto (a pagina 38).
- Accedere all'ambiente secondo quanto descritto nella sezione Utilizzo dell'ambiente CA Identity Manager di NeteAuto

Utilizzo dell'ambiente CA Identity Manager di NeteAuto

È possibile utilizzare l'ambiente CA Identity Manager di NeteAuto per gestire le attività di self-service e gli utenti.

Gestione delle attività self-service

Le attività self-service includono:

- Registrazione come nuovo utente
- Accesso come utente registrato automaticamente
- Utilizzo della funzionalità di password dimenticata

Registrazione come nuovo utente

Eseguire la procedura seguente per registrarsi come nuovo utente.

Procedere come descritto di seguito:

1. Digitare l'URL seguente in un browser:

   `http://hostname/iam/im/neteautopublic/index.jsp?task.tag=SelfRegistration`

   nomehost

   Definisce il nome di dominio completo del sistema su cui CA Identity Manager è in esecuzione.

   Nota: se non è stata configurata l'interfaccia di (a pagina 38) Neteauto, è possibile omettere imcss dall'URL nel modo seguente:

   http://*hostname*/iam/im/neteautopublic/index.jsp?task.tag=SelfRegistration

   Questo URL indirizza l'utente alla console CA predefinita.

   Durante la registrazione automatica, nella pagina del Contratto di licenza con l'utente finale, CA Identity Manager mostra il sito Web di CA.

   Nota: è possibile configurare l'attività di registrazione automatica predefinita in modo che venga visualizzato il Contratto di licenza con l'utente finale personalizzato. Per istruzioni, consultare la *Guida per l'amministratore*.

2. Per procedere, fare clic su Accetta.
3. Nella scheda Profilo, fornire i dettagli seguenti:
   a. Digitare i valori per i campi obbligatori, indicati con un asterisco (*).
   b. Digitare i suggerimenti per la password e le risposte.

      Se si dimentica la password, CA Identity Manager fornirà il suggerimento password e richiederà la risposta. Se la risposta è corretta, CA Identity Manager richiede all'utente di specificare e confermare una nuova password.
4. Lasciare la scheda Gruppi immutata.
5. Fare clic su Invia.

Accesso come utente registrato automaticamente

Eseguire la procedura seguente per accedere come utente registrato automaticamente.

Procedere come descritto di seguito:

1. Digitare l'URL seguente per l'ambiente CA Identity Manager di NeteAuto in un browser:

   `http://hostname/iam/im/neteauto/imcss/index.jsp`

   nomehost

   Definisce il nome di dominio completo del sistema su cui CA Identity Manager è in esecuzione.

2. Accedere mediante il nome utente e la password specificati durante la registrazione.

Impostazione dell'interfaccia di NeteAuto

Per impostare l'interfaccia di NeteAuto, si crea una risposta SiteMinder nel Policy Server SiteMinder.

Procedere come descritto di seguito:

1. Accedere a una delle seguenti interfacce come amministratore con privilegi di dominio:

   - Per CA SiteMinder Web Access Manager r12 o successive, accedere all'interfaccia utente di amministrazione.
   - Per CA eTrust SiteMinder 6.0 SP5, accedere all'interfaccia utente del Policy Server.

   Nota: per informazioni sull'utilizzo di queste interfacce, consultare la documentazione relativa alla versione di SiteMinder in uso.

2. Aprire neteautoDomain.
3. Sotto neteautoDomain, selezionare Realm.

   Viene visualizzata la seguente area di autenticazione:

   neteauto_ims_realm

   Protegge l'ambiente di CA Identity Manager.

   neteauto_pub_realm

   Abilita il supporto per le attività pubbliche, come la registrazione automatica e le attività relative alle password dimenticate.

4. Creare una regola in ciascuna delle aree di autenticazione. Specificare i dettagli seguenti:
   - Risorsa: *
   - Azioni: GET, POST

   Per semplificare l'amministrazione, includere l'interfaccia di NeteAuto nel nome della regola.
5. Creare una risposta per il dominio con gli attributi di risposta seguenti:
   - Attributo: WebAgent-HTTP-Header-Variable

     Questo attributo aggiunge una nuova intestazione HTTP alla risposta.
   - Tipo di attributo: Statico
   - Nome variabile: skin

     Valore variabile: neteauto
6. Modificare il criterio che CA Identity Manager ha creato in neteautoDomain. Specificare i dettagli seguenti:
   - Utenti
     - Per LDAP: selezionare ou=People, ou=Employees, ou=NeteAuto in Available Members (Membri disponibili) e aggiungerlo a Current Members (Membri attuali). Fare clic su OK.
     - Per i database relazionali: cercare gli utenti in cui l'attributo dell'ID equivale a *. Selezionare tutti gli utenti in Available Members (Membri disponibili) e aggiungerli a Current Members (Membri attuali). Fare clic su OK.
   - Regole:
     - Aggiungere le regole create al passaggio 4.
     - Per ciascuna regola, fare clic su Set response (Imposta risposta). Associare ciascuna regola alla risposta creata al passaggio 5.

Nota: l'interfaccia di NeteAuto si basa sulla console imcss. Per visualizzare l'interfaccia, aggiungere /imcss/index.jsp all'URL per l'ambiente CA Identity Manager di NeteAuto nel modo seguente:

http://*hostname*/iam/im/neteauto/imcss/index.jsp

La sezione Accesso all'ambiente CA Identity Manager di NeteAuto (a pagina 41)fornisce istruzioni complete per accedere all'ambiente di Neteauto.

Utilizzo della funzionalità per le password dimenticate

Eseguire la procedura seguente per utilizzare la funzionalità per le password dimenticate.

Procedere come descritto di seguito:

1. Digitare l'URL seguente in un browser:

   `http://hostname/iam/im/neteautopublic/index.jsp?task.tag=ForgottenPasswordReset`

   nomehost

   Definisce il nome di dominio completo del sistema su cui CA Identity Manager è in esecuzione.

2. Digitare l'ID univoco dell'utente registrato automaticamente creato nella sezione Registrazione come nuovo utente (a pagina 37) e fare clic su Avanti.
3. Ogni volta che viene richiesto, rispondere alla domanda di verifica. La risposta è quella fornita durante la registrazione.

   Nota: è necessario fornire una risposta corretta per ciascuna domanda. Annullare l'attività o chiudere i conteggi di browser equivale a un tentativo non riuscito.
4. Fare clic su Invia.

   CA Identity Manager richiede di fornire una nuova password.

Gestione degli utenti

La gestione utente include le operazioni seguenti:

- Accesso all'ambiente CA Identity Manager di NeteAuto
- Modifica di un utente
- Assegnazione del ruolo di Manager gruppi
- Creazione di un gruppo
- Gestione degli utenti registrati automaticamente

Accesso all'ambiente CA Identity Manager di NeteAuto.

Eseguire la procedura seguente per accedere all'ambiente CA Identity Manager di NeteAuto.

Procedere come descritto di seguito:

1. Digitare l'URL seguente in un browser:

   `http://hostname/iam/im/neteauto/imcss/index.jsp`

   nomehost

   Definisce il nome di dominio completo, come nell'esempio seguente:

   http://myserver.mycompany.com/iam/im/neteauto/imcss/index.jsp.

   Nota: se non si l'interfaccia di Neteauto non è stata configurata, è possibile utilizzare l'URL seguente per accedere all'ambiente di Neteauto:

   http://*hostname*/iam/im/neteauto

2. Nella schermata di accesso, digitare le credenziali seguenti:

   Nome utente

   SuperAdmin

   Password

   test

Modifica di un utente

Per modificare un utente, eseguire la procedura seguente.

Procedere come descritto di seguito:

1. Accedere all'ambiente di NeteAuto come SuperAdmin mediante il test della password.
2. Selezionare Utenti, Gestisci utenti, Modifica utente.

   Verrà visualizzato lo schermo Seleziona utente.

3. Fare clic su Cerca.

   CA Identity Manager mostra un elenco di utenti nell'ambiente di NeteAuto.

4. Selezionare l'amministratore di NeteAuto, nel modo seguente:

   - Per le directory LDAP, Amministratore NeteAuto
   - Per i database relazionali, Admin NeteAuto

   Fare clic su Seleziona. CA Identity Manager mostra il profilo dell'amministratore di NeteAuto.

5. Nel campo Titolo, digitare Manager. Fare clic su Invia.

   CA Identity Manager conferma l'invio dell'attività.

6. Fare clic su OK per tornare alla schermata principale.

Assegnazione del ruolo di Manager gruppi

L'assegnazione del ruolo di Manager gruppi è necessaria. Eseguire la procedura seguente per assegnare un manager di gruppi.

Procedere come descritto di seguito:

1. Come SuperAdmin, selezionare la scheda Ruoli e attività, quindi selezionare Ruoli di amministrazione, Modify Admin Roles (Modifica ruoli di amministrazione).
2. Selezionare il ruolo Manager gruppi e fare clic su Seleziona.

   Viene visualizzato il profilo per il ruolo di Manager gruppi.

3. Fare clic sulla scheda Membri e fare clic su Aggiungi sotto Criteri membri.

   Viene visualizzata la schermata Criterio membri.

4. Sotto Regola membri, fare clic sulla freccia in giù nel campo Utenti.

   Dall'elenco a discesa, selezionare dove <user-filter>.

   Il campo Utenti viene modificato per consentire di immettere un filtro per la regola.

5. Immettere la regola di appartenenza nel modo seguente:
   a. Nel primo campo, selezionare Titolo dall'elenco a discesa.
   b. Nel secondo campo, assicurarsi che sia selezionato il segno uguale (=).
   c. Nel terzo campo, digitare Manager.
6. Nella sezione Regole di ambito, definire le regole per gli utenti, i gruppi e le organizzazioni (quando supportate) nel modo seguente:
   a. Nel campo Utenti, fare clic sulla freccia in giù per visualizzare un elenco di opzioni. Selezionare (tutto) dall'elenco.
   b. Ripetere il passaggio A nei campi Gruppo e Organizzazione (se supportate).
   c. Lasciare il campo Attività di accesso vuoto.
7. Fare clic su OK.

   CA Identity Manager mostra il criterio membri creato.

8. Fare clic su Invia.

   CA Identity Manager conferma l'invio dell'attività.

9. Fare clic su OK per tornare alla schermata principale.
10. Chiudere CA Identity Manager.

Creazione di un gruppo

Eseguire la procedura seguente per creare un gruppo.

Procedere come descritto di seguito:

1. Accedere a CA Identity Manager come amministratore di NeteAuto, nel modo seguente:
   - Per le directory LDAP, digitare il nome utente Amministratore di NeteAuto e il test della password.
   - Per i database relazionali, digitare il nome utente Admin di NeteAuto e il test della password.

   Viene visualizzato l'elenco di attività che l'amministratore di NeteAuto può eseguire. Poiché l'amministratore di NeteAuto può eseguire solamente un numero limitato di attività, CA Identity Manager elenca le attività invece delle categorie.
2. Fare clic su Crea gruppo.
3. Assicurarsi che l'opzione Crea un nuovo gruppo sia selezionata, quindi fare clic su OK.
4. Implementare uno dei passaggi seguenti a seconda della situazione:
   - Se l'ambiente di NeteAuto supporta le organizzazioni:
     a. Nel campo Org Name (Nome organizzazione), fare clic sul simbolo di ellissi (...) per selezionare l'organizzazione in cui CA Identity Manager crea il gruppo.
     b. In fondo alla schermata Seleziona organizzazione, espandere NeteAuto.
     c. Selezionare l'organizzazione Dealer (Rivenditore).
   - Se l'ambiente di NeteAuto non supporta le organizzazioni, passare alla fase successiva.
5. Specificare le seguenti informazioni per il gruppo:
   - Nome gruppo: Dealer Administrators (Amministratori rivenditore)
   - Descrizione gruppo: Administrators for NeteAuto dealerships (Amministratori dei rivenditori di NeteAuto).
6. Fare clic sulla scheda Appartenenza e fare clic su Aggiungi un utente.

   Verrà visualizzato lo schermo Seleziona utente.
7. Fare clic su Cerca.
8. Selezionare l'amministratore di NeteAuto e fare clic su Seleziona.
9. Fare clic su Invia per creare il gruppo.

Gestione degli utenti registrati automaticamente

Eseguire la procedura seguente quando si desidera gestire utenti registrati automaticamente.

Procedere come descritto di seguito:

1. Accedere a CA Identity Manager come amministratore di NeteAuto, utilizzando le credenziali seguenti:

   - Per le directory LDAP:

     Nome utente

     Amministratore di NeteAuto

     Password

     test

   - Per i database relazionali:

     Nome utente

     Admin NeteAuto

     Password

     test

   L'elenco delle attività che l'amministratore di NeteAuto può eseguire viene visualizzato sul lato sinistro della console utente. Poiché l'amministratore di NeteAuto può eseguire solamente un numero limitato di attività, CA Identity Manager elenca le attività invece delle categorie.

2. Fare clic su Modifica gruppo.
3. Fare clic su Cerca.

   CA Identity Manager mostra un elenco di gruppi.

4. Selezionare Dealer Administrators (Amministratori rivenditore) e fare clic su Seleziona.
5. Fare clic sulla scheda Appartenenza e su Aggiungi un utente.

   Verrà visualizzato lo schermo Seleziona utente.

6. Fare clic su Cerca.
7. Nella schermata di ricerca utente, selezionare l'utente specificato nella sezione Registrazione come nuovo utente (a pagina 37). Fare clic su Seleziona.

8. Fare clic su Invia.

   CA Identity Manager conferma l'invio dell'attività.

9. Fare clic su OK per tornare alla schermata principale.

Per confermare che l'utente è un membro del gruppo creato, utilizzare l'attività Visualizza gruppo.

Configurazione delle funzionalità aggiuntive

Dopo aver installato l'ambiente di NeteAuto di esempio e aver testato la funzionalità di CA Identity Manager di base, utilizzare l'ambiente di NeteAuto per testare funzionalità di CA Identity Manager aggiuntive, incluse le notifiche di posta elettronica e il flusso di lavoro.

Nota: per ulteriori informazioni su queste funzionalità, consultare la *Guida per l'amministratore*.

Restrizioni del nome di accesso a SiteMinder per il nome dell'utente globale

I seguenti caratteri o stringhe di caratteri non possono essere inclusi nel nome di un utente globale se l'utente intende accedere al server dei criteri SiteMinder:

&
*
:
( )

Rimedio provvisorio

Evitare l'utilizzo di tali caratteri nel nome dell'utente globale.

Capitolo 3: Gestione dell'archivio utenti LDAP

Questa sezione contiene i seguenti argomenti:

Directory di CA Identity Manager

Una *directory di CA Identity Manager* descrive come oggetti quali utenti, gruppi e organizzazioni vengono archiviati in una directory utente e come questa viene rappresentata in CA Identity Manager. Una directory di CA Identity Manager viene associata a uno o più ambienti di CA Identity Manager.

Creazione di una directory di CA Identity Manager

La creazione di una directory di CA Identity Manager per un archivio utenti LDAP comprende i passaggi seguenti:

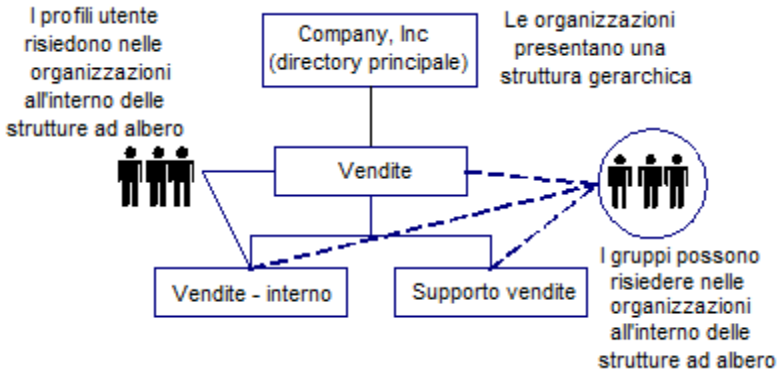
1. Determinazione della struttura di directory.
2. Descrizione degli oggetti nell'archivio utenti modificando un file di configurazione di directory (directory.xml) (a pagina 53).
3. Importazione del file di configurazione di directory e creazione della directory (a pagina 156).

Nota: quando si utilizza SiteMinder, verificare di avere applicato lo schema di Policy Store prima di creare una directory di CA Identity Manager. Per ulteriori informazioni sugli schemi di Policy Store specifici e sulla loro applicazione, consultare la *Guida all'installazione*.

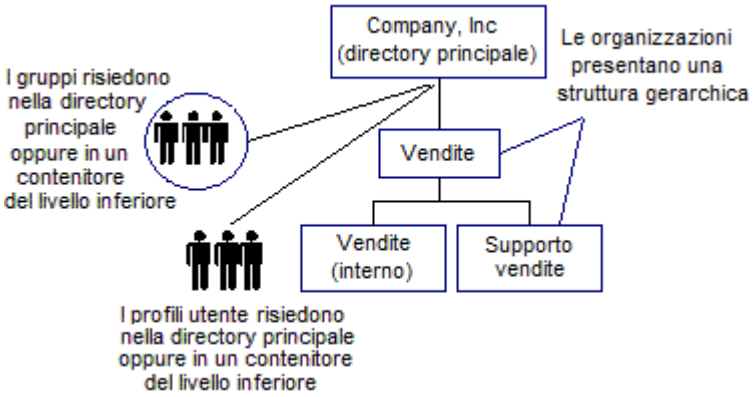
Struttura di directory

CA Identity Manager supporta le strutture di directory seguenti:

- Gerarchico: contiene un'organizzazione padre (root) e organizzazioni secondarie. A loro volta, le organizzazioni secondarie possono avere anch'esse organizzazioni secondarie, creando così una struttura multilivello, come viene mostrato nell'illustrazione seguente:

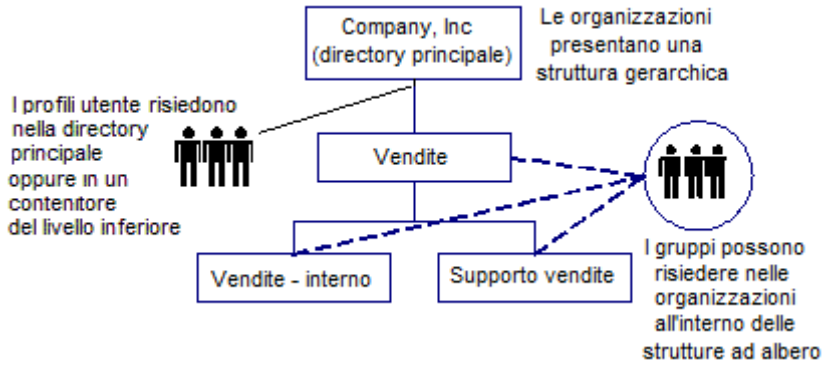


- Flat: l'utente e i gruppi vengono archiviati nella cartella principale di ricerca o in un contenitore a un livello sotto la cartella principale di ricerca. Le organizzazioni presentano una struttura gerarchica, come viene mostrato nella seguente illustrazione di una struttura di directory flat:



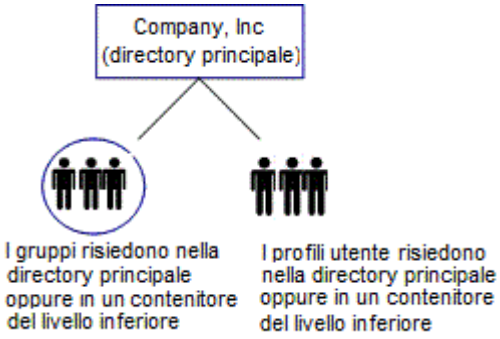
Per facilitare la gestione degli utenti e la delega in strutture di directory flat, gli utenti e i gruppi appartengono a organizzazioni logiche. L'organizzazione logica viene archiviata come attributo nei profili di utente e gruppi.

- Utente flat: le organizzazioni e i gruppi vengono archiviati in modo gerarchico, ma gli utenti vengono archiviati nella cartella principale di ricerca o in un contenitore a un livello sotto la cartella principale di ricerca. Nel diagramma seguente viene mostrata l'illustrazione di una struttura di directory utente flat:



Nelle strutture di directory utente flat, gli utenti appartengono a organizzazioni logiche. L'organizzazione logica di un utente viene archiviata come attributo in un profilo utente.

- Nessuna organizzazione: la directory non include organizzazioni. Gli utenti e i gruppi vengono archiviati nella root di ricerca o in un contenitore un livello sotto la root di ricerca. Nell'illustrazione seguente viene mostrata una struttura di directory senza organizzazioni:



Nota: una directory può contenere più di un tipo di struttura. Ad esempio, è possibile archiviare i profili utenti in una struttura di tipo flat in una parte della directory e in modo gerarchico in un altra. Per supportare una struttura di directory ibrida, creare più ambienti di CA Identity Manager.

File di configurazione di directory

Per descrivere la struttura di una directory utente a CA Identity Manager, creare un file di configurazione di directory.

Il file di configurazione di directory contiene una o più delle sezioni seguenti:

Informazioni sulla directory di CA Identity Manager

Contiene informazioni sulla directory di CA Identity Manager.

Nota: non modificare le informazioni in questa sezione. CA Identity Manager richiede di fornire queste informazioni quando si crea una directory di CA Identity Manager nella console di gestione.

Attribute Validation (Convalida dell'attributo)

Definisce le regole di convalida che si applicano alla directory di CA Identity Manager.

Provider Information (Informazioni sul provider)

Descrive l'archivio utenti che CA Identity Manager gestisce.

Directory Search Information (Informazioni sulla ricerca nella directory)

Consente di specificare la modalità di ricerca di CA Identity Manager nell'archivio utenti.

User Object (Oggetto utente)

Descrive come gli utenti vengono archiviati nell'archivio utenti e come questo viene rappresentato in CA Identity Manager.

Group Object (Oggetto gruppo)

Descrive come i gruppi vengono archiviati nell'archivio utenti e come questo viene rappresentato in CA Identity Manager.

Organization Object (Oggetto organizzazione)

Descrive come le organizzazioni vengono archiviate e come vengono rappresentate in CA Identity Manager. La sezione Organization Object (Oggetto organizzazione) fornisce dettagli solo quando l'archivio utenti include organizzazioni.

Oggetto Self-Subscribing

Configura il supporto per i gruppi a cui gli utenti self-service possono unirsi.

Comportamento dei gruppi di directory

Specifica se la directory di CA Identity Manager supporta gruppi dinamici e nidificati.

Per creare un file di configurazione di directory, modificare un modello di configurazione.

Selezione di un modello di configurazione di directory

CA Identity Manager fornisce modelli di configurazione di directory che supportano tipi di directory e strutture diversi. Per creare una directory di CA Identity Manager, modificare il modello che corrisponde più da vicino alla propria struttura di directory.

I modelli descritti nella tabella seguente vengono installati con gli strumenti di amministrazione:

admin_tools\directoryTemplates*directory_type*\

Gli Strumenti di amministrazione sono ora installati nelle seguenti posizioni predefinite:

- **Windows:** C:\Programmi\CA\Identity Manager\IAM Suite\Identity Manager\tools
- **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

I tipi di directory e i modelli di configurazione corrispondenti vengono mostrati nella tabella seguente:

Tipo di directory	Template
Directory LDAP Active Directory (ADSI) con una struttura gerarchica	ActiveDirectory\directory.xml
Directory Microsoft ADAM con una struttura gerarchica	ADAM\directory.xml
Directory IBM Directory Server con una struttura gerarchica	IBMDirectoryServer\directory.xml
Directory utente Novell eDirectory con una struttura gerarchica	eDirectory\directory.xml
Directory Oracle Internet Directory con una struttura gerarchica	OracleInternetDirectory\directory.xml
Directory LDAP del sistema Sun Java (SunOne o iPlanet) con una struttura gerarchica	IPlanetHierarchical\directory.xml
Directory LDAP del sistema Sun Java (SunOne o iPlanet) con una struttura flat	IPlanetFlat\directory.xml
Directory LDAP del sistema Sun Java (SunOne o iPlanet) che non include organizzazioni.	IPlanetNoOrganizations\directory.xml
Archivio utenti di CA Directory con una struttura gerarchica	eTrustDirectory\directory.xml
Directory di provisioning Questo modello configura la directory di provisioning per un ambiente di CA Identity Manager. **Nota:** è possibile utilizzare questo modello di configurazione così come è installato. Non è necessario modificare questo modello.	ProvisioningServer\directory.xml

Tipo di directory	Template
Directory personalizzata	Utilizzare il modello più simile alla propria directory.

Copiare il modello di configurazione in una directory nuova o salvarlo con un nome diverso per impedire che venga sovrascritto.

Descrizione di una directory utente in CA Identity Manager

Per gestire una directory, CA Identity Manager deve comprendere la struttura e il contenuto di una directory. Per descrivere la directory a CA Identity Manager, modificare il file di configurazione di directory (directory.xml) nella directory di modello appropriata.

Il file di configurazione di directory ha le seguenti importanti convenzioni:

- ##: indica i valori necessari.

  Per fornire tutte le informazioni necessarie, individuare tutti i segni di cancelletto doppi (##) e sostituirli con i valori appropriati. Ad esempio, ##DISABLED_STATE indica che si deve fornire un attributo per archiviare lo stato dell'account di un utente.

- @: indica i valori popolati da CA Identity Manager. Non modificare questi valori nel file di configurazione di directory. CA Identity Manager richiede di fornire i valori quando si importa il file di configurazione di directory.

Prima di modificare il file di configurazione di directory, sono necessarie le informazioni seguenti:

- Classi oggetto LDAP per gli oggetti utente, gruppo e organizzazione
- Elenco di attributi nei profili di utente, gruppo e organizzazione

Modifica del file di configurazione di directory

Eseguire i passaggi seguenti per modificare il file di configurazione di directory.

Nota: i passaggi obbligatori vengono indicati.

1. Limitare le dimensioni dei risultati della ricerca (a pagina 58).
2. Modificare gli oggetti gestiti utente, organizzazione o gruppo predefiniti.
3. Modificare le descrizioni di attributo predefinite.

4. Modificare gli attributi noti (a pagina 79). (obbligatorio)

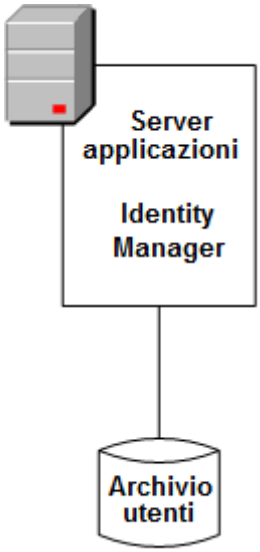
   Gli attributi noti identificano attributi speciali, come ad esempio l'attributo di password, in CA Identity Manager.

5. Configurare CA Identity Manager per la propria struttura di directory (a pagina 86)(obbligatorio).

6. Abilitare gli utenti per la sottoscrizione ai gruppi (a pagina 87).

Connessione alla directory utente

CA Identity Manager si connette a una directory utente per archiviare informazioni, come ad esempio le informazioni relative a un utente, gruppo e organizzazione, come viene mostrato nell'illustrazione seguente:



Una nuova directory o database non sono necessari. Tuttavia, la directory o il database esistente devono risiedere in un sistema che ha un nome di dominio completo (FQDN).

Per visualizzare un elenco di tipi di directory e database, consultare la matrice di supporto di CA Identity Manager nel sito Web del Supporto di CA.

Si configura una connessione all'archivio utenti quando si crea una directory di CA Identity Manager nella console di gestione.

Se si esporta la configurazione di directory dopo avere creato una directory di CA Identity Manager, le informazioni di connessione della directory utente vengono visualizzate Provider dei file di configurazione di directory.

Elemento Provider

Le informazioni di configurazione vengono archiviate nell'elemento Provider e nei relativi elementi secondari nel file directory.xml.

Nota: se si sta creando una directory di CA Identity Manager, non è necessario fornire informazioni di connessione sulla directory nel file directory.xml. Si forniscono informazioni di connessione nella procedura guidata di creazione della directory di CA Identity Manager nella console di gestione. Modificare l'elemento Provider solo per gli aggiornamenti.

L'elemento Provider include gli elementi secondari seguenti:

LDAP

Descrive la directory utente a cui ci si sta connettendo.

Credentials (Credenziali)

Fornisce il nome utente e la password per accedere all'archivio utenti LDAP.

Connessione

Fornisce il nome host e la porta del computer in cui si trova l'archivio utenti.

Provisioning Domain (Dominio di provisioning)

Definisce il dominio di provisioning gestito da CA Identity Manager (solo per gli utenti provisioning).

Un elemento Provider completo somiglia al codice seguente:

```
<Provider type="LDAP" userdirectory="@SMDirName">
   <LDAP searchroot="@SMDirSearchRoot" secure="@SMDirSecure" />
   <Credentials user="@SMDirUser"
     cleartext="true">@SMDirPassword</Credentials>
   <Connection host="@SMDirHost" port="@SMDirPort" />
   <eTrustAdmin domain="@SMDirETrustAdminDomain" />
</Provider>
```

L'elemento Provider include i parametri seguenti:

type

Specifica il tipo di database. Per tutti gli archivi utente LDAP, specificare LDAP (valore predefinito).

userdirectory

Specifica il nome della connessione della directory utente.

Nota: non specificare un nome per la connessione della directory utente nel file directory.xml. CA Identity Manager richiede di fornire il nome quando si crea la directory di CA Identity Manager nella console di gestione.

Nota: i parametri sono facoltativi.

Elemento secondario LDAP

L'elemento secondario LDAP include i parametri seguenti:

searchroot

Consente di specificare la posizione in una directory LDAP che serve come il punto di partenza per la directory, solitamente un'organizzazione (o) o un'unità organizzativa (ou).

secure

Questa opzione impone una connessione SSL (Secure Sockets Layer) alla directory utente LDAP nel modo seguente:

- True: CA Identity Manager utilizza una connessione sicura.
- False: CA Identity Manager si connette alla directory utente senza SSL (impostazione predefinita).

Nota: i parametri sono facoltativi.

Elemento secondario Credentials (Credenziali)

Per connettersi a una directory LDAP, CA Identity Manager deve fornire credenziali valide. Le credenziali vengono definite nell'elemento secondario Credentials (Credenziali) e somigliano al codice seguente:

```
<Credentials user="@SMDirUser" cleartext="true">
  "MyPassword"
</Credentials>
```

Se non si specifica una password nell'elemento secondario Credentials (Credenziali), quando si crea la directory di CA Identity Manager nella console di gestione, viene richiesta la password.

Nota: si consiglia di specificare la password nella console di gestione.

Se si specifica la password nella console di gestione, CA Identity Manager esegue la crittografia della password. Se non si desidera che la password venga visualizzata in testo non crittografato, crittografarla utilizzando lo strumento di password installato con CA Identity Manager.

Nota: è possibile specificare solo un set di credenziali. Se si definiscono più directory, come descritto nella sezione Elemento secondario di connessione, le credenziali specificate devono essere applicate a tutte le directory.

L'elemento secondario Credentials (Credenziali) include i parametri seguenti:

utente

Specifica l'ID di accesso per un account che può accedere alla directory.

Per gli utenti di provisioning, l'account utente specificato deve avere il profilo di Amministratore di dominio o un set equivalente di privilegi nel server di provisioning.

Nota: non specificare un valore per il parametro utente nel file directory.xml. CA Identity Manager richiede di fornire l'ID di accesso quando si crea la directory di CA Identity Manager nella console di gestione.

cleartext

Determina se la password viene mostrata con testo non crittografato nel file directory.xml, nel modo seguente:

- True: la password viene mostrata con testo non crittografato.
- False: la password è crittografata (impostazione predefinita).

Nota: i parametri sono facoltativi.

Elemento secondario di connessione

L'elemento secondario Connessione descrive la posizione dell'archivio utenti gestito da CA Identity Manager. Questo elemento secondario include i parametri seguenti:

host

Consente di specificare il nome host o l'indirizzo IP del sistema sul quale si trova la directory utente.

Nota: se il sistema di connessione ha un indirizzo IPv6, racchiudere l'indirizzo IP tra parentesi ([ ]) nel modo seguente:

<Connection host="[2::9255:214:22ff:fe72:525a]" port="20389"

failover="[2::9255:214:22ff:fe72:525a]:20389"/>

porta

Specifica il numero di porta della directory utente.

failover

Specifica il nome host e l'indirizzo IP del sistema in cui si trovano archivi utenti ridondanti, nel caso il sistema primario non sia disponibile. Quando il sistema primario diventa di nuovo disponibile, il sistema di failover continua a essere utilizzato. Per tornare a utilizzare il sistema primario, riavviare il sistema secondario. Se sono elencati più server, CA Identity Manager tenta di connettersi ai sistemi secondo l'ordine elencato.

Specificare il nome host e l'indirizzo IP nell'attributo di failover in un elenco *separato da spazi,* nel modo seguente:

failover="IPaddress:port IPaddress:port"

Ad esempio:

<Connection host="123.456.789.001" port="20389"

failover="123.456.789.002:20389 123.456.789.003:20389"/>

Nota: la porta 20389 è la porta predefinita per il server di provisioning.

Nota: i parametri sono facoltativi.

Elemento secondario Provisioning

Se l'ambiente di CA Identity Manager include il provisioning, definire il dominio di provisioning nel modo seguente:

```
<eTrustadmin domain="@SMDirProvisioningDomain" />
```

L'elemento secondario Provisioning include il parametro seguente:

domain

Contiene il nome del dominio di provisioning gestito da CA Identity Manager.

Quando si crea la directory di CA Identity Manager nella console di gestione, viene richiesto di fornire il nome del dominio. Specificare un valore per il parametro di dominio nel file di configurazione di directory (directory.xml).

Parametri di ricerca nella directory

Nell'elemento DirectorySearch, è possibile impostare i parametri di ricerca seguenti:

maxrows

Consente di specificare il numero massimo di oggetti che CA Identity Manager può restituire durante una ricerca in una directory utente. Quando il numero degli oggetti supera il limite, viene visualizzato un errore.

Impostando un valore per il parametro maxrows, è possibile sovrascrivere le impostazioni nella directory LDAP che limitano i risultati della ricerca. Quando si applicano impostazioni in conflitto, il server LDAP utilizza l'impostazione più bassa.

Nota: il parametro maxrows non limita il numero di oggetti che vengono visualizzati nella schermata delle attività di CA Identity Manager. Per configurare le impostazioni di visualizzazione, modificare la definizione della schermata elenco nella console utente di CA Identity Manager. Per istruzioni, consultare la *User Console Design Guide*.

maxpagesize

Specifica il numero di oggetti che può essere restituito in una singola ricerca. Se il numero degli oggetti supera la dimensione della pagina, CA Identity Manager esegue ricerche multiple.

Tenere presenti i punti seguenti quando si specifica maxpagesize:

- Per utilizzare l'opzione maxpagesize, l'archivio utenti gestito da CA Identity Manager deve supportare il paging. Per alcuni tipi di archivio utenti è necessaria un'ulteriore configurazione per consentire il paging. Per ulteriori informazioni, consultare la sezione Miglioramento delle prestazioni per ricerche di dimensioni elevate (a pagina 96).
- Se l'archivio utenti non supporta il paging ed è specificato un valore maxrows, CA Identity Manager utilizza solo il valore maxrows per controllare le dimensioni della ricerca.

timeout

Determina il numero massimo di secondi che CA Identity Manager utilizza per eseguire una ricerca in una directory prima di terminarla.

Nota: l'elemento DirectorySearch è facoltativo. Tuttavia, se la directory supporta il paging (a pagina 96), si consiglia di specificare l'elemento DirectorySearch.

Ulteriori informazioni:

Miglioramento delle prestazioni di ricerca nella directory (a pagina 95)
Miglioramento delle prestazioni per ricerche di dimensioni elevate (a pagina 96)

Descrizioni degli oggetti gestiti utenti, gruppi e organizzazioni

In CA Identity Manager, si gestiscono i tipi seguenti di oggetti che corrispondono alle voci di una directory utente:

Utenti

Rappresenta gli utenti di un'azienda. Un utente appartiene a una singola organizzazione.

Gruppi

Rappresenta le associazioni di utenti che hanno in comune qualcosa.

Organizzazioni

Rappresentano le unità aziendali. Le organizzazioni contengono dettagli quali utenti, gruppi e altre organizzazioni.

Una descrizione di oggetto contiene le informazioni seguenti:

- Informazioni sull'oggetto (a pagina 116), come la classe oggetto LDAP e il contenitore in cui gli oggetti vengono archiviati.
- Gli attributi che archiviano le informazioni relative a una voce (a pagina 121). Ad esempio, l'attributo del cercapersone archivia un numero di cercapersone.

Nota: un ambiente di CA Identity Manager supporta solo un tipo di oggetto utente, gruppo e organizzazione. Ad esempio, tutti gli oggetti utente hanno la stessa classe oggetto.

Descrizioni oggetto gestito

Un oggetto gestito viene descritto specificando le informazioni relative all'oggetto nelle sezioni User Object (Oggetto utente), Group Object (Oggetto gruppo) e Organization Object (Oggetto organizzazione) del file di configurazione di directory.

Nota: quando si utilizza il modello di configurazione (file directory.xml), la sezione Organization Object (Oggetto organizzazione) non è disponibile per quelle directory utente che non supportano le organizzazioni.

Ciascuna di queste sezioni contiene gli elementi ImsManagedObject, come nell'esempio seguente:

```
<ImsManagedObject name="User" description="My Users"
objectclass="top,person,organizationalperson,inetorgperson" objecttype="USER">
```

Facoltativamente, l'elemento ImsManagedObject può includere un elemento Contenitore, come nell'esempio seguente:

```
<Container objectclass="top,organizationalUnit" attribute="ou" value="people" />
```

Specificare le informazioni sull'oggetto

Le informazioni sull'oggetto vengono specificate fornendo valori per vari parametri.

Procedere come descritto di seguito:

1. Individuare l'elemento ImsManagedObject nella sezione User Object (Oggetto utente), Organization Object (Oggetto organizzazione) o Group Object (Oggetto gruppo).
2. Fornire i valori per i parametri seguenti:

   nome

   Specifica il nome univoco per l'oggetto gestito.

   Nota: questo parametro è obbligatorio.

   descrizione

   Contiene una descrizione dell'oggetto gestito.

   objectclass

   Specifica il nome della classe di oggetto LDAP per il tipo di oggetto (utente, gruppo o organizzazione). La classe oggetto determina l'elenco degli attributi disponibili per un oggetto.

   Se gli attributi da più classi oggetto si applicano a un tipo di oggetto, elencare le classi di oggetto in un elenco delimitato da virgole. Ad esempio, se un oggetto contiene attributi dalle classi oggetto person, organizationalperson e inetorgperson, aggiungere queste classi di oggetto come segue:

   objectclass="top,person,organizationalperson,inetorgperson"

   Ciascuna directory LDAP include un set di classi oggetto predefinite. Consultare la documentazione del server di directory per informazioni sulle classi oggetto predefinite.

   Nota: questo parametro è obbligatorio.

   objecttype

   Specifica il tipo di oggetto gestito. Di seguito sono elencati i valori validi:

   - Utente
   - Organizzazione
   - Gruppo

   Nota: questo parametro è obbligatorio.

   maxrows

   Consente di specificare il numero massimo di oggetti che CA Identity Manager può restituire durante una ricerca in una directory utente. Quando il numero degli oggetti supera il limite, viene visualizzato un errore.

Impostando un valore per il parametro maxrows, è possibile sovrascrivere le impostazioni nella directory LDAP che limitano i risultati della ricerca. Quando si applicano impostazioni in conflitto, il server LDAP utilizza l'impostazione più bassa.

Nota: il parametro maxrows non limita il numero di oggetti che vengono visualizzati nella schermata delle attività di CA Identity Manager. Per configurare le impostazioni di visualizzazione, modificare la definizione della schermata elenco nella console utente di CA Identity Manager. Per istruzioni, consultare la *User Console Design Guide*.

maxpagesize

Specifica il numero di oggetti che può essere restituito in una singola ricerca. Se il numero degli oggetti supera la dimensione della pagina, CA Identity Manager esegue ricerche multiple.

Prendere nota dei punti seguenti quando si specificano le dimensioni della pagina di ricerca:

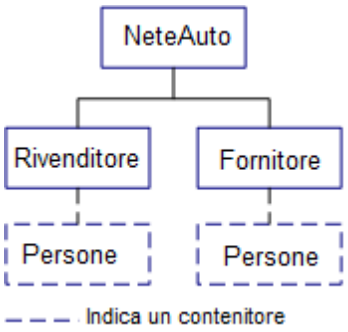
- Per utilizzare l'opzione Search Page Size (Dimensioni pagina di ricerca), l'archivio utenti che CA Identity Manager gestisce deve supportare il paging. Per alcuni tipi di archivio utenti è necessaria un'ulteriore configurazione per consentire il paging. Per ulteriori informazioni, consultare la sezione Miglioramento delle prestazioni di ricerca (a pagina 96).
- Se l'archivio utenti non supporta il paging ed è specificato un valore maxrows, CA Identity Manager utilizza solo il valore maxrows per controllare le dimensioni della ricerca.

3. Se lo si desidera, è specificare informazioni sui contenitori.

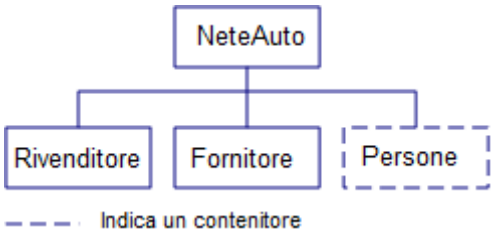
Contenitori

Per semplificare l'amministrazione, è possibile raggruppare oggetti di un tipo specifico in un contenitore. Quando si specifica un contenitore nel file di configurazione di directory, CA Identity Manager gestisce solo le voci nel contenitore. Ad esempio, se si specifica un contenitore utente chiamato People, CA Identity Manager gestisce gli utenti nel contenitore People, come viene mostrato nelle illustrazioni seguenti:

- Directory gerarchica



- Directory flat



In questi esempi, tutti gli utenti esistono nei contenitori People.

Quando si specifica un contenitore, prendere nota dei punti seguenti:

- Se non esiste nessun contenitore in un'organizzazione, CA Identity Manager crea il contenitore non appena viene aggiunta la prima voce. Per una directory gerarchica, CA Identity Manager crea il contenitore nell'organizzazione in cui viene aggiunta la voce. Nel caso di directory flat e directory che non supportano le organizzazioni, CA Identity Manager crea il contenitore sotto la cartella principale di ricerca, specificata al momento di creare la directory di CA Identity Manager.
- CA Identity Manager ignora le voci che non si trovano nel contenitore specificato. Ad esempio, se si specifica il contenitore People, non sarà possibile gestire gli utenti che si trovano al di fuori di questo contenitore.

  Nota: per gestire gli utenti che non si trovano nel contenitore specificato, è possibile creare un altro ambiente di CA Identity Manager.

Contenitori e attributi noti

Gli attributi noti sono attributi che hanno un significato speciale in CA Identity Manager. Quando CA Identity Manager gestisce un archivio utenti che include dei contenitori, gli attributi noti seguenti identificano le informazioni riguardanti il contenitore:

%ORG_MEMBERSHIP%

Identifica l'attributo che archivia il nome completo (DN) del contenitore.

Ad esempio, il nome completo assomiglia a:

ou=People, ou=Employee, ou=NeteAuto, dc=security, dc=com

%ORG_MEMBERSHIP_NAME%

Identifica l'attributo che memorizza il nome descrittivo dell'attributo.

Ad esempio, il nome descrittivo del contenitore nell'esempio precedente è People.

Questi attributi noti vengono visualizzati nelle descrizioni dell'attributo nelle sezioni User Object (Oggetto utente) o Group Object (Oggetto gruppo) del file directory.xml, come segue:

```
 <ImsManagedObjectAttr physicalname="someattribute" description="Organization"
displayname="Organization" valuetype="String" required="true"
wellknown="%ORG_MEMBERSHIP%" maxlength="0" permission="WRITEONCE"
searchable="false" />
```

Per le strutture di archivio utenti gerarchiche, viene eseguito il mapping di physicalname e dei parametri noti sull'attributo noto nel modo seguente:

```
<ImsManagedObjectAttr physicalname="%ORG_MEMBERSHIP%" description="Organization"
displayname="Organization" valuetype="String" required="true"
wellknown="%ORG_MEMBERSHIP%" maxlength="0" permission="WRITEONCE"
searchable="false" />
```

L'esempio indica che CA Identity Manager trae automaticamente il DN e il nome descrittivo del contenitore da altre informazioni presenti nel file directory.xml.

Per le strutture di archivio utenti flat, fornire i nomi dell'attributo fisico.

Nota: per ulteriori informazioni, consultare la sezione Descrizione di una struttura di directory utente flat (a pagina 87).

Specificare un contenitore di utenti o gruppi

Eseguire la procedura seguente per specificare un contenitore di utenti o gruppi.

Procedere come descritto di seguito:

1. Individuare l'elemento Contenitore nella sezione User Object (Oggetto utente) o Group Object (Oggetto gruppo).
2. Fornire i valori per i parametri seguenti:

   objectclass

   Determina la classe oggetto LDAP del contenitore in cui vengono creati gli oggetti di un tipo specifico. Ad esempio, il valore predefinito per il contenitore utenti è "top,organizationalUnit", che indica che gli utenti vengono creati in unità organizzative LDAP (ou).

   Quando si gestiscono gruppi dinamici o nidificati, assicurarsi di specificare un objectclass che supporti questi tipi di gruppo (a pagina 89).

   Nota: questo parametro è obbligatorio.

   attribute

   Specifica l'attributo che archivia il nome del contenitore, ad esempio ou.

   L'attributo viene associato al valore per formare il DN relativo del contenitore, come nell'esempio seguente:

   ou=People

   Nota: questo parametro è obbligatorio.

   valore

   Specifica il nome del contenitore.

   Nota: questo parametro è obbligatorio.

Nota: non è possibile specificare contenitori per le organizzazioni.

Descrizioni di attributi

Un attributo memorizza le informazioni riguardanti una voce, come un numero di telefono o un indirizzo. L'attributo di una voce ne determina il profilo.

Nel file di configurazione di directory, gli attributi vengono descritti negli elementi ImsManagedObjectAttr. Nelle sezioni User Object (Oggetto utente), Group Object (Oggetto gruppo) e Organization Object (Oggetto organizzazione) del file di configurazione di directory, è possibile eseguire le azioni seguenti:

- Modificare le descrizioni di attributo predefinite per descrivere gli attributi nell'archivio utenti.
- Creare nuove descrizioni di attributi copiando una descrizione esistente e modificando i valori secondo le esigenze.

Per ciascun attributo nei profili utente, gruppo e organizzazione, è presente un elemento ImsManagedObjectAttr. Ad esempio, un elemento ImsManagedObjectAttr viene descritto come un ID utente.

Un elemento ImsManagedObjectAttr somiglia al codice seguente:

```
<ImsManagedObjectAttr physicalname="uid" displayname="User ID" description="User
ID" valuetype="String" required="true" multivalued="false" wellknown="%USER_ID%"
maxlength="0" />
```

L'elemento ImsManagedObjectAttr ha i parametri seguenti:

physicalname

Questo parametro deve contenere uno degli elementi seguenti:

- Il nome dell'attributo LDAP in cui viene memorizzato il valore di profilo. Ad esempio, l'ID utente viene memorizzato nell'attributo uid nella directory utente.

  Nota: per migliorare le prestazioni, indicizzare gli attributi LDAP utilizzati nelle query di ricerca nella console utente.

- Un attributo noto (a pagina 79). Quando si fornisce un attributo noto, CA Identity Manager calcola il valore automaticamente. Ad esempio, specificando l'attributo noto %ORG_MEMBERSHIP%, CA Identity Manager determina l'organizzazione a cui appartiene la voce, in base al DN di una voce.

descrizione

Contiene la descrizione dell'attributo

displayname

Specifica un nome univoco per l'attributo.

Nella console utente, il nome visualizzato viene mostrato nell'elenco degli attributi disponibili per essere aggiunti a una schermata di attività. Questo parametro è obbligatorio.

Nota: non modificare il nome visualizzato di un attributo nel file di configurazione di directory (directory.xml). Per modificare il nome dell'attributo su una schermata di attività, è possibile specificare un'etichetta per l'attributo nella definizione della schermata di attività. Per ulteriori informazioni, consultare la *Guida per l'amministratore*.

valuetype

Specifica tipo di dati dell'attributo. Di seguito sono elencati i valori validi:

Stringa

Il valore può essere qualsiasi stringa.

Questo è il valore predefinito.

Numero intero

Il valore deve essere un numero intero.

Nota: l'attributo numero intero non supporta numeri decimali.

Numero

Il valore deve essere un numero intero. L'opzione Numero supporta numeri decimali.

Data

Il valore deve trasformarsi in una data valida secondo il modello:

MM/dd/yyyy

ISODate

Il valore deve trasformarsi in una data valida secondo il modello yyyy-MM-dd.

UnicenterDate

Il valore deve trasformarsi in una data valida secondo il modello YYYYYYYDDD dove:

YYYYYYY è una rappresentazione di sette numeri di un anno che inizia con tre zero. Ad esempio: 0002008

DDD è una rappresentazione di tre numeri per il giorno che inizia con degli zero, a seconda delle esigenze. I valori validi sono compresi tra 001 e 366.

Strutturato

Questo tipo di attributo consiste di dati strutturati che abilitano un valore di attributo singolo per memorizzare più valori relativi. Ad esempio, un attributo strutturato contiene valori come Nome, Cognome e Indirizzo e-mail.

Alcuni tipi di endpoint utilizzano questi attributi ma vengono gestiti mediante CA Identity Manager.

Nota: CA Identity Manager può visualizzare attributi strutturati in una tabella nella console utente. Quando gli utenti modificano dei valori nella tabella, questi vengono memorizzati nell'archivio utenti, propagandosi all'endpoint. Per ulteriori informazioni sulla visualizzazione degli attributi multuivalore, consultare la *Guida per l'amministratore*.

obbligatorio

Indica se l'attributo è obbligatorio, nel modo seguente:

- True: l'attributo è obbligatorio.
- False: l'attributo è facoltativo (impostazione predefinita).

Nota: se un attributo è obbligatorio per un server di directory LDAP, impostare il parametro obbligatorio su True.

multivalore

Indica se l'attributo può avere più valori. Ad esempio, l'attributo di appartenenza al gruppo ha più valori per memorizzare il DN utente di ciascun membro del gruppo. Di seguito sono elencati i valori validi:

- True: l'attributo può avere più valori.
- False: l'attributo può avere solamente un valore singolo (impostazione predefinita).

Importante. Gli attributi Appartenenza al gruppo e Ruoli di amministrazione nella definizione dell'oggetto utente devono avere più valori.

noto

Definisce il nome dell'attributo noto.

Gli attributi noti hanno un significato specifico in CA Identity Manager (a pagina 79). Vengono identificati nella sintassi:

%ATTRIBUTENAME%

maxlength

Definisce la lunghezza massima che il valore di un attributo può avere. Impostare il parametro maxlength a 0 per specificare una lunghezza illimitata.

Nota: questo parametro è obbligatorio.

permission

Indica se è possibile modificare il valore di un attributo in una schermata di attività. Di seguito sono elencati i valori validi:

READONLY

Il valore viene visualizzato ma non può essere modificato.

WRITEONCE

Non è possibile modificare il valore una volta che l'oggetto è stato creato. Ad esempio, non è possibile modificare un ID utente dopo che l'utente è stato creato.

READWRITE

È possibile modificare il valore (impostazione predefinita).

nascosto

Indica se un attributo viene visualizzato nei moduli delle attività di CA Identity Manager. Di seguito sono elencati i valori validi:

- True: l'attributo non viene visualizzato dagli utenti.
- False: l'attributo viene visualizzato dagli utenti (impostazione predefinita).

Gli attributi logici utilizzano attributi nascosti.

Nota: per ulteriori informazioni, consultare la *Programming Guide for Java*.

sistema

Specifica solo gli attributi utilizzati da CA Identity Manager. Gli utenti della console utente non devono modificare gli attributi. Di seguito sono elencati i valori validi:

- True: gli utenti non possono modificare l'attributo. L'attributo è nascosto nell'interfaccia utente di CA Identity Manager.
- False: gli utenti possono modificare questo attributo. L'attributo è disponibile per essere aggiunto alle schermate delle attività nell'interfaccia utente di CA Identity Manager. (impostazione predefinita).

validationruleset

Associa un set di regole di convalida all'attributo.

Verificare che il set di regole di convalida specificato sia definito in un elemento ValidationRuleSet nel file di configurazione di directory.

objectclass

Indica la classe ausiliaria LDAP di un attributo utente, gruppo o organizzazione quando l'attributo non è parte della classe oggetto primaria specificata nell'elemento ImsManagedObject.

Ad esempio, supporre che la classe oggetto primario per gli utenti sia top, person e organizationalperson, che definisce gli attributi utente seguenti:

- nome comune (cn)
- cognome (sn)
- ID utente (uid)
- password (userPassword)

Per includere l'attributo employeeID, che viene definito nella classe ausiliaria Employee, si aggiunge la descrizione di attributo seguente:

```
<ImsManagedObjectAttr physicalname="employeeID" displayname="Employee ID"
description="Employee ID" valuetype="String" required="true" multivalued="false"
maxlength="0" objectclass="Employee"/>
```

Specificare le descrizioni degli attributi

Le descrizioni degli attributi comprendono i passaggi seguenti:

1. Leggere le sezioni attinenti tra gli argomenti seguenti:
   - Considerazioni su CA Directory (a pagina 77)
   - Considerazioni su Microsoft Active Directory (a pagina 78)
   - Considerazioni su IBM Directory Server (a pagina 78)
   - Considerazioni su Oracle Internet Directory (a pagina 79)
2. Nelle sezioni User Object (Oggetto utente), Group Object (Oggetto gruppo) e Organization Object (Oggetto organizzazione) del file di configurazione di directory, eseguire le azioni seguenti:
   - Modificare le descrizioni di attributo predefinite per descrivere gli attributi della directory.
   - Creare nuove descrizioni di attributi copiando una descrizione esistente e modificando i valori secondo le esigenze.

   Nota: supporre che venga creata una nuova descrizione di attributo e che venga specificato un attributo fisico. Assicurarsi che l'attributo fisico esista nelle classi oggetto specificate per il tipo di oggetto.
3. (Facoltativo) Modificare le impostazioni di visualizzazione (a pagina 74) dell'attributo per evitare la visualizzazione delle informazioni sensibili nella console utente, quali la password o i salari.
4. (Facoltativo) Configurare un ordinamento predefinito.
5. In caso di gestione di una directory con una struttura flat o una struttura utente flat o una directory che esclude le organizzazioni, consultare la sezione Descrizione della struttura della directory utente (a pagina 86).

Gestione degli attributi sensibili

CA Identity Manager fornisce i metodi seguenti per la gestione degli attributi sensibili:

- Classificazioni dei dati per gli attributi

  Le classificazioni dei dati consentono di specificare le proprietà di visualizzazione e crittografia per gli attributi che si trovano nel file di configurazione di directory (directory.xml).

  È possibile definire le classificazioni dei dati che gestiscono attributi sensibili nel modo seguente:

  - Nelle schermate delle attività di CA Identity Manager, visualizzare il valore di un attributo come una serie di asterischi.

    Ad esempio, è possibile visualizzare le password come asterischi invece di visualizzarle come testo semplice (non crittografato).

  - Nella schermata Visualizza attività inoltrate, nascondere il valore attributo.

    Questa opzione consente di nascondere attributi agli amministratori. Ad esempio, è possibile nascondere i dettagli sugli stipendi agli amministratori che visualizzano lo stato dell'attività relativa in CA Identity Manager ma non devono visualizzare i dettagli sugli stipendi.

  - Ignorare certi attributi quando si crea una copia di un oggetto esistente.
  - Crittografia di un attributo

- Stili di campo nelle schermate dei profili di attività

  Se non si desidera modificare un attributo nel file directory.xml, impostare la proprietà di visualizzazione dell'attributo nelle definizioni della schermata in cui viene visualizzato l'attributo sensibile.

  Lo stile di campo consente di visualizzare gli attributi, come ad esempio la password, come una serie di asterischi invece di semplice testo.

  Nota: per ulteriori informazioni sullo stile del campo per gli attributi sensibili, cercare gli stili di campo nella Guida in linea della console utente.

Attributi di classificazione dei dati

L'elemento di classificazione dei dati fornisce un modo di associare proprietà aggiuntive a una descrizione di attributo. I valori di questo elemento determinano come CA Identity Manager gestisce l'attributo. Questo elemento supporta i parametri seguenti:

- sensitive

  Consente a CA Identity Manager di visualizzare l'attributo come una serie di asterischi (*) nella schermata Visualizza attività inoltrate. Questo parametro impedisce a valori vecchi e nuovi dell'attributo di essere visualizzati in testo non crittografato nelle schermata Visualizza attività inoltrate.

  In aggiunta, se si crea una copia di un utente esistente nella console utente, questo parametro impedisce all'attributo di essere copiato nel nuovo utente.

- vst_hide

  Nasconde l'attributo nella schermata Dettagli evento della scheda Visualizza attività inoltrate. A differenza degli attributi sensibili, che vengono visualizzati come asterischi, gli attributi vst_hidden non vengono visualizzati.

  È possibile utilizzare questo parametro per impedire che eventuali modifiche a un attributo, ad esempio relative ai dettagli sullo stipendio, vengano visualizzate in Visualizza attività inoltrate.

- ignore_on_copy

  Consente a CA Identity Manager di ignorare un attributo quando un amministratore crea una copia di un oggetto nella console utente. Ad esempio, supporre di avere specificato ignore_on_copy per l'attributo di password su un oggetto utente. Quando si copia un profilo utente, CA Identity Manager non applica la password dell'utente attuale al nuovo profilo utente.

- AttributeLevelEncrypt

  Consente di crittografare i valori di attributo quando vengono archiviati nell'archivio utenti. Se CA Identity Manager è abilitato per FIPS 140-2, CA Identity Manager utilizza la crittografia RC2 o la crittografia FIPS 140-2.

  Per ulteriori informazioni sulla conformità FIPS 140-2 in CA Identity Manager, consultare la *Guida alla configurazione*.

  Gli attributi vengono visualizzati in testo non crittografato durante il runtime.

  Nota: per impedire agli attributi di venire visualizzati in testo non crittografato nelle schermate, è possibile aggiungere un elemento di classificazione di dati sensibile agli attributi crittografati. Per ulteriori informazioni, consultare la sezione Aggiunta della crittografia a livello di attributo (a pagina 75).

- PreviouslyEncrypted

  Consente a CA Identity Manager di individuare e decrittografare qualsiasi valore crittografato nell'attributo quando accede all'oggetto nell'archivio utenti.

  Si utilizza questa classificazione dei dati per decrittografare qualsiasi valore precedentemente crittografato.

  Il valore di testo non crittografato viene salvato nell'archivio quando si salva l'oggetto.

Configurazione di attributi di classificazione dei dati

Procedere come descritto di seguito:

1. Individuare l'attributo nel file di configurazione di directory.
2. Dopo la descrizione dell'attributo, aggiungere l'attributo seguente:

   <DataClassification name="*parameter*">

   parameter

   Rappresenta uno dei parametri seguenti:

   sensitive

   vst_hide

   ignore_on_copy

   AttributeLevelEncrypt

   PreviouslyEncrypted

   Ad esempio, una descrizione di attributo che include l'attributo di classificazione di dati vst_hide assomiglia al codice seguente:

```
<ImsManagedObjectAttr physicalname="salary" displayname="Salary"
description="salary" valuetype="String" required="false" multivalued="false"
maxlength="0">
    <DataClassification name="vst_hide"/>
```

Crittografia a livello di attributo

È possibile crittografare un attributo nell'archivio utenti specificando una classificazione dei dati AttributeLevelEncypt per quell'attributo nel file di configurazione di directory (directory.xml). Quando la crittografia a livello di attributo viene abilitata, CA Identity Manager crittografa il valore di quell'attributo prima di archiviarlo nell'archivio utenti. L'attributo viene visualizzato come testo non crittografato nella console utente.

Nota: per impedire agli attributi di venire visualizzati in testo non crittografato nelle schermate, è possibile aggiungere un elemento di classificazione di dati sensibile agli attributi crittografati. Per ulteriori informazioni, consultare la sezione Aggiunta della crittografia a livello di attributo (a pagina 75).

Se il supporto FIPS 140-2 è abilitato, l'attributo viene crittografato mediante la crittografia RC2 o la crittografia FIPS 140-2.

Prima di implementare la crittografia a livello di attributo, prendere nota dei punti seguenti:

- CA Identity Manager non è in grado di trovare attributi crittografati in una ricerca.

  Supporre che un attributo crittografato sia aggiunto a un criterio di membro, amministratore, titolare o a un criterio di identità. CA Identity Manager non è in grado di risolvere il criterio correttamente perché non può cercare l'attributo.

  Considerare di impostare l'attributo su searchable="false" nel file directory.xml—Ad esempio:

  <ImsManagedObjectAttr physicalname="title" description="Title" displayname="Title" valuetype="String" maxlength="0" searchable="false">

  <DataClassification name="AttributeLevelEncrypt"/>

  </ImsManagedObjectAttr>

- Se CA Identity Manager utilizza un archivio utenti condiviso e una directory di provisioning, è necessario non crittografare gli attributi del server di provisioning.
- Non abilitare AttributeLevelEncrypt per le password utente negli ambienti che soddisfano i criteri seguenti:
  - l'inclusione dell'integrazione con CA SiteMinder e
  - l'archiviazione degli utenti in un database relazionale

  Quando CA Identity Manager si integra con CA SiteMinder, le password crittografate causano degli errori quando i nuovi utenti provano ad accedere, immettendo le password con testo non crittografato.
- Se si abilita la crittografia a livello di attributo per un archivio utenti utilizzato da applicazioni diverse da CA Identity Manager, le altre applicazioni non potranno utilizzare l'attributo crittografato.

Aggiunta della crittografia a livello di attributo

Supporre di avere aggiunto una crittografia a livello di attributo a una directory di CA Identity Manager. CA Identity Manager esegue automaticamente la crittografia dei valori dell'attributo di testo non crittografato quando si salva l'oggetto associato all'attributo. Ad esempio, se si crittografa l'attributo di password, la password viene crittografata al momento di salvare il profilo dell'utente.

Nota: per crittografare il valore dell'attributo, l'attività che si utilizza per salvare l'oggetto deve includere l'attributo. Per crittografare l'attributo di password nell'esempio precedente, assicurarsi che il campo Password venga aggiunto all'attività che si utilizza per salvare l'oggetto, come ad esempio l'attività Modifica utente.

Tutti i nuovi oggetti vengono creati con valori crittografati nell'archivio utenti.

Procedere come descritto di seguito:

1. Completare una delle seguenti attività:
   - Creare una directory di CA Identity Manager
   - Aggiornare una directory esistente esportando le impostazioni della directory.
2. Aggiungere gli attributi di classificazione dei dati seguenti all'attributo che si desidera crittografare nel file directory.xml:

   AttributeLevelEncrypt

   Mantiene il valore dell'attributo in un modulo crittografato nell'archivio utenti.

   Maiuscole/minuscole (facoltativo)

   Nasconde il valore dell'attributo nelle schermate di CA Identity Manager. Ad esempio, una password viene visualizzata come asterischi (*).

   Ad esempio:

```
<ImsManagedObjectAttr physicalname="salary"
displayname="Salary" description="salary" valuetype="String"
required="false" multivalued="false" maxlength="0"
searchable="false">
<DataClassification name="AttributeLevelEncrypt"/>
<DataClassification name="sensitive"/>
```

3. Se è stata creata una directory di CA Identity Manager, associare la directory a un ambiente.
4. Per obbligare CA Identity Manager a crittografare immediatamente tutti i valori, modificare tutti gli oggetti mediante l'Utilità di caricamento in blocco.

   Nota: per ulteriori informazioni sull'Utilità di caricamento in blocco, consultare la *Guida per l'amministratore*.

Rimozione della crittografia a livello di attributo

Se si dispone di un attributo crittografato nella directory di CA Identity Manager e questo viene archiviato con il valore di quell'attributo come testo non crittografato, è possibile rimuovere la classificazione dei dati AttributeLevelEncrypt.

Una volta che la classificazione dei dati è stata rimossa, CA Identity Manager smette di crittografare i nuovi valori di attributo. I valori esistenti vengono decrittografati quando si salva l'oggetto associato all'attributo.

Nota: per decrittografare il valore dell'attributo, l'attività che si utilizza per salvare l'oggetto deve includere l'attributo. Ad esempio, per decrittografare una password per un utente esistente, si salva l'oggetto utente con un'attività che include il campo Password, come ad esempio l'attività Modifica utente.

Per obbligare CA Identity Manager a individuare e decrittografare qualsiasi valore crittografato che rimane nell'archivio utenti per l'attributo, è possibile specificare un'altra classificazione dei dati, PreviouslyEncrypted. Il valore di testo non crittografato viene salvato nell'archivio utenti quando si salva l'oggetto.

Nota: l'aggiunta della classificazione dei dati PreviouslyEncrypted consente di aggiungere ulteriore elaborazione a ogni caricamento di oggetti. Per prevenire problemi di prestazioni, si consiglia di aggiungere la classificazione dei dati PreviouslyEncrypted, di caricare e salvare ciascun oggetto associato a quell'attributo e infine rimuovere la classificazione dei dati. Questo metodo converte automaticamente tutti i valori crittografati in testo non crittografato archiviato.

Procedere come descritto di seguito:

1. Esportare le impostazioni della directory per la directory di CA Identity Manager appropriata.
2. Nel file directory.xml, rimuovere la classificazione dei dati, AttributeLevelEncrypt, dagli attributi che si desidera decrittografare.
3. Se si desidera obbligare CA Identity Manager a rimuovere valori precedentemente crittografati, aggiungere l'attributo di classificazione dei dati PreviouslyEncrypted.

   Ad esempio:

   ```
   <ImsManagedObjectAttr physicalname="salary" displayname="Salary"
   description="salary" valuetype="String" required="false" multivalued="false"
   maxlength="0" searchable="false">
   <DataClassification name="PreviouslyEncrypted"/>
   ```

4. Per obbligare CA Identity Manager a decrittografare immediatamente tutti i valori, modificare tutti gli oggetti mediante l'Utilità di caricamento in blocco.

   Nota: per ulteriori informazioni sull'Utilità di caricamento in blocco, consultare la *Guida per l'amministratore*.

Considerazioni su CA Directory

Quando si descrivono gli attributi per un archivio utenti di CA Directory, prendere nota dei punti seguenti:

- I nomi di attributo distinguono tra maiuscole e minuscole.
- L'utilizzo dell'attributo seeAlso come l'attributo che indica un gruppo di sottoscrizione automatica può causare errori quando gli amministratori creano i gruppi.

L'utilizzo dell'attributo di foto come l'attributo che indica lo stato di un account utente (abilitato o disabilitato) può causare errori quando un amministratore crea un utente.

Nota: per informazioni aggiuntive sui requisiti di CA Directory, consultare la documentazione di CA Directory.

Considerazioni su Microsoft Active Directory

Quando si descrivono gli attributi per Active Directory, prendere nota dei punti seguenti:

- La distinzione tra maiuscole/minuscole degli attributi specificata nelle descrizioni degli attributi deve corrispondere a quella degli attributi di Active Directory. Ad esempio, quando si seleziona l'attributo unicodePwd come l'attributo per memorizzare le password degli utenti, specificare unicodePwd (con P maiuscola) nel file di configurazione di directory.
- Per gli oggetti utente e gruppo, assicurarsi di includere l'attributo sAMAccountName.

Considerazioni su IBM Directory Server

Quando si descrivono attributi per una directory utente di IBM Directory Server, consultare le sezioni seguenti:

- Gruppi nelle directory di Directory Server (a pagina 78)
- L'Objectclass "Top" nella descrizione di Organization Object (Oggetto organizzazione) (a pagina 79)

Gruppi nelle directory di Directory Server

IBM Directory Server richiede che i gruppi contengano almeno un membro. Per soddisfare questo requisito, CA Identity Manager aggiunge un *utente fittizio* come membro di un nuovo gruppo quando il gruppo viene creato.

Configurazione di un utente fittizio

Procedere come descritto di seguito:

1. Nella sezione Group Object (Oggetto gruppo) del file di configurazione di directory, individuare gli elementi seguenti:

   ```
   <PropertyDict name="DUMMY_USER">
       <Property name="DUMMY_USER_DN">##DUMMY_USER_DN</Property>
   </PropertyDict>
   ```

   Nota: se questi elementi non esistono nel file di configurazione di directory, aggiungerli esattamente come vengono visualizzati qui.

2. Sostituire ##DUMMY_USER_DN con un DN utente. CA Identity Manager aggiunge questo DN come membro di tutti i nuovi gruppi.

   Nota: se si specifica il DN di un utente esistente, tale utente viene visualizzato come membro di tutti i gruppi di CA Identity Manager. Per impedire che l'*utente fittizio* venga visualizzato come membro del gruppo, specificare un DN che non esiste nella directory.

3. Salvare il file di configurazione di directory.

Objectclass "Top" nella descrizione dell'oggetto organizzazione

Importante. Nella descrizione dell'oggetto organizzazione nel file di configurazione di directory, non includere l'objectclass "Top".

Ad esempio, quando l'objectclass dell'oggetto organizzazione è "Top", organizationalUnit, specificare l'objectclass come segue:

```
<ImsManagedObject name="Organization" description="My Organizations"
objectclass="organizationalUnit" objecttype="ORG">
```

L'inclusione di "Top" può causare dei risultati di ricerca imprevedibili.

Considerazioni su Oracle Internet Directory

Quando si descrivono gli attributi per un archivio utenti Oracle Internet Directory (OID), specificare gli attributi LDAP usando solo lettere minuscole.

Attributi noti per un archivio utenti LDAP

Gli attributi noti hanno un significato speciale in CA Identity Manager. Vengono identificati secondo la sintassi seguente:

%ATTRIBUTENAME%

In questa sintassi, *ATTRIBUTENAME* deve essere in maiuscolo.

Mediante una descrizione di attributo (a pagina 121), viene eseguito il mapping di un attributo noto su un attributo fisico.

Nella descrizione di attributo seguente, viene eseguito il mapping dell'attributo userpassword sull'attributo famoso %PASSWORD% in modo che CA Identity Manager tratti il valore in userpassword come password nel modo seguente:

```
<ImsManagedObjectAttr
        physicalname="userpassword"
        displayname="Password"
        description="Password"
        valuetype="String"
        required="false"
        multivalued="false"
        wellknown="%PASSWORD%"
        maxlength="0" />
```

Alcuni attributi noti sono obbligatori, altri facoltativi.

Attributi utente noti

Di seguito viene riportato un elenco di attributi noti e degli elementi su cui viene eseguito il mapping:

%ADMIN_ROLE_CONSTRAINT%

Esegue il mapping sull'elenco dei ruoli di amministrazione di un amministratore.

L'attributo fisico mappato su %ADMIN_ROLE_CONSTRAINT% deve presentare più valori per potersi adattare a più ruoli.

Si consiglia di indicizzare l'attributo LDAP di cui viene eseguito il mapping su %ADMIN_ROLE_CONSTRAINT%.

%CERTIFICATION_STATUS%

Esegue il mapping sullo stato di certificazione di un utente.

Questo attributo è obbligatorio per utilizzare la funzionalità di certificazione utente.

Nota: per ulteriori informazioni sulla certificazione utente, consultare la *Guida per l'amministratore*.

%DELEGATORS%

Esegue il mapping su un elenco di utenti che hanno delegato elementi di lavoro all'utente attuale.

Questo attributo è obbligatorio per utilizzare la delega. È necessario che l'attributo fisico che ha eseguito il mapping su %DELEGATORS% sia multivalore e in grado di contenere stringhe.

Importante. La modifica diretta di questo campo tramite le attività di CA Identity Manager o uno strumento esterno può avere implicazioni di protezione significative.

%EMAIL%

Esegue il mapping su un indirizzo e-mail di un utente.

Obbligatorio per utilizzare la funzionalità di notifica di posta elettronica.

%ENABLED_STATE%

(Obbligatorio)

Esegue il mapping sullo stato di un utente.

Nota: questo attributo deve corrispondere all'attributo di directory utente Flag disabilitato nella connessione della directory utente di SiteMinder.

%FIRST_NAME%

Esegue il mapping sul nome di un utente.

%FULL_NAME%

Esegue il mapping sul nome e cognome di un utente.

%IDENTITY_POLICY%

Specifica l'elenco dei criteri di identità che sono stati applicati a un account utente e un elenco di ID di criteri di Policy Xpress univoci che hanno eseguito azioni di aggiunta o rimozione sull'oggetto utente.

CA Identity Manager utilizza questo attributo per determinare se l'applicazione di un criterio di identità a un utente è necessaria o meno. Supporre che il criterio abbia l'impostazione Applicare una volta abilitata e che il criterio sia elencato nell'attributo %IDENTITY_POLICY%. CA Identity Manager non applica le modifiche del criterio all'utente.

Nota: per ulteriori informazioni sui criteri di identità, consultare la *Guida per l'amministratore*.

%LAST_CERTIFIED_DATE%

Esegue il mapping sulla data in cui i ruoli vengono certificati a un utente.

L'attributo è obbligatorio per utilizzare la funzionalità di certificazione utente.

Nota: per ulteriori informazioni sulla certificazione utente, consultare la *Guida per l'amministratore*.

%LAST_NAME%

Esegue il mapping sul cognome di un utente.

%MEMBER_OF%

Esegue il mapping sull'elenco dei gruppi di cui l'utente è un membro.

L'attributo fisico mappato su %ADMIN_ROLE_CONSTRAINT% deve disporre di più valori per potersi adattare a più gruppi.

L'utilizzo di questo attributo consente di migliorare i tempi di risposta quando si effettua la ricerca dei gruppi di un utente.

È possibile utilizzare questo attributo con Active Directory o qualsiasi schema di directory che mantiene l'appartenenza al gruppo di un utente nell'oggetto utente.

%ORG_MEMBERSHIP%

(Obbligatorio)

Esegue il mapping sul DN dell'organizzazione a cui l'utente appartiene.

CA Identity Manager utilizza questo attributo noto per determinare la struttura di una directory (a pagina 86).

Questo attributo non è obbligatorio se la directory utente non include organizzazioni.

%ORG_MEMBERSHIP_NAME%

(Obbligatorio)

Esegue il mapping sul nome descrittivo dell'organizzazione in cui esiste il profilo dell'utente.

Questo attributo non è obbligatorio se la directory utente non include organizzazioni.

%PASSWORD%

Esegue il mapping sulla password di un utente.

Questo attributo deve corrispondere all'attributo Password nella connessione della directory utente di SiteMinder.

Nota: il valore dell'attributo %PASSWORD% viene sempre visualizzato come una serie di caratteri asterisco (*) nelle schermate di CA Identity Manager, anche quando l'attributo o il campo non sono impostati per nascondere le password.

%PASSWORD_DATA%

(Obbligatorio per il supporto ai criteri di password)

Specifica l'attributo che tiene traccia delle informazioni sui criteri di password.

Nota: il valore dell'attributo %PASSWORD_DATA% viene sempre visualizzato come una serie di caratteri asterisco (*) nelle schermate di CA Identity Manager, anche quando l'attributo o il campo non sono impostati per nascondere le password.

%PASSWORD_HINT%

(Obbligatorio)

Esegue il mapping su una coppia di domanda e risposta specificata dell'utente. La coppia di domanda e risposta viene utilizzata quando gli utenti dimenticano le password.

Per consentire più coppie di domande e risposte, assicurarsi che l'attributo %PASSWORD_HINT% sia multivalore.

Se si sta utilizzando la funzionalità dei servizi password di SiteMinder per gestire le password, l'attributo Password Hint deve corrispondere all'attributo Challenge/Response nella directory utente di SiteMinder.

Nota: il valore dell'attributo %PASSWORD% viene sempre visualizzato come una serie di caratteri asterisco (*) nelle schermate di CA Identity Manager, anche quando l'attributo o il campo non sono impostati per nascondere le password.

%USER_ID%

(Obbligatorio)

Esegue il mapping sull'ID di un utente.

Attributi di gruppo noti

Gli elementi seguenti rappresentano un elenco di attributi di gruppo noti:

%GROUP_ADMIN_GROUP%

Indica quale attributo memorizza un elenco di gruppi che sono amministratori del gruppo. Ad esempio, se il gruppo 1 è un amministratore del gruppo A, il gruppo 1 viene memorizzato nell'attributo %GROUP_ADMIN_GROUP%.

Nota: se non si specifica un attributo %GROUP_ADMIN_GROUP%, CA Identity Manager memorizza i gruppi di amministratori nell'attributo %GROUP_ADMIN%.

Nota: per aggiungere un gruppo come amministratore di un altro gruppo, consultare la *Guida per l'Amministratore*.

%GROUP_ADMIN%

Indica quale attributo contiene i DN degli amministratori di un gruppo.

L'attributo fisico che ha eseguito il mapping su %GROUP_ADMIN% deve essere multivalore.

%GROUP_DESC%

Indica quale attributo contiene la descrizione di un gruppo.

%GROUP_MEMBERSHIP%

(Obbligatorio)

Indica quale attributo contiene un elenco dei membri di un gruppo.

L'attributo fisico che ha eseguito il mapping su %GROUP_MEMBERSHIP% deve essere multivalore.

L'attributo noto %GROUP_MEMBERSHIP% non è richiesto per le directory utente di provisioning.

%GROUP_NAME%

(Obbligatorio)

Indica quale attributo memorizza un nome di gruppo.

%ORG_MEMBERSHIP%

(Obbligatorio)

Indica quale attributo contiene il DN dell'organizzazione a cui il gruppo appartiene.

CA Identity Manager utilizza questo attributo noto per determinare la struttura della directory (a pagina 86).

Questo attributo non è obbligatorio se la directory utente non include organizzazioni.

%ORG_MEMBERSHIP_NAME%

Indica quale attributo contiene il nome descrittivo dell'organizzazione in cui si trova il gruppo.

Questo attributo non è valido per directory utente che non includono le organizzazioni.

%SELF_SUBSCRIBING%

Indica quale attributo determina se gli utenti possono registrarsi a un gruppo (a pagina 86).

%NESTED_GROUP_MEMBERSHIP%

Indica quale attributo memorizza un elenco di gruppi che sono membri del gruppo. Ad esempio, se il gruppo 1 è un membro del gruppo A, il gruppo 1 viene memorizzato nell'attributo %NESTED_GROUP_MEMBERSHIP%.

Se non si specifica un attributo %NESTED_GROUP_MEMBERSHIP%, CA Identity Manager memorizza i gruppi nidificati nell'attributo %GROUP_MEMBERSHIP%.

Per includere gruppi come membri di altri gruppi, configurare il supporto per i gruppi nidificati come viene descritto nella sezione Configurazione di gruppi dinamici e nidificati.

%DYNAMIC_GROUP_MEMBERSHIP%

Indica quale attributo memorizza la query LDAP che genera un gruppo dinamico (a pagina 147).

Nota: per estendere gli attributi disponibili per l'oggetto gruppo e includere gli attributi %NESTED_GROUP_MEMBERSHIP% e %DYNAMIC_GROUP_MEMBERSHIP%, è possibile utilizzare classi oggetto ausiliarie.

Attributi di organizzazione noti

Gli attributi noti seguenti si applicano solo agli ambienti che supportano le organizzazioni:

%ORG_DESCR%

Indica quale attributo contiene la descrizione di un'organizzazione.

%ORG_MEMBERSHIP%

(Obbligatorio)

Indica quale attributo contiene il DN dell'organizzazione padre di un'organizzazione.

%ORG_MEMBERSHIP_NAME%

Indica quale attributo contiene il nome descrittivo dell'organizzazione padre di un'organizzazione.

%ORG_NAME%

(Obbligatorio)

Indica quale attributo contiene il nome dell'organizzazione.

Attributo %ADMIN_ROLE_CONSTRAINT%

Quando si crea un ruolo di amministrazione, si specificano una o più regole per l'appartenenza al ruolo. Il ruolo viene concesso agli utenti che soddisfano le regole di appartenenza. Ad esempio, quando la regola di appartenenza al ruolo per il ruolo di Manager utenti è title=User Manager, gli utenti che hanno il titolo di Manager utenti possiedono il ruolo di Manager utenti.

Nota: per ulteriori informazioni sui ruoli, consultare la *Guida per l'amministratore*.

%ADMIN_ROLE_CONSTRAINT% consente di designare un attributo di profilo per la memorizzazione dei ruoli di amministrazione di un amministratore.

Utilizzo dell'attributo %ADMIN_ROLE_CONSTRAINT%

Per utilizzare %ADMIN_ROLE_CONSTRAINT% come vincolo per tutti i ruoli di amministrazione, eseguire le attività seguenti:

- Associare l'attributo noto %ADMIN_ROLE_CONSTRAINT% a un attributo di profilo multivalore per consentire più ruoli.
- Quando si configura un ruolo di amministrazione nella console utente, verificare il vincolo seguente:

  `Ruoli di amministrazione equivale a` *`nome ruolo`*

  nome ruolo

  Definisce il nome del ruolo per cui si sta fornendo il vincolo, come nell'esempio seguente:

  `Ruoli di amministrazione equivale a Manager utenti`

Nota: Ruoli di amministrazione è il nome visualizzato predefinito per l'attributo %ADMIN_ROLE_CONSTRAINT%.

Configurazione degli attributi noti

Eseguire la procedura seguente per configurare gli attributi noti.

Procedere come descritto di seguito:

1. Nel file di configurazione di directory, cercare il segno seguente:

   ##
2. Sostituire il valore che inizia con ## con l'attributo LDAP appropriato.
3. Ripetere i passaggi 1 e 2 finché tutti i valori richiesti non sono stati sostituiti.
4. Eseguire il mapping degli attributi noti su attributi fisici, secondo le esigenze.
5. Salvare il file di configurazione di directory.

Descrizione della struttura della directory utente

CA Identity Manager utilizza l'attributo noto %ORG_MEMBERSHIP% per determinare la struttura di una directory utente.

La procedura per descrivere la struttura della directory utente dipende dal tipo di struttura di directory.

Descrizione di una struttura di directory gerarchica

Il file di configurazione di directory è già configurato per una struttura di directory gerarchica. Pertanto, non è necessario modificare la descrizione dell'attributo %ORG_MEMBERSHIP%.

Descrizione di una struttura di directory utente flat

Procedere come descritto di seguito:

1. Individuare la descrizione dell'attributo %ORG_MEMBERSHIP% nella sezione User Object (Oggetto utente) del file directory.xml.
2. Nel parametro physicalname, sostituire %ORG_MEMBERSHIP% con il nome dell'attributo che memorizza l'organizzazione a cui l'utente appartiene.

Descrizione di una struttura di directory flat

Procedere come descritto di seguito:

1. Individuare la descrizione dell'attributo %ORG_MEMBERSHIP% nella sezione User Object (Oggetto utente) del file directory.xml.
2. Nel parametro physicalname, sostituire %ORG_MEMBERSHIP% con il nome dell'attributo che memorizza l'organizzazione a cui l'utente appartiene.
3. Ripetere il passaggio 1 nella sezione Group Object (Oggetto gruppo).
4. Nel parametro physicalname, sostituire %ORG_MEMBERSHIP% con il nome dell'attributo che memorizza l'organizzazione a cui il gruppo appartiene.

Descrizione di una directory utente che non supporta organizzazioni

Verificare che nessuna descrizione di oggetto o di attributi noti sia definita per le organizzazioni in directory.xml.

Configurazione dei gruppi

Per la configurazione, è possibile dividere i gruppi come segue:

- Gruppi auto-sottoscriventi
- Gruppi dinamici e nidificati

Configurazione dei gruppi auto-sottoscriventi

È possibile abilitare gli utenti self-service per la sottoscrizione ai gruppi configurando il supporto per i gruppi auto-sottoscriventi nel file di configurazione di directory.

Quando un utente si registra automaticamente, CA Identity Manager cerca i gruppi in organizzazioni specifiche e mostra i gruppi auto-sottoscriventi all'utente.

Procedere come descritto di seguito:

1. Nella sezione Self-subscribing Groups (Gruppi auto-sottoscriventi), aggiungere l'elemento SelfSubscribingGroups nel modo seguente:

   <SelfSubscribingGroups type=*search_type* org=*org_dn*>

2. Aggiungere i valori per i parametri seguenti:

   type

   Indica la posizione in cui CA Identity Manager cerca i gruppi auto-sottoscriventi nel modo seguente:

   - NONE—CA Identity Manager non cerca gruppi. Specificare NONE per impedire agli utenti di registrarsi automaticamente ai gruppi.
   - ALL: CA Identity Manager inizia a cercare i gruppi nella cartella principale. Specificare ALL se gli utenti possono registrarsi ai gruppi all'interno di una directory gerarchica.
   - INDICATEDORG: CA Identity Manager cerca i gruppi auto-sottoscriventi nell'organizzazione di un utente e nelle relative organizzazioni secondarie. Ad esempio, se il profilo di un utente si trova nell'organizzazione Marketing, CA Identity Manager cerca i gruppi auto-sottoscriventi nell'organizzazione Marketing e in tutte le organizzazioni secondarie.
   - SPECIFICORG: CA Identity Manager cerca in un'organizzazione specifica. Fornire il nome distinto (DN) dell'organizzazione specifica nel parametro org.

   org

   Specifica l'ID univoco dell'organizzazione in cui CA Identity Manager cerca i gruppi auto-sottoscriventi.

   Nota: assicurarsi di specificare il parametro org se type=SPECIFICORG.

Una volta che il supporto per i gruppi auto-sottoscriventi è stato configurato nella directory di CA Identity Manager, gli amministratori di CA Identity Manager possono specificare quali gruppi eseguono la sottoscrizione automatica nella console utente.

Nota: per ulteriori informazioni sulla gestione dei gruppi, consultare la *Guida per l'amministratore*.

Configurazione di gruppi dinamici e nidificati

Se si sta gestendo un archivio utenti LDAP, è possibile configurare il supporto per i tipi seguenti di gruppi nel file di configurazione di directory:

Gruppi dinamici

Consente di definire l'appartenenza ai gruppi specificando una query di filtro LDAP nella console utente in modo dinamico. Con i gruppi dinamici, gli amministratori non devono cercare e aggiungere i membri dei gruppi individualmente.

Gruppi nidificati

Consente di aggiungere gruppi come membri di altri gruppi.

È possibile abilitare i gruppi dinamici e nidificati utilizzando il file di configurazione di directory.

Procedere come descritto di seguito:

1. Eseguire il mapping degli attributi noti (a pagina 83) seguenti su un attributo fisico per l'oggetto gestito gruppo secondo le esigenze:
   - %DYNAMIC_GROUP_MEMBERSHIP%
   - %NESTED_GROUP_MEMBERSHIP%

   Nota: l'attributo fisico selezionato deve supportare più valori.
2. Nella sezione Directory Groups Behavior (Comportamento gruppi di directory), aggiungere l'elemento GroupTypes seguente:

   `<GroupTypes type=`*`group`*`>`

   Nota: l'elemento GroupTypes rispetta l'uso delle lettere maiuscole e minuscole.
3. Digitare un valore per il parametro seguente:

   group

   Abilita il supporto per i gruppi dinamici e nidificati. Di seguito sono elencati i valori validi:
   - NONE: CA Identity Manager non supporta i gruppi dinamici e nidificati.
   - ALL: CA Identity Manager supporta i gruppi dinamici e nidificati.
   - DYNAMIC: CA Identity Manager supporta solo i gruppi dinamici.
   - NESTED: CA Identity Manager supporta solo i gruppi nidificati.

Una volta configurato il supporto per i gruppi dinamici e nidificati nella directory di CA Identity Manager, gli amministratori di CA Identity Manager possono specificare quali gruppi sono dinamici e nidificati nella console utente.

Nota: considerare che il tipo di gruppo NESTED o ALL è stato impostato *senza* impostare il parametro noto %NESTED_GROUP_MEMBERSHIP%. In tal caso, CA Identity Manager memorizza sia i gruppi nidificati sia gli utenti nel parametro noto %GROUP_MEMBERSHIP%. I tempi di elaborazione dell'appartenenza al gruppo potrebbero essere leggermente superiori.

Aggiunta del supporto per i gruppi come amministratori di gruppi

Se si sta gestendo un archivio utenti LDAP, è possibile abilitare i gruppi in modo che servano da amministratori di altri gruppi. Quando si assegna un gruppo come amministratore, solo gli amministratori di quel gruppo sono amministratori del gruppo specificato. I membri del gruppo di amministrazione specificato non dispongono di alcun privilegio di gestione del gruppo.

Procedere come descritto di seguito:

1. Eseguire il mapping dell'attributo noto %GROUP_ADMIN_GROUP% su un attributo fisico che memorizza l'elenco dei gruppi che servono come amministratori.

   Nota: l'attributo fisico selezionato deve supportare più valori.

   Gli attributi di gruppo noti (a pagina 83) forniscono ulteriori informazioni sull'attributo %GROUP_ADMIN_GROUP%.

   Nota:se si imposta il tipo admin group su ALL senza impostare %GROUP_ADMIN_GROUP%, CA Identity Manager memorizza i gruppi di amministratori nell'attributo %GROUP_ADMIN%.

2. Nella sezione Directory AdminGroups Behavior, configurare l'elemento AdminGroupTypes come segue:

   <AdminGroupTypes type="ALL">

   Il valore predefinito per AdminGroupTypes è NONE.

   Nota: l'elemento AdminGroupTypes rispetta l'uso delle lettere maiuscole e minuscole.

Una volta configurato il supporto per i gruppi come amministratori nella directory di CA Identity Manager, gli amministratori di CA Identity Manager possono specificare gruppi come amministratori di altri gruppi nella console utente.

Regole di convalida

Una regola di convalida impone requisiti sui dati che un utente digita in un campo di una schermata di attività. I requisiti possono imporre un tipo di dati o un formato. Pertanto, assicurarsi che i dati siano validi nel contesto degli altri dati presenti nella schermata di attività.

Le regole di convalida sono associate agli attributi di profilo. CA Identity Manager assicura che i dati immessi per un attributo di profilo soddisfino tutte le regole di convalida associate prima di elaborare un'attività.

Nel file di configurazione di directory, è possibile definire le regole di convalida e associarle ad attributi di profilo.

Proprietà aggiuntive della directory di CA Identity Manager

È possibile configurare le seguenti proprietà aggiuntive:

- Ordinamento dei risultati della ricerca.
- Cercare nelle classi oggetto per verificare che un nuovo utente non esista già.
- Attendere per evitare il timeout di CA Identity Manager prima del completamento della replica dei dati, dalla directory LDAP principale alla directory LDAP secondaria.

Configurazione dell'ordinamento

È possibile specificare un attributo di ordinamento per ciascun oggetto gestito, quali utenti, gruppi o organizzazioni. CA Identity Manager utilizza questo attributo per ordinare i risultati della ricerca secondo una logica aziendale personalizzata, creata mediante le API di CA Identity Manager.

Nota: l'attributo di ordinamento non influisce sul modo in cui i risultati della ricerca vengono visualizzati nella console utente.

Ad esempio, quando si specifica l'attributo cn per l'oggetto utente, CA Identity Manager ordina alfabeticamente i risultati della ricerca utenti in base all'attributo cn.

Procedere come descritto di seguito:

1. Dopo l'ultimo elemento IMSManagedObjectAttr nella sezione dell'oggetto gestito a cui viene applicato l'ordinamento, aggiungere le dichiarazioni seguenti:

```
<PropertyDict name="SORT_ORDER">
    <Property name="ATTR">your_sort_attribute
    </Property>
</PropertyDict>
```

2. Sostituire *your_sort_attribute* con l'attributo su cui CA Identity Manager ordina i risultati della ricerca.

Nota: specificare un solo attributo fisico. Non specificare un attributo noto.

Ad esempio, si desidera ordinare i risultati di una ricerca utenti in base al valore dell'attributo cn. Aggiungere gli elementi seguenti dopo l'ultimo elemento IMSManagedObjectAttr nella sezione User Object (Oggetto utente) del file di configurazione di directory:

```
<!-- ******************** User Object ******************** -->
   <ImsManagedObject name="User" description="My Users"
      objectclass="top,person,organizationalperson,user"
      objecttype="USER">
   .
   .
   .
        <ImsManagedObjectAttr physicalname="departmentnumber"
                displayname="Department" description="Department"
                valuetype="String" required="true"
                multivalued="false" maxlength="0" />
        <PropertyDict name="SORT_ORDER">
                <Property name="ATTR">cn</Property>
        </PropertyDict>
  </ImsManagedObject>
```

Ricerca tra le classi oggetto

Quando si crea un utenteCA Identity Manager cerca nell'archivio utenti per verificare se l'utente esiste o meno. Questa ricerca è limitata agli utenti con la classe oggetto specificata nella definizione dell'oggetto utente nel file di configurazione di directory (directory.xml). Se non viene trovato alcun utente esistente nelle definizioni della classe oggetto, CA Identity Manager prova a creare l'utente.

Se un utente esiste con lo stesso ID univoco (ID utente) ma una diversa classe oggetto, il server LDAP non riesce a creare l'utente. L'errore viene segnalato nel server LDAP, ma CA Identity Manager non lo riconosce. Sembra che CA Identity Manager crei l'utente correttamente.

Per prevenire questo problema, è possibile configurare una proprietà SEARCH_ACROSS_CLASSES che spinge CA Identity Manager a cercare gli utenti in tutte le definizioni della classe oggetto quando verifica gli utenti esistenti.

Nota: questa proprietà influisce solo sulle ricerche di utenti duplicati quando si eseguono attività come la creazione di un utente. Per tutte le altre ricerche, si applicano i vincoli della classe oggetto.

Procedere come descritto di seguito:

1. Nel file di configurazione di directory (directory.xml), individuare l'elemento ImsManagedObject che descrive l'oggetto utente.
2. Aggiungere l'elemento PropertyDict seguente:

```
<PropertyDict name="SEARCH_ACROSS_CLASSES" description="allowing checking an
attribute across classes ">
<Property name="ENABLE">true</Property>
</PropertyDict>
```

Nota: l'elemento di PropertyDict deve essere l'ultimo elemento nell'elemento ImsManagedObject, come nell'esempio seguente:

```
<ImsManagedObject name="User" description="My Users"
objectclass="top,person,organizationalperson,inetorgperson,customClass"
objecttype="USER">
<ImsManagedObjectAttr physicalname="departmentnumber"
displayname="Department" description="Department" valuetype="String"
required="true" multivalued="false" maxlength="0" />
.
.
.
<PropertyDict name="SEARCH_ACROSS_CLASSES" description="allow checking an
attribute across classes ">
<Property name="ENABLE">true</Property>
</PropertyDict>
```

Determinazione del tempo di attesa per la replica

In una distribuzione che include una replica tra directory LDAP principale e secondaria, è possibile configurare il Policy Server di SiteMinder per la comunicazione con una directory secondaria. In questa configurazione, il Policy Server individua automaticamente dei riferimenti che puntano alla directory principale durante le operazioni di scrittura dati nella directory LDAP. I dati vengono archiviati nella directory LDAP principale e replicati nella directory LDAP secondaria secondo lo schema di replica delle risorse di rete.

In questa configurazione, quando si crea un oggetto in CA Identity Manager, l'oggetto viene creato nella directory principale e replicato anche nella directory secondaria. Durante il processo di replica può verificarsi un ritardo che causa un errore dell'azione di creazione in CA Identity Manager.

Per impedire che questo problema si verifichi, è possibile specificare il periodo di tempo (in secondi) che CA Identity Manager attende prima del timeout nella proprietà REPLICATION_WAIT_TIME.

Procedere come descritto di seguito:

1. Nel file di configurazione di directory (directory.xml), individuare l'elemento ImsManagedObject che descrive l'oggetto utente.
2. Aggiungere l'elemento PropertyDict seguente:

```
<PropertyDict name="REPLICATION_WAIT_TIME" description="time delay in seconds
for LDAP provider to allow replication to propagate from master to slave">
<Property name=REPLICATION_WAIT_TIME><time in seconds></Property>
</PropertyDict>
```

Nota: l'elemento di PropertyDict deve essere l'ultimo elemento nell'elemento ImsManagedObject, come nell'esempio seguente:

```
<ImsManagedObject name="User" description="My Users"
objectclass="top,person,organizationalperson,inetorgperson,customClass"
objecttype="USER">
<ImsManagedObjectAttr physicalname="departmentnumber"
displayname="Department" description="Department" valuetype="String"
required="true" multivalued="false" maxlength="0" />
.
.
.
<PropertyDict name="REPLICATION_WAIT_TIME" description="time delay in seconds
for LDAP provider to allow replication to propagate from master to slave">
<Property name=REPLICATION_WAIT_TIME>800</Property>
</PropertyDict>
```

Quando il tempo di attesa della replica non viene definito, viene utilizzato il valore predefinito 0.

Determinazione delle impostazioni di connessione LDAP

Per migliorare le prestazioni, è possibile specificare i parametri seguenti nel file di configurazione di directory (directory.xml):

Timeout connessione

Consente di specificare il numero massimo di millisecondi che CA Identity Manager utilizza per eseguire una ricerca in una directory prima di terminarla.

Questa proprietà viene specificata nel file di configurazione di directory come segue:

com.sun.jndi.ldap.connect.timeout

Dimensione massima del pool di connessioni

Specifica il numero massimo di connessioni che CA Identity Manager può effettuare alla directory LDAP.

Questa proprietà viene specificata nel file di configurazione di directory come segue:

com.sun.jndi.ldap.connect.pool.maxsize

Dimensione predefinita del pool di connessioni

Specifica il numero predefinito di connessioni tra CA Identity Manager e la directory LDAP.

Questa proprietà viene specificata nel file di configurazione di directory come segue:

com.sun.jndi.ldap.connect.pool.prefsize

Procedere come descritto di seguito:

1. Nel file di configurazione di directory (directory.xml), individuare l'elemento ImsManagedObject che descrive l'oggetto utente.
2. Aggiungere l'elemento PropertyDict seguente:

```
<PropertyDict name="LDAP_CONNECTION_SETTINGS" description="LDAP Connection
Settings">
    <Property name="com.sun.jndi.ldap.connect.timeout">5000</Property>
    <Property name="com.sun.jndi.ldap.connect.pool.maxsize">200</Property>
    <Property name="com.sun.jndi.ldap.connect.pool.prefsize">10</Property>
</PropertyDict>
```

3. Salvare il file directory.xml.

   CA Identity Manager configura queste impostazioni quando si crea la directory di CA Identity Manager con questo file.

Miglioramento delle prestazioni di ricerca nella directory

Per migliorare il prestazioni di ricerca nella directory per utenti, organizzazioni e gruppi, attenersi ai punti seguenti:

- Indicizzare gli attributi che gli amministratori possono specificare nelle query di ricerca.

  Nota: per Oracle Internet Directory, una ricerca può non riuscire se un attributo in una query di ricerca non viene indicizzato.

- Configurare le impostazioni della dimensione di pagina e del numero massimo di righe (a pagina 96) per determinare la modalità di gestione delle ricerche di dimensioni elevate da parte di CA Identity Manager .

- Ottimizzare la directory utente. Consultare la documentazione relativa alla directory utente utilizzata.

Miglioramento delle prestazioni per ricerche di dimensioni elevate

Quando CA Identity Manager gestisce un archivio utenti di grandi dimensioni, le ricerche che restituiscono molti risultati possono far esaurire la memoria del sistema. Per impedire problemi di memoria, è possibile definire dei limiti per le ricerche di dimensioni elevate.

Le due impostazioni seguenti determinano come CA Identity Manager gestisce le ricerche di dimensioni elevate:

- Maximum number of rows (Numero massimo di righe)

  Consente di specificare il numero massimo di risultati che CA Identity Manager può restituire durante una ricerca in una directory utente. Quando il numero dei risultati supera il limite, viene visualizzato un errore.

- Page size (Dimensione pagina)

  Specifica il numero di oggetti che può essere restituito in una singola ricerca. Se il numero degli oggetti supera la dimensione della pagina, CA Identity Manager esegue ricerche multiple.

  Prendere nota dei punti seguenti quando si specificano le dimensioni della pagina:

  - Per utilizzare l'opzione Search Page Size (Dimensioni pagina di ricerca), l'archivio utenti che CA Identity Manager gestisce deve supportare il paging. Per alcuni tipi di archivio utenti è necessaria un'ulteriore configurazione per consentire il paging. Per ulteriori informazioni, consultare gli argomenti seguenti:

    Configurare il supporto per il paging del server di directory del sistema Sun Java (a pagina 98)

    Configurare il supporto per il paging di Active Directory

  - Se l'archivio utenti non supporta il paging ed è specificato un valore maxrows, CA Identity Manager utilizza solo il valore maxrows per controllare le dimensioni della ricerca.

È possibile configurare un numero massimo di righe e le dimensioni della pagina nelle posizioni seguenti:

- Archivio utenti

  Nella maggior parte degli archivi utenti e dei database, è possibile configurare dei limiti per la ricerca.

  Nota: per ulteriori informazioni, consultare la documentazione relativa all'archivio utenti o al database utilizzato.

- Directory di CA Identity Manager

  È possibile configurare l'elemento DirectorySearch (a pagina 58) nel file di configurazione della directory (directory.xml) utilizzato per creare la directory di CA Identity Manager.

  Per impostazione predefinita, il valore massimo delle righe e delle dimensioni delle pagine è illimitato per le directory esistenti. Per le nuove directory, il valore del numero massimo di righe è illimitato e il valore della dimensione delle pagine è pari a 2000.

- Definizione di oggetto gestito

  Per impostare i limiti massimi per il numero di righe e le dimensioni della pagina da applicare a un tipo di oggetto invece che a un'intera directory, configurare la *definizione dell'oggetto gestito* (a pagina 61) nel file directory.xml utilizzato per creare la directory di CA Identity Manager.

  L'impostazione di limiti per un tipo di oggetto gestito consente di apportare modifiche in base ai requisiti aziendali. Ad esempio, la maggior parte delle aziende ha più utenti che gruppi. Tali aziende possono impostare i limiti per le sole ricerche di oggetti utente.

- Schermate di ricerca attività

  È possibile controllare il numero dei risultati della ricerca che gli utenti visualizzano nelle schermate di ricerca e di elenco nella console utente. Se il numero di risultati supera il numero di risultati per pagina definiti per l'attività, gli utenti visualizzano dei collegamenti a pagine di risultati aggiuntive.

  Questa impostazione non influisce sul numero dei risultati restituiti da una ricerca.

  Nota: per informazioni sull'impostazione delle dimensioni di pagina nelle schermata di ricerca e di elenco, consultare la *Guida per l'amministratore*.

Se il limite massimo per il numero di righe e dimensioni della pagina è definito in più posizioni, viene applicata l'impostazione più specifica. Ad esempio, le impostazioni di un oggetto gestito hanno la precedenza sulle impostazioni a livello di directory.

Configurare il supporto per il paging del server di directory del sistema Sun Java

I server di directory del sistema Sun Java supportano la visualizzazione VLV (Virtual List View), un metodo per la restituzione dei risultati di una ricerca in un certo ordine o in determinati sottoinsiemi. Questo metodo differisce dal metodo Simple Paged Results (Risultati semplici per pagina) che CA Identity Manager prevede.

Per utilizzare il metodo VLV, è necessario impostare delle autorizzazioni e creare degli indici. CA Identity Manager include i file seguenti che è necessario configurare per il supporto di paging:

- vlvcntrl.ldif
- vlvindex.ldif
- runvlvindex.cmd, runvlvindex.sh

Questi file sono inclusi come parte dell'ambiente di NeteAuto di esempio, in samples\NeteAuto negli strumenti di amministrazione.

Gli strumenti di amministrazione sono installati nelle seguenti posizioni predefinite:

Windows: C:\Programmi\CA\Identity Manager\IAM Suite\Identity Manager

UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/

Procedere come descritto di seguito:

1. Aggiungere il parametro seguente all'elemento DirectorySearch (a pagina 58) nel file directory.xml per la directory di CA Identity Manager, nel modo seguente:

   ```
   minsortrules="1"
   ```

   Nota: se si sta modificando una directory di CA Identity Manager esistente, consultare la sezione Aggiornamento di una directory di CA Ide (a pagina 185)ntity Manager.

2. Impostare le autorizzazioni per il file vlvcntrl.ldif come segue:
   `ldapmodify -D "cn=Directory Manager" -w password -p port -f vlvcntrl.ldif`

3. Importare la ricerca VLV e le definizioni dell'indice come segue:
   `ldapmodify -D "cn=Directory Manager" -w password -p port -f vlvindex.ldif`

4. Interrompere la directory come segue:
   `stop-slapd`

5. Costruire gli indici mediante runvlvindex.

6. Avviare la directory come segue:
   `start-slapd`

Configurare il supporto per il paging di Active Directory

Per configurare il supporto per il paging in Active Directory, completare i passaggi seguenti:

- Configurare il supporto per VLV (Virtual List View) (a pagina 99).
- Configurare MaxPageSize per Active Directory (a pagina 100). (Solo per le **directory create prima di CA Identity Manager r12.5 SP7**)

Configurazione del supporto per VLV (Virtual List View).

Active Directory supporta la visualizzazione VLV (Virtual List View), un metodo per la restituzione dei risultati di una ricerca in un certo ordine o in determinati sottoinsiemi. Questo metodo differisce dal metodo Simple Paged Results (Risultati semplici per pagina) che CA Identity Manager prevede.

Per utilizzare il metodo VLV, è necessario impostare delle autorizzazioni e creare degli indici. CA Identity Manager include i file seguenti che è necessario configurare per il supporto di paging:

- vlvcntrl.ldif
- vlvindex.ldif
- runvlvindex.cmd, runvlvindex.sh

Questi file sono inclusi come parte dell'ambiente di NeteAuto di esempio, in samples\NeteAuto negli strumenti di amministrazione.

Gli strumenti di amministrazione sono installati nelle seguenti posizioni predefinite:

Windows: C:\Programmi\CA\Identity Manager\IAM Suite\Identity Manager

UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/

Procedere come descritto di seguito:

1. Aggiungere il parametro seguente all'elemento DirectorySearch (a pagina 58) nel file directory.xml per la directory di CA Identity Manager, nel modo seguente:

   ```
   minsortrules="1"
   ```

   Nota: se si sta modificando una directory di CA Identity Manager esistente, consultare la sezione Aggiornamento di una directory di CA Ide (a pagina 185)ntity Manager.

2. Impostare le autorizzazioni per il file vlvcntrl.ldif come segue:
   ```
   ldapmodify -D "cn=Directory Manager" -w password -p port -f
   vlvcntrl.ldif
   ```

3. Importare la ricerca VLV e le definizioni dell'indice come segue:
   ```
   ldapmodify -D "cn=Directory Manager" -w password -p port -f
   vlvindex.ldif
   ```

4. Interrompere la directory come segue:
   ```
   stop-slapd
   ```

5. Costruire gli indici mediante runvlvindex.

6. Avviare la directory come segue:
   ```
   start-slapd
   ```

Configurazione di MaxPageSize per Active Directory

Per l'impostazione di MaxPageSize, Active Directory utilizza 1000 come valore predefinito. Supporre che il valore dell'attributo maxpagesize in directory.xml sia superiore o equivalente a 1000. In tal caso, CA Identity Manager non riesce a visualizzare un avviso quando il numero di risultati della ricerca supera il valore di maxrows in directory.xml. In questo caso, gli amministratori che eseguono la ricerca non si rendono conto che alcuni risultati della ricerca vengono omessi.

Per prevenire questo problema, verificare che il valore dell'attributo maxpagesize per la directory e tutti gli oggetti gestiti sia inferiore al valore MaxPageSize di Active Directory.

Supporre di creare una directory di CA Identity Manager mediante il file directory.xml di modello che viene installato con CA Identity Manager versione 12.5 SP7 o superiore. In questo caso, non è necessario eseguire nessun passaggio aggiuntivo per il supporto al paging. L'attributo maxpagesize in directory.xml è impostato per impostazione predefinita.

Se si aggiunge il supporto per il paging a una directory di CA Identity Manager esistente, il valore dell'attributo maxpagesize in directory.xml deve essere inferiore a 1000.

Inoltre, se il valore MaxPageSize di Active Directory è 1000, assicurarsi di impostare l'attributo maxpagesize in modo appropriato per la directory di CA Identity Manager e tutti gli oggetti gestiti.

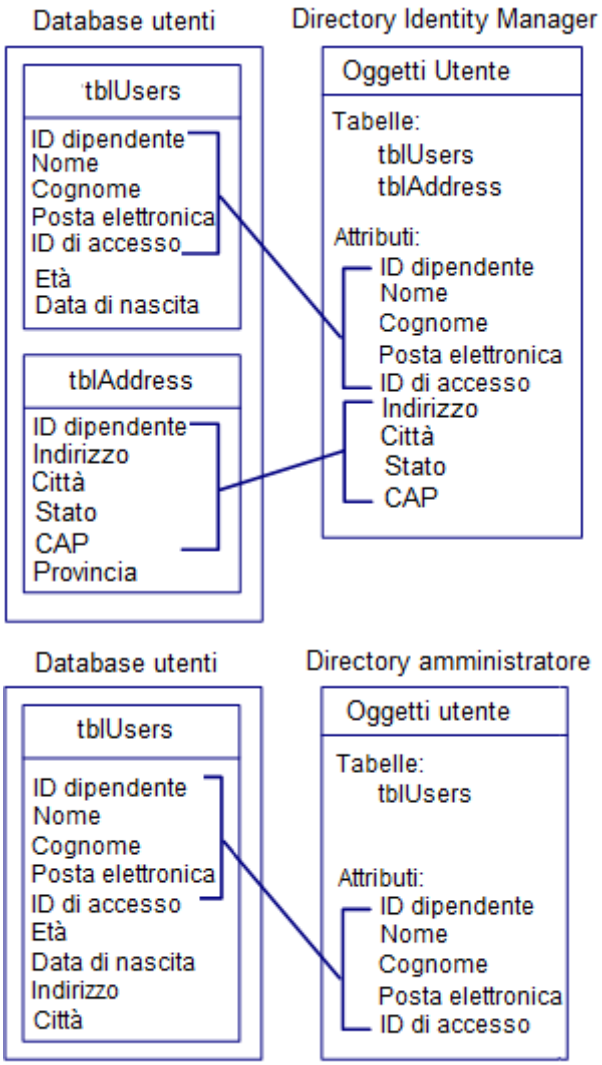
Capitolo 4: Gestione del database relazionale

Questa sezione contiene i seguenti argomenti:

Directory di CA Identity Manager

Una *directory di CA Identity Manager* descrive come oggetti quali utenti, gruppi e organizzazioni vengono archiviati nell'archivio utenti e rappresentati in CA Identity Manager. Una directory di CA Identity Manager viene associata a uno o più ambienti di CA Identity Manager.

L'illustrazione seguente mostra come una directory di CA Identity Manager è correlata a un archivio utenti:



Nota: alcuni attributi dell'utente nel database non fanno parte della directory di CA Identity Manager e pertanto CA Identity Manager non li gestisce.

Note importanti per quando si configura CA Identity Manager per i database relazionali

Prima di configurare CA Identity Manager per la gestione di un database relazionale, verificare che il database soddisfi i requisiti seguenti:

- Il database deve essere accessibile mediante un driver JDBC o un driver ODBC (Open Database Connectivity), quando CA Identity Manager si integra con SiteMinder. Il driver deve supportare join esterni. Se vengono utilizzate più di due tabelle per rappresentare un oggetto gestito, il driver deve supportare anche join esterni nidificati.

  Nota: se il driver non supporta join esterni, CA Identity Manager utilizza join interni quando esegue query nel database. Questo può causare risultati di query imprevisti.

- Identificare in modo univoco ciascun oggetto gestito da CA Identity Manager, come un utente, gruppo o organizzazione (quando supportata). Ad esempio, l'ID univoco per gli utenti può essere un ID di accesso.

  Nota: assicurarsi che l'ID univoco venga memorizzato in una colonna singola.

- CA Identity Manager richiede alcuni attributi multivalore, che è possibile memorizzare come elenco delimitato in una cella singola o in più righe in una tabella separata. Ad esempio, la tabella di tblGroupMembers seguente memorizza i membri di un gruppo:

ID	Membri
Ricerca	dmason
Ricerca	rsavory
Marketing	dmason
Marketing	awelch

  La colonna ID contiene l'ID univoco di un gruppo e la colonna Membri contiene l'ID univoco di un membro del gruppo. Ad esempio, dmason e rsavory sono membri del gruppo Ricerca. Quando un nuovo membro viene aggiunto a quel gruppo, un'altra riga viene aggiunta a tblGroupMembers.

- Quando l'ambiente include le organizzazioni, eseguire l'attività seguente:
  - Modificare ed eseguire uno script SQL, incluso in CA Identity Manager, sul database per configurare il supporto per le organizzazioni (a pagina 149).
  - CA Identity Manager richiede un'organizzazione di livello superiore, chiamata root. Tutte le altre organizzazioni sono correlate all'organizzazione root.

    Per ulteriori informazioni sui requisiti delle organizzazioni, consultare la sezione Gestione delle organizzazioni (a pagina 148).

Creazione di un'origine dati Oracle per WebSphere

Procedere come descritto di seguito:

1. Nella console di amministrazione di WebSphere, accedere al provider JDBC creato durante la configurazione del driver JDBC.
2. Creare un'origine dati con le proprietà seguenti e fare clic su Applica:

   Nome: Origine dati archivio utenti

   Nome JNDI: userstore

   URL: jdbc:oracle:thin:@*db_systemname*:1521:*oracle_sid*
3. Configurare una nuova voce dati di autenticazione J2C per l'origine dati dell'archivio utenti:
   a. Immettere le seguenti proprietà:

      Alias: Archivio utenti

      ID utente: *username*

      password: *password*

      dove *username* e *password* sono il nome utente e la password dell'account specificato al momento della creazione del database.

   b. Fare clic su OK, quindi utilizzare i collegamenti di navigazione nella parte superiore della schermata per tornare all'origine dati in fase di creazione.
4. Selezionare la voce dei dati di autenticazione J2C dell'archivio utenti creata dalla casella di riepilogo nei campi seguenti:
   - Component-managed Authentication Alias (Alias di autenticazione gestito dal componente)
   - Container-managed Authentication Alias (Alias di autenticazione gestito dal contenitore)
5. Fare clic su OK, quindi salvare la configurazione.

   Nota: per verificare che l'origine dati sia configurata correttamente, fare clic su Verifica connessione nella schermata di configurazione dell'origine dati. Se la verifica della connessione non riesce, riavviare WebSphere e verificare di nuovo la connessione.

Creazione di una directory di CA Identity Manager

Procedere come descritto di seguito:

1. Se si utilizza SiteMinder, applicare lo schema del Policy Store prima di creare una directory di CA Identity Manager.

   Nota: per ulteriori informazioni sugli schemi di Policy Store specifici e sulla loro applicazione, consultare la *Guida all'installazione*.

2. Se si utilizza SiteMinder, creare un'origine dati ODBC per utilizzarla con SiteMinder (a pagina 113).
3. Creare un'origine dati per il database degli utenti gestito da CA Identity Manager.
4. Descrivere il database a CA Identity Manager modificando un file di configurazione di directory (directory.xml). Per ulteriori informazioni, consultare la sezione Descrizione di un database in un file di configurazione di directory.
5. Nella console di gestione, importare il file di configurazione di directory e creare la directory.

Creazione di un'origine dati JDBC

Per consentire la connessione tra CA Identity Manager e l'archivio utenti, è necessario che il server applicazioni su cui è installato CA Identity Manager contenga un'origine dati JDBC. Le istruzioni per creare un'origine dati variano in base al tipo di server applicazioni.

Creazione di un'origine dati JDBC per i server applicazioni JBoss

Procedere come descritto di seguito:

1. Creare una copia del file seguente:

   jboss_home\server\default\deploy\objectstore-ds.xml

   jboss home

   La posizione di installazione del server applicazioni Jboss in cui CA Identity Manager viene installato.

   Il nuovo file deve esistere nella stessa posizione.

2. Rinominare il file in userstore-ds.xml.

3. Modificare userstore-ds.xml come segue:
   a. Individuare l'elemento <jndi-name>.
   b. Modificare il valore dell'elemento <jndi-name> da jdbc/objectstore a userstore come segue:

      <jndi-name>userstore</jndi-name>

   c. Nell'elemento <connection-url>, modificare il parametro DatabaseName con il nome del database che serve da archivio utenti nel modo seguente:

      <connection-url>

      jdbc:sqlserver://*ipaddress:port*;selectMethod=cursor;DatabaseName=*userstore_name*

      </connection-url>

      ipaddress

      Specifica l'indirizzo IP del computer su cui è installato l'archivio utenti.

      porta

      Specifica il numero della porta del database

      userstore_name

      Specifica il nome del database che serve da archivio utenti.

4. Eseguire i passaggi seguenti se si intende creare un'area di autenticazione di protezione JBoss, necessaria per il supporto FIPS:
   a. Rinominare il dominio di protezione in <security-domain>imuserstoredb</security-domain>.
   b. Salvare il file.
   c. Omettere i passaggi restanti. Invece, completare i passaggi nella sezione Creazione di un'area di autenticazione di protezione JBoss per l'origine dati JDBC (a pagina 109).
5. Apportare le seguenti modifiche aggiuntive al file userstore-ds.xml:
   a. Modificare il valore dell'elemento <user-name> con il nome utente di un account che dispone di accesso in lettura e scrittura all'archivio utenti.
   b. Modificare il valore dell'elemento <password> con la password dell'account specificato nell'elemento <user-name>.

   Nota: in questo file il nome utente e la password vengono visualizzati come testo non crittografato. Pertanto, si può decidere di creare un'area di autenticazione di protezione JBoss invece di modificare userstore-ds.xml.
6. Salvare il file.

Utilizzare un'area di autenticazione di protezione JBoss per l'origine dati JDBC

Assicurarsi di creare un'origine dati JDBC in un server applicazioni JBoss. È possibile configurare l'origine dati per l'utilizzo di un nome utente e password o configurarla per l'utilizzo di un'area di autenticazione di protezione.

Importante. Assicurarsi che l'opzione dell'area di autenticazione di protezione JBoss sia utilizzata se FIPS viene utilizzato.

Procedere come descritto di seguito:

1. Completare i passaggi nella sezione Creazione di un'origine dati JDBC per i server applicazioni JBoss (a pagina 107).

   Non specificare un nome utente e una password nel file userstore-ds.xml come descritto al passaggio 4.

2. Aprire login-cfg.xml in *jboss_home*\server\default\conf.

3. Individuare la voce seguente nel file:

```
<application-policy name="imobjectstoredb">
  <authentication>
    <login-module
code="com.netegrity.jboss.datasource.PasswordEncryptedLogin" flag="required">
      <module-option name="userName">fwadmin</module-option>
      <module-option name="password">{PBES}:gSex2/BhDGzEKWvFmzca4w==</module-
option>
      <module-option
name="managedConnectionFactoryName">jboss.jca:name=jdbc/objectstore,service=N
oTxCM</module-option>
    </login-module>
  </authentication>
</application-policy>
```

4. Copiare la voce completa e incollarla all'interno dei tag <policy> e </policy> nel file login-cfg.xml.

5. Nella voce incollata nel file, effettuare le modifiche seguenti:

   a. Modificare il valore dell'attributo nome da imobjectstoredb a imuserstoredb come segue:

      ```
      <application-policy name="imuserstoredb">
      ```

   b. Specificare il nome dell'utente utilizzato per l'autenticazione nell'archivio utenti come segue:

      ```
      <module-option name="userName">user_store_user</module-option>
      ```

   c. Specificare la password per l'utente nel passaggio precedente come segue:

      ```
      <module-option name="password">user_store_user_password</module-option>
      ```

      Nota: per crittografare la password dell'archivio utenti, utilizzare lo strumento di password (pwdtools) che viene installato con CA Identity Manager.

d. Nell'elemento <module-option name="managedConnectionFactoryName">, fornire il jdbc.jca:name corretto come segue:

```
<module-option name="managedConnectionFactoryName">
    jboss.jca:name=userstore,service=NoTxCM
</module-option>
```

6. Salvare il file.
7. Riavviare il server applicazioni.

Creare un'origine dati JDBC per WebLogic

Si crea un'origine dati nella console di amministrazione di WebLogic.

Nota: consultare la documentazione su Oracle WebLogic 11 per informazioni complete sui pool di connessione di Weblogic.

Procedere come descritto di seguito:

1. Creare un'origine dati JDBC con i parametri seguenti nella console di amministrazione di WebLogic:

   Nome: Origine dati archivio utenti

   Nome JNDI: userstore

2. Creare il pool di connessione per l'origine dati con le informazioni seguenti:

   - Per i database SQL Server 2005, utilizzare i valori seguenti:

     URL: jdbc:sqlserver://*db_systemName*:1433

     Nome classe del driver: com.microsoft.sqlserver.jdbc.SQLServerDriver

     Proprietà: user=*username*

     databaseName=*user store name*

     selectMethod=cursor

     Password: *password*

   - Per i database Oracle, utilizzare i valori seguenti:

     URL: jdbc:oracle:thin:@*tp_db_systemname*:1521:*oracle_SID*

     Nome classe del driver: oracle.jdbc.driver.OracleDriver

     Proprietà: user=*username*

     Password: *password*

3. Dopo la configurazione, impostare la destinazione per il pool nell'istanza server *wl_server_name*.

   Dopo avere distribuito il pool, controllare la console per verificare l'eventuale presenza di errori.

   Nota: è possibile visualizzare un errore che informa che non è possibile creare l'origine dati con un pool non esistente. Per risolvere questo errore, riavviare WebLogic.

Origini dati di WebSphere

Le sezioni seguenti descrivono come creare un'origine dati SQL o Oracle per i server applicazioni WebSphere.

Creazione di un'origine dati SQL Server per WebSphere

Procedere come descritto di seguito:

1. Nella console di amministrazione di WebSphere, accedere al provider JDBC creato durante la configurazione del driver JDBC.
2. Selezionare Origini di dati nella sezione Additional Properties (Proprietà aggiuntive).
3. Creare un'origine dati con le proprietà seguenti e fare clic su Applica:

   Nome: Origine dati archivio utenti

   Nome JNDI: userstore

   databaseName: *userstore_name*

   serverName: *db_systemname*

4. Configurare la proprietà selectMethod come segue:
   a. Selezionare Custom Properties (Proprietà personalizzate) nella sezione Additional Properties (Proprietà aggiuntive).
   b. Fare clic sulla proprietà personalizzata selectMethod.
   c. Immettere il testo seguente nel campo Valore:

      cursor

   d. Fare clic su OK, quindi utilizzare i collegamenti di navigazione nella parte superiore della schermata per tornare all'origine dati in fase di creazione.

5. Configurare una nuova voce dati di autenticazione J2C per l'origine dati dell'archivio utenti:
   a. Selezionare le voci dei dati di autenticazione di J2EE Connector Architecture (J2C) nella sezione Related Items (Elementi correlati).
   b. Fare clic su Nuovo.
   c. Immettere le seguenti proprietà:

      Alias: Archivio utenti

      ID utente: *username*

      password: *password*

      dove *username* e *password* sono il nome utente e la password dell'account specificato al momento della creazione del database.
   d. Fare clic su OK, quindi utilizzare i collegamenti di navigazione nella parte superiore della schermata per tornare all'origine dati in fase di creazione.
6. Selezionare la voce di dati di autenticazione dell'archivio utenti di J2C creata dalla casella di riepilogo nel campo Component-managed Authentication Alias (Alias di autenticazione gestito dal componente).
7. Fare clic su OK, quindi salvare la configurazione.

   Nota: per verificare che l'origine dati sia configurata correttamente, fare clic su Verifica connessione nella schermata di configurazione dell'origine dati. Se la verifica della connessione non riesce, riavviare WebSphere e verificare di nuovo la connessione.

Creazione di un'origine dati Oracle per WebSphere

Procedere come descritto di seguito:

1. Nella console di amministrazione di WebSphere, accedere al provider JDBC creato durante la configurazione del driver JDBC.
2. Creare un'origine dati con le proprietà seguenti e fare clic su Applica:

   Nome: Origine dati archivio utenti

   Nome JNDI: userstore

   URL: jdbc:oracle:thin:@*db_systemname*:1521:*oracle_sid*

3. Configurare una nuova voce dati di autenticazione J2C per l'origine dati dell'archivio utenti:
   a. Immettere le seguenti proprietà:

      Alias: Archivio utenti

      ID utente: *username*

      password: *password*

      dove *username* e *password* sono il nome utente e la password dell'account specificato al momento della creazione del database.

   b. Fare clic su OK, quindi utilizzare i collegamenti di navigazione nella parte superiore della schermata per tornare all'origine dati in fase di creazione.
4. Selezionare la voce dei dati di autenticazione J2C dell'archivio utenti creata dalla casella di riepilogo nei campi seguenti:
   - Component-managed Authentication Alias (Alias di autenticazione gestito dal componente)
   - Container-managed Authentication Alias (Alias di autenticazione gestito dal contenitore)
5. Fare clic su OK, quindi salvare la configurazione.

   Nota: per verificare che l'origine dati sia configurata correttamente, fare clic su Verifica connessione nella schermata di configurazione dell'origine dati. Se la verifica della connessione non riesce, riavviare WebSphere e verificare di nuovo la connessione.

Creazione di un'origine dati ODBC per l'utilizzo con SiteMinder

Se CA Identity Manager si integra con SiteMinder, definire un'origine dati ODBC nel computer SiteMinder che fa riferimento al database. Prendere nota del nome dell'origine dati per riferimento futuro. Procedere come segue:

- **Windows:** configurare l'origine dati ODBC come DN di sistema. Consultare la documentazione del sistema operativo Windows per istruzioni.
- **UNIX:** aggiungere una voce che specifica i parametri per l'origine dati ODBC nel file system_odbc.ini localizzato in *policy_server_installation*/db.

Descrizione di un database in un file di configurazione di directory

Per gestire un database, CA Identity Manager deve comprendere la struttura e il contenuto del database. Descrivere il database a CA Identity Manager modificando il file di configurazione di directory (directory.xml).

Il file di configurazione di directory contiene una o più delle sezioni seguenti:

Informazioni sulla directory di CA Identity Manager

Contiene informazioni sulla directory di CA Identity Manager che CA Identity Manager utilizza.

Attribute Validation (Convalida dell'attributo)

Definisce le regole di convalida che si applicano alla directory di CA Identity Manager.

Provider Information (Informazioni sul provider)

Descrive l'archivio utenti che CA Identity Manager gestisce.

Directory Search Information (Informazioni sulla ricerca nella directory)

Consente di specificare la modalità di ricerca di CA Identity Manager nell'archivio utenti.

User Object (Oggetto utente) (a pagina 116)

Descrive come gli utenti vengono archiviati nell'archivio utenti e come vengono rappresentati in CA Identity Manager.

Group Object (Oggetto gruppo) (a pagina 116)

Descrive come i gruppi vengono archiviati nell'archivio utenti e come vengono rappresentati in CA Identity Manager.

Organization Object (Oggetto organizzazione) (a pagina 116)

Descrive come le organizzazioni vengono archiviate e come vengono rappresentate in CA Identity Manager.

Gruppi auto-sottoscriventi

Configura il supporto per i gruppi a cui gli utenti self-service possono unirsi.

La directory in cui si sono installati gli strumenti di amministrazione di CA Identity Manager include il modello del file di configurazione di directory seguente per i database relazionali:

admin_tools\directoryTemplates\RelationalDatabase\directory.xml

admin_tools

Definisce la posizione di installazione degli strumenti di amministrazione di CA Identity Manager, come negli esempi seguenti:

- **Windows:** C:\Programmi\CA\Identity Manager\IAM Suite\Identity Manager\tools
- **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

Nota: il modello del file di configurazione di directory in directoryTemplates\RelationalDatabase viene configurato per gli ambienti che supportano le organizzazioni. Per visualizzare un file di configurazione della directory per un ambiente che non include organizzazioni, consultare il file directory.xml per l'ambiente di NeteAuto di esempio in *admin_tools*\samples\NeteAutoRDB\NoOrganization

Copiare il modello di configurazione in una directory nuova o salvarlo con un nome diverso per impedire che venga sovrascritto. È quindi possibile modificare il modello per riflettere la struttura del database.

Il file di configurazione di directory ha due importanti convenzioni:

- ##: indica i valori necessari.

  Per fornire tutte le informazioni richieste, individuare tutti i segni di cancelletto doppi (##) e sostituirli con i valori appropriati. Ad esempio, ##PASSWORD_HINT indica che è necessario fornire un attributo per memorizzare una domanda a cui l'utente dovrà rispondere per ricevere una password temporanea in caso di password dimenticata.

- @: indica i valori popolati da CA Identity Manager. Non modificare questi valori nel file di configurazione di directory. CA Identity Manager richiede di fornire i valori quando si importa il file di configurazione di directory.

Prima di modificare il file di configurazione di directory, sono necessarie le informazioni seguenti:

- Nomi tabelle per gli oggetti utente, gruppo e organizzazione (quando la struttura include organizzazioni).
- Un elenco di attributi nei profili utente, gruppo e organizzazione (quando la struttura include organizzazioni).

Modifica del file di configurazione di directory

Eseguire la procedura seguente per modificare il file di configurazione di directory.

Procedere come descritto di seguito:

1. Configurare una connessione al database.
2. Specificare il periodo di tempo che CA Identity Manager impiega per eseguire una ricerca in una directory prima di terminare la ricerca.
3. Definire gli oggetti gestiti utente e gruppo che CA Identity Manager gestisce (a pagina 116).
4. Modificare gli attributi noti.

   Gli attributi noti identificano attributi speciali, come ad esempio l'attributo di password, in CA Identity Manager.

5. Configurare il supporto per i gruppi auto-sottoscriventi.
6. Se l'ambiente include organizzazioni, configurare il supporto per le organizzazioni.

Ulteriori informazioni:

Descrizioni oggetto gestito (a pagina 116)
Gestione organizzazione (a pagina 148)
Configurazione dei gruppi auto-sottoscriventi (a pagina 147)
Attributi noti di un database relazionale (a pagina 141)

Descrizioni oggetto gestito

In CA Identity Manager, si gestiscono i tipi seguenti di oggetti, che corrispondono alle voci in un archivio utenti:

- Utenti: rappresentano gli utenti di un'azienda.
- Gruppi**:** rappresentano le associazioni di utenti che hanno qualcosa in comune.
- Organizzazioni (Facoltativo): rappresentano le unità aziendali. Le organizzazioni possono contenere utenti, gruppi e altre organizzazioni.

  Nota: la sezione Gestione organizzazione (a pagina 148)fornisce informazioni sulla configurazione delle organizzazioni.

Una descrizione di oggetto contiene le informazioni seguenti:

- Informazioni sull'oggetto (a pagina 116), come le tabelle in cui l'oggetto viene archiviato.
- Gli attributi che archiviano le informazioni relative a una voce (a pagina 121). Ad esempio, l'attributo del cercapersone archivia un numero di cercapersone.

Importante. Un ambiente di CA Identity Manager supporta solo un tipo di oggetto utente, gruppo e organizzazione.

Descrizione di un oggetto gestito

Un oggetto gestito viene descritto specificando le informazioni relative all'oggetto nelle sezioni User Object (Oggetto utente), Group Object (Oggetto gruppo) e Organization Object (Oggetto organizzazione), (quando il file include le organizzazioni), del file di configurazione di directory.

Ciascuna di queste sezioni contiene un elemento ImsManagedObject, come ad esempio il codice seguente:

```
<ImsManagedObject name="User" description="My Users">
```

L'elemento ImsManagedObject può includere gli elementi seguenti:

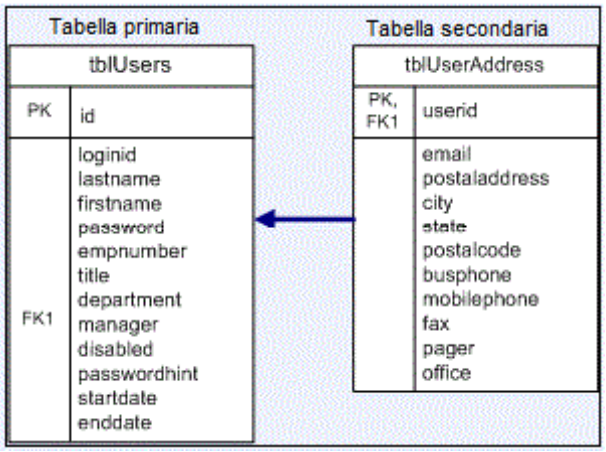
- Tabella (obbligatorio)
- UniqueIdentifier (obbligatorio)
- ImsManagedObjectAttr (obbligatorio)
- RootOrg (solo per gli oggetti organizzazione)

Tabelle di database

Utilizzare l'elemento Tabella nel file di configurazione di directory per definire le tabelle che archiviano le informazioni su un oggetto gestito.

Ciascun oggetto gestito deve avere una tabella primaria che contiene l'ID univoco dell'oggetto. È possibile archiviare informazioni aggiuntive in tabelle secondarie.

L'illustrazione seguente mostra un database che archivia le informazioni sugli utenti in una tabella primaria e secondaria:



Se le informazioni di un oggetto vengono archiviate in più tabelle, creare un elemento Tabella per ciascuna tabella. Utilizzare l'elemento Riferimento nell'elemento Tabella per definire la relazione della tabella secondaria con la tabella primaria.

Ad esempio, se le informazioni di base su un utente vengono archiviate in tblUsers e le informazioni di indirizzo vengono archiviate in tblUserAddress, le definizioni della tabella per l'oggetto gestito utente sono simili alle voci seguenti:

```
<Table name="tblUsers" primary="true" />
<Table name="tblUserAddress">
  <Reference childcol="userid" primarycol="id" />
</Table name>
```

Elementi della tabella

I parametri di un elemento tabella sono i seguenti:

nome

(Obbligatorio)

Specifica il nome della tabella che archivia alcuni o tutti gli attributi in un profilo gestito di un oggetto.

primary

Indica se la tabella è la tabella primaria per l'oggetto gestito. La tabella primaria contiene l'ID univoco dell'oggetto, come segue:

- True: la tabella è la tabella primaria.
- False: la tabella è la tabella secondaria (valore predefinito).

Se non si specifica il parametro primario, CA Identity Manager suppone che la tabella sia quella secondaria.

Nota: solo una tabella può essere la tabella primaria.

filtro

Identifica un sottoinsieme di voci della tabella applicata all'oggetto gestito.

Il parametro di filtro facoltativo può somigliare all'esempio seguente:

```
filter="ORG=2"
```

Nota: il filtro si applica solo a query generate da CA Identity Manager. Se si sovrascrive una query generata con una query personalizzata, specificare il filtro nella query personalizzata.

fullouterjoin

Indica se il join esterno è un join esterno completo.

- True: il join esterno è un join esterno completo. In questo caso, la condizione necessaria per restituire una riga valida si trova in ambedue le tabelle nel join di una riga restituita.
- False: il join esterno è un join esterno sinistro, relativo alla tabella primaria. In questo caso, solo le righe di una tabella della query devono soddisfare la condizione (valore predefinito).

Nota: salvo indicazione contraria, i parametri sono facoltativi.

Il parametro Tabella può contenere uno o più elementi Riferimento per collegare una tabella primaria a tabelle secondarie.

Elemento Riferimento

I parametri nell'elemento di Riferimento sono i seguenti:

childcol

Indica la colonna nella tabella secondaria (specificata nell'elemento Tabella corrispondente) che esegue il mapping sulla colonna nella tabella primaria.

primarycol

Indica la colonna nella tabella primaria che esegue il mapping sulla colonna nella tabella secondaria.

Nota: salvo indicazione contraria, i parametri sono facoltativi.

Specificare le informazioni sull'oggetto

Le informazioni sull'oggetto vengono specificate fornendo valori per vari parametri.

Procedere come descritto di seguito:

1. Individuare l'elemento ImsManagedObject nella sezione User Object (Oggetto utente), Group Object (Oggetto gruppo) o Organization Object (Oggetto organizzazione).
2. Fornire i valori per i parametri seguenti:

   nome

   (Obbligatorio)

   Specifica il nome univoco dell'oggetto gestito.

   descrizione

   Fornisce la descrizione dell'oggetto gestito.

   objecttype

   (Obbligatorio)

   Specifica il tipo di oggetto gestito. Di seguito sono elencati i valori validi:

   - USER
   - GROUP
   - ORGANIZATION (ORGANIZZAZIONE)

   L'elemento ImsManagedObject deve somigliare al codice seguente:

   ```
   <ImsManagedObject name="User" description="My  Users" objecttype="USER">
   ```

3. Fornire informazioni sulla tabella, come descritto nella sezione Tabelle di database (a pagina 117).
4. Specificare la colonna che contiene l'ID univoco dell'oggetto (a pagina 120).

5. Descrivere gli attributi che costituiscono il profilo dell'oggetto (a pagina 121).
6. In caso di configurazione di un oggetto di organizzazione, consultare la sezione Gestione organizzazioni (a pagina 148).

Definizione dell'ID univoco di un oggetto gestito

Ciascun oggetto che CA Identity Manager gestisce deve avere un ID univoco. Assicurarsi che l'ID univoco venga archiviato in una colonna singola nella tabella primaria dell'oggetto gestito. Le tabelle primarie vengono descritte in Tabelle di database (a pagina 117).

Utilizzare gli elementi UniqueIdentifier e UniqueIdentifierAttr per definire l'ID univoco come segue:

```
<UniqueIdentifier>
  <UniqueIdentifierAttr name="tablename.columnname" />
</UniqueIdentifier>
```

L'elemento UniqueIdentifierAttr richiede il parametro di nome. Il valore del parametro di nome è l'attributo in cui l'ID univoco viene archiviato. Il valore può essere un attributo fisico o un attributo noto (a pagina 79).

Quando si specifica un attributo fisico, prendere nota dei punti seguenti:

- Assicurarsi che l'attributo specificato esista nel database e che sia definito nel file di configurazione di directory, come descritto nella sezione Modifica delle descrizioni degli attributi (a pagina 121). Nella descrizione dell'attributo, assicurarsi di specificare l'autorizzazione di sola lettura o di scrittura una sola volta per impedire che l'ID univoco venga modificato durante una sessione.
- Utilizzare la sintassi seguente per specificare un attributo fisico:

  tablename.columnname

  tablename

  Definisce il nome della tabella in cui si trova l'attributo. La tabella specificata deve corrispondere alla tabella primaria.

  columnname

  Definisce il nome della colonna che archivia l'attributo.

- Se il database genera l'ID univoco, specificare un'operazione personalizzata per l'attributo (a pagina 132). Ad esempio, può essere necessario specificare un'operazione per acquisire l'ID generato dal database più recente.

Modifica delle descrizioni degli attributi

Un attributo archivia le informazioni su un'entità utente, gruppo o organizzazione, come ad esempio un numero di telefono o un indirizzo. Gli attributi di un'entità determinano il suo profilo.

Nel file di configurazione di directory, gli attributi vengono descritti negli elementi ImsManagedObjectAttr. Nelle sezioni User Object (Oggetto utente), Group Object (Oggetto gruppo) e Organization Object (Oggetto organizzazione) del file di configurazione di directory:

- Modificare le descrizioni di attributo predefinite per descrivere gli attributi del database.
- Creare nuove descrizioni di attributi copiando una descrizione esistente e modificando i valori secondo le esigenze.

Per ciascun attributo nei profili utente, gruppo e organizzazione, è presente un solo elemento ImsManagedObjectAttr. Ad esempio, un elemento ImsManagedObjectAttr può descrivere un ID utente.

Un elemento ImsManagedObjectAttr somiglia al codice seguente:

```
<ImsManagedObjectAttr
 physicalname="tblUsers.id"
 displayname="User Internal ID"
 description="User Internal ID"
 valuetype="Number"
 required="false"
 multivalued="false"
 maxlength="0"
 hidden="false"
 permission="READONLY">
```

Nota: quando si utilizza un database Oracle, prendere nota dei punti seguenti durante la configurazione degli attributi di oggetti gestiti:

- Per impostazione predefinita, i database Oracle distinguono tra lettere maiuscole e minuscole. La distinzione tra maiuscole e minuscole per gli attributi e i nomi di tabelle nel file di configurazione di directory deve corrispondere a quella degli attributi in Oracle.

  Assicurarsi di specificare una lunghezza massima per i tipi di dati String per impedire il troncamento. Per limitare la lunghezza delle stringhe, è possibile creare una regola di convalida in modo da visualizzare un errore quando un utente digita una stringa che supera la lunghezza massima.

I parametri ImsManagedObjectAttr sono i seguenti:

Nota: salvo indicazione contraria, i parametri sono facoltativi.

physicalname

(Obbligatorio)

Specifica il nome fisico dell'attributo e deve contenere uno dei dettagli seguenti:

- Il nome e la posizione in cui il valore viene archiviato.

  Formato: *tablename.columnname*

  Ad esempio, quando un attributo viene archiviato nella colonna dell'ID nella tabella tblUsers, il nome fisico di tale attributo è il seguente:

  tblUsers.id

  È obbligatorio definire ciascuna tabella che contiene un attributo nell'elemento Tabella (a pagina 117).

- Un attributo noto.

  Un attributo noto può rappresentare un valore calcolato. Ad esempio, è possibile utilizzare un attributo noto per fare riferimento a un attributo calcolato mediante un'operazione personalizzata. (a pagina 132)

displayname

(Obbligatorio)

Specifica un nome univoco per l'attributo.

Nella console utente, il nome visualizzato viene mostrato nell'elenco degli attributi disponibili per essere aggiunti a una schermata di attività.

Nota: non modificare il nome visualizzato di un attributo nel file di configurazione di directory (directory.xml). Per modificare il nome dell'attributo su una schermata di attività, è possibile specificare un'etichetta per l'attributo nella definizione della schermata di attività. Per ulteriori informazioni, consultare la *Guida per l'amministratore*.

descrizione

Contiene la descrizione dell'attributo.

valuetype

Specifica il tipo di dati dell'attributo. Di seguito sono elencati i valori validi:

Stringa

Il valore può essere qualsiasi stringa.

Questo è il valore predefinito.

Numero intero

Il valore deve essere un numero intero.

Nota: l'attributo numero intero non supporta numeri decimali.

Numero

Il valore deve essere un numero intero. L'opzione Numero supporta numeri decimali.

Data

Il valore deve trasformarsi in una data valida secondo il modello:

MM/dd/yyyy

ISODate

Il valore deve trasformarsi in una data valida secondo il modello yyyy-MM-dd.

UnicenterDate

Il valore deve trasformarsi in una data valida secondo il modello YYYYYYYDDD dove:

YYYYYYYDDD è una rappresentazione di sette numeri di un anno che inizia con tre zero. Ad esempio: 0002008

DDD è una rappresentazione di tre numeri per il giorno che inizia con degli zero, a seconda alle esigenze. I valori validi sono compresi tra 001 e 366.

Se il valuetype di un attributo è errato, le query di CA Identity Manager non possono riuscire correttamente.

Per assicurarsi che un attributo venga archiviato correttamente nel database, è possibile associarlo con una regola di convalida.

obbligatorio

Indica se è necessario specificare un valore per l'attributo, come segue:

- True: obbligatorio
- False: facoltativo (valore predefinito)

multivalore

Indica se l'attributo può avere più valori, come segue:

- True: un attributo può avere più valori.
- False: l'attributo può avere un solo valore singolo (impostazione predefinita).

Ad esempio, l'attributo di appartenenza di gruppo in un profilo utente è multivalore per archiviare i gruppi a cui un utente appartiene.

Per archiviare attributi multivalore in un elenco delimitato invece che in una tabella con più righe, viene richiesto di definire il carattere di delimitazione nel parametro di delimitazione.

Assicurarsi che il numero di valori possibili e la lunghezza di ciascun valore che la colonna abilita siano sufficienti.

Importante. Assicurarsi che l'attributo Appartenenza al gruppo nella definizione dell'oggetto utente sia multivalore.

noto

Fornisce il nome dell'attributo noto.

Gli attributi noti hanno un significato specifico in CA Identity Manager.

Formato: %*ATTRIBUTENAME*%

Nota: quando un'operazione personalizzata viene associata a un attributo, viene richiesto di specificare un attributo famoso (a pagina 79).

maxlength

Determina la dimensione massima della colonna.

permission

Indica se è possibile modificare il valore di un attributo in una schermata di attività, come segue:

READONLY

Il valore viene visualizzato ma non può essere modificato.

WRITEONCE

Non è possibile modificare il valore una volta che l'oggetto è stato creato. Ad esempio, non è possibile modificare un ID utente dopo che l'utente è stato creato.

READWRITE

È possibile modificare il valore (impostazione predefinita).

nascosto

Indica se un attributo viene visualizzato nelle schermate di attività di CA Identity Manager, come segue:

- True: l'attributo non viene visualizzato dagli utenti.
- False: l'attributo viene visualizzato dagli utenti (impostazione predefinita).

Gli attributi logici utilizzano attributi nascosti.

Nota: per ulteriori informazioni sugli attributi logici, consultare la *Programming Guide for Java*.

sistema

Indica che gli attributi sono stati utilizzati solo da CA Identity Manager. Gli utenti non devono modificare gli attributi nella console utente, come segue:

- True: gli utenti non possono modificare l'attributo. L'attributo non verrà visualizzato nella console utente.
- False: gli utenti possono modificare questo attributo ed è possibile aggiungerlo alle schermate di attività nella console utente (impostazione predefinita).

validationruleset

Associa un set di regole di convalida all'attributo.

Verificare che il set di regole di convalida specificato sia definito in un elemento ValidationRuleSet nel file di configurazione di directory.

delimitatore

Definisce il carattere che separa i valori quando vengono archiviati più valori in una singola colonna.

Importante. Assicurarsi che il parametro multivalore sia impostato su True per applicare il parametro di delimitazione.

Nota: per impedire la visualizzazione di informazioni sensibili, come password o salari, nella console utente è possibile specificare i parametri DataClassification. (a pagina 74)

Gestione degli attributi sensibili

CA Identity Manager fornisce i metodi seguenti per la gestione degli attributi sensibili:

- Classificazioni dei dati per gli attributi

  Le classificazioni dei dati consentono di specificare le proprietà di visualizzazione e crittografia per gli attributi che si trovano nel file di configurazione di directory (directory.xml).

  È possibile definire le classificazioni dei dati che gestiscono attributi sensibili nel modo seguente:

  - Nelle schermate delle attività di CA Identity Manager, visualizzare il valore di un attributo come una serie di asterischi.

    Ad esempio, è possibile visualizzare le password come asterischi invece di visualizzarle come testo semplice (non crittografato).

  - Nella schermata Visualizza attività inoltrate, nascondere il valore attributo.

    Questa opzione consente di nascondere attributi agli amministratori. Ad esempio, è possibile nascondere i dettagli sugli stipendi agli amministratori che visualizzano lo stato dell'attività relativa in CA Identity Manager ma non devono visualizzare i dettagli sugli stipendi.

  - Ignorare certi attributi quando si crea una copia di un oggetto esistente.
  - Crittografia di un attributo

- Stili di campo nelle schermate dei profili di attività

  Se non si desidera modificare un attributo nel file directory.xml, impostare la proprietà di visualizzazione dell'attributo nelle definizioni della schermata in cui viene visualizzato l'attributo sensibile.

  Lo stile di campo consente di visualizzare gli attributi, come ad esempio la password, come una serie di asterischi invece di semplice testo.

  Nota: per ulteriori informazioni sullo stile del campo per gli attributi sensibili, cercare gli stili di campo nella Guida in linea della console utente.

Attributi di classificazione dei dati

L'elemento di classificazione dei dati fornisce un modo di associare proprietà aggiuntive a una descrizione di attributo. I valori di questo elemento determinano come CA Identity Manager gestisce l'attributo. Questo elemento supporta i parametri seguenti:

- sensitive

  Consente a CA Identity Manager di visualizzare l'attributo come una serie di asterischi (*) nella schermata Visualizza attività inoltrate. Questo parametro impedisce a valori vecchi e nuovi dell'attributo di essere visualizzati in testo non crittografato nelle schermata Visualizza attività inoltrate.

  In aggiunta, se si crea una copia di un utente esistente nella console utente, questo parametro impedisce all'attributo di essere copiato nel nuovo utente.

- vst_hide

  Nasconde l'attributo nella schermata Dettagli evento della scheda Visualizza attività inoltrate. A differenza degli attributi sensibili, che vengono visualizzati come asterischi, gli attributi vst_hidden non vengono visualizzati.

  È possibile utilizzare questo parametro per impedire che eventuali modifiche a un attributo, ad esempio relative ai dettagli sullo stipendio, vengano visualizzate in Visualizza attività inoltrate.

- ignore_on_copy

  Consente a CA Identity Manager di ignorare un attributo quando un amministratore crea una copia di un oggetto nella console utente. Ad esempio, supporre di avere specificato ignore_on_copy per l'attributo di password su un oggetto utente. Quando si copia un profilo utente, CA Identity Manager non applica la password dell'utente attuale al nuovo profilo utente.

- AttributeLevelEncrypt

  Consente di crittografare i valori di attributo quando vengono archiviati nell'archivio utenti. Se CA Identity Manager è abilitato per FIPS 140-2, CA Identity Manager utilizza la crittografia RC2 o la crittografia FIPS 140-2.

  Per ulteriori informazioni sulla conformità FIPS 140-2 in CA Identity Manager, consultare la *Guida alla configurazione*.

  Gli attributi vengono visualizzati in testo non crittografato durante il runtime.

  Nota: per impedire agli attributi di venire visualizzati in testo non crittografato nelle schermate, è possibile aggiungere un elemento di classificazione di dati sensibile agli attributi crittografati. Per ulteriori informazioni, consultare la sezione Aggiunta della crittografia a livello di attributo (a pagina 75).

- PreviouslyEncrypted

  Consente a CA Identity Manager di individuare e decrittografare qualsiasi valore crittografato nell'attributo quando accede all'oggetto nell'archivio utenti.

  Si utilizza questa classificazione dei dati per decrittografare qualsiasi valore precedentemente crittografato.

  Il valore di testo non crittografato viene salvato nell'archivio quando si salva l'oggetto.

Configurazione di attributi di classificazione dei dati

Procedere come descritto di seguito:

1. Individuare l'attributo nel file di configurazione di directory.
2. Dopo la descrizione dell'attributo, aggiungere l'attributo seguente:

   <DataClassification name="*parameter*">

   parameter

   Rappresenta uno dei parametri seguenti:

   sensitive

   vst_hide

   ignore_on_copy

   AttributeLevelEncrypt

   PreviouslyEncrypted

   Ad esempio, una descrizione di attributo che include l'attributo di classificazione di dati vst_hide assomiglia al codice seguente:

```
<ImsManagedObjectAttr physicalname="salary" displayname="Salary"
description="salary" valuetype="String" required="false" multivalued="false"
maxlength="0">
    <DataClassification name="vst_hide"/>
```

Crittografia a livello di attributo

È possibile crittografare un attributo nell'archivio utenti specificando una classificazione dei dati AttributeLevelEncypt per quell'attributo nel file di configurazione di directory (directory.xml). Quando la crittografia a livello di attributo viene abilitata, CA Identity Manager crittografa il valore di quell'attributo prima di archiviarlo nell'archivio utenti. L'attributo viene visualizzato come testo non crittografato nella console utente.

Nota: per impedire agli attributi di venire visualizzati in testo non crittografato nelle schermate, è possibile aggiungere un elemento di classificazione di dati sensibile agli attributi crittografati. Per ulteriori informazioni, consultare la sezione Aggiunta della crittografia a livello di attributo (a pagina 75).

Se il supporto FIPS 140-2 è abilitato, l'attributo viene crittografato mediante la crittografia RC2 o la crittografia FIPS 140-2.

Prima di implementare la crittografia a livello di attributo, prendere nota dei punti seguenti:

- CA Identity Manager non è in grado di trovare attributi crittografati in una ricerca.

  Supporre che un attributo crittografato sia aggiunto a un criterio di membro, amministratore, titolare o a un criterio di identità. CA Identity Manager non è in grado di risolvere il criterio correttamente perché non può cercare l'attributo.

  Considerare di impostare l'attributo su searchable="false" nel file directory.xml—Ad esempio:

  <ImsManagedObjectAttr physicalname="title" description="Title" displayname="Title" valuetype="String" maxlength="0" searchable="false">

  <DataClassification name="AttributeLevelEncrypt"/>

  </ImsManagedObjectAttr>

- Se CA Identity Manager utilizza un archivio utenti condiviso e una directory di provisioning, è necessario non crittografare gli attributi del server di provisioning.
- Non abilitare AttributeLevelEncrypt per le password utente negli ambienti che soddisfano i criteri seguenti:
  - l'inclusione dell'integrazione con CA SiteMinder e
  - l'archiviazione degli utenti in un database relazionale

  Quando CA Identity Manager si integra con CA SiteMinder, le password crittografate causano degli errori quando i nuovi utenti provano ad accedere, immettendo le password con testo non crittografato.
- Se si abilita la crittografia a livello di attributo per un archivio utenti utilizzato da applicazioni diverse da CA Identity Manager, le altre applicazioni non potranno utilizzare l'attributo crittografato.

Aggiunta della crittografia a livello di attributo

Supporre di avere aggiunto una crittografia a livello di attributo a una directory di CA Identity Manager. CA Identity Manager esegue automaticamente la crittografia dei valori dell'attributo di testo non crittografato quando si salva l'oggetto associato all'attributo. Ad esempio, se si crittografa l'attributo di password, la password viene crittografata al momento di salvare il profilo dell'utente.

Nota: per crittografare il valore dell'attributo, l'attività che si utilizza per salvare l'oggetto deve includere l'attributo. Per crittografare l'attributo di password nell'esempio precedente, assicurarsi che il campo Password venga aggiunto all'attività che si utilizza per salvare l'oggetto, come ad esempio l'attività Modifica utente.

Tutti i nuovi oggetti vengono creati con valori crittografati nell'archivio utenti.

Procedere come descritto di seguito:

1. Completare una delle seguenti attività:
   - Creare una directory di CA Identity Manager
   - Aggiornare una directory esistente esportando le impostazioni della directory.
2. Aggiungere gli attributi di classificazione dei dati seguenti all'attributo che si desidera crittografare nel file directory.xml:

   AttributeLevelEncrypt

   Mantiene il valore dell'attributo in un modulo crittografato nell'archivio utenti.

   Maiuscole/minuscole (facoltativo)

   Nasconde il valore dell'attributo nelle schermate di CA Identity Manager. Ad esempio, una password viene visualizzata come asterischi (*).

   Ad esempio:

```
<ImsManagedObjectAttr physicalname="salary"
displayname="Salary" description="salary" valuetype="String"
required="false" multivalued="false" maxlength="0"
searchable="false">
<DataClassification name="AttributeLevelEncrypt"/>
<DataClassification name="sensitive"/>
```

3. Se è stata creata una directory di CA Identity Manager, associare la directory a un ambiente.
4. Per obbligare CA Identity Manager a crittografare immediatamente tutti i valori, modificare tutti gli oggetti mediante l'Utilità di caricamento in blocco.

   Nota: per ulteriori informazioni sull'Utilità di caricamento in blocco, consultare la *Guida per l'amministratore*.

Rimozione della crittografia a livello di attributo

Se si dispone di un attributo crittografato nella directory di CA Identity Manager e questo viene archiviato con il valore di quell'attributo come testo non crittografato, è possibile rimuovere la classificazione dei dati AttributeLevelEncrypt.

Una volta che la classificazione dei dati è stata rimossa, CA Identity Manager smette di crittografare i nuovi valori di attributo. I valori esistenti vengono decrittografati quando si salva l'oggetto associato all'attributo.

Nota: per decrittografare il valore dell'attributo, l'attività che si utilizza per salvare l'oggetto deve includere l'attributo. Ad esempio, per decrittografare una password per un utente esistente, si salva l'oggetto utente con un'attività che include il campo Password, come ad esempio l'attività Modifica utente.

Per obbligare CA Identity Manager a individuare e decrittografare qualsiasi valore crittografato che rimane nell'archivio utenti per l'attributo, è possibile specificare un'altra classificazione dei dati, PreviouslyEncrypted. Il valore di testo non crittografato viene salvato nell'archivio utenti quando si salva l'oggetto.

Nota: l'aggiunta della classificazione dei dati PreviouslyEncrypted consente di aggiungere ulteriore elaborazione a ogni caricamento di oggetti. Per prevenire problemi di prestazioni, si consiglia di aggiungere la classificazione dei dati PreviouslyEncrypted, di caricare e salvare ciascun oggetto associato a quell'attributo e infine rimuovere la classificazione dei dati. Questo metodo converte automaticamente tutti i valori crittografati in testo non crittografato archiviato.

Procedere come descritto di seguito:

1. Esportare le impostazioni della directory per la directory di CA Identity Manager appropriata.
2. Nel file directory.xml, rimuovere la classificazione dei dati, AttributeLevelEncrypt, dagli attributi che si desidera decrittografare.
3. Se si desidera obbligare CA Identity Manager a rimuovere valori precedentemente crittografati, aggiungere l'attributo di classificazione dei dati PreviouslyEncrypted.

   Ad esempio:

   ```
   <ImsManagedObjectAttr physicalname="salary" displayname="Salary"
   description="salary" valuetype="String" required="false" multivalued="false"
   maxlength="0" searchable="false">
   <DataClassification name="PreviouslyEncrypted"/>
   ```

4. Per obbligare CA Identity Manager a decrittografare immediatamente tutti i valori, modificare tutti gli oggetti mediante l'Utilità di caricamento in blocco.

   Nota: per ulteriori informazioni sull'Utilità di caricamento in blocco, consultare la *Guida per l'amministratore*.

Operazioni personalizzate

È possibile definire le operazioni personalizzate per certi oggetti gestiti in modo da poter eseguire le attività seguenti:

- Utilizzare le procedure archiviate
- Ottimizzare le query per la propria struttura di database.
- Recuperare un ID univoco generato dal database

Le operazioni personalizzate sono applicabili solo agli attributi.

Quando si specificano le operazioni personalizzate, ricordarsi dei punti seguenti:

- Gli utenti che specificano le operazioni personalizzate devono conoscere il linguaggio SQL.
- CA Identity Manager non convalida le operazioni personalizzate. Fino al runtime, gli errori di sintassi e le query non valide non vengono segnalati.
- Se si specifica un'operazione personalizzata per un attributo, non è possibile utilizzare quell'attributo nei filtri di ricerca nelle attività di CA Identity Manager.
- Le operazioni personalizzate devono essere compatibili con gli standard XML. Rappresentare caratteri speciali mediante la sintassi XML. Ad esempio, specificare una virgoletta singola (') come '

Per specificare un'operazione personalizzata, utilizzare l'elemento Operazione.

Elemento Operazione

L'elemento Operazione definisce una dichiarazione SQL che consente di eseguire una query personalizzata o di chiamare una procedura archiviata per la creazione, il recupero, la modifica o l'eliminazione di un attributo. L'elemento Operazione è un elemento secondario dell'elemento IMSManagedObjectAttr, come viene mostrato nell'esempio seguente:

```
<ImsManagedObjectAttr physicalname="tblUsers.id" displayname="User Internal ID"
description="User Internal ID" valuetype="Number" required="false"
multivalued="false" maxlength="0" hidden="false" permission="READONLY">
  <Operation name="GetDb" value="select @@identity" />
```

I parametri dell'elemento Operazione sono i seguenti:

nome

Specifica un nome predefinito per un'operazione. Di seguito sono elencate le operazioni valide:

- Creazione
- Acquisisci
- Imposta
- Eliminazione
- GetDB (Acquisizione DB)

  L'operazione GetDB (Acquisizione DB) recupera un ID univoco dal database durante un'attività di creazione, quando l'ID univoco viene generato mediante il database o tramite una procedura archiviata.

valore

Definisce la dichiarazione SQL o la procedura archiviata da eseguire. Di seguito sono elencati i valori validi:

- INSERT
- SELECT
- UPDATE
- DELETE
- CALL (per procedure archiviate)

Nota: salvo indicazione contraria, i parametri sono facoltativi.

L'elemento Operazione può contenere uno o più elementi Parametro.

Elemento Parametro

Un elemento Parametro specifica i valori che vengono passati alla query. Quando sono definiti più elementi Parametro, i valori vengono passati alla query nell'ordine elencato dato.

Un elemento Parametro richiede il parametro di nome. Il valore del parametro di nome può essere un attributo fisico o un attributo noto (a pagina 79).

Nota: CA Identity Manager deve comprendere i valori trasferiti a una query con l'elemento Parametro. Ad esempio, il valore può corrispondere a un nome fisico o a un attributo noto definito negli attributi ImsManagedObjectAttr.

Quando si specifica un attributo fisico, prendere nota dei punti seguenti:

- Utilizzare la sintassi seguente per specificare un attributo fisico:

  tablename.columnname

  - *tablename*

    Fornisce il nome della tabella in cui si trova l'attributo. La tabella specificata deve corrispondere alla tabella primaria.

  - *columnname*

    Fornisce il nome della colonna che archivia l'attributo.

- L'attributo specificato deve esistere nel database ed è definito nel file di configurazione di directory, come descritto nella sezione Modifica delle descrizioni di attributo (a pagina 121).

Esempio: operazioni personalizzate per l'attributo Business Number

Nell'esempio seguente, l'attributo Business Number viene generato mediante la chiamata di una procedura archiviata. Non si tratta di un attributo fisico nel database.

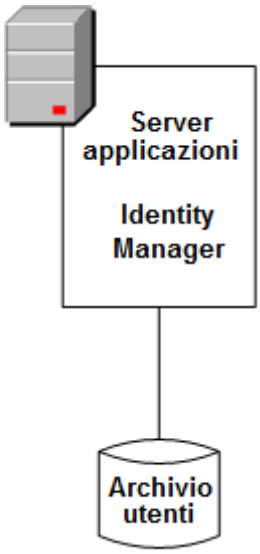
```
<ImsManagedObjectAttr wellknown="%BUSINESS_NUMBER%"     displayname="Business
Number" description="Business Number"     valuetype="String" required="false"
multivalued="false"     maxlength="0">
<Operation name="Get" value="call sp_getbusinessnumber(?)">
    <Parameter name="%USER_ID%"/>
</Operation>
<Operation name="Set" value="call sp_setbusinessnumber(?,?)">
    <Parameter name="%USER_ID%"/>
    <Parameter name="%BUSINESS_NUMBER%"/>
</Operation>
<Operation name="Delete" value="call sp_deletebusinessnumber(?)">
    <Parameter name="%USER_ID%"/>
</Operation>
```

Si noti quanto segue:

- sp_getbusinessnumber, sp_setbusinessnumber e sp_deletebusinessnumber sono procedure archiviate definite dall'utente.
- Viene eseguito il mapping del valore che viene restituito dall'operazione Acquisisci all'attributo %BUSINESS_NUMBER%.
- Il punto interrogativo (?) indica le sostituzioni effettuate al runtime prima dell'esecuzione della query. Ad esempio, nell'operazione Acquisisci l'attributo noto %USER_ID% viene passato alla procedura archiviata sp_getbusinessnumber.

Connessione alla directory utente

CA Identity Manager si connette a una directory utente per archiviare informazioni, come ad esempio le informazioni relative a un utente, gruppo e organizzazione, come viene mostrato nell'illustrazione seguente:



Una nuova directory o database non sono necessari. Tuttavia, la directory o il database esistente devono risiedere in un sistema che ha un nome di dominio completo (FQDN).

Per visualizzare un elenco di tipi di directory e database, consultare la matrice di supporto di CA Identity Manager nel sito Web del Supporto di CA.

Si configura una connessione all'archivio utenti quando si crea una directory di CA Identity Manager nella console di gestione.

Se si esporta la configurazione di directory dopo avere creato una directory di CA Identity Manager, le informazioni di connessione della directory utente vengono visualizzate Provider dei file di configurazione di directory.

Descrizione di una connessione di database

Per descrivere una connessione di database, utilizzare l'elemento Provider e i relativi elementi secondari nel file directory.xml.

Nota: se si sta creando una directory di CA Identity Manager, non è necessario fornire informazioni di connessione sulla directory nel file directory.xml. Si forniscono informazioni di connessione nella procedura guidata di creazione della directory di CA Identity Manager nella console di gestione.

Modificare l'elemento Provider solo per gli aggiornamenti.

Elemento Provider

L'elemento Provider include gli elementi secondari seguenti:

JDBC (obbligatorio)

Identifica l'origine dati JDBC da utilizzare quando ci si connette all'archivio utenti. Specificare il nome JNDI fornito al momento della creazione dell'origine dati JDBC (a pagina 107).

Credentials (Credenziali) (obbligatorio)

Fornisce il nome utente e la password per accedere al database.

DSN

Identifica l'origine dati ODBC da utilizzare quando ci si connette all'archivio utenti.

Nota: questo elemento secondario si applica solo quando CA Identity Manager si integra con SiteMinder. Negli ambienti di CA Identity Manager che non includono SiteMinder, questo elemento secondario viene ignorato.

SiteMinderQuery (Query di SiteMinder)

Specifica gli schemi di query personalizzati per individuare le informazioni relative all'utente in un database relazionale.

Nota: questo elemento secondario si applica solo quando CA Identity Manager si integra con SiteMinder. Negli ambienti di CA Identity Manager che non includono SiteMinder, questo elemento secondario viene ignorato.

Una connessione di database completata somiglia all'esempio seguente:

```
<Provider type="RDB" userdirectory="@SMDirName">
        <JDBC datasource="@SMDirJDBCDataSource"/>
        <Credentials user="@SMDirUser"
                cleartext="true">@SMDirPassword</Credentials>
        <DSN name="@SMDirDSN" />
        <SiteMinderQuery name="AuthenticateUser" query="SELECT TBLUSERS.LOGINID
FROM    TBLUSERS WHERE TBLUSERS.LOGINID='%s' AND TBLUSERS.PASSWORD='%s'" />
</provider>
```

Gli attributi per l'elemento Provider sono i seguenti:

type

Specifica il tipo di database. Per i database Microsoft SQL Server e Oracle, specificare RDB (valore predefinito).

userdirectory

Specifica il nome della connessione della directory utente. Questo parametro corrisponde al nome dell'oggetto Connessione fornito durante la creazione della directory.

Se CA Identity Manager si integra con SiteMinder per l'autenticazione, crea una connessione alla directory utente in SiteMinder con il nome specificato per l'oggetto di connessione durante l'installazione. Se si desidera connettersi a una directory utente di SiteMinder esistente, immettere il nome di quella directory utente quando viene richiesto per l'oggetto Connessione. CA Identity Manager popola il parametro userdirectory con il nome specificato.

Se CA Identity Manager non viene integrato con SiteMinder, il valore del parametro userdirectory corrisponde a qualsiasi nome assegnato alla connessione JDBC con l'archivio utenti.

Nota: non specificare un nome per la connessione della directory utente nel file directory.xml. CA Identity Manager richiede di fornire il nome durante la creazione della directory.

Credenziali di database

Per connettersi al database, CA Identity Manager deve fornire credenziali valide all'origine dati. Le credenziali vengono definite nell'elemento Credenziali, che è simile all'esempio seguente:

```
<Credentials user="@SMDirUser" cleartext="true">
  "MyPassword"
</Credentials>
```

Se non si specifica una password nell'elemento Credentials (Credenziali) e si tenta di creare la directory di CA Identity Manager nella console di gestione, vengono richieste le credenziali di password.

Nota: si consiglia di specificare la password nella console di gestione.

Se si specifica la password nella console di gestione, CA Identity Manager esegue la crittografia della password. Se non si desidera che la password venga visualizzata in testo non crittografato, crittografarla utilizzando lo strumento di password installato con CA Identity Manager. Le password di SiteMinder hanno istruzioni sull'utilizzo dello strumento di password.

Nota: è possibile specificare solo un set di credenziali. Quando si definiscono più origini dati, le credenziali specificate devono essere applicate a tutte le origini dati.

I parametri delle credenziali sono i seguenti:

utente

Specifica l'ID di accesso per un account che può accedere all'origine dati.

Non specificare un valore per il parametro utente nel file directory.xml. CA Identity Manager richiede di fornire l'ID di accesso quando si crea la directory di CA Identity Manager nella console di gestione.

cleartext

Determina se la password viene visualizzata con testo non crittografato nel file directory.xml:

- True: la password viene mostrata con testo non crittografato.
- False: la password è crittografata (impostazione predefinita).

Nota: questi parametri sono facoltativi.

Nome origine dati (DSN, Data Source Name)

L'elemento DSN nel file directory.xml ha un solo parametro: il nome dell'origine dati ODBC che CA Identity Manager utilizza per connettersi al database. Il valore del parametro di nome deve corrispondere al nome di un'origine dati esistente.

Nota: questo elemento è valido solo se CA Identity Manager si integra con SiteMinder. Se CA Identity Manager non si integra con SiteMinder, questo elemento viene ignorato.

Se il valore del parametro di nome è @SmDirDSN, non è necessario specificare un nome DSN nel file directory.xml. CA Identity Manager richiede di fornire il nome DSN quando si importa il file di configurazione di directory.

Per configurare un failover, definire più elementi DSN. Se l'origine dati primaria non riesce a rispondere a una richiesta, l'origine dati successiva definita risponderà alla richiesta.

Ad esempio, supporre di avere configurato il failover nel modo seguente:

```
<DSN name="DSN1">
<DSN name="DSN2">
```

CA Identity Manager utilizza l'origine dati DSN1 per connettersi al database. Se si verifica un problema con DSN1, CA Identity Manager prova a connettersi al database mediante DSN2.

Nota: le credenziali specificate nell'elemento Credentials (Credenziali) (a pagina 138) devono essere applicate a tutti i DSN definiti.

Schemi di query SQL

CA Identity Manager utilizza gli schemi di query per trovare le informazioni relative a utenti e gruppi in un database relazionale.

Nota: questo elemento è valido solo se CA Identity Manager si integra con SiteMinder. Negli ambienti che non includono SiteMinder, questo parametro viene ignorato.

Quando si crea una directory di CA Identity Manager nella console di gestione, CA Identity Manager genera un insieme di schemi di query basati sugli schemi di query obbligatori di SiteMinder. (Per informazioni complete sugli schemi di query di SiteMinder, consultare la guida *CA SiteMinder Web Access Manager Policy Server Configuration Guide*.) I nomi di tabella e colonna negli schemi di query di SiteMinder vengono sostituiti con i dati specificati nel file di configurazione di directory.

Definizione degli schemi di query personalizzati

Gli schemi di query vengono definiti negli elementi Query di SiteMinder nel file di configurazione di directory. Un elemento Query di SiteMinder è simile al seguente:

```
<SiteMinderQuery name="SetUserProperty" query="update tblUsers set %s =
&apos;%s&apos; where loginid = &apos;%s&apos;" />
```

Nota: nella query di esempio, ' è la sintassi XML è per la virgoletta singola (’).

L'elemento Query di SiteMinder è valido solo quando CA Identity Manager si integra con SiteMinder.

I parametri di schema di query sono i seguenti:

nome

Specifica il nome ridefinito di uno schema di query di SiteMinder.

Non modificare questo valore.

query

Specifica la dichiarazione SQL o la procedura archiviata da eseguire. Di seguito sono elencati i valori validi:

- INSERT
- SELECT
- UPDATE
- DELETE
- CALL (per procedure archiviate)

Nota: questi parametri sono obbligatori per l'elemento Query di SiteMinder.

Prima di personalizzare gli schemi di query, attenersi ai punti seguenti:

- Acquisire familiarità con gli schemi di query predefiniti.

  Nota: per ulteriori informazioni sugli schemi di query predefiniti, consultare la *CA SiteMinder Web Access Manager Policy Server Configuration Guide*.

- Acquisire vasta esperienza nello sviluppo di query SQL.

Modificare gli schemi di query predefiniti

Eseguire la procedura seguente per modificare gli schemi di query predefiniti.

Procedere come descritto di seguito:

1. Esportare il file di configurazione di directory.

   CA Identity Manager genera un file di configurazione di directory che contiene tutte le impostazioni correnti della directory di CA Identity Manager, inclusi gli schemi di query generati.

2. Salvare il file di configurazione di directory.

   Nota: se si desidera creare un backup del file di configurazione di directory originale, salvare il file con un nome diverso o in una posizione diversa prima di salvare il file esportato.

3. Individuare lo schema di query generato da CA Identity Manager che si desidera modificare.

4. Immettere lo schema di query o la procedura archiviata da eseguire nel parametro di query.

   Nota: non modificare il nome della query.

5. Dopo avere eseguito le modifiche necessarie, salvare il file di configurazione di directory.

   Importare il file per aggiornare la directory di CA Ide (a pagina 185)ntity Manager.

Attributi noti di un database relazionale

Gli attributi noti hanno un significato speciale in CA Identity Manager. Vengono identificati dalla sintassi seguente:

%ATTRIBUTENAME%

In questa sintassi, *ATTRIBUTENAME* deve essere in maiuscolo.

Mediante una descrizione di attributo (a pagina 121), viene eseguito il mapping di un attributo noto su un attributo fisico.

Nella descrizione di attributo seguente, viene eseguito il mapping dell'attributo tblUsers.password sull'attributo noto %PASSWORD% in modo che CA Identity Manager tratti il valore tblUsers.password come password:

```
<ImsManagedObjectAttr
        physicalname="tblUsers.password"
        displayname="Password"
        description="Password"
        valuetype="String"
        required="false"
        multivalued="false"
        wellknown="%PASSWORD%"
        maxlength="0" />
```

Alcuni attributi noti sono obbligatori, altri facoltativi.

Attributi utente noti

Di seguito viene riportato un elenco di attributi utente noti:

%ADMIN_ROLE_CONSTRAINT%

Contiene l'elenco di ruoli di amministrazione (a pagina 145) che vengono assegnati all'amministratore (a pagina 145).

L'attributo fisico mappato su %ADMIN_ROLE_CONSTRAINT% deve disporre di più valori per potersi adattare a più ruoli.

Si consiglia di indicizzare l'attributo di cui viene eseguito il mapping su %ADMIN_ROLE_CONSTRAINT%.

%CERTIFICATION_STATUS%

(Obbligatorio per utilizzare la funzionalità di certificazione utente)

Contiene lo stato di certificazione di un utente.

Nota: per ulteriori informazioni sulla certificazione utente, consultare la *Guida per l'amministratore*.

%DELEGATORS%

Esegue il mapping su un elenco di utenti che hanno delegato elementi di lavoro all'utente attuale.

Questo attributo è obbligatorio per utilizzare la delega. È necessario che l'attributo fisico che ha eseguito il mapping su %DELEGATORS% sia multivalore e in grado di contenere stringhe.

Importante. La modifica diretta di questo campo tramite le attività di CA Identity Manager o uno strumento esterno può avere implicazioni di protezione significative.

%EMAIL%

(Obbligatorio per abilitare la funzionalità di notifica di posta elettronica)

Memorizza l'indirizzo e-mail di un utente.

%ENABLED_STATE%

(Obbligatorio)

Tiene traccia dello stato di un utente.

Nota: il tipo di dati dell'attributo fisico di cui viene eseguito il mapping su %ENABLED_STATE% deve essere String.

%FIRST_NAME%

Contiene il nome di un utente.

%FULL_NAME%

(Obbligatorio)

Contiene il nome e il cognome di un utente.

%IDENTITY_POLICY%

Contiene l'elenco di criteri di identità che sono stati applicati a un account utente.

CA Identity Manager utilizza questo attributo per determinare se è necessario applicare un criterio di identità a un utente. Se il criterio ha l'impostazione Applicare una volta abilitata e il criterio è elencato nell'attributo %IDENTITY_POLICY%, CA Identity Manager non applica le modifiche nel criterio all'utente.

Nota: per ulteriori informazioni sui criteri di identità, consultare la *Guida per l'amministratore*.

%LAST_CERTIFIED_DATE%

(Obbligatorio per utilizzare la funzionalità di certificazione utente)

Contiene la data in cui è stato certificato il ruolo di un utente.

Nota: per ulteriori informazioni sulla certificazione utente, consultare la *Guida per l'amministratore*.

%LAST_NAME%

Contiene il cognome di un utente.

%ORG_MEMBERSHIP%

(Obbligatorio se le organizzazioni vengono supportate)

Contiene l'ID univoco dell'organizzazione a cui appartiene l'utente.

%ORG_MEMBERSHIP_NAME%

(Obbligatorio se le organizzazioni vengono supportate)

Contiene il nome descrittivo dell'organizzazione a cui appartiene l'utente.

%PASSWORD%

Contiene la password utente.

Nota: il valore dell'attributo %PASSWORD% viene sempre visualizzato come una serie di caratteri asterisco (*) nelle schermate di CA Identity Manager, anche quando l'attributo o il campo non sono impostati per nascondere le password.

%PASSWORD_DATA%

(Obbligatorio per il supporto ai criteri di password)

Specifica l'attributo che tiene traccia delle informazioni sui criteri di password.

Nota: il valore dell'attributo %PASSWORD_DATA% viene sempre visualizzato come una serie di caratteri asterisco (*) nelle schermate di CA Identity Manager, anche quando l'attributo o il campo non sono impostati per nascondere le password.

%PASSWORD_HINT%

(Obbligatorio)

Contiene coppie di domanda e risposta specificate dall'utente. Le coppie di domanda e risposta vengono utilizzate in caso di password dimenticate.

Nota: il valore dell'attributo %PASSWORD_HINT% viene sempre visualizzato come una serie di caratteri asterisco (*) nelle schermate di CA Identity Manager, anche quando l'attributo o il campo non sono impostati per nascondere le password.

%USER_ID%

(Obbligatorio)

Memorizza un ID di accesso dell'utente.

Attributi di gruppo noti

Di seguito viene riportato un elenco di attributi di gruppo noti:

%GROUP_ADMIN%

Contiene gli amministratori di un gruppo.

Nota: l'attributo %GROUP_ADMIN% deve essere multivalore.

%GROUP_DESC%

Contiene la descrizione di un gruppo.

%GROUP_ID%

Contiene l'ID univoco di un gruppo.

%GROUP_MEMBERSHIP%

(Obbligatorio)

Contiene l'elenco di membri di un gruppo.

Nota: l'attributo %GROUP_MEMBERSHIP% deve essere multivalore.

%GROUP_NAME%

(Obbligatorio)

Memorizza il nome di un gruppo.

%ORG_MEMBERSHIP%

(Obbligatorio se le organizzazioni vengono supportate).

Contiene l'ID univoco dell'organizzazione a cui appartiene il gruppo.

%ORG_MEMBERSHIP_NAME%

(Obbligatorio se le organizzazioni vengono supportate).

Contiene il nome descrittivo dell'organizzazione a cui appartiene il gruppo.

%SELF_SUBSCRIBING%

Determina se gli utenti possono registrarsi a un gruppo.

Attributo %ADMIN_ROLE_CONSTRAINT%

Quando si crea un ruolo di amministrazione, si specificano una o più regole per l'appartenenza al ruolo. Hanno questo ruolo gli utenti che soddisfano le regole di appartenenza. Ad esempio, se la regola di appartenenza al ruolo per il ruolo di Manager utenti è title=User Manager, gli utenti che hanno il titolo di Manager utenti possiedono il ruolo di Manager utenti.

Nota: per ulteriori informazioni sui ruoli, consultare la *Guida per l'amministratore*.

%ADMIN_ROLE_CONSTRAINT% consente di designare un attributo di profilo per memorizzare tutti i ruoli di amministrazione di un amministratore.

Utilizzo dell'attributo %ADMIN_ROLE_CONSTRAINT%

Per utilizzare %ADMIN_ROLE_CONSTRAINT% come vincolo per tutti i ruoli di amministrazione, eseguire le attività seguenti:

- Associare l'attributo noto %ADMIN_ROLE_CONSTRAINT% a un attributo di profilo multivalore per consentire più ruoli.

- Quando si configura un ruolo di amministrazione nell'interfaccia utente di CA Identity Manager, lo scenario seguente può essere un vincolo:

  Ruoli di amministrazione equivale a *nome ruolo*

  nome ruolo

  Definisce il nome del ruolo per cui si sta fornendo il vincolo.

  Ad esempio, Ruoli di amministrazione equivale a Manager utenti

Nota: Ruoli di amministrazione è il nome visualizzato predefinito per l'attributo %ADMIN_ROLE_CONSTRAINT%.

Configurazione degli attributi noti

Eseguire la procedura seguente per configurare gli attributi noti.

Procedere come descritto di seguito:

1. Nel file di configurazione di directory, cercare il segno seguente:

   ##

   I valori obbligatori vengono identificati da due segni di cancelletto (##).

2. Sostituire il valore che inizia con ## con il nome fisico dell'attributo che si desidera visualizzare nel database. Specificare il nome di attributo con il formato seguente:

   tablename.columnname

   Ad esempio, se l'attributo di password viene archiviato nella colonna di password nella tabella tblUsers, specificarlo nel modo seguente:

   tblUsers.password

3. Ripetere i passaggi 1 e 2 finché non sono stati sostituiti tutti i valori obbligatori e sono stati inclusi i valori facoltativi desiderati.
4. Eseguire il mapping degli attributi noti su attributi fisici, secondo le esigenze.
5. Salvare il file di configurazione di directory.

Configurazione dei gruppi auto-sottoscriventi

È possibile abilitare gli utenti self-service per la sottoscrizione ai gruppi configurando il supporto per i gruppi auto-sottoscriventi nel file di configurazione di directory.

Procedere come descritto di seguito:

1. Nella sezione Self-subscribing Groups (Gruppi auto-sottoscriventi), aggiungere l'elemento SelfSubscribingGroups nel modo seguente:

   `<SelfSubscribingGroups type=`*`search_type`* `org=`*`org_dn`*`>`

2. Digitare i valori per i parametri seguenti:

   type

   Indica la posizione in cui CA Identity Manager cerca i gruppi auto-sottoscriventi. Di seguito sono elencati i valori validi:

   - NONE—CA Identity Manager non cerca gruppi. Specificare NONE per impedire agli utenti di registrarsi ai gruppi.
   - ALL: CA Identity Manager cerca tutti i gruppi nell'archivio utenti. Specificare ALL se gli utenti possono registrarsi a tutti i gruppi.
   - INDICATEDORG (*solo per gli ambienti che supportano le organizzazioni*): CA Identity Manager cerca gruppi auto-sottoscriventi nell'organizzazione di un utente e nelle organizzazioni secondarie. Ad esempio, se il profilo di un utente si trova nell'organizzazione Marketing, CA Identity Manager cerca i gruppi auto-sottoscriventi nell'organizzazione Marketing e in tutte le organizzazioni secondarie.
   - SPECIFICORG (*solo per gli ambienti che supportano organizzazioni*): CA Identity Manager cerca in un'organizzazione specifica. Fornire l'ID univoco dell'organizzazione specifica nel parametro org.

   org

   Definisce l'ID univoco dell'organizzazione in cui CA Identity Manager cerca gruppi auto-sottoscriventi.

   Nota: assicurarsi di specificare il parametro org se type=SPECIFICORG.

3. Riavviare il Policy Server di SiteMinder se è stato modificato uno degli elementi seguenti:

   - Il parametro del tipo a o da SPECIFICORG
   - Il valore del parametro org

Una volta che il supporto per i gruppi auto-sottoscriventi è stato configurato nella directory di CA Identity Manager, gli amministratori di CA Identity Manager possono specificare quali gruppi eseguono la sottoscrizione automatica nella console utente.

Quando un utente si registra automaticamente, CA Identity Manager cerca i gruppi in organizzazioni specifiche e mostra i gruppi auto-sottoscriventi all'utente.

Regole di convalida

Una regola di convalida impone requisiti sui dati che un utente digita in un campo di una schermata di attività. I requisiti possono imporre un tipo di dati o un formato o possono verificare che i dati siano validi nel contesto di altri dati nella schermata di attività.

Le regole di convalida sono associate agli attributi di profilo. Prima di elaborare un'attività, CA Identity Manager assicura che i dati immessi per un attributo di profilo soddisfino tutte le regole di convalida associate.

È possibile definire le regole di convalida e associarle ad attributi di profilo nel file di configurazione di directory.

Gestione organizzazione

Per i database relazionali, CA Identity Manager dispone dell'opzione di gestione delle organizzazioni. Quando il database supporta le organizzazioni, i punti seguenti sono veri:

- Le organizzazioni hanno una struttura gerarchica.
- Tutti gli oggetti gestiti, quali utenti, gruppi e altre organizzazioni appartengono a un'organizzazione.
- Quando si elimina un'organizzazione, anche gli oggetti che appartengono a quell'organizzazione vengono eliminati.

Si configura l'oggetto organizzazione nello stesso modo in cui si configurano gli oggetti utente e gruppo con qualche passaggio aggiuntivo.

Impostazione del supporto per le organizzazioni

Per impostare il supporto per le organizzazioni, implementare i passaggi seguenti:

1. Configurare il supporto per le organizzazioni nel database (a pagina 149).
2. Descrivere l'oggetto organizzazione in ImsManagedObject (a pagina 116).

   Assicurarsi di configurare gli elementi secondari Tabella e UniqueIdentifier.
3. Configurare l'organizzazione al livello superiore (a pagina 149).
4. Descrivere gli attributi (a pagina 121) che costituiscono un'organizzazione.
5. Definire gli attributi noti per l'oggetto organizzazione (a pagina 150).

Configurazione del supporto per le organizzazioni nel database

Procedere come descritto di seguito:

1. Aprire uno degli script SQL seguenti in un editor:
   - Database Microsoft SQL Server:

     ims_mssql_rdb.sql
   - Database Oracle:

     ims_oracle_rdb.sql

     Questi file si trovano nella posizione seguente:

     admin_tools\directoryTemplates\RelationalDatabase

     admin_tools fa riferimento alla posizione di installazione degli strumenti di installazione, che vengono installati per impostazione predefinita in una delle posizioni seguenti:

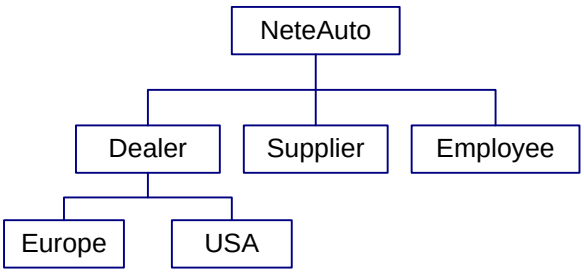
     Windows: C:\Programmi\CA\Identity Manager\IAM Suite\Identity Manager\tools

     UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools
2. Nello script SQL, cercare e sostituire <@primary organization table@> con il nome della tabella primaria dell'oggetto organizzazione. Salvare lo script SQL.
3. Eseguire lo script SQL nel database.

Specifiche dell'organizzazione principale

L'organizzazione principale serve da organizzazione al livello superiore o come organizzazione padre nella directory. Tutte le organizzazioni sono correlate all'organizzazione principale.

Nell'illustrazione seguente, NeteAuto è l'organizzazione principale. Le altre organizzazioni sono organizzazioni secondarie di NeteAuto:



Una definizione di organizzazione principale completa è simile all'esempio seguente:

```
<ImsManagedObject name="Organization" description="My  Organizations"
objecttype="ORG">
   <RootOrg value="select orgid from tblOrganizations where parentorg is null">
      <Result name="%ORG_ID%" />
   </RootOrg>
```

Dopo avere definito le informazioni di base per l'oggetto organizzazione, incluse le tabelle che costituiscono il profilo dell'organizzazione e l'ID univoco dell'oggetto organizzazione, specificare l'organizzazione principale nel file directory.xml:

- Nel parametro di valore dell'elemento RootOrg, definire la query che CA Identity Manager utilizza per recuperare l'organizzazione principale, come nell'esempio seguente:

  ```
  <RootOrg value="select orgid from tblOrganizations where parentorg  is null">
  ```

- Nel parametro di nome dell'elemento Risultato, digitare l'ID univoco dell'organizzazione, come nell'esempio seguente:

  ```
  <Result name="%ORG_ID%" />
  ```

  Nota: il valore del parametro di nome deve essere l'ID univoco dell'oggetto organizzazione.

Attributi noti per le organizzazioni

Definire gli attributi noti per gli attributi nel profilo di un profilo di organizzazione, come descritto nella sezione Attributi noti (a pagina 79).

Gli attributi noti obbligatori e facoltativi di un'organizzazione sono i seguenti:

%ORG_DESCR%

Contiene la descrizione di un'organizzazione.

%ORG_MEMBERSHIP%

(Obbligatorio)

Contiene l'organizzazione padre di un'organizzazione.

Nota: per ulteriori informazioni sull'attributo %ORG_MEMBERSHIP%, consultare la sezione Definizione di una gerarchia organizzativa.

%ORG_MEMBERSHIP_NAME%

(Obbligatorio)

Contiene il nome descrittivo dell'organizzazione padre (a pagina 151) di un'organizzazione.

%ORG_NAME%

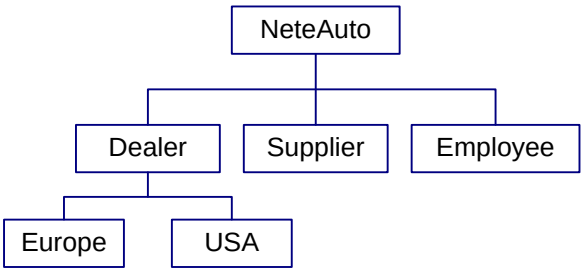
(Obbligatorio)

Contiene il nome dell'organizzazione.

Definizione della gerarchia organizzativa

In CA Identity Manager, le organizzazioni hanno una struttura gerarchica che include un'organizzazione principale e organizzazioni secondarie. Le organizzazioni secondarie possono disporre a loro volta di organizzazioni secondarie.

Ciascuna organizzazione, tranne l'organizzazione principale, ha un'organizzazione padre. Ad esempio, nell'illustrazione seguente, Dealer (Rivenditore) corrisponde all'organizzazione padre per le organizzazioni degli Stati Uniti e dell'Europa:



L'ID univoco dell'organizzazione padre viene archiviato in un attributo nel profilo di un'organizzazione. Mediante le informazioni in questo attributo, CA Identity Manager può costruire la gerarchia dell'organizzazione.

Per specificare l'attributo che archivia l'organizzazione padre, utilizzare gli attributi noti %ORG_MEMBERSHIP% e %ORG_MEMBERSHIP_NAME% con l'attributo fisico che archivia il nome dell'organizzazione padre in una descrizione di attributo nel modo seguente:

```
<ImsManagedObjectAttr physicalname="tblOrganizations.parentorg"
displayname="Organization" description="Parent Organization" valuetype="Number"
required="false" multivalued="false" wellknown="%ORG_MEMBERSHIP%" maxlength="0"
/>
```

Miglioramento delle prestazioni di ricerca nella directory

Per migliorare le prestazioni di ricerca nelle directory per utenti, organizzazioni e gruppi, attenersi ai punti seguenti:

- Indicizzare gli attributi che gli amministratori possono specificare nelle query di ricerca.

- Sovrascrivere il timeout di directory predefinito specificando dei valori per il timeout dei parametri di ricerca in un file di configurazione di directory (directory.xml).
- Ottimizzare la directory utente. Consultare la documentazione relativa al database utilizzato.

Configurare le opzioni specifiche del database nell'origine dati ODBC. Per ulteriori informazioni, consultare la documentazione relativa all'origine dati.

Miglioramento delle prestazioni per ricerche di dimensioni elevate

Quando CA Identity Manager gestisce un archivio utenti di grandi dimensioni, le ricerche che restituiscono molti risultati possono far esaurire la memoria del sistema.

Le due impostazioni seguenti determinano come CA Identity Manager gestisce le ricerche di dimensioni elevate:

- Maximum number of rows (Numero massimo di righe)

  Consente di specificare il numero massimo di risultati che CA Identity Manager può restituire durante una ricerca in una directory utente. Quando il numero dei risultati supera il limite, viene visualizzato un errore.

- Page size (Dimensione pagina)

  Specifica il numero di oggetti che può essere restituito in una singola ricerca. Se il numero degli oggetti supera la dimensione della pagina, CA Identity Manager esegue ricerche multiple.

  Nota: se l'archivio utenti non supporta il paging ed è specificato un valore per maxrows, CA Identity Manager utilizza solo il valore maxrows per controllare le dimensioni della ricerca.

È possibile configurare un numero massimo di righe e le dimensioni della pagina nelle posizioni seguenti:

- Archivio utenti

  Nella maggior parte degli archivi utenti e dei database, è possibile configurare dei limiti per la ricerca.

  Nota: per ulteriori informazioni, consultare la documentazione relativa all'archivio utenti o al database utilizzato.

- Directory di CA Identity Manager

  È possibile configurare l'elemento DirectorySearch (a pagina 58) nel file di configurazione della directory (directory.xml) utilizzato per creare la directory di CA Identity Manager.

  Per impostazione predefinita, il valore massimo delle righe e delle dimensioni delle pagine è illimitato per le directory esistenti. Per le nuove directory, il valore del numero massimo di righe è illimitato e il valore della dimensione delle pagine è pari a 2000.

- Definizione di oggetto gestito

  Per impostare i limiti massimi di righe e di dimensioni della pagina da applicare a un tipo di oggetto invece che a un'intera directory, configurare la *definizione dell'oggetto gestito* (a pagina 61) nel file directory.xml utilizzato per creare la directory di CA Identity Manager.

  L'impostazione di limiti per un tipo di oggetto gestito consente di apportare modifiche in base ai requisiti aziendali. Ad esempio, la maggior parte delle aziende ha più utenti che gruppi. Tali aziende possono impostare i limiti solo per le ricerche di oggetti utente.

- Schermate di ricerca attività

  È possibile controllare il numero dei risultati della ricerca che gli utenti visualizzano nelle schermate di ricerca e di elenco nella console utente. Se il numero dei risultati supera il numero di risultati per pagina definiti per l'attività, gli utenti visualizzano dei collegamenti a pagine di risultati aggiuntive.

  Questa impostazione non influisce sul numero dei risultati restituiti da una ricerca.

  Nota: per informazioni sull'impostazione delle dimensioni di pagina nelle schermata di ricerca e di elenco, consultare la *Guida per l'amministratore*.

Se il limite massimo per il numero di righe e dimensioni della pagina è definito in più posizioni, viene applicata l'impostazione più specifica. Ad esempio, le impostazioni di un oggetto gestito hanno la precedenza sulle impostazioni a livello di directory.

Capitolo 5: Directory di CA Identity Manager

Una directory di CA Identity Manager fornisce informazioni su una directory utente gestita da CA Identity Manager. Queste informazioni descrivono la modalità di archiviazione nell'archivio utenti di oggetti come ad esempio utenti, gruppi e organizzazioni e la loro visualizzazione in CA Identity Manager.

Nella sezione relativa alle directory di CA Identity Manager della console di gestione, è possibile creare, visualizzare, esportare, aggiornare ed eliminare le directory CA Identity Manager.

Nota: se CA Identity Manager utilizza un cluster di Policy Server di SiteMinder, arrestarli tutti tranne uno prima di creare o di aggiornare directory di CA Identity Manager.

Questa sezione contiene i seguenti argomenti:

Prerequisiti per la creazione di una directory di CA Identity Manager

Prima di creare una directory di CA Identity Manager, è necessario effettuare le seguenti operazioni:

- Prima di creare o modificare una directory di CA Identity Manager, arrestare tutti i nodi di CA Identity Manager tranne uno.

  Nota: se si dispone di un cluster di nodi di CA Identity Manager, è possibile abilitare solamente un nodo di CA Identity Manager quando si apportano modifiche alla console di gestione.

- Prima di creare o aggiornare directory di CA Identity Manager, arrestare tutti i Policy Server tranne uno.

  Nota: se si dispone di un cluster di Policy Server di SiteMinder, è possibile abilitare solamente un Policy Server di SiteMinder quando si apportano modifiche alla console di gestione.

Creazione di una directory

Nella console di gestione, creare una directory di CA Identity Manager che descrive la struttura e il contenuto dell'archivio utenti e la directory di provisioning, che archivia le informazioni necessarie per il server di provisioning. Queste directory vengono associate all'ambiente di CA Identity Manager.

Per creare directory, è possibile utilizzare uno dei seguenti metodi:

- Utilizzare la procedura guidata di configurazione delle directory

  Questa guida gli amministratori attraverso il processo di creazione di una directory per il loro archivio utenti. Questo metodo aiuta a ridurre la possibilità di errori di configurazione.

  Nota: utilizzare la procedura guidata di configurazione delle directory per creare nuove directory solo per gli archivi utenti LDAP. Per creare una directory per un database relazionale o aggiornare una directory esistente, importare direttamente un file directory.xml.

- Utilizzare un file di configurazione XML

  Consente agli amministratori di selezionare un file XML configurato completamente per creare o modificare l'archivio utenti o il server di provisioning.

  Selezionare questo metodo se si sta creando una directory per un database relazionale o se si sta aggiornando una directory esistente.

Ulteriori informazioni:

Creazione di una directory con un file di configurazione XML (a pagina 170)
Creazione di directory utilizzando la procedura guidata di configurazione directory (a pagina 157)

Creazione di directory utilizzando la procedura guidata di configurazione directory

La procedura guidata di configurazione directory guida gli amministratori attraverso la procedura di creazione di una directory per l'archivio utenti e aiuta a ridurre gli errori di configurazione. Prima di avviare la procedura guidata, è necessario caricare il modello di configurazione di directory LDAP di CA Identity Manager. Tali modelli sono preconfigurati con attributi noti e necessari. Prima di immettere i dettagli di connessione per l'archivio utenti LDAP o la directory di provisioning, è possibile selezionare gli attributi LDAP, eseguire il mapping degli attributi noti e immettere i metadati relativi a tali attributi. Una volta conclusa l'operazione di mapping, fare clic su Fine per creare la directory.

Avvio della procedura guidata di configurazione directory

La procedura guidata di configurazione directory consente a un amministratore di selezionare un modello di CA Identity Manager e di modificare tale modello per utilizzarlo nell'ambiente.

Procedere come descritto di seguito:

1. Dalla console di gestione, fare clic su Directory e selezionare Create from Wizard (Creazione mediante procedura guidata).

   Viene richiesto di selezionare un file di configurazione di directory per configurare l'archivio utenti.

2. Fare clic su Sfoglia per selezionare il file di configurazione per configurare l'archivio utenti o il server di provisioning dalla posizione predefinita seguente e fare clic su Avanti.

   ```
   admin_tools\directoryTemplates\directory\
   ```

   Nota: admin_tools specifica la directory in cui vengono installati gli strumenti di amministrazione e directory specifica il nome del fornitore LDAP.

   Gli Strumenti di amministrazione sono ora installati nelle seguenti posizioni predefinite:

   - Windows: C:\Programmi\CA\Identity Manager\IAM Suite\Identity Manager\tools
   - UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

3. Nella schermata Dettagli di connessione, specificare le informazioni per la directory LDAP o il server di provisioning, i parametri di ricerca nella directory e le informazioni sulle connessioni di failover, quindi fare clic su Avanti.

4. Nella schermata Configure Managed Object (Configura oggetto gestito), specificare gli oggetti da configurare e fare clic su Avanti. È possibile scegliere tra gli oggetti seguenti:
   - Configure User Managed Object (Configura oggetto gestito utente)
   - Configure Group Managed Object (Configura oggetto gestito gruppo)
   - Configure Organization Object (Configura oggetto organizzazione)
   - Show summary and deploy directory (Mostra riepilogo e distribuisci directory)

     Nota: scegliere il riepilogo e la distribuzione della directory solo dopo aver completato la configurazione della directory.

   a. Nella schermata Seleziona attributo, visualizzare e modificare le classi strutturali e ausiliarie secondo le esigenze e fare clic su Avanti.

   b. Nella schermata Select Attributes: Mapping Well-Knowns (Seleziona attributi: mapping attributi noti), eseguire il mapping degli alias noti di CA Identity Manager su attributi LDAP selezionati e fare clic su Avanti.

   c. (Facoltativo) Nella schermata Describe User Attributes (Descrivi attributi utente), visualizzare e modificare le definizioni di attributo, quindi fare clic su Avanti. È possibile modificare il nome visualizzato e la descrizione.

   d. (Facoltativo) Nella schermata User Attribute Details (Dettagli attributi utente), definire i metadati per ciascun attributo selezionato da gestire e fare clic su Avanti.

      Viene visualizzata la schermata di selezione dell'oggetto gestito.

      Per configurare Gruppi o Organizzazioni, selezionare l'oggetto gestito e fare clic su Avanti per procedere attraverso le schermate Attributi di questi oggetti.

5. Selezionare Show Summary and Deploy Directory (Mostra riepilogo e distribuisci directory) dall'elenco, quindi fare clic su Avanti.

   Viene visualizzata la schermata di conferma.

6. Visualizzare i dettagli dello stato.

   Se ci sono errori, fare clic sul pulsante Indietro per modificare le schermate appropriate. Fare clic su Fine per applicare le modifiche.

   CA Identity Manager conferma la configurazione e crea la directory. Si viene quindi riportati alla schermata di elenco delle directory in cui è possibile visualizzare la nuova directory.

Selezionare la schermata dei modelli di directory

Utilizzare questa schermata per selezionare un file XML di directory perché LDAP configuri un archivio utenti o un server di provisioning.

Fare clic sul pulsante Sfoglia per selezionare il file di configurazione per configurare l'archivio utenti o il server di provisioning dalla posizione predefinita seguente:

```
admin_tools\directoryTemplates\directory\
```

Nota: admin_tools specifica la directory in cui vengono installati gli strumenti di amministrazione e directory specifica il nome del fornitore LDAP.

Gli Strumenti di amministrazione sono ora installati nelle seguenti posizioni predefinite:

- Windows: C:\Programmi\CA\Identity Manager\IAM Suite\Identity Manager\tools
- UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

Dopo avere selezionato il file XML di directory, fare clic su Avanti per accedere alla schermata Dettagli di connessione.

Schermata Dettagli di connessione

Utilizzare questa schermata per immettere le credenziali di configurazione per l'archivio utenti. È possibile immettere anche i parametri di ricerca nella directory e aggiungere connessioni di failover. Dopo aver inserito le informazioni di connessione, fare clic su Avanti per selezionare gli oggetti da gestire.

Nota: i campi che vengono visualizzati in questa schermata dipendono dal tipo di archivio utenti, e a seconda che la connessione sia creata mediante la procedura guidata di configurazione directory o importando direttamente un file XML.

In questa schermata sono disponibili i campi seguenti:

Nome

Consente di specificare il nome della directory dell'utente a cui ci si sta connettendo.

Descrizione

Consente di specificare una descrizione della directory dell'utente.

Host

Consente di specificare il nome host del computer in cui si trova l'archivio utenti.

Porta

Consente di specificare la porta del computer in cui si trova l'archivio utenti.

DN utente

Consente di specificare il nome di dominio dell'utente per accedere all'archivio utenti LDAP.

Nome JNDI origine dati JDBC

Specifica il nome di un'origine dati JDBC esistente utilizzata da CA Identity Manager per connettersi al database.

Nome utente

Consente di specificare il nome utente per accedere al server di provisioning.

Nota: solo per i server di provisioning.

Dominio

Consente di specificare il nome di dominio per accedere al server di provisioning.

Nota: solo per i server di provisioning.

Password

Consente di specificare la password per accedere all'archivio utenti LDAP/server di provisioning.

Conferma password

Consente di confermare la password per accedere all'archivio utenti LDAP/server di provisioning.

Connessione protetta

Quando questa opzione è selezionata, impone una connessione SSL (Secure Sockets Layer) alla directory utente LDAP.

Cerca in principale

Consente di specificare la posizione in una directory LDAP che serve come il punto di partenza per la directory, solitamente un'organizzazione (o) o un'unità organizzativa (ou).

Nota: solo per gli archivi utente LDAP.

Search Maximum Rows (Numero massimo di righe per ricerca)

Consente di specificare il numero massimo di risultati che CA Identity Manager può restituire durante una ricerca in una directory utente. Quando il numero dei risultati supera il limite, viene visualizzato un errore.

L'impostazione del numero massimo di righe può sostituire le impostazioni nella directory LDAP che limitano i risultati della ricerca. Quando si applicano impostazioni in conflitto, il server LDAP utilizza l'impostazione più bassa.

Search Page Size (Dimensioni pagina di ricerca)

Specifica il numero di oggetti che può essere restituito in una singola ricerca. Se il numero degli oggetti supera la dimensione della pagina, CA Identity Manager esegue ricerche multiple.

Prendere nota dei punti seguenti quando si specificano le dimensioni della pagina di ricerca:

- Per utilizzare l'opzione Search Page Size (Dimensioni pagina di ricerca), l'archivio utenti che CA Identity Manager gestisce deve supportare il paging. Per alcuni tipi di archivio utenti potrebbe essere necessaria un'ulteriore configurazione per consentire il paging. Per ulteriori informazioni, consultare la *Guida alla configurazione*.
- Se l'archivio utenti non supporta il paging e viene specificato un valore per il numero massimo di righe della ricerca, CA Identity Manager utilizza solo il valore di Search Maximum Rows (Numero massimo di righe per ricerca) per controllare le dimensioni della ricerca.

Search timeout (Timeout di ricerca)

Consente di specificare il numero massimo di secondi che CA Identity Manager utilizza per eseguire una ricerca in una directory prima di terminarla.

Failover Host (Host di failover)

Consente di specificare il nome host del sistema in cui esistono un archivio utenti ridondante o un server di provisioning alternativo, se il sistema primario non è disponibile. Se sono elencati più server multipli, CA Identity Manager tenta di connettersi ai sistemi secondo l'ordine dell'elenco.

Failover port (Porta di failover)

Consente di specificare la porta del sistema in cui esistono un archivio utenti ridondante o un server di provisioning alternativo, se il sistema primario non è disponibile. Se sono elencati più server multipli, CA Identity Manager tenta di connettersi ai sistemi secondo l'ordine dell'elenco.

Pulsante Aggiungi

Fare clic per aggiungere il nome host di failover e i numeri di porta aggiuntivi.

Schermata Configure Managed Objects (Configura oggetti gestiti)

Utilizzare questa schermata per selezionare un oggetto da configurare.

L'elenco seguente indica i campi in questa schermata:

Configure User Managed Object (Configura oggetto gestito utente)

Descrive come gli utenti vengono archiviati nell'archivio utenti e come vengono rappresentati in CA Identity Manager.

Configure Group Managed Object (Configura oggetto gestito gruppo)

Descrive come i gruppi vengono archiviati nell'archivio utenti e come vengono rappresentati in CA Identity Manager.

Configure Organization Managed Object (Configura oggetto gestito organizzazione)

Se l'archivio utenti include organizzazioni, descrive come le organizzazioni vengono archiviate e rappresentate in CA Identity Manager.

Show Summary and Deploy Directory (Mostra riepilogo e distribuisci directory)

Specifica che tutti gli oggetti gestiti sono stati definiti e che si desidera eseguire la distribuzione della directory. Dopo avere selezionato Show Summary and Deploy Directory (Mostra riepilogo e distribuisci directory), fare clic su Avanti per accedere alla pagina di riepilogo.

Pulsante Salva

Fare clic su questo pulsante per salvare il file XML.

Pulsante Indietro

Fare clic su questo pulsante per tornare alla schermata Dettagli di connessione da modificare.

Pulsante Avanti

Fare clic su questo pulsante per continuare fino alla schermata di selezione attributi per selezionare l'utente, il gruppo o gli attributi dell'organizzazione da configurare.

Selezionare la schermata Attributi

Utilizzare questa schermata per modificare o aggiungere classi strutturali e ausiliarie per gli oggetti Utente, Gruppo o Organizzazione. Questa schermata è preconfigurata con valori basati su schemi di directory comuni e procedure consigliate per il tipo di directory che si sta utilizzando. Un amministratore può modificare la classe strutturale selezionando una nuova classe dal menu a discesa. Selezionando una classe si aggiorna la tabella con gli attributi che appartengono alla classe strutturale nuova.

È possibile aggiungere una classe ausiliaria selezionandone una dal menu a discesa. Selezionando una classe ausiliaria si aggiorna la tabella con gli attributi che appartengono alla classe ausiliaria nuova.

L'elenco seguente rappresenta i campi in questa schermata:

Structural Class Name (Nome classe strutturale)

Specifica la classe strutturale dell'attributo da configurare.

Pulsante Modifica

Fare clic su questo pulsante per modificare la classe strutturale.

Auxiliary Class Name (Nome classe ausiliaria)

Specifica la classe ausiliaria dell'attributo da configurare.

Pulsante Aggiungi

Fare clic su questo pulsante per aggiungere una classe ausiliaria da configurare.

Classe di oggetto

Consente di specificare il contenitore della classe oggetto.

ID

Consente di specificare l'ID del contenitore.

Nome

Specifica il nome del contenitore.

Tabella Attributi

Specifica il nome fisico, la classe oggetto, se l'attributo è multivalore e il tipo di dati degli attributi selezionati. È possibile ordinare gli attributi in questa tabella per Selezionato, Classe oggetto, Multivalore e Tipo di dati.

Pulsante Indietro

Fare clic su questo pulsante per tornare alla schermata di configurazione degli oggetti gestiti.

Successivo

Fare clic su questo pulsante per accedere alla schermata Well-Known Mapping (Mapping noti) per eseguire il mapping degli alias noti obbligatori e facoltativi.

Schermata Well-Known Mapping (Mapping noti)

Utilizzare questa schermata per eseguire il mapping degli attributi noti di CA Identity Manager su attributi LDAP selezionati. Un amministratore può aggiungere elementi all'elenco degli attributi noti (se vengono richiesti per il codice personalizzato) immettendo un nuovo attributo noto nel campo di testo e facendo clic sul pulsante Aggiungi. La schermata si aggiorna permettendo così di continuare ad aggiungere tutti gli attributi noti a seconda delle esigenze.

L'elenco seguente rappresenta i campi in questa schermata:

Required Well-Knowns (Attributi noti obbligatori)

Consente di specificare gli attributi noti per Utenti, Gruppi o Organizzazioni (se applicabile) di cui è necessario eseguire il mapping su attributi LDAP.

Optional Well-Knowns (Attributi noti facoltativi)

Specifica gli attributi noti per Utenti, Gruppi, o Organizzazioni (se applicabile) di cui è facoltativo eseguire il mapping.

Nuovo Well-Known

Consente di specificare un attributo noto a cui fa riferimento il codice personalizzato.

Pulsante Aggiungi

Fare clic su questo pulsante per aggiungere un nuovo attributo noto alla tabella degli attributi noti facoltativi.

Pulsante Indietro

Fare clic su questo pulsante per tornare alla schermata Select User Attributes (Seleziona attributi utente) per selezionare più attributi. I mapping già eseguiti vengono salvati e saranno disponibili quando si ritorna a questa schermata.

Pulsante Avanti

Fare clic su questo pulsante per accedere alla schermata Basic Object Attribute Definition (Definizione attributi oggetto di base) per specificare le definizioni degli attributi.

Ulteriori informazioni

Attributi noti per un archivio utenti LDAP (a pagina 79)
Attributi di gruppo noti (a pagina 83)
Attributi utente noti (a pagina 80)
Attributi di organizzazione noti (a pagina 85)

Schermata Basic Object Attribute Definition (Definizione attributi oggetto di base)

Utilizzare questa schermata per visualizzare e modificare le definizioni comunemente definite: Nome visualizzato e Descrizione.

L'elenco seguente rappresenta i campi in questa schermata:

Tabella Oggetto gestito

Specifica il nome visualizzato, il nome fisico, il nome noto e la descrizione dell'oggetto gestito. Utilizzare il menu a discesa per modificare la descrizione, se necessario. Una volta effettuate le modifiche, fare clic su Avanti per continuare.

Pulsante Indietro

Fare clic su questo pulsante per tornare alla schermata Well-Known Mapping (Mapping noti) per modificare i dettagli dei mapping.

Pulsante Avanti

Fare clic su questo pulsante per accedere alla schermata Detailed Object Attribute Definition (Definizione attributi oggetto dettagliata) in cui è possibile specificare definizioni degli attributi aggiuntive.

Schermata Detailed Object Attribute Definition (Definizione attributi oggetto dettagliata)

Utilizzare questa schermata per specificare altre definizioni degli attributi. Un amministratore può definire i metadati per ciascun attributo selezionato modificando il nome visualizzato, gestendo l'attributo nelle schermate della console utente, il tipo di dati del valore, la lunghezza massima e il set di regole di convalida. Una volta che si sono specificate le definizioni degli attributi, fare clic su Avanti per continuare.

Di seguito sono descritti i campi presenti in questa schermata:

Visualizza nome

Specifica il nome univoco per l'attributo dell'oggetto gestito. Questo è il nome che viene visualizzato nella console utente.

Tag

Specifica i tag della classificazione dei dati per il valore di attributo dell'oggetto gestito. Tutti i tag sono facoltativi e tutti hanno come impostazione predefinita False tranne Searchable (Ricercabile). È possibile selezionare i tag seguenti:

Obbligatorio

Indica che l'attributo è obbligatorio quando si creano oggetti.

Multiple Values (Più valori)

Indica che l'attributo viene visualizzato come multivalore.

Nascosto

Indica che l'attributo è nascosto.

Sistema

Indica che l'attributo è un attributo di sistema e non viene aggiunto alle schermate delle attività.

Searchable (Ricercabile)

Indica che l'attributo viene aggiunto ai filtri di ricerca. L'impostazione predefinita è True.

Sensitive Encrypt (Crittografia sensibile)

Indica che l'attributo è sensibile e viene visualizzato come una serie di asterischi (*).

Hide in VST (Nascondi in VST)

Indica che l'attributo viene nascosto nella schermata Dettagli evento per Visualizza attività inoltrate.

Do not copy (Non copiare)

Indica che è necessario ignorare l'attributo quando un amministratore crea una copia di un oggetto.

Previously encrypted (Crittografato in precedenza)

Indica che l'attributo a cui si accede nell'archivio utenti è stato crittografato in precedenza e richiede la decrittografia. Il valore di testo non crittografato viene salvato nell'archivio utenti quando si salva l'oggetto.

Untagged encrypted (Crittografato senza tag)

Indica che l'attributo è stato crittografato in precedenza nell'archivio utenti e che non ha il nome tag dell'algoritmo di crittografia all'inizio del testo crittografato.

Tipo di dati

Specifica il tipo di dati del valore per l'attributo dell'oggetto gestito nella console utente. È possibile scegliere tra le voci seguenti:

- READONLY
- WRITEONCE
- READWRITE

Lunghezza massima

Specifica la lunghezza massima del valore per l'attributo dell'oggetto gestito

Impostazione predefinita: 0

Validation Rule Set (Set di regole di convalida)

Specifica i set di regole di convalida per convalidare il valore dell'attributo dell'oggetto gestito. È possibile scegliere tra le voci seguenti:

- Convalida dell'utente
- Formato numeri di telefono
- Formato numeri di telefono internazionale

Pulsante Indietro

Fare clic su questo pulsante per tornare alla schermata Basic Object Attribute Definition (Definizione attributi oggetto di base) da modificare.

Pulsante Avanti

Fare clic su questo pulsante per accedere alla schermata Configure Managed Objects (Configura oggetti gestiti). In questa schermata, è possibile selezionare il successivo oggetto gestito da configurare. Una volta configurati gli oggetti gestiti, selezionare Show summary and the deploy directory (Mostra riepilogo e distribuisci directory) per visualizzare le informazioni sulla directory ed effettuare la distribuzione di quest'ultima.

Ulteriori informazioni

Gestione degli attributi sensibili (a pagina 71)

Schermata di conferma

Questa schermata mostra un riepilogo dei dettagli della directory.

Nell'elenco seguente sono riportati i campi in questa schermata:

Dettagli di connessione

Specifica i dettagli di connessione per la directory dell'utente.

User/Group/Organization Details (Dettagli utente/gruppo/organizzazione)

Specifica le modifiche eseguite nel file directory.xml.

Pulsante Indietro

Fare clic su questo pulsante per modificare qualsiasi dettaglio nella procedura guidata.

Pulsante Salva

Fare clic su questo pulsante per salvare le selezioni.

Pulsante Fine

Fare clic su questo pulsante se tutti i dettagli della directory sono corretti per uscire dalla procedura guidata.

La configurazione viene confermata e la directory viene creata. Si viene quindi riportati alla pagina di elenco delle directory dove la nuova directory viene visualizzata nell'elenco. Per modificare o esportare la nuova directory, selezionarla nell'elenco delle directory.

Creazione di una directory con un file di configurazione XML

È possibile creare o aggiornare una directory di CA Identity Manager importando un file directory.xml completo nella console di gestione.

Nota: se si sta creando una directory utilizzando un file directory.xml anziché la procedura guidata di configurazione delle directory, assicurarsi di aver modificato il modello di configurazione predefinito. Per ulteriori informazioni, consultare la *Guida alla configurazione*.

Procedere come descritto di seguito:

1. Aprire la console di gestione digitando il seguente URL in un browser:

   http://*hostname*:*port*/iam/immanage

   nomehost

   Definisce il nome di dominio completo del server su cui è installato CA Identity Manager.

   porta

   Definisce il numero di porta del server applicazioni.

2. Fare clic su Directory.

   Viene visualizzata la finestra Directory di CA Identity Manager.

3. Fare clic su Create or Update from XML (Crea o aggiorna da XML).

4. Digitare il percorso e il nome del file XML di configurazione della directory per creare la directory di CA Identity Manager oppure sfogliare per cercare il file. Fare clic su Avanti.

5. Fornire i valori per i campi in questa finestra nel seguente modo:

   Nota: la visualizzazione dei campi in questa finestra dipende dal tipo di archivio utenti e dalle informazioni fornite nel file di configurazione di directory nella fase 4. Se nel file di configurazione di directory sono stati forniti valori per uno qualsiasi di questi campi, CA Identity Manager non richiede di fornirli di nuovo.

   Nome

   Determina il nome della directory di CA Identity Manager in fase di creazione.

   Descrizione

   (Facoltativo) Descrive la directory di CA Identity Manager.

Connection Object Name (Nome oggetto di connessione)

Specifica il nome della directory utente descritta dalla directory di CA Identity Manager. Immettere *uno* dei seguenti dettagli:

- Se CA Identity Manager non è integrato con SiteMinder, specificare un qualsiasi nome significativo per l'oggetto utilizzato da CA Identity Manager per connettersi all'archivio utenti.
- Se CA Identity Manager è integrato con SiteMinder e si desidera creare un oggetto di connessione della directory utente in SiteMinder, specificare un qualsiasi nome significativo. CA Identity Manager crea l'oggetto di connessione della directory utente in SiteMinder con il nome specificato.
- Se CA Identity Manager è integrato con SiteMinder e si desidera connettersi a una directory utente di SiteMinder esistente, specificare esattamente il nome oggetto di connessione della directory utente di SiteMinder, così come viene visualizzato nell'interfaccia utente del Policy Server.

JDBC Data Source JNDI Name (Nome JNDI dell'origine dati JDBC) (solo per directory relazionali)

Specifica il nome di un'origine dati JDBC esistente utilizzata da CA Identity Manager per connettersi al database.

Host (solo per directory LDAP)

Specifica il nome host o l'indirizzo IP del server sul quale è installata la directory utente.

Per gli archivi utenti di CA Directory, utilizzare il nome di dominio completo del sistema host. Non utilizzare localhost.

Per gli archivi utenti di Active Directory, specificare il nome di dominio, non l'indirizzo IP.

Porta (solo per directory LDAP)

Specifica il numero di porta della directory utente.

Provisioning Domain (Dominio di provisioning)

Dominio di provisioning gestito da CA Identity Manager.

Nota: nel nome del dominio di provisioning è rilevante la distinzione tra maiuscole e minuscole.

Username/User DN (Nome utente/DN utente)

Specifica il nome utente per un account che può accedere all'archivio utenti.

Per gli archivi utenti di provisioning, l'account utente specificato deve avere il profilo di Amministratore di dominio o un insieme equivalente di privilegi per il dominio di provisioning.

Password

Specifica la password per l'account utente specificato in Nome utente (per database relazionali) o nel campo DN utente (per directory LDAP).

Conferma password

Immettere nuovamente la password digitata nel campo Password per la conferma.

Connessione protetta (solo per directory LDAP)

Indica se CA Identity Manager utilizza una connessione protetta.

Assicurarsi di selezionare questa opzione per gli archivi utenti di Active Directory.

Fare clic su Avanti.

6. Rivedere le impostazioni per la directory di CA Identity Manager. Fare clic su Fine per creare la directory di CA Identity Manager con le impostazioni correnti o fare clic su Precedente per modificarle.

   Le informazioni di stato vengono mostrate nella finestra Directory Configuration Output (Output di configurazione della directory).

7. Fare clic su Continua per uscire.

   CA Identity Manager crea la directory.

Attivazione dell'accesso al server di provisioning

L'accesso al server di provisioning viene abilitato utilizzando il collegamento Directory nella console di gestione.

Nota: un prerequisito di questa procedura è l'installazione della directory di provisioning in CA Directory. Per ulteriori informazioni, consultare la *Guida all'installazione*.

Procedere come descritto di seguito:

1. Aprire la console di gestione digitando il seguente URL in un browser:

   `http://hostname:porta/iam/immanage`

   nomehost

   Definisce il nome host completo del sistema in cui il server di CA Identity Manager è installato.

   porta

   Definisce il numero di porta del server applicazioni.

2. Fare clic su Directory.

   Viene visualizzata la finestra Directory di CA Identity Manager.

3. Fare clic su Create from Wizard (Crea da procedura guidata).
4. Digitare il percorso e il nome del file XML della directory per configurare la directory di provisioning. Tale directory viene archiviata nel percorso directoryTemplates\ProvisioningServer della cartella Administrative Tools (Strumenti di amministrazione). La posizione predefinita di questa cartella è:
   - Windows: C:\Programmi\CA\Identity Manager\IAM Suite\Identity Manager\tools
   - UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

   Nota: è possibile utilizzare questo file di configurazione di directory così come sono installati, ossia senza alcuna modifica.
5. Fare clic su Avanti.
6. Fornire i valori per i campi in questa finestra nel seguente modo:

   Nome

   Nome della directory di provisioning associata al server di provisioning in fase di configurazione.
   - Se CA Identity Manager non è integrato con SiteMinder, specificare un nome significativo per l'oggetto utilizzato da CA Identity Manager per connettersi all'archivio utenti.
   - Se CA Identity Manager è integrato con SiteMinder, si hanno due possibilità:

     Se si desidera creare un oggetto di connessione della directory utente in SiteMinder, specificare un qualsiasi nome significativo. CA Identity Manager crea questo oggetto in SiteMinder con il nome specificato.

     Se si desidera connettersi a una directory utente di SiteMinder esistente, specificare esattamente il nome oggetto di connessione della directory utente di SiteMinder così come viene visualizzato nell'interfaccia utente del Policy Server.

   Descrizione

   (Facoltativo) Descrive la directory di CA Identity Manager.

   Host

   Specifica il nome host o l'indirizzo IP del server sul quale è installata la directory utente.

   Porta

   Specifica il numero di porta della directory utente.

Dominio

Definisce il nome del dominio di provisioning gestito da CA Identity Manager.

Importante. Durante la creazione di una directory di provisioning attraverso la console di gestione, se si utilizzano caratteri di una lingua straniera come nome di dominio, la creazione della directory di provisioning non riesce.

Il nome deve corrispondere al nome del dominio di provisioning specificato durante l'installazione.

Nota: nel nome di dominio è rilevante la distinzione tra maiuscole e minuscole.

Nome utente

Specifica un utente che può accedere al Manager di provisioning.

L'utente deve disporre del profilo di Amministratore di dominio o di un insieme equivalente di privilegi per il dominio di provisioning.

Password

Specifica la password per l'utente globale specificato nel campo Nome utente.

Conferma password

Immettere nuovamente la password digitata nel campo Password per la conferma.

Connessione protetta

Indica se CA Identity Manager utilizza una connessione protetta.

Assicurarsi di selezionare questa opzione per gli archivi utenti di Active Directory.

Parametri di ricerca nella directory

maxrows definisce il numero massimo di risultati che CA Identity Manager può restituire durante la ricerca in una directory utente. Questo valore sostituisce qualsiasi limite impostato nella directory LDAP. Quando si applicano impostazioni in conflitto, il server LDAP utilizza l'impostazione più bassa.

Nota: il parametro maxrows non limita il numero di risultati visualizzati nella schermata di attività di CA Identity Manager. Per configurare le impostazioni di visualizzazione, modificare la definizione della schermata elenco nella console utente di CA Identity Manager. Per istruzioni, consultare la *User Console Design Guide*.

timeout determina la durata massima in secondi della ricerca di una directory da parte di CA Identity Manager prima della sua interruzione.

Failover Connections (Connessioni di failover)

Il nome host e il numero di porta di uno o più sistemi facoltativi che sono server di provisioning alternativi. Se vengono elencati server multipli, CA Identity Manager tenta di connettersi ai sistemi nell'ordine in cui vengono elencati.

I server di provisioning alternativi vengono utilizzati se il server di provisioning primario non riesce. Quando il server di provisioning primario diventa nuovamente disponibile, il server di provisioning alternativo continua a essere utilizzato. Se si desidera riprendere a utilizzare il server di provisioning, riavviare i server di provisioning alternativi.

7. Fare clic su Avanti.
8. Selezionare gli oggetti da gestire, come ad esempio Utenti o Gruppi.
9. Dopo avere configurato gli oggetti in base alle necessità, fare clic su Show summary deploy directory (Mostra riepilogo e distribuisci directory) e rivedere le impostazioni per la directory di provisioning.
10. Fare clic su una di queste azioni:
    a. Fare clic su Indietro per modificare.
    b. Fare clic su Salva per salvare le informazioni di directory se si desidera effettuare la distribuzione in un secondo momento.
    c. Fare clic su Fine per completare questa procedura e procedere alla configurazione di un ambiente con il provisioning (a pagina 195).

Visualizzazione di una directory di CA Identity Manager

Eseguire la seguente procedura per visualizzare una directory di CA Identity Manager.

Procedere come descritto di seguito:

1. Nella console di gestione di CA Identity Manager, fare clic su Directory.
2. Fare clic sul nome della directory di CA Identity Manager da visualizzare. Viene visualizzata la finestra Directory Properties (Proprietà directory), che mostra le proprietà della directory di CA Identity Manager.

Proprietà directory di CA Identity Manager

Le proprietà della directory di CA Identity Manager sono le seguenti:

Nota: la visualizzazione delle proprietà dipende dal tipo di database o di directory associati alla directory di CA Identity Manager.

Nome

Definisce il nome univoco della directory di CA Identity Manager.

Descrizione

Fornisce una descrizione della directory di CA Identity Manager.

Tipo

Definisce il tipo di provider di directory.

Connection Object Name (Nome oggetto di connessione)

Visualizza il nome della directory utente descritta dalla directory di CA Identity Manager.

Se CA Identity Manager è integrato con SiteMinder, il nome dell'oggetto di connessione corrisponde al nome della connessione della directory utente di SiteMinder.

Root Organization (Organizzazione principale) (per gli archivi utenti che includono organizzazioni)

Specifica il punto di accesso all'archivio utenti.

Per le directory LDAP, l'organizzazione principale viene specificata come DN. Per i database relazionali, viene visualizzato l'ID univoco per l'organizzazione principale.

JDBC Data Source (Origine dati JDBC)

Specifica il nome dell'origine dati JDBC utilizzata da CA Identity Manager per connettersi al database.

URL

Fornisce l'URL o l'indirizzo IP dell'archivio utenti.

Nome utente

Specifica il nome utente per un account che può accedere all'archivio utenti.

Search Maximum Rows (Numero massimo di righe per ricerca)

Indica il numero massimo di righe restituite come risultato di una ricerca.

Search Page Size (Dimensioni pagina di ricerca)

Specifica il numero di oggetti che può essere restituito in una singola ricerca. Se il numero degli oggetti supera la dimensione della pagina, CA Identity Manager esegue ricerche multiple.

Nota: l'archivio utenti gestito da CA Identity Manager deve supportare il paging. Per alcuni tipi di archivio utenti potrebbe essere necessaria un'ulteriore configurazione per consentire il paging. Per ulteriori informazioni, consultare la *Guida alla configurazione*.

Supports Paging (Supporta il paging)

Indica che la directory supporta il paging.

Search Timeout (Timeout di ricerca) (solo per directory LDAP)

Specifica la durata massima in secondi della ricerca di un archivio utenti da parte di CA Identity Manager prima della sua interruzione.

Provisioning Domain (Dominio di provisioning) (solo per directory di server di provisioning)

Dominio di provisioning gestito da CA Identity Manager.

Finestra CA Identity Manager Directory Properties (Proprietà directory di CA Identity Manager)

Le informazioni generali su una directory di CA Identity Manager vengono presentate nella finestra di proprietà per la directory selezionata. La finestra Directory Properties (Proprietà directory) è suddivisa nelle seguenti sezioni:

Directory Properties (Proprietà directory)

Visualizza le proprietà di base della directory di CA Identity Manager, incluso il dominio di provisioning associato, se il provisioning è abilitato per l'ambiente.

Managed Objects (Oggetti gestiti) (a pagina 178)

Fornisce descrizioni del tipo di oggetti dell'archivio utenti gestiti da CA Identity Manager.

Validation Rule Sets (Set di regole di convalida) (a pagina 183)

Elenca i set di regole di convalida applicabili alla directory di CA Identity Manager.

Environments (Ambienti)

Elenca gli ambienti associati alla directory di CA Identity Manager. È possibile associare una directory a più ambienti di CA Identity Manager.

Per visualizzare più informazioni su un ambiente di CA Identity Manager, fare clic sul nome dell'ambiente.

Per modificare le proprietà in una directory di CA Identity Manager, importare un file di configurazione di directory così come descritto in Aggiornamento di una directory di CA Ide (a pagina 185)ntity Manager.

Oltre a visualizzare le proprietà, è possibile eseguire anche le seguenti azioni:

Update Authentication (Aggiorna autenticazione)

Consente agli amministratori di modificare la directory utilizzata da CA Identity Manager per autenticare gli amministratori della console di gestione. Gli amministratori possono anche aggiungere altri amministratori della console di gestione nella directory di autenticazione esistente.

Nota: le opzioni di aggiornamento di autenticazione si applicano solo quando la protezione di CA Identity Manager nativa protegge la console di gestione. Per informazioni sull'attivazione della protezione nativa o sull'utilizzo di un metodo di protezione diverso, consultare la *Guida alla configurazione*.

Esporta (a pagina 185)

Esporta la definizione della directory come file XML. Dopo aver esportato le impostazioni della directory, è possibile modificare il file XML, quindi reimportarlo per aggiornare la directory. È anche possibile importare il file XML in un'altra directory per configurare le stesse impostazioni per quella directory.

Aggiornamento (a pagina 185)

Consente agli amministratori di aggiungere o modificare definizioni di oggetti gestiti, come ad esempio gli attributi di un oggetto, l'impostazione dei parametri di ricerca e la modifica delle proprietà della directory.

Visualizzazione di proprietà e attributi di oggetti gestiti

Un oggetto gestito descrive un tipo di voce nell'archivio utenti, come ad esempio un utente, un gruppo o un'organizzazione. Le proprietà e gli attributi applicabili a un oggetto gestito si applicano anche a tutte le voci di tale tipo. Ad esempio, un profilo utente consiste di tutte le proprietà e gli attributi dell'oggetto gestito Utente.

Per visualizzare i dettagli di un oggetto gestito, fare clic sul nome dell'oggetto per aprire la finestra Managed Object Properties (Proprietà dell'oggetto gestito).

Proprietà dell'oggetto gestito

La finestra Managed Object Properties (Proprietà dell'oggetto gestito) descrive le proprietà e gli attributi di un tipo di oggetto gestito.

Le informazioni sulla finestra Managed Object Properties (Proprietà dell'oggetto gestito) dipendono dal tipo di archivio utenti che viene gestito. Le proprietà gestite di un oggetto sono le seguenti:

Descrizione

Fornisce una descrizione dell'oggetto gestito.

Tipo

Indica il tipo di voce rappresentata dall'oggetto gestito. Un tipo di oggetto può essere uno dei seguenti:

- Utente
- Gruppo
- Organizzazione

Classe oggetto (solo per directory LDAP)

Specifica le classi di oggetto per l'oggetto gestito. Un oggetto gestito può avere più classi di oggetto.

Ordinamento (solo per directory LDAP)

Specifica l'attributo utilizzato da CA Identity Manager per ordinare i risultati della ricerca nella logica aziendale personalizzata. L'ordinamento non influisce sull'ordine dei risultati della ricerca nella console utente.

Ad esempio, quando si specifica l'attributo cn per l'oggetto utente, CA Identity Manager ordina alfabeticamente i risultati della ricerca utenti in base all'attributo cn.

Primary Table (Tabella primaria) (solo per database relazionali)

Specifica la tabella contenente l'ID univoco per l'oggetto gestito.

Numero massimo di righe

Specifica il numero massimo di risultati che possono essere restituiti da CA Identity Manager durante la ricerca di oggetti di questo tipo. Quando il numero dei risultati supera il limite, viene visualizzato un errore.

L'impostazione del numero massimo di righe può sostituire le impostazioni nella directory LDAP che limitano i risultati della ricerca. Quando si applicano impostazioni in conflitto, il server LDAP utilizza l'impostazione più bassa.

Page Size (Dimensione pagina)

Specifica il numero di oggetti che può essere restituito in una singola ricerca. Se il numero degli oggetti supera la dimensione della pagina, CA Identity Manager esegue ricerche multiple.

Nota: l'archivio utenti gestito da CA Identity Manager deve supportare il paging. Per alcuni tipi di archivio utenti potrebbe essere necessaria un'ulteriore configurazione per consentire il paging. Per ulteriori informazioni, consultare la *Guida alla configurazione*.

Container Properties (Proprietà contenitore) (solo per directory LDAP)

In una directory LDAP, i gruppi *contenitore* contengono oggetti di un tipo specifico. Quando viene specificato un contenitore, in CA Identity Manager vengono gestite solamente le voci nel contenitore. Ad esempio, quando si specifica il contenitore ou=People, CA Identity Manager gestisce solo gli utenti esistenti nel contenitore People.

Nota: gli utenti e i gruppi che si trovano nella directory LDAP, ma non nel contenitore definito, possono venire visualizzati nella console utente. Durante la gestione di quegli utenti e quei gruppi, potrebbero verificarsi dei problemi.

I contenitori raggruppano soltanto utenti e gruppi. Non è possibile specificare un contenitore per le organizzazioni.

Le proprietà di un contenitore sono le seguenti:

objectclass

Specifica la classe oggetto LDAP del contenitore in cui vengono creati gli oggetti di un tipo specifico. Ad esempio, il valore predefinito per il contenitore utenti è "top,organizationalUnit", che indica che gli utenti vengono creati in unità organizzative LDAP (ou).

ID

Specifica l'attributo che archivia il nome del contenitore, ad esempio ou. L'attributo è combinato con il valore Nome per formare il DN relativo del contenitore, come nell'esempio seguente:

ou=People

Nome

Specifica il nome del contenitore.

Secondary Table Properties (Proprietà tabella secondaria) (solo per database relazionali)

Le tabelle secondarie contengono attributi aggiuntivi per un oggetto gestito. Ad esempio, una tabella secondaria denominata tblUserAddress può contenere gli attributi via, città, stato e codice postale per l'oggetto gestito Utente.

Per le tabelle secondarie vengono visualizzate le seguenti proprietà:

Tabella

Specifica il nome della tabella.

Riferimento

Descrive il mapping tra la tabella primaria e la tabella secondaria.

Il riferimento viene visualizzato mediante il formato seguente:

primarytable.attribute=secondarytable.attribute

Ad esempio, tblUsers.id = tblUserAddress.userid indica che l'attributo ID nella tabella primaria, tblUsers, esegue il mapping sull'attributo userid nella tabella tblUserAddress.

Proprietà degli attributi nella finestra Managed Object Properties (Proprietà dell'oggetto gestito)

Per gli attributi vengono visualizzate le seguenti proprietà nella finestra Managed Object Properties (Proprietà dell'oggetto gestito):

Visualizza nome

Il nome descrittivo dell'attributo. Questo nome viene visualizzato nell'elenco degli attributi disponibili quando si progetta una finestra di attività per un'attività particolare nella console utente.

Physical Name (Nome fisico)

Il nome dell'attributo nell'archivio utenti.

Nome Well-Known

I nomi noti indicano attributi con un significato speciale in CA Identity Manager, come l'attributo utilizzato per archiviare le password degli utenti.

Proprietà degli attributi nelle finestre Attribute Properties (Proprietà attributi)

È possibile visualizzare dettagli aggiuntivi su un attributo facendo clic sul suo nome per aprire la finestra Attribute Properties (Proprietà attributi).

Nella finestra Attribute Properties (Proprietà attributi) vengono visualizzate le seguenti proprietà degli attributi:

Descrizione

Fornisce una descrizione dell'attributo.

Physical Name (Nome fisico)

Specifica il nome dell'attributo nell'archivio utenti.

Classe oggetto (solo per gli attributi di utenti, gruppi e organizzazioni nelle directory LDAP)

La classe ausiliaria LDAP per un attributo utente, quando l'attributo non è parte della classe dell'oggetto primario specificata per l'oggetto utente.

È possibile specificare una classe dell'oggetto ausiliaria solo per gli oggetti utente e gruppo.

Nome Well-Known

Indica attributi con un significato speciale in CA Identity Manager, come l'attributo utilizzato per archiviare le password degli utenti.

Obbligatorio

Indica se un valore è obbligatorio per l'attributo, così come segue:

- True indica che l'attributo deve avere un valore.
- False indica che un valore è facoltativo.

Sola lettura

Indica il livello di autorizzazione per un attributo, così come segue:

- True indica che non è possibile modificare l'attributo.
- False indica che è possibile modificare l'attributo.

Nascosto

Indica se è possibile mostrare un attributo in una finestra di attività per un'attività particolare.

Gli attributi nascosti spesso vengono utilizzati in schemi di attributi logici.

Nota: per ulteriori informazioni, consultare la *Programming Guide for Java*.

Supports Multiple Values (Supporta valori multipli)

Indica se l'attributo può avere valori multipli oppure no, così come segue (ad esempio, l'attributo utilizzato per archiviare i membri di un gruppo ha valori multipli):

- True indica che l'attributo può supportare valori multipli.
- False indica che l'attributo può avere solamente un valore singolo.

Multiple Value Delimiter (Delimitatore di valori multipli) (solo per database relazionali)

Il carattere che separa i valori quando i valori multipli vengono archiviati in una singola colonna.

System Attribute (Attributo di sistema)

Indica se l'attributo viene utilizzato solamente da CA Identity Manager oppure no, così come segue:

- True indica che l'attributo è un attributo di sistema. L'attributo non può essere aggiunto nelle finestre di attività.
- False indica che gli utenti possono utilizzare questo attributo. L'attributo può venire visualizzato in finestre di attività.

Tipo di dati

Specifica il tipo di dati dell'attributo. Il valore predefinito è Stringa.

Lunghezza massima

Specifica la lunghezza massima di un valore attributo. Se impostato su 0, non vi è alcun limite alla lunghezza del valore.

Validation Rule Set (Set di regole di convalida)

Specifica il nome di un set di regole di convalida, quando l'attributo è associato a uno di essi.

Validation Rule Sets (Set di regole di convalida)

Una regola di convalida applica requisiti ai dati che un utente digita in un campo di una finestra di attività. I requisiti possono applicare un tipo o un formato di dati o possono assicurare che i dati siano validi nel contesto di altri dati nella finestra di attività.

Una o più regole di convalida vengono raggruppate in un set di regole di convalida. Un set di regole di convalida viene quindi associato a un attributo di profilo. Ad esempio, è possibile creare un set di regole di convalida che contiene una regola di convalida Format Date, che applica il formato della data mm-dd-yyyy. Quindi è possibile associare il set di regole di convalida all'attributo che archivia la data di inizio di un dipendente.

Nota: le regole di convalida e i set di regole vengono creati nei file di configurazione di directory o nella console utente.

La finestra Managed Object Properties (Proprietà dell'oggetto gestito) visualizza un elenco di set di regole di convalida applicabili alla directory di CA Identity Manager. Per visualizzare i dettagli di un set di regole di convalida, fare clic sul nome del set di regole per aprire la finestra Validation Rule Set Properties (Proprietà del set di regole di convalida).

Proprietà della regola di convalida

Nella finestra Validation Rule Properties (Proprietà della regola di convalida) vengono visualizzate le seguenti informazioni:

Nome

Fornisce il nome della regola di convalida.

Descrizione

Fornisce una descrizione della regola.

Classe

Fornisce il nome della classe Java che implementa la regola di convalida.

Questo campo non viene visualizzato a meno che la regola di convalida non venga definita in una classe Java.

Nome file

Fornisce il nome del file che contiene l'implementazione JavaScript della regola di convalida.

Questo campo non viene visualizzato a meno che la regola di convalida non venga definita in un file.

Espressione regolare

Fornisce l'espressione regolare che implementa la regola di convalida.

Questo campo non viene visualizzato a meno che la regola di convalida non venga definita come espressione regolare.

Proprietà del set di regole di convalida

Nella finestra Validation Rule Set Properties (Proprietà del set di regole di convalida) vengono visualizzate le seguenti informazioni:

Nome

Specifica il nome del set di regole di convalida.

Descrizione

Fornisce una descrizione del set di regole di convalida.

La pagina Validation Rule Set Properties (Proprietà del set di regole di convalida) include anche un elenco di regole di convalida presenti nel set. È possibile fare clic sul nome della regola di convalida per aprire la finestra Validation Rule Properties (Proprietà della regola di convalida).

Aggiornamento delle impostazioni di una directory di CA Identity Manager

Per visualizzare le impostazioni correnti di una directory di CA Identity Manager, esportare le impostazioni della directory e salvarle come file XML.

Dopo aver esportato le impostazioni della directory, è possibile modificare e importare di nuovo il file XML per aggiornare la directory. È anche possibile importare il file XML in un'altra directory per configurare le stesse impostazioni per quella directory.

Esportazione di una directory di CA Identity Manager

Eseguire la seguente procedura per esportare una directory di CA Identity Manager.

Procedere come descritto di seguito:

1. Fare clic su Directory.

   Viene visualizzato l'elenco delle directory di CA Identity Manager.

2. Fare clic sul nome della directory da esportare.

   Viene visualizzata la finestra delle proprietà della directory di CA Identity Manager.

3. Nella parte inferiore della finestra delle proprietà, fare clic su Esporta.

4. Quando richiesto, salvare il file XML.

Aggiornamento di una directory di CA Identity Manager

Lo scopo dell'aggiornamento di una directory di CA Identity Manager è:

- Aggiungere o modificare definizioni di oggetti gestiti, inclusi gli attributi di un oggetto.
- Impostare i parametri di ricerca
- Modificare le proprietà della directory

Nota: CA Identity Manager non elimina le definizioni di oggetti o attributi.

Il file di configurazione della directory può contenere solamente le modifiche che si desidera apportare. Non includere proprietà o attributi già definiti.

Nota: se si dispone di un cluster di nodi di CA Identity Manager, è possibile abilitare solamente un nodo di CA Identity Manager quando si apportano modifiche alla console di gestione. Prima di creare o modificare una directory di CA Identity Manager, arrestare tutti i nodi di CA Identity Manager tranne uno.

Procedere come descritto di seguito:

1. Esportare le impostazioni correnti della directory di CA Identity Manager in un file XML.
2. Modificare il file XML per rispecchiare le modifiche.
3. Fare clic su Directory.

   Viene visualizzato l'elenco delle directory di CA Identity Manager.
4. Fare clic sul nome della directory da aggiornare.

   Vengono visualizzate le proprietà della directory di CA Identity Manager.
5. Nella parte inferiore della finestra delle proprietà, fare clic su Aggiorna.
6. Digitare il percorso e il nome del file XML per aggiornare la directory di CA Identity Manager oppure sfogliare per cercare il file. Fare clic su Fine.

   Le informazioni di stato vengono mostrate nel campo Directory Configuration Output (Output di configurazione della directory).
7. Fare clic su Continua.

Eliminazione di una directory di CA Identity Manager

Prima di eliminare una directory di CA Identity Manager, eliminare qualsiasi ambiente di CA Identity Manager a essa associato.

Procedere come descritto di seguito:

1. Nella console di gestione, fare clic su Directory.

   Viene visualizzato l'elenco delle directory di CA Identity Manager.
2. Selezionare la casella di controllo a sinistra della directory (o delle directory) da eliminare.
3. Fare clic su Elimina.

   Viene visualizzato un messaggio di conferma.
4. Fare clic su OK per confermare l'eliminazione.

Capitolo 6: Ambienti di CA Identity Manager

Questa sezione contiene i seguenti argomenti:

Ambienti di CA Identity Manager

Un ambiente di CA Identity Manager è una visualizzazione di un archivio utenti. In un ambiente di CA Identity Manager, è possibile gestire utenti, gruppi, organizzazioni, attività e ruoli. È possibile inoltre concedere account agli utenti in endpoint gestiti, come ad esempio account di posta elettronica o di altre applicazioni.

Mediante la console di gestione, è possibile eseguire le attività seguenti:

- Creare, modificare o eliminare un ambiente di CA Identity Manager.
- Esportare e importare un ambiente di CA Identity Manager.
- Configurare le impostazioni avanzate.
- Importare ruoli e attività.
- Ripristinare l'account di Manager di sistema

Prerequisiti per la creazione di un ambiente di CA Identity Manager

Prima di iniziare, utilizzare il foglio di calcolo nella tabella seguente per raccogliere le informazioni di cui si ha bisogno:

Foglio di calcolo di configurazione ambiente di CA Identity Manager	
Informazioni richieste	**Valore**
Un nome di ambiente di CA Identity Manager significativo a scelta. Ad esempio: MyEnvironment	
Una base URL che CA Identity Manager utilizza per formare l'URL di reindirizzamento per il criterio di password predefinito per l'ambiente. Ad esempio: http://server.yourcompany.org	
Un alias che viene aggiunto all'URL per accedere ad attività protette nell'ambiente. Ad esempio: http://server.yourcompany.org/iam/im/alias	
Un alias che viene aggiunto all'URL per accedere ad attività pubbliche, come la registrazione automatica e le attività relative alle password dimenticate. Ad esempio: http://server.yourcompany.org/iam/im/public_alias/index.jsp?task.tag=SelfRegistration **Nota:** quando l'ambiente non include attività pubbliche, non è necessario specificare un alias pubblico.	
Se è stato fornito un alias pubblico, specificare il nome di un utente esistente che serve come utente pubblico. CA Identity Manager utilizza le credenziali dell'utente pubblico al posto delle credenziali fornite dall'utente quando accede ad attività pubbliche.	
Il nome di un CA Identity Manager (a pagina 103)	
Il nome della directory di provisioning, se l'ambiente di CA Identity Manager supporta il provisioning.	

Foglio di calcolo di configurazione ambiente di CA Identity Manager	
Informazioni richieste	**Valore**
L'ID univoco di un utente esistente che amministra l'ambiente di CA Identity Manager. Ad esempio: myadmin	
Il nome dell'agente o gruppo agenti SiteMinder che protegge l'ambiente di CA Identity Manager, se CA Identity Manager si integra con SiteMinder.	

Creazione di un ambiente di CA Identity Manager

Gli ambienti di CA Identity Manager consentono di gestire oggetti in una directory con un set di ruoli e attività. Utilizzare la procedura guidata di creazione ambiente di CA Identity Manager per seguire i passaggi necessari per creare un ambiente di CA Identity Manager.

Notare i punti seguenti prima di creare un ambiente di CA Identity Manager:

- Ad esempio, l'utente utilizza un archivio utenti LDAP configurato come contenitore utente, ad esempio ou=People, nei file di configurazione della directory (directory.xml) per la directory di CA Identity Manager. Verificare che gli utenti selezionati durante la creazione dell'ambiente di CA Identity Manager esistano in quel contenitore. La selezione di un account utente che non esiste nel contenitore utente può causare errori.
- Quando si configura un ambiente di CA Identity Manager per gestire una directory utente LDAP con una struttura flat o una struttura utente flat il profilo dell'utente selezionato deve includere l'organizzazione dell'utente. Per assicurare che il profilo di un utente sia configurato correttamente, aggiungere il nome dell'organizzazione dell'utente all'attributo fisico che corrisponde all'attributo noto %ORG_MEMBERSHIP% nel file directory.xml (a pagina 86). Ad esempio, quando viene eseguito il mapping della descrizione dell'attributo fisico sull'attributo noto %ORG_MEMBERSHIP% nel file directory.xml e l'utente appartiene all'organizzazione Employees (Dipendenti), il profilo dell'utente deve contenere la coppia di attributo/valore description=Employees.

Procedere come descritto di seguito:

1. Se CA Identity Manager utilizza un cluster di server dei criteri, interrompere tutti i server dei criteri, salvo uno.
2. Se si dispone di un cluster di nodi CA Identity Manager, interrompere tutti i nodi CA Identity Manager, salvo uno.
3. Nella Console di gestione, fare clic su Environments (Ambienti).

4. Fare clic su Nuovo.

   Si apre la procedura guidata di creazione ambiente di CA Identity Manager.

5. Specificare le seguenti informazioni:

   - **Nome dell'ambiente**

     Specifica un nome univoco per l'ambiente.

   - **Descrizione**

     Descrive l'ambiente.

   - **Protected Alias (Alias protetto)**

     Specifica un nome univoco, ad esempio dipendenti. Questo alias viene aggiunto all'URL per accedere alle attività protette dell'ambiente di CA Identity Manager. Ad esempio, se l'alias è dipendenti, l'URL per accedere all'ambiente dipendenti sarà http://my*server.mycompany.com*/iam/im/dipendenti

     Nota: l'alias distingue tra maiuscole e minuscole e non può contenere spazi. Si consiglia di utilizzare lettere minuscole senza punteggiatura o spazi quando si specifica l'alias.

   - **URL di base**

     Specifica l'URL per CA Identity Manager. L'URL richiede un nome host e non può includere un host locale. Inoltre, non includere l'alias, ad esempio, http://*myserver.mycompany.com*/iam/im.

     Se si sta utilizzando un agente Web, assicurarsi che l'URL di base venga modificato per riflettere l'URL dell'agente Web.

     Nota: se si sta utilizzando un agente Web per proteggere risorse di CA Identity Manager, non specificare un numero di porta nel campo URL di base. Se si sta utilizzando un agente Web e l'URL di base contiene un numero di porta, i collegamenti alle attività di CA Identity Manager non funzionano correttamente.

     Per ulteriori informazioni sulla protezione delle risorse di CA Identity Manager, consultare la *Guida all'installazione* del server applicazioni.

     Fare clic su Avanti.

6. Selezionare una directory di CA Identity Manager da associare all'ambiente che si sta creando e fare clic su Avanti.

7. Se l'ambiente di CA Identity Manager supporta il provisioning, selezionare il server di provisioning appropriato da utilizzare.

   Nota: nnon è necessario selezionare un server di provisioning se è stata selezionata una directory di provisioning come directory di CA Identity Manager.

8. Configurare il supporto per le attività pubbliche. Di solito, le attività pubbliche sono attività self-service, come la registrazione automatica o le attività legate alle password dimenticate. Non è necessario eseguire l'accesso per svolgere le attività pubbliche.

   Nota: per abilitare gli utenti all'utilizzo delle attività self-service, configurare supporto per le attività pubbliche.

   a. Specificare un nome univoco da aggiungere all'URL per l'accesso alle attività pubbliche.

      Esempio: si utilizza l'URL seguente per accedere all'attività di registrazione automatica predefinita:

      http://*myserver.mycompany.com*/iam/im/*alias*/index.jsp?task.tag=SelfRegistration

      In questo URL, l'*alias* è il nome univoco fornito.

   b. Specificare uno degli account utente esistenti seguenti che serva da account utente pubblico. CA Identity Manager utilizza questo account per consentire a utenti sconosciuti di accedere ad attività pubbliche senza dovere fornire le credenziali.

      - Gli utenti LDAP immettono l'ID univoco o il DN relativo dell'account utente pubblico. Assicurarsi che di questo valore venga eseguito il mapping sullo %USER_ID% noto (a pagina 79). Ad esempio, se il DN del DN utente è uid=Admin1, ou=People, ou=Employees, ou=NeteAuto, digitare Admin1.
      - Gli utenti del database relazionale digitano il valore di cui viene eseguito il mapping sull'attributo noto %USER_ID% nel file di configurazione della directory o nell'ID univoco dell'utente.

   Fare clic su Convalida per visualizzare l'ID completo dell'utente.

9. Selezionare le attività e i ruoli da creare per questo ambiente. È possibile eseguire le attività seguenti:

   - **Creazione di ruoli predefiniti**

     Consente di creare un insieme di attività e ruoli predefiniti che sono inizialmente disponibili nell'ambiente. Gli amministratori possono utilizzare queste attività e ruoli come modelli per creare nuove attività e ruoli nella console utente.

   - **Creazione soltanto del ruolo di manager di sistema**

     Consente di creare solo il ruolo di manager di sistema e le attività a esso associate.

     Per accedere all'ambiente, è necessario il ruolo di manager di sistema.

     Un manager di sistema può creare nuove attività e ruoli nella console utente.

- **Importazione di ruoli dal file**

  Consente di importare un file delle definizioni del ruolo esportato da un altro ambiente di CA Identity Manager.

  Nota: per utilizzare l'ambiente di CA Identity Manager, il file delle definizioni del ruolo deve includere almeno il ruolo di Manager di sistema o un ruolo che includa attività simili.

  Selezionare i ruoli di importazione dal pulsante di opzione del file e digitare il percorso e il nome file del file delle definizioni del ruolo o accedere al file da importare.

10. Selezionare i file delle definizioni dei ruoli per creare set di attività predefinite per il proprio ambiente e fare clic su Avanti.

    I file delle definizioni dei ruoli sono file XML che definiscono un set di attività e ruoli richiesti per supportare specifiche funzionalità. Ad esempio, se si desidera gestire Active Directory ed endpoint UNIX NIS, selezionare i file delle definizioni dei ruoli.

    Nota: questo passaggio è facoltativo. Se non si desidera creare attività predefinite aggiuntive per supportare la nuova funzionalità, ignorare questa schermata.

11. Definire un utente per servire da manager di sistema per questo ambiente nel modo seguente:

    a. Nel campo Manager di sistema, digitare il valore di cui viene eseguito il mapping sull'attributo noto %USER_ID% nel file di configurazione della directory o specificare uno degli account utente seguenti:

       - Gli utenti LDAP immettono l'ID univoco o il DN relativo dell'utente. Ad esempio, se il DN del DN utente è uid=Admin1, ou=People, ou=Employees, ou=NeteAuto, digitare Admin1.
       - Gli utenti del database relazionale digitano l'ID univoco dell'utente.

    b. Fare clic su Aggiungi.

       CA Identity Manager aggiunge l'ID completo dell'utente all'elenco di utenti.

    c. Fare clic su Avanti.

    Prendere nota dei punti seguenti quando si specifica il Manager di sistema:

    - Il Manager di sistema *non* deve essere lo stesso utente dell'amministratore dell'archivio utenti.
    - È possibile specificare più manager di sistema per l'ambiente. Tuttavia, è possibile specificare solo il manager di sistema iniziale nella console di gestione. Per specificare ulteriori manager di sistema, assegnare il ruolo di Manager di sistema agli utenti appropriati nella console utente.

12. Nel campo Inbound Administrator (Amministratore in entrata), specificare un account di amministratore di CA Identity Manager in grado di eseguire attività di amministrazione di cui è stato eseguito il mapping sui mapping in entrata.

    L'utente deve essere in grado di eseguire tutte queste attività su qualsiasi utente. Il ruolo di Manager di provisioning della sincronizzazione contiene le attività di provisioning nei mapping in entrata predefiniti.

13. Immettere una password per il keystore, il database delle chiavi che codificano e decriptano i dati.

    La definizione di questa password è un prerequisito per la definizione delle chiavi dinamiche. È possibile modificare la password dopo aver creato l'ambiente mediante l'attività Sistema, Chiavi segrete.

    Viene visualizzata una pagina che riassume le impostazioni per l'ambiente.

14. Rivedere le impostazioni per l'ambiente. Fare clic su Precedente per modificare o fare clic su Fine per creare l'ambiente di CA Identity Manager con le impostazioni attuali.

    La schermata Environment Configuration Output (Output di configurazione ambiente) mostra l'avanzamento dell'operazione di creazione ambiente.

15. Fare clic su Continua per uscire dalla procedura guidata di creazione dell'ambiente di CA Identity Manager.

16. Avviare l'ambiente.

    Fare clic sul nome dell'ambiente, quindi fare clic su Inizio.

17. In caso di interruzione dei server dei criteri al passaggio 1, riavviarli ora.

Accesso a un ambiente di CA Identity Manager

Dopo aver creato un ambiente di CA Identity Manager, è possibile accedervi digitando un URL nel browser.

Nota: abilitare JavaScript nel browser che si utilizza per accedere alla console di gestione.

Il formato dell'URL dipende dalla configurazione dell'ambiente e dal tipo di attività a cui si desidera accedere.

- Per accedere alle attività protette dalla console utente, utilizzare l'URL seguente:

  `http://`*`hostname`*`/iam/im/`*`alias`*

  nomehost

  Definisce il nome di dominio completo del server in cui CA Identity Manager è installato: ad esempio, myserver.mycompany.com

  alias

  Definisce l'alias dell'alias di ambiente, ad esempio, employees.

  Accedere all'ambiente di CA Identity Manager con un account di amministratore con privilegi, come ad esempio l'account di manager di sistema creato per l'ambiente di CA Identity Manager.

  Nota: tutte le attività di CA Identity Manager sono protette a meno che non si configurino attività pubbliche.

- Per accedere alle attività pubbliche, che non richiedono che gli utenti forniscano credenziali, utilizzare un URL con il formato seguente:

  `http://`*`hostname`*`/iam/im/`*`alias`*`/index.jsp?task.tag=`*`tasktag`*

  nomehost

  Definisce il nome di dominio completo del server in cui CA Identity Manager è installato: ad esempio, myserver.mycompany.com

  alias

  Definisce l'alias per le attività pubbliche, ad esempio, self-service.

  task_tag

  Definisce il tag per l'attività da richiamare.

  Si specifica il tag di attività quando si configura un'attività nella console utente.

  I tag di attività per la registrazione automatica predefinita e le attività di ripristino delle password dimenticate sono SelfRegistration e ForgottenPasswordReset.

  Nota: per ulteriori informazioni, consultare la *Guida per l'amministratore*.

Configurazione di un ambiente per il provisioning

Dopo avere abilitato l'accesso al server di provisioning (a pagina 172), è possibile configurare un ambiente per il provisioning.

Successivamente, si crea un utente CA Identity Manager speciale, chiamato Inbound administrator (Amministratore in entrata), una connessione al server di provisioning e si configura la sincronizzazione in entrata in Manager di provisioning.

Nota: quando si modificano le proprietà di provisioning per un ambiente, assicurarsi di riavviare il server applicazioni per rendere le modifiche effettive.

Configurazione dell'amministratore in entrata

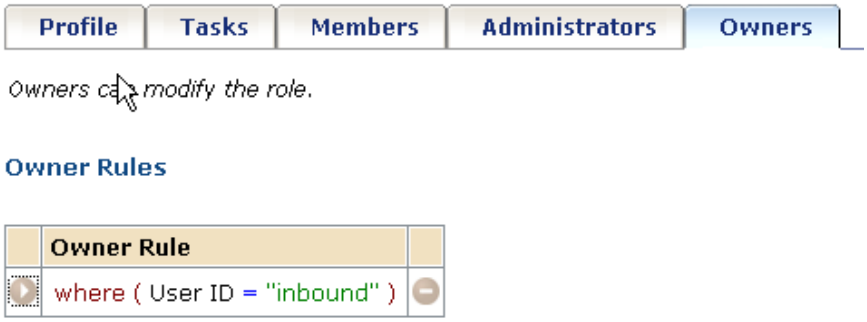
Per garantire il corretto funzionamento della sincronizzazione in entrata, creare un utente CA Identity Manager speciale denominato *amministratore in entrata*. Nelle versioni precedenti di CA Identity Manager, l'amministratore in entrata veniva denominato *utente aziendale*. Questo account utente non è utilizzato dagli utenti, ma viene utilizzato internamente da CA Identity Manager. Tuttavia, è necessario creare questo account utente e assegnare a esso le attività appropriate.

Procedere come descritto di seguito:

1. Accedere all'ambiente di CA Identity Manager come utente con il ruolo di Manager di sistema.
2. Creare un utente. È possibile denominare l'utente **in entrata** come promemoria dello scopo.
3. Scegliere Ruoli di amministrazione, Modify Admin Roles (Modifica ruoli di amministrazione) e selezionare un ruolo che contenga le attività utilizzate per la sincronizzazione.
   - Provisioning - Crea utente
   - Fare clic su Enable/Disable User (Abilita/disabilita utente).
   - Provisioning - Modifica utente

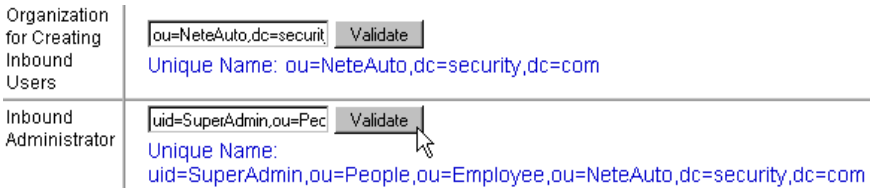
   Nota: se non si sono modificate le attività di sincronizzazione predefinite, utilizzare il ruolo di Manager di provisioning della sincronizzazione.

4. Nella scheda Membri, aggiungere un criterio membri che includa:
   - Una regola membri che il nuovo utente soddisfa.
   - Una regola di ambito che fornisce l'accesso a tutti gli utenti interessati dalle modifiche alla directory di provisioning che attiva la sincronizzazione in entrata.



5. Nella console di gestione:
   a. Selezionare l'ambiente.
   b. Aprire le impostazioni avanzate e selezionare Provisioning.
   c. Completare il campo Organizzazione per la creazione di utenti in entrata se la directory di CA Identity Manager include un'organizzazione.

      Questa organizzazione si trova nella posizione in cui gli utenti vengono creati quando si verifica la sincronizzazione in entrata. Ad esempio, quando un utente viene aggiunto alla directory di provisioning, CA Identity Manager aggiunge l'utente a questa organizzazione.
   d. Completare il campo Inbound administrator (Amministratore in entrata) con l'ID utente creato al passaggio 2.
   e. Fare clic su Convalida per confermare che l'ID utente sia accettato come viene mostrato nell'esempio seguente in cui l'ID utente completo viene visualizzato sotto l'ID utente inserito.



   f. Modificare altri campi in questa schermata. Nessuna modifica viene richiesta.

      Se si effettua una modifica, assicurarsi di comprendere correttamente il funzionamento dei campi. Per ulteriori informazioni su ciascun campo, fare clic sul collegamento ? disponibile nella schermata.

Connessione di un ambiente a un server di provisioning

Procedere come descritto di seguito:

1. Nella Console di gestione, fare clic su Environments (Ambienti).

   Viene visualizzato un elenco degli ambienti esistenti.
2. Fare clic sul nome dell'ambiente che si vuole associare al server di provisioning.
3. Fare clic sull'icona della freccia a destra nel campo Server di provisioning.

   Viene visualizzata la schermata Provisioning Properties (Proprietà di provisioning).
4. Selezionare il server di provisioning.
5. Fare clic su Salva in fondo alla pagina.
6. Configurare la sincronizzazione nel Manager di provisioning (a pagina 197).

Configurazione della sincronizzazione nel Manager di provisioning

La sincronizzazione in entrata mantiene CA Identity Manager aggiornato con le modifiche effettuate nella directory di provisioning. Le modifiche includono quelle eseguite mediante il Manager di provisioning e le modifiche apportate agli endpoint per i quali il server di provisioning ha un connettore. Ciascun server di provisioning supporta un unico ambiente. Tuttavia, è possibile configurare ambienti di backup su sistemi diversi di un cluster se l'ambiente attuale non è disponibile.

Procedere come descritto di seguito:

1. Scegliere Inizio, CA Identity Manager, Manager di provisioning.
2. Fare clic su Sistema, CA Identity Manager Setup (Impostazione di CA Identity Manager).
3. Completare il campo Nome host con il nome del sistema su cui è installato il server CA Identity Manager.

4. Completare il campo Porta con il numero di porta del server applicazioni.
5. Completare il campo Environment name (Nome ambiente) con l'alias dell'ambiente.
6. Selezionare Connessione protetta se si desidera utilizzare il protocollo HTTPS per comunicare con il server CA Identity Manager invece di utilizzare HTTP e codificare le singole notifiche.
7. Fare clic su Aggiungi.
8. Ripetere i passaggi da 3 a 6 per ciascuna versione di backup dell'ambiente.

   Se il server applicazioni per l'ambiente attuale non è disponibile, CA Identity Manager esegue il failover su un ambiente di backup. È possibile riordinare gli ambienti di backup correnti per impostare l'ordine di failover.
9. Se questo è il primo ambiente, riempire i campi Segreto condiviso mediante la password inserita durante l'installazione di CA Identity Manager per l'utente per i componenti inclusi.

   Nota: questi campi non sono applicabili se FIPS è abilitato in questa installazione.
10. Impostare Livello log nel modo seguente:
    - No log (Nessun registro): nessuna informazione viene scritta nel file di registro.
    - Errore: vengono registrati solo i messaggi di errore.
    - Informazioni: vengono registrati messaggi di errore e informativi (valore predefinito).
    - Avviso: vengono registrati i messaggi di errore, di avviso e informativi.
    - Debug: vengono registrate tutte le informazioni.
11. Riavviare il server applicazioni prima di accedere all'ambiente.

Nota: per visualizzare un registro di operazioni di sincronizzazione in entrata e per qualsiasi problema verificatosi durante la sincronizzazione, consultare il file seguente:

PSHOME\logs\etanotify<date>.log

Importazione di ruoli di provisioning personalizzati

Quando si crea l'ambiente, si ha la scelta di utilizzare i ruoli predefiniti o di creare un file di definizioni di ruolo personalizzato. Se si importano definizioni di ruoli personalizzate, importare *anche* le definizioni di ruolo Provisioning only (Solo provisioning). Dopo avere creato l'ambiente, importare le definizioni di ruolo dal file ProvisioningOnly-RoleDefinitions.xml, che si trova in una di queste cartelle:

admin_tools\ProvisioningOnlyRoleDefinitions/Organization

admin_tools\ProvisioningOnlyRoleDefinitions/NoOrganization

La posizione predefinita per *admin_tools* è:

- **Windows**: C:\Programmi\CA\Identity Manager\IAM Suite\Identity Manager\tools
- **UNIX**: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

Sincronizzazione degli account per l'attività Reimposta password utente

Per attivare la fornitura per un ambiente CA Identity Manager, importare un file di configurazione denominato ProvisioningOnly-RoleDefinitions.xml, che crea i ruoli e le attività per la fornitura di utenti.

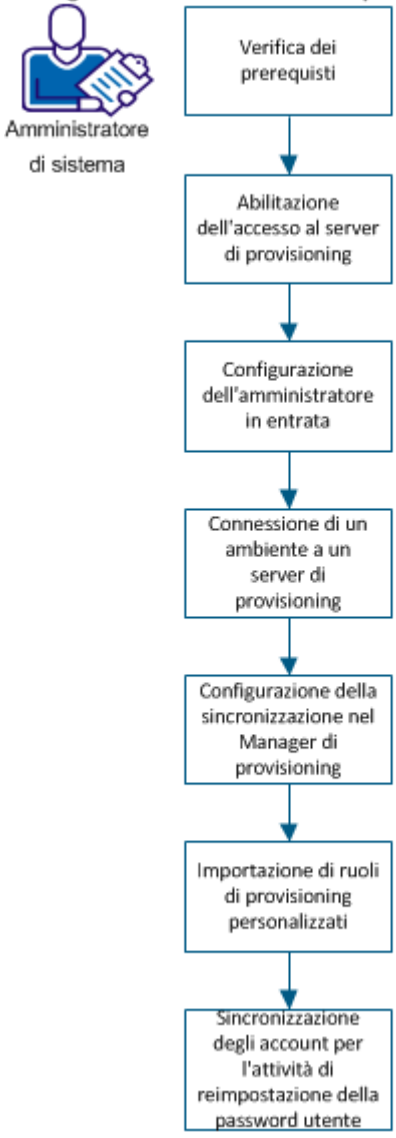
In tale file, per impostazione predefinita la sincronizzazione degli account per l'attività Reimposta password utente è impostata su Disattivata. Prima di attivare la fornitura, la sincronizzazione è impostata su Al completamento dell'attività.

Per utilizzare l'attività Reimposta password utente per attivare la sincronizzazione degli account, impostare l'opzione Sincronizzazione account dopo l'importazione del file ProvisioningOnly-RoleDefinitions.xml per abilitare la fornitura.

Creazione e distribuzione dei connettori tramite Connector Xpress

È possibile configurare il provisioning affinché un ambiente fornisca account in altri sistemi agli utenti gestiti da CA Identity Manager. Gli account forniscono agli utenti l'accesso a risorse aggiuntive, come ad esempio un account di posta elettronica. Questi account aggiuntivi vengono forniti assegnando ruoli di provisioning creati tramite CA Identity Manager.

Configurazione di un ambiente per il provisioning



L'amministratore deve completare i passaggi seguenti:

1. Verifica dei prerequisiti (a pagina 201)
2. Abilitazione dell'accesso al server di provisioning (a pagina 172)

3. Configurazione dell'amministratore in entrata (a pagina 195)
4. Connessione di un ambiente a un server di provisioning (a pagina 197)
5. Configurazione della sincronizzazione nel Manager di provisioning (a pagina 197)
6. Importazione di ruoli di provisioning personalizzati (a pagina 199)
7. Sincronizzazione degli account per l'attività di reimpostazione della password utente (a pagina 199)

Verifica dei prerequisiti

Prima di configurare l'ambiente per il provisioning, verificare che la directory di provisioning sia installata su CA Directory. Per ulteriori informazioni, consultare la *Guida all'installazione*.

Attivazione dell'accesso al server di provisioning

L'accesso al server di provisioning viene abilitato utilizzando il collegamento Directory nella console di gestione.

Nota: un prerequisito di questa procedura è l'installazione della directory di provisioning in CA Directory. Per ulteriori informazioni, consultare la *Guida all'installazione*.

Procedere come descritto di seguito:

1. Aprire la console di gestione digitando il seguente URL in un browser:

   `http://hostname:port/iam/immanage`

   nomehost

   Definisce il nome host completo del sistema in cui il server di CA Identity Manager è installato.

   porta

   Definisce il numero di porta del server applicazioni.

2. Fare clic su Directory.

   Viene visualizzata la finestra Directory di CA Identity Manager.

3. Fare clic su Create from Wizard (Crea da procedura guidata).

4. Digitare il percorso e il nome del file XML della directory per configurare la directory di provisioning. Tale directory viene archiviata nel percorso directoryTemplates\ProvisioningServer della cartella Administrative Tools (Strumenti di amministrazione). La posizione predefinita di questa cartella è:
   - Windows: C:\Programmi\CA\Identity Manager\IAM Suite\Identity Manager\tools
   - UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

   Nota: è possibile utilizzare questo file di configurazione di directory così come sono installati, ossia senza alcuna modifica.
5. Fare clic su Avanti.
6. Fornire i valori per i campi in questa finestra nel seguente modo:

   Nome

   Nome della directory di provisioning associata al server di provisioning in fase di configurazione.
   - Se CA Identity Manager non è integrato con SiteMinder, specificare un nome significativo per l'oggetto utilizzato da CA Identity Manager per connettersi all'archivio utenti.
   - Se CA Identity Manager è integrato con SiteMinder, si hanno due possibilità:

     Se si desidera creare un oggetto di connessione della directory utente in SiteMinder, specificare un qualsiasi nome significativo. CA Identity Manager crea questo oggetto in SiteMinder con il nome specificato.

     Se si desidera connettersi a una directory utente di SiteMinder esistente, specificare esattamente il nome oggetto di connessione della directory utente di SiteMinder così come viene visualizzato nell'interfaccia utente del Policy Server.

   Descrizione

   (Facoltativo) Descrive la directory di CA Identity Manager.

   Host

   Specifica il nome host o l'indirizzo IP del server sul quale è installata la directory utente.

   Porta

   Specifica il numero di porta della directory utente.

Dominio

Definisce il nome del dominio di provisioning gestito da CA Identity Manager.

Importante. Durante la creazione di una directory di provisioning attraverso la console di gestione, se si utilizzano caratteri di una lingua straniera come nome di dominio, la creazione della directory di provisioning non riesce.

Il nome deve corrispondere al nome del dominio di provisioning specificato durante l'installazione.

Nota: nel nome di dominio è rilevante la distinzione tra maiuscole e minuscole.

Nome utente

Specifica un utente che può accedere al Manager di provisioning.

L'utente deve disporre del profilo di Amministratore di dominio o di un insieme equivalente di privilegi per il dominio di provisioning.

Password

Specifica la password per l'utente globale specificato nel campo Nome utente.

Conferma password

Immettere nuovamente la password digitata nel campo Password per la conferma.

Connessione protetta

Indica se CA Identity Manager utilizza una connessione protetta.

Assicurarsi di selezionare questa opzione per gli archivi utenti di Active Directory.

Parametri di ricerca nella directory

maxrows definisce il numero massimo di risultati che CA Identity Manager può restituire durante la ricerca in una directory utente. Questo valore sostituisce qualsiasi limite impostato nella directory LDAP. Quando si applicano impostazioni in conflitto, il server LDAP utilizza l'impostazione più bassa.

Nota: il parametro maxrows non limita il numero di risultati visualizzati nella schermata di attività di CA Identity Manager. Per configurare le impostazioni di visualizzazione, modificare la definizione della schermata elenco nella console utente di CA Identity Manager. Per istruzioni, consultare la *User Console Design Guide*.

timeout determina la durata massima in secondi della ricerca di una directory da parte di CA Identity Manager prima della sua interruzione.

Failover Connections (Connessioni di failover)

Il nome host e il numero di porta di uno o più sistemi facoltativi che sono server di provisioning alternativi. Se vengono elencati server multipli, CA Identity Manager tenta di connettersi ai sistemi nell'ordine in cui vengono elencati.

I server di provisioning alternativi vengono utilizzati se il server di provisioning primario non riesce. Quando il server di provisioning primario diventa nuovamente disponibile, il server di provisioning alternativo continua a essere utilizzato. Se si desidera riprendere a utilizzare il server di provisioning, riavviare i server di provisioning alternativi.

7. Fare clic su Avanti.
8. Selezionare gli oggetti da gestire, come ad esempio Utenti o Gruppi.
9. Dopo avere configurato gli oggetti in base alle necessità, fare clic su Show summary deploy directory (Mostra riepilogo e distribuisci directory) e rivedere le impostazioni per la directory di provisioning.
10. Fare clic su una di queste azioni:
    a. Fare clic su Indietro per modificare.
    b. Fare clic su Salva per salvare le informazioni di directory se si desidera effettuare la distribuzione in un secondo momento.
    c. Fare clic su Fine per completare questa procedura e procedere alla configurazione di un ambiente con il provisioning (a pagina 195).

Configurazione dell'amministratore in entrata

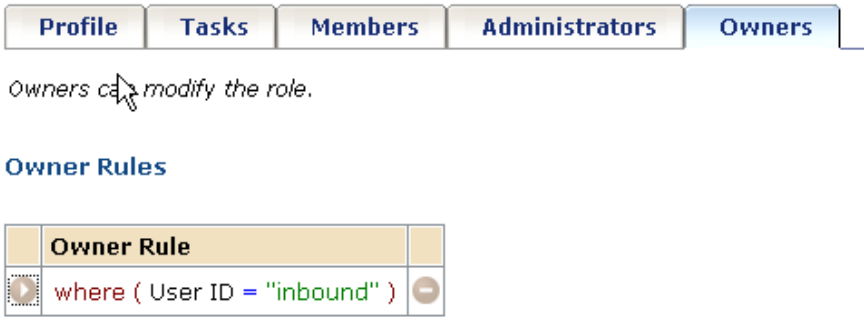
Per garantire il corretto funzionamento della sincronizzazione in entrata, creare un utente CA Identity Manager speciale denominato *amministratore in entrata*. Nelle versioni precedenti di CA Identity Manager, l'amministratore in entrata veniva denominato *utente aziendale*. Questo account utente non è utilizzato dagli utenti, ma viene utilizzato internamente da CA Identity Manager. Tuttavia, è necessario creare questo account utente e assegnare a esso le attività appropriate.

Procedere come descritto di seguito:

1. Accedere all'ambiente di CA Identity Manager come utente con il ruolo di Manager di sistema.
2. Creare un utente. È possibile denominare l'utente **in entrata** come promemoria dello scopo.

3. Scegliere Ruoli di amministrazione, Modify Admin Roles (Modifica ruoli di amministrazione) e selezionare un ruolo che contenga le attività utilizzate per la sincronizzazione.
   - Provisioning - Crea utente
   - Fare clic su Enable/Disable User (Abilita/disabilita utente).
   - Provisioning - Modifica utente

   Nota: se non si sono modificate le attività di sincronizzazione predefinite, utilizzare il ruolo di Manager di provisioning della sincronizzazione.
4. Nella scheda Membri, aggiungere un criterio membri che includa:
   - Una regola membri che il nuovo utente soddisfa.
   - Una regola di ambito che fornisce l'accesso a tutti gli utenti interessati dalle modifiche alla directory di provisioning che attiva la sincronizzazione in entrata.

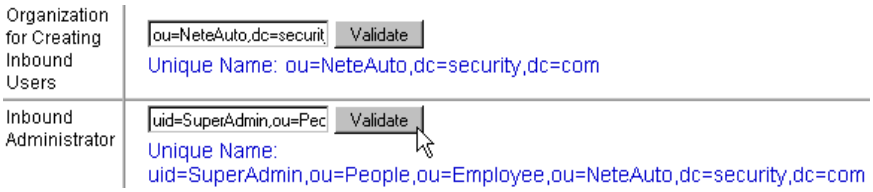


5. Nella console di gestione:
   a. Selezionare l'ambiente.
   b. Aprire le impostazioni avanzate e selezionare Provisioning.
   c. Completare il campo Organizzazione per la creazione di utenti in entrata se la directory di CA Identity Manager include un'organizzazione.

      Questa organizzazione si trova nella posizione in cui gli utenti vengono creati quando si verifica la sincronizzazione in entrata. Ad esempio, quando un utente viene aggiunto alla directory di provisioning, CA Identity Manager aggiunge l'utente a questa organizzazione.

d. Completare il campo Inbound administrator (Amministratore in entrata) con l'ID utente creato al passaggio 2.

e. Fare clic su Convalida per confermare che l'ID utente sia accettato come viene mostrato nell'esempio seguente in cui l'ID utente completo viene visualizzato sotto l'ID utente inserito.



f. Modificare altri campi in questa schermata. Nessuna modifica viene richiesta.

Se si effettua una modifica, assicurarsi di comprendere correttamente il funzionamento dei campi. Per ulteriori informazioni su ciascun campo, fare clic sul collegamento ? disponibile nella schermata.

Connessione di un ambiente a un server di provisioning

Procedere come descritto di seguito:

1. Nella Console di gestione, fare clic su Environments (Ambienti).

   Viene visualizzato un elenco degli ambienti esistenti.

2. Fare clic sul nome dell'ambiente che si vuole associare al server di provisioning.

3. Fare clic sull'icona della freccia a destra nel campo Server di provisioning.

   Viene visualizzata la schermata Provisioning Properties (Proprietà di provisioning).

4. Selezionare il server di provisioning.

5. Fare clic su Salva in fondo alla pagina.

6. Configurare la sincronizzazione nel Manager di provisioning (a pagina 197).

Configurazione della sincronizzazione nel Manager di provisioning

La sincronizzazione in entrata mantiene CA Identity Manager aggiornato con le modifiche effettuate nella directory di provisioning. Le modifiche includono quelle eseguite mediante il Manager di provisioning e le modifiche apportate agli endpoint per i quali il server di provisioning ha un connettore. Ciascun server di provisioning supporta un unico ambiente. Tuttavia, è possibile configurare ambienti di backup su sistemi diversi di un cluster se l'ambiente attuale non è disponibile.

Procedere come descritto di seguito:

1. Scegliere Inizio, CA Identity Manager, Manager di provisioning.
2. Fare clic su Sistema, CA Identity Manager Setup (Impostazione di CA Identity Manager).
3. Completare il campo Nome host con il nome del sistema su cui è installato il server CA Identity Manager.
4. Completare il campo Porta con il numero di porta del server applicazioni.
5. Completare il campo Environment name (Nome ambiente) con l'alias dell'ambiente.
6. Selezionare Connessione protetta se si desidera utilizzare il protocollo HTTPS per comunicare con il server CA Identity Manager invece di utilizzare HTTP e codificare le singole notifiche.
7. Fare clic su Aggiungi.
8. Ripetere i passaggi da 3 a 6 per ciascuna versione di backup dell'ambiente.

   Se il server applicazioni per l'ambiente attuale non è disponibile, CA Identity Manager esegue il failover su un ambiente di backup. È possibile riordinare gli ambienti di backup correnti per impostare l'ordine di failover.
9. Se questo è il primo ambiente, riempire i campi Segreto condiviso mediante la password inserita durante l'installazione di CA Identity Manager per l'utente per i componenti inclusi.

   Nota: questi campi non sono applicabili se FIPS è abilitato in questa installazione.
10. Impostare Livello log nel modo seguente:
    - No log (Nessun registro): nessuna informazione viene scritta nel file di registro.
    - Errore: vengono registrati solo i messaggi di errore.
    - Informazioni: vengono registrati messaggi di errore e informativi (valore predefinito).
    - Avviso: vengono registrati i messaggi di errore, di avviso e informativi.
    - Debug: vengono registrate tutte le informazioni.
11. Riavviare il server applicazioni prima di accedere all'ambiente.

Nota: per visualizzare un registro di operazioni di sincronizzazione in entrata e per qualsiasi problema verificatosi durante la sincronizzazione, consultare il file seguente:

PSHOME\logs\etanotify<date>.log

Importazione di ruoli di provisioning personalizzati

Quando si crea l'ambiente, si ha la scelta di utilizzare i ruoli predefiniti o di creare un file di definizioni di ruolo personalizzato. Se si importano definizioni di ruoli personalizzate, importare *anche* le definizioni di ruolo Provisioning only (Solo provisioning). Dopo avere creato l'ambiente, importare le definizioni di ruolo dal file ProvisioningOnly-RoleDefinitions.xml, che si trova in una di queste cartelle:

admin_tools\ProvisioningOnlyRoleDefinitions/Organization
admin_tools\ProvisioningOnlyRoleDefinitions/NoOrganization

La posizione predefinita per *admin_tools* è:

- **Windows**: C:\Programmi\CA\Identity Manager\IAM Suite\Identity Manager\tools
- **UNIX**: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

Sincronizzazione degli account per l'attività Reimposta password utente

Per attivare la fornitura per un ambiente CA Identity Manager, importare un file di configurazione denominato ProvisioningOnly-RoleDefinitions.xml, che crea i ruoli e le attività per la fornitura di utenti.

In tale file, per impostazione predefinita la sincronizzazione degli account per l'attività Reimposta password utente è impostata su Disattivata. Prima di attivare la fornitura, la sincronizzazione è impostata su Al completamento dell'attività.

Per utilizzare l'attività Reimposta password utente per attivare la sincronizzazione degli account, impostare l'opzione Sincronizzazione account dopo l'importazione del file ProvisioningOnly-RoleDefinitions.xml per abilitare la fornitura.

Gestione ambienti

Questa sezione descrive le operazioni di gestione di un ambiente.

Modificare le proprietà di ambiente di CA Identity Manager

La schermata Environment Properties (Proprietà ambiente) di CA Identity Manager nella console di gestione consente di eseguire le attività seguenti:

- Visualizzare le impostazioni attuali per l'ambiente.
- Modificare la descrizione, l'URL di base e gli alias protetti e pubblici.

- Importare un ambiente di CA Identity Manager esistente dopo un aggiornamento.

  Nota: per ulteriori informazioni sull'importazione di ambienti di CA Identity Manager esistenti, consultare la sezione sugli aggiornamenti della *Guida all'installazione*.

- Avviare e interrompere l'ambiente
- Accedere alle pagine per configurare le attività seguenti:
  - **Impostazioni avanzate**

    Configura le funzionalità avanzate, incluse le funzionalità generate mediante le API di CA Identity Manager.

  - **Role and Task Settings (Impostazioni ruolo e attività).**

    Consente di importare un file delle definizioni di ruolo esportato da un altro ambiente di CA Identity Manager.

  - **Manager di sistema**

    Assegna ruoli di Manager di sistema.

Procedere come descritto di seguito:

1. Se CA Identity Manager utilizza un cluster di Policy Server di SiteMinder, interrompere tutti i Policy Server eccetto uno.
2. Se si dispone di un cluster di nodi CA Identity Manager, interrompere tutti i nodi CA Identity Manager eccetto uno.
3. Fare clic su Environments (Ambienti).

   Viene visualizzata la schermata degli ambienti di CA Identity Manager, in cui è visualizzato un elenco degli ambienti di CA Identity Manager.

4. Fare clic sul nome dell'ambiente di CA Identity Manager da modificare.

   Viene visualizzata la schermata Proprietà di CA Identity Manager in cui sono riportate le proprietà seguenti:

   OID

   Definisce un identificatore univoco per l'ambiente. CA Identity Manager genera questo ID quando si crea un ambiente di CA Identity Manager.

   Si utilizza l'OID quando si configura la rimozione di attività da un database di persistenza delle attività. Consultare la *Guida all'installazione*.

   Nome

   Specifica il nome univoco dell'ambiente di CA Identity Manager.

   Descrizione

   Fornisce una descrizione dell'ambiente di CA Identity Manager.

Directory di CA Identity Manager

Specifica la directory di CA Identity Manager con cui l'ambiente è associato.

Enable Verbose Log Output (Abilita output registro dettagliato)

Controlla quante informazioni CA Identity Manager registra e mostra nel registro di ambiente quando si importa un ambiente. Il registro di ambiente viene visualizzato nella finestra di stato della console di gestione quando si importano un ambiente o altre definizioni di oggetto da un file.

Nota: la selezione di questa casella di controllo può avere un impatto significativo sulle prestazioni.

Il registro dettagliato include i messaggi di convalida e distribuzione per ciascun oggetto (attività, schermata, ruolo e criterio) e i relativi attributi nell'ambiente.

Per visualizzare il registro dettagliato, selezionare questa casella di controllo e salvare le proprietà dell'ambiente. Quando si importano ruoli o altre impostazioni da un file, le informazioni aggiuntive vengono visualizzate nel registro.

Server di provisioning

Specifica la directory di provisioning utilizzata come archivio utenti di provisioning.

Fare clic sul pulsante freccia a destra per configurare la directory di provisioning nella pagina Provisioning Properties (Proprietà di provisioning).

Versione

Definisce il numero di versione di CA Identity Manager.

URL di base

Specifica la porzione dell'URL CA Identity Manager che non include l'alias protetto o pubblico dell'ambiente.

CA Identity Manager utilizza l'URL di base per formare l'URL di reindirizzamento in modo che faccia riferimento all'attività dei servizi password nel criterio di password predefinito dell'ambiente.

Protected Alias (Alias protetto)

Definisce il nome dell'URL di base per accedere alle attività protette nella console utente per un ambiente di CA Identity Manager.

Public Alias (Alias pubblico)

Definisce il nome dell'URL di base per accedere alle attività pubbliche, come ad esempio la registrazione automatica e le attività relative alle password dimenticate.

Public User (Utente pubblico)

Definisce l'account utente che CA Identity Manager utilizza al posto delle credenziali fornite dell'utente per accedere alle attività pubbliche.

Job Timeout (Timeout processo)

Determina il periodo di tempo che CA Identity Manager attende dopo che un'attività è stata inoltrata prima che venga visualizzato un messaggio di stato.

Questo valore viene impostato nella pagina della console utente in Impostazioni avanzate.

Status (Stato)

Interrompe o riavvia l'ambiente di CA Identity Manager.

Migrate Task Persistence Data from CA Identity Manager 8.1 (Esegui migrazione dati di persistenza attività da CA Identity Manager 8.1)

Consente di eseguire la migrazione dei dati da un database di persistenza delle attività di CA Identity Manager 8.1 a un database di persistenza delle attività di CA Identity Manager 12.6.4.

Per ulteriori informazioni, consultare la *Guida all'installazione*.

Nota: il pulsante Migrate Task Persistence Data from CA Identity Manager 8.1 (Esegui migrazione dati di persistenza attività da CA Identity Manager 8.1) è visibile solo negli ambienti creati in versioni precedenti di CA Identity Manager e di cui è stata eseguita la migrazione a CA Identity Manager 12.6.4.

5. Modificare la descrizione, l'URL di base o l'alias protetto o pubblico, secondo le esigenze.
6. Se si sono modificate le proprietà dell'ambiente, riavviare l'ambiente di CA Identity Manager.
7. In caso di interruzione dei server dei criteri al passaggio 1, riavviarli ora.

Impostazioni ambiente

Le informazioni specifiche all'ambiente vengono archiviate in tre file di impostazioni di ambiente:

- *alias*_environment_roles.xml
- *alias*_environment_settings.xml
- *alias*_environment.xml

Nota: l'*alias* fa riferimento all'alias dell'ambiente. L'alias viene specificato quando si crea l'ambiente.

Un file .zip contenente questi file, che riflettono la configurazione attuale, viene generato quando si esportano le impostazioni di ambiente.

Dopo avere esportato le impostazioni di ambiente, importare le impostazioni per completare una delle attività seguenti:

- Gestire più ambienti con impostazioni simili. In questo caso, si crea un ambiente con le impostazioni necessarie, si importano tali impostazioni in altri ambienti e si personalizzano in ciascun ambiente, secondo le esigenze.
- Eseguire la migrazione di un ambiente da un sistema di sviluppo a un sistema di produzione.
- Aggiornare un ambiente esistente dopo avere eseguito l'aggiornamento a una nuova versione di CA Identity Manager.

Esportazione di un ambiente di CA Identity Manager

Per effettuare la distribuzione di un ambiente di CA Identity Manager su un sistema di produzione, si esporta l'ambiente da un sistema di sviluppo o gestione temporanea e lo si importa nel sistema di produzione.

Nota: quando si importa un ambiente precedentemente esportato, CA Identity Manager mostra un registro in una finestra di stato nella console di gestione. Per visualizzare le informazioni di convalida e distribuzione per ciascuno oggetto distribuito e relativi attributi in questo registro, selezionare il campo Enable Verbose Log Output (Abilita output registro dettagliato) nella pagine delle proprietà dell'ambiente *prima* di esportare l'ambiente. La selezione del campo Enable Verbose Log Output (Abilita output registro dettagliato) può causare problemi di prestazioni significativi durante l'importazione.

Procedere come descritto di seguito:

1. Fare clic su Environments (Ambienti) nella console di gestione.

   Viene visualizzata la schermata degli ambienti di CA Identity Manager, in cui è visualizzato un elenco degli ambienti di CA Identity Manager.
2. Selezionare l'ambiente che si desidera esportare.
3. Fare clic sul pulsante Esporta.

   Viene visualizzata la schermata di download file.
4. Salvare il file .zip in una posizione accessibile per il sistema di produzione.
5. Fare clic su Fine.

Le informazioni di ambiente vengono esportate in un file .zip che è possibile importare in un altro ambiente.

Importazione di un ambiente di CA Identity Manager

È possibile importare le impostazioni di ambiente di CA Identity Manager per completare una delle attività seguenti:

- Gestire più ambienti con impostazioni simili. In questo caso, si crea un ambiente con le impostazioni necessarie, si importano tali impostazioni in altri ambienti e si personalizzano in ciascun ambiente, secondo le esigenze.
- Eseguire la migrazione di un ambiente da un sistema di sviluppo a un sistema di produzione.
- Aggiornare un ambiente esistente dopo avere eseguito l'aggiornamento a una nuova versione di CA Identity Manager.

Procedere come descritto di seguito:

1. Fare clic su Environments (Ambienti) nella console di gestione.

   Viene visualizzata la schermata degli ambienti di CA Identity Manager, in cui è visualizzato un elenco degli ambienti di CA Identity Manager.
2. Fare clic sul pulsante Importa.

   Viene visualizzata la schermata Importa ambiente.
3. Accedere al file .zip richiesto per importare un ambiente.
4. Fare clic su Fine.

L'ambiente viene importato in CA Identity Manager.

Riavvio di un ambiente di CA Identity Manager

Procedere come descritto di seguito:

1. Fare clic su Environments (Ambienti) nella console di gestione.

   Viene visualizzata la schermata degli ambienti di CA Identity Manager, in cui è visualizzato un elenco degli ambienti di CA Identity Manager.
2. Fare clic sul nome dell'ambiente di CA Identity Manager da avviare.

   Viene visualizzata la schermata Environment Properties (Proprietà ambiente) di CA Identity Manager.

3. Selezionare una delle seguenti opzioni:

   Restart Environment (Riavvia ambiente)

   Interrompe e avvia un ambiente.

   Arresta

   Arresta un ambiente attualmente in esecuzione.

   Inizio

   Avvia un ambiente attualmente non in esecuzione.

Eliminazione di un ambiente di CA Identity Manager

Utilizzare questa procedura per rimuovere un ambiente di CA Identity Manager.

Nota: se CA Identity Manager si integra con SiteMinder per l'autenticazione avanzata, CA Identity Manager elimina anche il dominio di criterio di SiteMinder che protegge l'ambiente e gli schemi di autenticazione predefiniti creati per l'ambiente.

Procedere come descritto di seguito:

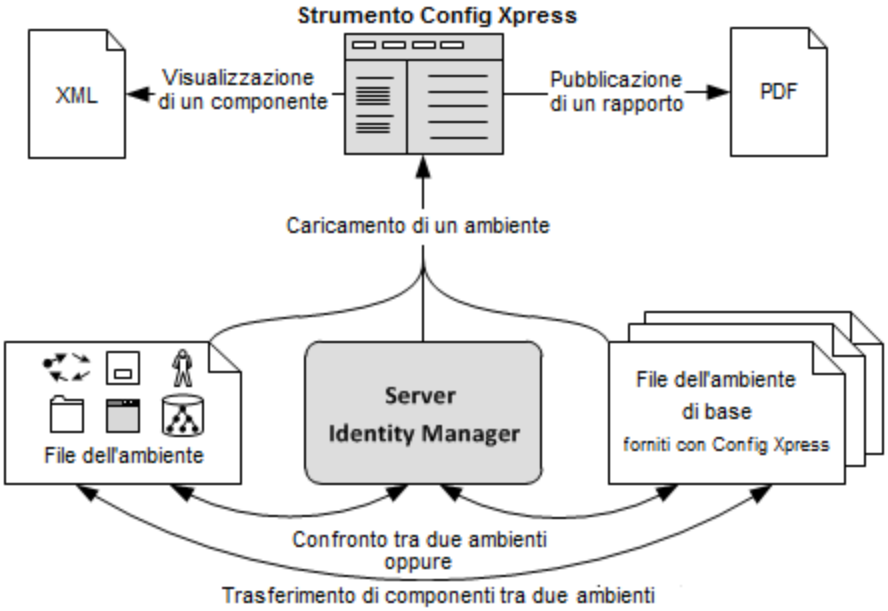
1. Nella schermata Envirnoments (Ambienti), selezionare la casella di controllo corrispondente agli ambienti di CA Identity Manager da eliminare.
2. Fare clic su Elimina.

   In CA Identity Manager viene visualizzato un messaggio di conferma.
3. Fare clic su OK per confermare l'eliminazione.

Gestione configurazione

Config Xpress è uno strumento incluso in CA Identity Manager. È possibile utilizzare questo strumento per analizzare e lavorare con le configurazioni dei propri ambienti CA Identity Manager.

Lo strumento consente di spostare i componenti tra gli ambienti. Config Xpress rileva automaticamente qualsiasi altro componente richiesto e richiede che venga spostato. Questa funzionalità consente di risparmiare tempo e di ridurre il rischio che si verifichino problemi.



Procedere come descritto di seguito:

1. Impostare Config Xpress (a pagina 216).
2. Prima di poter utilizzare lo strumento, caricare un ambiente di CA Identity Manager (a pagina 217) in Config Xpress per fare un'analisi.
3. Utilizzare Config Xpress per eseguire queste attività con l'ambiente caricato:
   - Spostare i componenti tra gli ambienti (a pagina 219).
   - Pubblicare un rapporto in formato PDF dei componenti di sistema (a pagina 220).
   - Visualizzare la configurazione XML per un particolare componente (a pagina 221).

Impostazione di Config Xpress

I file di installazione di Config Xpress sono inclusi nell'unità di installazione, ma lo strumento non viene installato.

Config Xpress ha i requisiti software seguenti:

- CA Identity Manager r12.0 e successive
- Sistema operativo Windows
- Adobe Air Runtime
- Lettore PDF per visualizzare i rapporti

Procedere come descritto di seguito:

1. Scaricare Adobe Air Runtime da http://get.adobe.com/air e installarlo.
2. Assicurarsi che gli strumenti di amministrazione siano installati.
3. Cercare il file di installazione di Config Xpress nella posizione seguente:

   ```
   C:\Programmi\CA\Identity Manager\IAM Suite\Identity Manager\tools\ConfigXpress
   ```

4. Eseguire Config Xpress.air per installare Config Xpress.
5. Quando l'installazione è completa, Config Xpress si avvia.

Caricamento di un ambiente in Config Xpress

Prima di utilizzare Config Xpress, caricare uno o più ambienti nello strumento. Questa attività consente di lavorare con l'ambiente in Config Xpress.

È possibile caricare un ambiente in Config Xpress direttamente da un server CA Identity Manager attivo oppure da un file di ambiente. Se si utilizza uno dei file di ambiente linea di base che vengono installati con Config Xpress, è possibile confrontare il proprio ambiente con la configurazione predefinita.

Il processo di caricamento di un ambiente può richiedere alcuni minuti.

Procedere come descritto di seguito:

1. Aprire Config Xpress.
2. Per caricare un **ambiente attivo** direttamente da un server CA Identity Manager:
   a. Fare clic sulla scheda Server (Rete).
   b. Immettere il nome e la porta del server CA Identity Manager. Ad esempio:

      ```
      servername.ca.com:8080
      ```

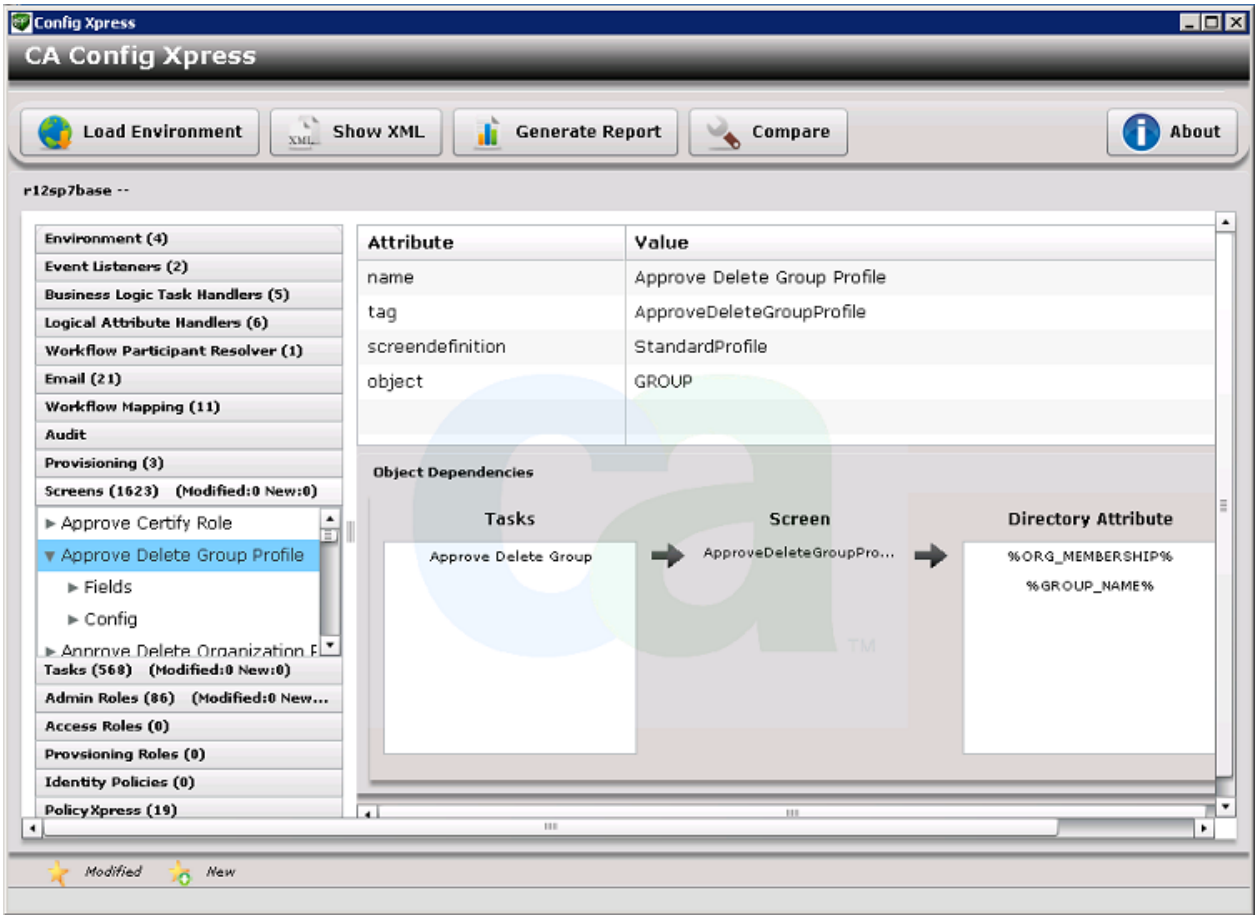
   c. Selezionare Usa HTTPS se il server è impostato per consentire solo HTTPS.
   d. Selezionare 12.5 SP7 se la versione del server è più recente di r12.5 SP6.
   e. Fare clic su Connetti.
   f. Scegliere un ambiente dall'elenco *Choose Environment to load (Scegliere ambiente da caricare)*, quindi fare clic su Carica.
3. Per caricare un **file di ambiente** esportato dall'ambiente di CA Identity Manager:
   a. Esportare un ambiente di CA Identity Manager.
   b. In Config Xpress, fare clic sulla scheda File System.
   c. Selezionare la versione, quindi accedere al file di ambiente e fare clic su Carica.
4. Per caricare un **file di ambiente linea di base** che è stato installato con Config Xpress:
   a. Fare clic sulla scheda Base Versions (Versioni di base).
   b. Selezionare la versione richiesta, quindi fare clic su Seleziona.

Config Xpress analizza l'ambiente, quindi visualizza i dettagli dell'ambiente.

A questo punto è possibile pubblicare una parte o l'intero ambiente come PDF (a pagina 220) o XML (a pagina 221). Se si carica un secondo ambiente, è possibile confrontare tali ambienti e spostare componenti (a pagina 219) tra di essi.

Esempio: Config Xpress dopo avere caricato uno file di configurazione linea di base

Questa schermata mostra come Config Xpress visualizza gli oggetti dipendenti:



Spostamento di un componente da un ambiente a un altro

Senza Config Xpress, l'attività di spostare componenti tra aree a gestione temporanea è complessa e potrebbe non riuscire.

Quando si utilizza Config Xpress per spostare componenti, lo strumento sposta anche tutti gli oggetti richiesti. Ad esempio, se si sposta un'attività che richiede una schermata, Config Xpress chiede se si desidera selezionare anche i componenti richiesti. Config Xpress capisce che l'attività utilizza questa schermata e dovrebbe essere anch'essa spostata nell'ambiente di destinazione.

Se si desidera spostare un componente in un ambiente attivo, Config Xpress lo carica immediatamente. Se si desidera spostare il componente in un file di ambiente, salvare il componente come file XML e importare quel file nell'ambiente.

Procedere come descritto di seguito:

1. Caricare l'ambiente che contiene il componente che si desidera spostare.
2. Confrontare questo ambiente con un secondo:
   a. Fare clic su Compare (Confronta).
   b. Caricare l'ambiente di destinazione.

      Config Xpress mostra un elenco delle differenze tra i due ambienti.
3. Nell'elenco delle differenze, trovare un componente che si desidera spostare. È possibile fare clic sulla colonna Nome per ordinare l'elenco.
4. Per ciascun componente, eseguire i passaggi seguenti:
   a. Selezionare l'elemento nella colonna Azione.

      Config Xpress analizza il componente, un'operazione che può richiedere del tempo.
   b. Se il componente ha dei componenti dipendenti, viene visualizzata la casella Add Modified Dependant Screens (Aggiungi schermate dipendenti modificate). Fare clic su Sì o Non per continuare.

   Dopo aver selezionato tutti i componenti che si desidera spostare, è possibile spostare i componenti aggiornati.
5. Se si spostano i componenti in un server attivo, fare clic su Upload To (Carica in).

   I componenti vengono spostati immediatamente.
6. Se si spostano i componenti in un file di ambiente:
   a. Fare clic su Salva.
   b. Immettere un nome file, quindi fare clic di nuovo su Salva.

      Config Xpress salva tutti i componenti selezionati in un file XML. A questo punto è possibile importare questo file XML nell'ambiente di destinazione effettivo.

Pubblicazione di un rapporto PDF

Config Xpress può generare un rapporto che documenta lo stato attuale di un ambiente di CA Identity Manager. È possibile utilizzare questo rapporto per acquisire una snapshot di un ambiente di produzione. Quando si genera il rapporto, si sceglie se includere la configurazione completa o solo le modifiche successive all'installazione.

Questo rapporto è utile per riferimento futuro o come parte di un piano di recupero del sistema.

Procedere come descritto di seguito:

1. Caricare un ambiente in Config Xpress
2. Fare clic su Generate Report (Genera rapporto).

   Nella finestra di dialogo Generate PDF Report (Genera rapporto PDF), è possibile modificare la dimensione del carattere e immettere del testo per le pagine del titolo o della copertina. È inoltre possibile scegliere se includere tutti gli elementi di configurazione o solo gli elementi nuovi o modificati.

   Importante. Se non si fa clic sulla casella *Only include details of new or modified tasks, screens, roles (Includi solo dettagli di attività, schermate, ruoli nuovi o modificati*), il rapporto conterrà l'intero ambiente. Il file PDF sarà lungo circa 2000 pagine e oltre 40 MB di dimensioni.
3. Fare clic su OK.
4. Immettere un nome di file e salvare il rapporto. Il salvataggio può richiedere qualche minuto o tempi più lunghi se nel caso in cui si desideri pubblicare l'intero ambiente.

   Il rapporto si apre nel lettore PDF.

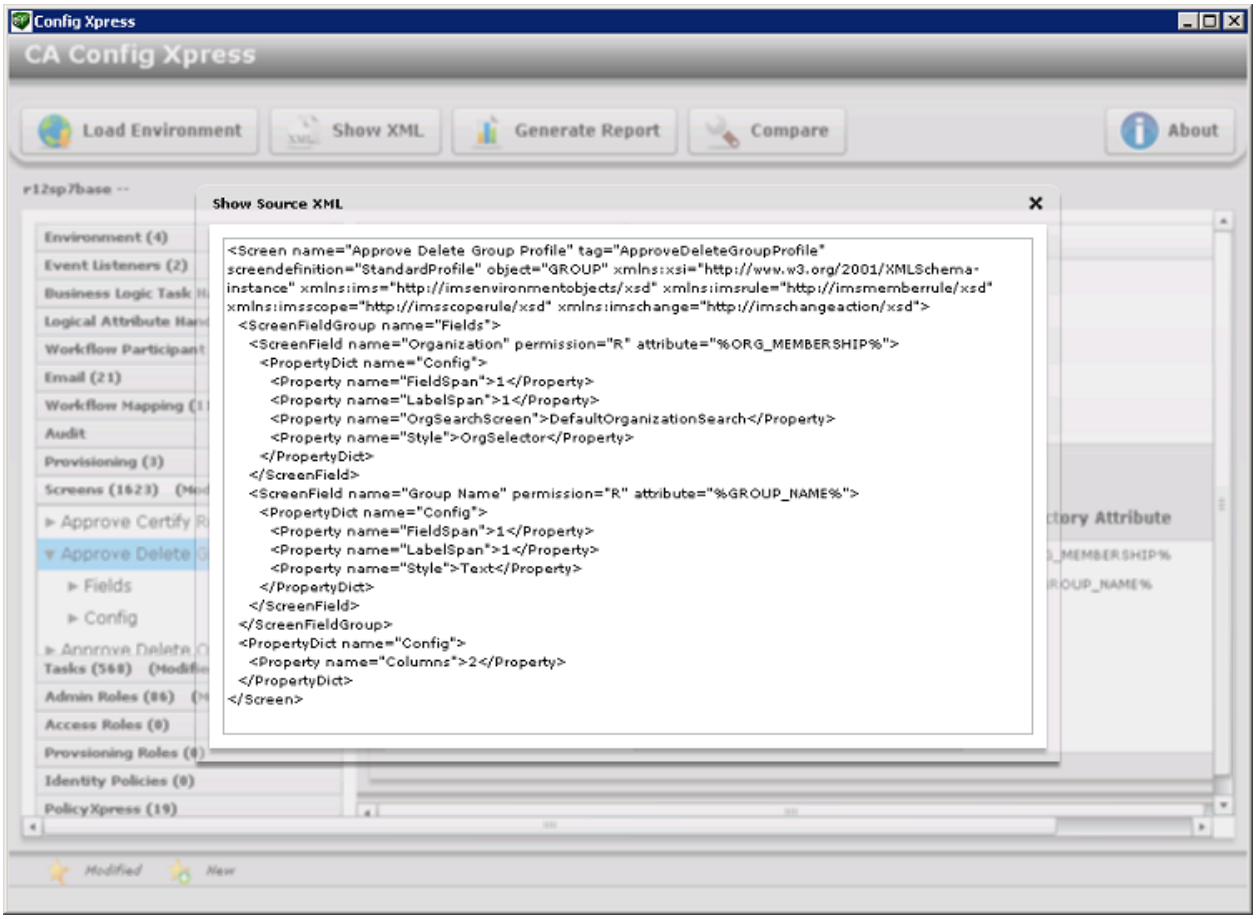
Visualizzazione della configurazione

Config Xpress può visualizzare la configurazione XML per un particolare componente. È possibile studiare questo file XML per comprendere un sistema.

Procedere come descritto di seguito:

1. Caricare un ambiente in Config Xpress
2. Fare clic su un componente nella schermata Config Xpress.
3. Fare clic su Visualizza XML.

   Viene visualizzata la configurazione XML:



Ottimizzazione della valutazione delle regole di criterio

Le regole di criterio, che identificano in modo dinamico un set di utenti, vengono utilizzate nella valutazione dei criteri del membro del ruolo, amministratore e titolare e dei criteri di identità. La valutazione di queste regole può richiedere molto tempo nel caso di implementazioni di CA Identity Manager di dimensioni elevate.

Nota: per ulteriori informazioni sui criteri relativi a membri, amministratore, titolare e identità, consultare la *Guida per l'amministratore*.

Per ridurre il tempo necessario alla valutazione delle regole che includono attributi utente, è possibile attivare l'opzione di valutazione in memoria. Quando l'opzione di valutazione in memoria è abilitata, CA Identity Manager recupera dall'archivio utenti le informazioni su un utente da valutare e archivia una rappresentazione di quell'utente in memoria. CA Identity Manager utilizza la rappresentazione in memoria per confrontare i valori di attributo con le regole dei criteri. Questa operazione limita il numero di chiamate effettuate direttamente da CA Identity Manager all'archivio utenti.

Abilitare l'opzione di valutazione in memoria per un ambiente nella console di gestione.

Procedere come descritto di seguito:

1. Aprire la console di gestione.
2. Selezionare Environments (Ambienti), *Environment Name (Nome ambiente)*, Impostazioni avanzate, Varie.

   Si apre la pagina delle proprietà definite dall'utente.
3. Immettere il testo seguente nel campo Proprietà:

   UseInMemoryEvaluation
4. Immettere *uno* dei numeri seguenti nel campo Valore:

   0

   La valutazione in memoria viene disabilitata.

   1

   La valutazione in memoria viene abilitata. Quando si specifica questa opzione, il confronto di attributo tiene conto della distinzione tra maiuscole e minuscole.

   3

   La valutazione in memoria viene abilitata. Quando si specifica questa opzione, il confronto di attributo non tiene conto della distinzione tra maiuscole e minuscole.
5. Fare clic su Aggiungi.

   CA Identity Manager aggiunge la nuova proprietà all'elenco delle proprietà esistenti dell'ambiente.
6. Fare clic su Salva.

Role and Task Settings (Impostazioni ruolo e attività).

Dalla schermata Role and Task Settings (Impostazioni ruolo e attività) nella console di gestione, è possibile importare o esportare le impostazioni di schermate, schede, ruoli e attività in un file XML, chiamato file delle definizioni di ruolo. CA Identity Manager fornisce file delle definizioni di ruolo predefiniti che consentono di creare schermate, schede, ruoli e attività per un insieme di funzionalità. Ad esempio, esiste un file delle definizioni di ruolo che supporta Smart Provisioning, e altri file che supportano schermate di gestione di endpoint.

In aggiunta, è possibile utilizzare un file delle definizioni di ruolo per applicare le impostazioni da un singolo ambiente a più ambienti. Eseguire le attività seguenti:

- Configurare le impostazioni di schermata, scheda, attività e ruolo in un ambiente.
- Esportare tali impostazioni in un file XML.
- Importare il file XML nell'ambiente richiesto.

Esportare Role and Task Settings (Impostazioni ruolo e attività).

Eseguire la procedura seguente per esportare le impostazioni di ruolo e attività.

Procedere come descritto di seguito:

1. Nella Console di gestione, fare clic su Environments (Ambienti).

   Viene visualizzato un elenco di ambienti di CA Identity Manager.

2. Fare clic sul nome dell'ambiente di CA Identity Manager appropriato.

   Viene visualizzata la schermata Proprietà di quell'ambiente.

3. Fare clic su Role and Task Settings (Impostazioni ruolo e attività), e fare clic su Esporta.

4. Fare clic su Apri per visualizzare il file in una finestra di browser o Salva per salvare le impostazioni in un file XML.

Importare Role and Task Settings (Impostazioni ruolo e attività).

Le impostazioni di ruolo e attività vengono definite in file XML, denominati file delle definizioni di ruolo. È possibile importare file delle definizioni di ruolo predefiniti per supportare set specifici di funzionalità di CA Identity Manager (ad esempio, Smart Provisioning) o importare file delle definizioni di ruolo da un ambiente a un altro.

Nota: è possibile importare anche definizioni di ruolo per connettori personalizzati creati con Connector Xpress. Si creano questi file di definizioni di ruolo con il Role Definitions Generator (Generatore di definizioni di ruolo). Per ulteriori informazioni, consultare la *Guida di Connector Xpress*.

Eseguire la procedura seguente per importare le impostazioni di ruolo e attività.

Procedere come descritto di seguito:

1. Nella Console di gestione, fare clic su Environments (Ambienti).

   Viene visualizzato un elenco di ambienti di CA Identity Manager.

2. Fare clic sul nome dell'ambiente di CA Identity Manager in cui si desidera importare le impostazioni di ruolo e attività.

   Viene visualizzata la schermata Proprietà di quell'ambiente.

3. Fare clic su Role and Task Settings (Impostazioni ruolo e attività), e fare clic su Importa.

4. Completare una delle seguenti azioni:

   - Selezionare uno o più file di definizioni di ruolo per creare ruoli e attività predefinite per l'ambiente.

     Per selezionare tutti i file di definizioni di ruolo disponibili, fare clic su Select/Deselect All (Seleziona/Deseleziona tutto).

   - Digitare il percorso e il nome file per il file delle definizioni di ruolo da importare o accedere al file. Quindi fare clic su Fine.

5. Fare clic su Fine.

   Lo stato viene visualizzato nella finestra Role Configuration Output (Output di configurazione ruolo).

6. Fare clic su Continua per uscire.

Creazione di ruoli e attività per endpoint dinamici

Mediante Connector Xpress, è possibile configurare connettori dinamici per consentire il provisioning e la gestione di database SQL e directory LDAP. Per ciascun connettore dinamico, è possibile utilizzare il generatore delle definizioni di ruolo per creare definizioni di attività e schermate per le schermate di gestione account che vengono visualizzate nella console utente.

Dopo avere eseguito il generatore delle definizioni di ruolo, si importa il file delle definizioni di ruolo risultante (a pagina 224) nella console di gestione.

Nota: per ulteriori informazioni sul generatore delle definizioni di ruolo, consultare la *Guida di Connector Xpress*.

Modifica dell'account Manager di sistema

Un manager di sistema è responsabile dell'installazione e gestione di un ambiente di CA Identity Manager. In generale, le attività di un manager di sistema includono:

- Creazione e gestione dell'ambiente iniziale
- Creazione e modifica dei ruoli di amministrazione
- Creazione e modifica di altri account di amministratore

Si crea un account di manager di sistema quando si crea un ambiente di CA Identity Manager. Se questo account è bloccato, ad esempio, se il manager di sistema ha dimenticato la password, è possibile ricreare l'account utilizzando la procedura guidata Manager di sistema.

La procedura guidata Manager di sistema guida attraverso i passaggi necessari per assegnare un ruolo di gestione di sistema a un utente.

Notare i punti seguenti prima di modificare l'account di Manager di sistema:

- Assicurarsi di stare utilizzando un archivio utenti LDAP e di avere configurato un contenitore utente, come ad esempio ou=People nel file di configurazione della directory (directory.xml) per la directory di CA Identity Manager. Gli utenti selezionati devono esistere nello stesso contenitore in cui si configura il manager di sistema. La selezione di un account utente che non esiste nel contenitore utente può causare errori.
- Quando l'ambiente di CA Identity Manager gestisce una directory utente con una struttura flato o una struttura utente flat, il profilo dell'utente selezionato deve includere anche l'organizzazione. Per assicurare che il profilo di un utente venga configurato correttamente, aggiungere il nome dell'organizzazione dell'utente all'attributo fisico che corrisponde all'attributo noto %ORG_MEMBERSHIP% nel file directory (a pagina 86).xml. Ad esempio, quando viene eseguito il mapping della descrizione dell'attributo fisico sull'attributo noto %ORG_MEMBERSHIP% nel file directory.xml e l'utente appartiene all'organizzazione Employees (Dipendenti), il profilo dell'utente deve contenere la coppia di attributo/valore description=Employees.

Procedere come descritto di seguito:

1. Nella schermata degli ambienti di CA Identity Manager, fare clic sul nome dell'ambiente di CA Identity Manager appropriato.

   Vengono visualizzate le proprietà della schermata di quel particolare ambiente.

2. Fare clic su Manager di sistema.

   Viene visualizzata la procedura guidata Manager di Sistema.

3. Digitare il nome univoco per l'utente che ha il ruolo di Manager di Sistema nel modo seguente:

   - Per gli utenti del database relazionale, digitare l'ID univoco per l'utente o il valore di cui viene eseguito il mapping all'attributo noto %USER_ID% nel file di configurazione della directory.
   - Per gli utenti LDAP, digitare il DN relativo dell'utente. Ad esempio, se il DN dell'utente è uid=Admin1, ou=People, ou=Employees, ou=NeteAuto, digitare Admin1.

   Nota: assicurarsi che il Manager di sistema *non* sia lo stesso utente dell'amministratore dell'archivio utenti.

4. Fare clic su Convalida per visualizzare l'ID completo dell'utente.

5. Fare clic su Avanti.

6. Nella seconda pagina della procedura guidata, selezionare un ruolo da assegnare all'utente nel modo seguente:
   - Se si desidera assegnare il ruolo di Manager di sistema, eseguire le operazioni seguenti:
     a. Selezionare il pulsante di opzione accanto al ruolo Manager di sistema.
     b. Fare clic su Fine.
   - Se si desidera assegnare un ruolo diverso da quello di Manager di sistema, eseguire le operazioni seguenti:
     a. Selezionare una condizione nel primo elenco.
     b. Digitare un nome di ruolo parziale o completo o un asterisco (*) nella seconda casella di riepilogo. Fare clic su Cerca.
     c. Selezionare il ruolo da assegnare dall'elenco dei risultati della ricerca.
     d. Fare clic su Fine.

   La schermata System Manager Configuration Output (Output di configurazione Manager di sistema) mostra le informazioni di stato.
7. Fare clic su Continua per chiudere la procedura guidata Manager di sistema.

Accedere allo stato di un ambiente di CA Identity Manager

CA Identity Manager include una pagina di stato che è possibile utilizzare per verificare lo stato seguente:

- La directory di CA Identity Manager viene caricata correttamente.
- CA Identity Manager può connettersi all'archivio utenti.
- L'ambiente di CA Identity Manager viene caricato correttamente.

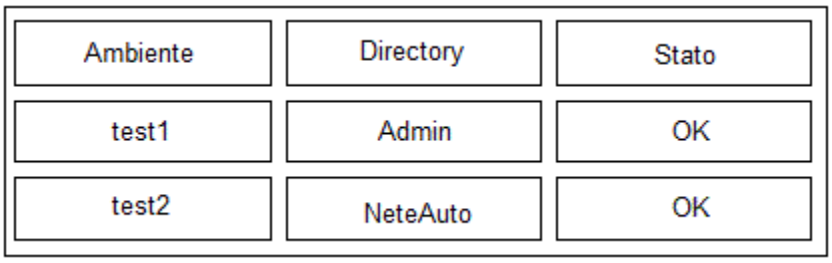
Per accedere alla pagina di stato, digitare l'URL seguente in un browser:

`http://`*`hostname`*`/iam/im/status.jsp`

nomehost

Determina il nome di dominio completo del server in cui CA Identity Manager è installato, ad esempio, myserver.mycompany.com.

Se l'ambiente di CA Identity Manager si avvia correttamente e tutte le connessioni vengono eseguite correttamente, la pagina di stato assomiglia all'illustrazione seguente:



La pagina di stato indica anche se l'ambiente è conforme a FIPS 140-2.

Risoluzione dei problemi degli ambienti di CA Identity Manager

La tabella seguente descrive i messaggi di errore possibili e la procedura di risoluzione dei problemi:

Messaggio	Descrizione	Risoluzione dei problemi
Non caricato	La directory di CA Identity Manager associata all'ambiente non è stata caricata all'avvio di CA Identity Manager.	1. Verificare che l'archivio utenti sia in esecuzione. Se CA Identity Manager si integra con SiteMinder, verificare che SiteMinder sia in grado di stabilire la connessione all'archivio utenti.
Non riuscita	CA Identity Manager non è in grado di stabilire la connesione alla directory di CA Identity Manager.	Nell'interfaccia utente del Policy Server, per verificare la connessione aprire la pagina delle proprietà della connessione della directory utente di SiteMinder associata all'archivio utenti e fare clic sul pulsante View Contents (Visualizza contenuto). Se è possibile visualizzare i contenuti dell'archivio utenti, significa che SiteMinder può connettersi correttamente. Per ulteriori informazioni sul Policy Server, consultare CA *SiteMinder Web Access Manager Policy Server Configuration Guide*. 2. Riavviare CA Identity Manager e il Policy Server.

Messaggio	Descrizione	Risoluzione dei problemi
La connessione di SM non è riuscita	CA Identity Manager non è in grado di connettersi al Policy Server di SiteMinder (per implementazioni che includono SiteMinder)	1. Verificare le seguenti condizioni: ■ Il Policy Server è in esecuzione. ■ L'agente Web sta proteggendo le risorse. È possibile verificare che l'agente Web sia correttamente in esecuzione accedendo all'interfaccia utente del Policy Server. Se vengono richieste le credenziali, significa che l'agente Web sta funzionando correttamente. 2. Riavviare CA Identity Manager e il Policy Server.
IMS non è disponibile	Si è verificato un errore in CA Identity Manager.	Controllare il registro del server applicazioni per i dettagli di errore.
Messaggio di errore 500 di Windows	La pagina di stato non viene visualizzata quando vi si accede rimuovendo la connettività con la directory utente LDAP.	Impostare l'opzione del browser Internet Show friendly error message (Mostra messaggio di errore descrittivo) su Disattivato per visualizzare la pagina di stato.

Capitolo 7: Impostazioni avanzate

La finestra Impostazioni avanzate nella console di gestione consente di definire le impostazioni seguenti:

- Accedere a schermate per configurare le impostazioni avanzate
- Importare ed esportare le impostazioni avanzate come descritto nella sezione Importazione/Esportazione di impostazioni personalizzate (a pagina 245).

Questa sezione contiene i seguenti argomenti:

Verifica

I registri di verifica mantengono i record delle operazioni eseguite in un ambiente di CA Identity Manager. È possibile utilizzare i dati nei registri di verifica per monitorare le attività del sistema.

Eventi di verifica di CA Identity Manager. Un evento è un'operazione generata da un'attività di CA Identity Manager. Un'attività può generare più eventi. Ad esempio, l'attività CreateUser può generare gli eventi CreateUserEvent e AddToGroupEvent.

Per impostazione predefinita, CA Identity Manager esporta tutte le informazioni sugli eventi nel database di verifica. Per controllare il tipo e la quantità di informazioni sugli eventi registrate da CA Identity Manager, è possibile eseguire le attività seguenti:

- Abilitare la verifica per le attività di amministrazione di CA Identity Manager.
- Abilitare la verifica di alcuni o tutti gli eventi di CA Identity Manager generati da attività di amministrazione.
- Registrare le informazioni sugli eventi corrispondenti a stati specifici, ad esempio, quando un evento viene completato o annullato.
- Registrare le informazioni relative agli attributi coinvolti in un evento. Ad esempio, è possibile registrare attributi che vengono modificati durante un evento ModifyUserEvent.
- Impostare il livello di verifica per eventi e attributi.

Gestori attività di logica aziendale

Un gestore dell'attività di logica aziendale esegue una logica aziendale personalizzata prima che un'attività di CA Identity Manager venga inoltrata per l'elaborazione. Generalmente, la logica aziendale personalizzata convalida i dati. Ad esempio, un gestore dell'attività di logica aziendale può controllare il limite di appartenenza a un gruppo prima che CA Identity Manager aggiunga un membro al gruppo. Quando il limite di appartenenza al gruppo viene raggiunto, il gestore dell'attività di logica aziendale mostra un messaggio che informa l'amministratore del gruppo che l'aggiunta del nuovo membro non è andata a buon fine.

È possibile utilizzare i gestori di attività di logica aziendale predefiniti o è possibile creare gestori personalizzati mediante l'API del gestore dell'attività di logica aziendale.

Nota: per informazioni sulla creazione di una logica aziendale personalizzata, consultare la *Programming Guide for Java*.

La schermata Gestori attività di logica aziendale contiene un elenco dei gestori di attività di logica aziendale globali esistenti. L'elenco comprende i gestori predefiniti forniti con CA Identity Manager ed eventuali gestori personalizzati definiti presso la sede dell'utente. CA Identity Manager esegue i gestori nell'ordine in cui sono visualizzati in questo elenco.

È possibile implementare i gestori di attività di logica aziendale globali solo in Java.

Svuotare automaticamente i campi Password nell'attività di ripristino delle password utente

È possibile configurare CA Identity Manager per svuotare automaticamente i campi delle password quando un valore precedentemente immesso viola un criterio di password o quando i valori nei campi Password e Conferma password non corrispondono.

Procedere come descritto di seguito:

1. Avviare la console di gestione.
2. Selezionare l'ambiente che si desidera gestire, quindi fare clic su Impostazioni avanzate.

   Viene visualizzata la pagina delle impostazioni avanzate.
3. Fare clic su Gestori attività di logica aziendale, BlthPasswordServices.

   Viene visualizzata la pagina delle proprietà del gestore di logica aziendale.
4. Creare le proprietà seguenti:

   ClearPwdIfInvalid=true

   PwdConfirmAttrName=|passwordConfirm|
5. Verificare che le impostazioni di ConfirmPasswordHandler siano come segue:
   - Object type – User
   - Class – ConfirmPasswordHandler
   - ConfirmationAttributeName = |passwordConfirm|
   - OldPasswordAttributeName = |oldPassword|
   - passwordAttributeName = %PASSWORD%

   Gli utenti possono svuotare i campi della password nell'attività Reset User Password (Ripristina password utente).

Elenco eventi

Le attività di amministrazione includono *eventi*, ovvero azioni eseguite da CA Identity Manager per completare un'attività specifica. Un'attività può includere più eventi. Ad esempio, l'attività Crea utente può includere eventi che comportano la creazione del profilo dell'utente, la aggiunta dell'utente a un gruppo e l'assegnazione di ruoli.

CA Identity Manager controlla gli eventi, applica regole aziendali specifiche del cliente associate agli eventi e, quando viene eseguito il mapping degli eventi viene eseguito sui processi del flusso di lavoro, richiede l'approvazione per gli eventi.

Utilizzare questa pagina per visualizzare un elenco degli eventi che sono disponibili in CA Identity Manager.

Notifiche di posta elettronica

CA Identity Manager può inviare notifiche di posta elettronica quando un'attività o un evento viene completato o quando un evento sotto il controllo del flusso di lavoro raggiunge uno stato specifico. Ad esempio, un messaggio di posta elettronica può informare un responsabile dell'approvazione che un evento richiede approvazione.

Per specificare il contenuto delle notifiche di posta elettronica, è possibile utilizzare modelli di messaggio di posta elettronica predefiniti o personalizzare i modelli per soddisfare le proprie esigenze.

Mediante la console di gestione, è possibile eseguire le attività seguenti:

- Abilitare le notifiche di posta elettronica per un ambiente di CA Identity Manager.
- Specificare i set di modelli per creare messaggi di posta elettronica.
- Indicare gli eventi e le attività per i quali vengono inviate le notifiche di posta elettronica.

Listener di evento

Un'attività di CA Identity Manager è costituita da una o più azioni, eventi con nome che CA Identity Manager esegue durante l'esecuzione dell'attività. Ad esempio, l'attività Crea utente può includere gli eventi seguenti:

- CreateUserEvent: crea un profilo utente in un'organizzazione
- AddToGroupEvent: (Facoltativo) aggiunge l'utente come membro di un gruppo
- AssignAccessRole: (Facoltativo) assegna un ruolo di accesso all'utente

Un *listener di evento* "ascolta" un evento specifico ed esegue una logica aziendale personalizzata in un punto specifico del ciclo di vita di un evento. Ad esempio, dopo la creazione di un nuovo utente in CA Identity Manager, un listener di evento può aggiungere le informazioni di un utente al database di un'altra applicazione.

Nota: per ulteriori informazioni sulla configurazione dei listener di evento, consultare la *Programming Guide for Java*.

Criteri di identità

Un criterio di identità applica un insieme di modifiche aziendali agli utenti che soddisfano certe regole o condizioni. È possibile utilizzare i criteri di identità per le attività seguenti:

- Automazione di specifiche attività di gestione dell'identità, ad esempio l'assegnazione di ruoli e di appartenenza ai gruppi, l'allocazione di risorse o la modifica degli attributi dei profili utenti.
- Applicazione dell'imposizione di mansioni. Ad esempio, è possibile creare un criterio di identità che impedisce ai membri del ruolo di Check Signer (Firmatario assegni) di avere il ruolo di Check Approver (Approvatore assegni).
- Applicazione della conformità. Ad esempio, è possibile verificare gli utenti che hanno un determinato titolo e con un reddito superiore a 100.000 €.

Nella console utente è possibile creare e gestire set di criteri di identità. Per ulteriori informazioni sui criteri di identità, consultare la *Guida per l'amministratore*.

Prima di utilizzare i criteri di identità, utilizzare la console di gestione per eseguire le attività seguenti:

- Abilitare criteri di identità per un ambiente di CA Identity Manager.
- Impostare il livello di ricorsione (facoltativo).

Gestori di attributi logici

Gli attributi logici di CA Identity Manager consentono di visualizzare gli attributi dell'archivio utenti (denominati *attributi fisici*) in un formato accessibile nelle schermate delle attività. Gli amministratori di CA Identity Manager utilizzano le schermate delle attività per eseguire funzioni in CA Identity Manager.

Gli attributi logici non esistono in un archivio utenti. In genere, rappresentano uno o più attributi fisici per semplificarne la presentazione. Ad esempio, la *data* dell'attributo logico può rappresentare gli attributi fisici *mese*, *giorno* e *anno*.

Gli attributi logici vengono elaborati dall'attributo logico che consiste in oggetti Java scritti mediante l'API dell'attributo logico. Ad esempio, quando una schermata di attività viene visualizzata, un gestore attributo logico può convertire i dati di attributo fisico dall'archivio utenti a dati di attributo logico.

È possibile utilizzare attributi logici predefiniti e i gestori attributo logico inclusi con CA Identity Manager oppure crearne di nuovi mediante l'API dell'attributo logico.

Nota: per ulteriori informazioni, consultare la *Programming Guide for Java*.

Varie

Le proprietà definite dall'utente definite in questa schermata vengono applicare all'intero ambiente di CA Identity Manager. Vengono trasferite sotto forma di coppie nome/valore al metodo init() di ogni oggetto Java personalizzato creato con le API di CA Identity Manager. Un oggetto personalizzato può utilizzare questi dati in qualsiasi modo che la logica aziendale dell'oggetto richiede.

Le proprietà definite dall'utente vengono definite anche per un oggetto personalizzato particolare. Ad esempio, supporre che le proprietà definite dall'utente vengano definite nella schermata Proprietà per un listener di evento chiamato MyListener. Le proprietà definite dall'utente specifiche dell'oggetto e le proprietà a livello di ambiente definite nelle schermate Varie vengono passate in una singola chiamata a MyListener.init().

Per aggiungere una proprietà definita dall'utente, specificare un nome e un valore per la proprietà e fare clic su Aggiungi.

Per eliminare una o più proprietà definite dall'utente, selezionare la casella di controllo a fianco di ciascuna coppia nome/valore da eliminare e fare clic su Elimina.

Una volta effettuate le modifiche, fare clic su Salva. Affinché le modifiche diventino effettive, è necessario riavviare il server applicazioni.

Nota: tutte le proprietà varie distinguono tra maiuscole e minuscole. Pertanto, se si definisce una proprietà denominata SelfRegistrationLogoutUrl e un'altra proprietà denominata selfregistrationlogouturl, vengono aggiunte entrambe le proprietà.

Regole di notifica

Una regola di notifica determina che gli utenti ricevano notifiche di posta elettronica. Quando un'attività viene completata o un evento in un'attività raggiunge un certo stato, ad esempio in attesa di approvazione, approvato o rifiutato, gli utenti ricevono una notifica di posta elettronica in base alla regola di notifica.

Nota: per ulteriori informazioni sulla funzionalità delle notifiche di posta elettronica, consultare la *Guida per l'amministratore*.

CA Identity Manager include le regole di notifica predefinite seguenti:

ADMIN_ADAPTER

Invia un messaggio di posta elettronica all'amministratore che inizia l'attività

USER_ADAPTER

Invia un messaggio di posta elettronica all'utente interessato dall'attività

USER_MANAGER

Invia un messaggio di posta elettronica al manager dell'utente nel contesto corrente

Per creare regole di notifica personalizzate, utilizzare l'API delle regole di notifica.

Nota: per ulteriori informazioni sulle regole di notifica, consultare la *Programming Guide for Java*.

Selezionatori di organizzazione

Un selezionatore di organizzazione è un gestore attributo logico personalizzato che determina la posizione in cui CA Identity Manager crea il profilo di un utente registrato automaticamente, che viene basato sulle informazioni che l'utente fornisce durante la registrazione. Ad esempio, il profilo per gli utenti che forniscono un codice promozionale quando si registrano può essere aggiunto a un'organizzazione Utenti promozionali.

Provisioning

Utilizzare questa schermata quando si utilizza CA Identity Manager con il provisioning.

Nota: per informazioni più dettagliate, consultare la sezione Configurazione di un ambiente per il provisioning (a pagina 195).

Le opzioni Provisioning Properties (Proprietà di provisioning) sono le seguenti:

Abilitato

Specifica l'uso di due archivi utenti, uno per CA Identity Manager e un archivio utenti separato (chiamato directory di provisioning) per gli account di provisioning. Se questa opzione viene disabilitata, viene utilizzato solo l'archivio utenti di CA Identity Manager.

Use Session Pool (Usa pool di sessione)

Abilita l'uso di un pool di sessione.

Session Pool Initial Sessions (Sessioni iniziali pool di sessione)

Definisce il numero minimo di sessioni che sono disponibili nel pool all'avvio.

Valore predefinito: 8

Session Pool Maximum Sessions (Numero massimo di sessioni del pool di sessione)

Definisce il numero massimo di sessioni nel pool.

Valore predefinito: 32

Enable Password Changes from Endpoint Accounts (Attiva le modifiche di password dagli account di endpoint)

Definisce l'impostazione per Enable Password Synchronization Agent (Attiva agente sincronizzazione password) per ciascun utente nel server di provisioning. Questa opzione consente la sincronizzazione di password tra utenti di CA Identity Manager e gli account di endpoint associati.

Enable Accumulation of Provisioning Role Membership Events (Attiva accumulo di eventi di appartenenza al ruolo di provisioning)

Se abilitata, questa casella di controllo assicura che CA Identity Manager esegua eventi che sono collegati all'appartenenza ai ruoli di provisioning in un ordine specifico. Tutte le azioni di aggiunta vengono unite in un'unica operazione e inviate al server di provisioning per l'elaborazione. Una volta completata l'elaborazione delle azioni di aggiunta, CA Identity Manager unisce le azioni di rimozione in un'unica operazione che viene inviata al server di provisioning. Un evento singolo, chiamato AccumulatedProvisioningRoleEvent, viene generato per eseguire gli eventi in questo ordine.

Nota: per ulteriori informazioni su AccumulatedProvisioningRoleEvent, consultare la *Guida per l'amministratore*.

Organization for Creating Inbound Users (Organizzazione per la creazione di utenti in entrata)

Definisce il percorso completo all'archivio utenti utilizzato da CA Identity Manager. Questo campo viene visualizzato solo se l'archivio utenti include un'organizzazione.

Amministratore in entrata

Definisce un account di amministratore di CA Identity Manager che può eseguire attività di cui viene eseguito il mapping sui mapping in entrata. Queste attività vengono incluse nel ruolo di Manager di sincronizzazione di provisioning. L'amministratore deve essere in grado di eseguire ciascuna attività su qualsiasi utente di CA Identity Manager.

Directory di provisioning

La directory di provisioning è un repository per le informazioni di provisioning, inclusi dominio, utenti globali, tipi di endpoint, endpoint, account e modelli di account. Quando si seleziona, vengono visualizzate altre opzioni per l'esecuzione del mapping dell'archivio utenti di CA Identity Manager sulla directory di provisioning.

Enable Session Pooling (Attiva pooling di sessione)

Per migliorare le prestazioni, CA Identity Manager può preallocare un numero di sessioni per il pooling durante la comunicazione con il server di provisioning.

Se l'opzione Session Pools (Pool di sessione) viene disattivata, CA Identity Manager crea e distrugge sessioni a seconda delle esigenze.

In un ambiente nuovo, l'opzione Session Pools (Pool di sessione) vengono abilitati per impostazione predefinita. In ambienti esistenti, è possibile abilitare l'opzione Session Pools (Pool di sessione).

Procedere come descritto di seguito:

1. Nella console di gestione, selezionare Impostazioni avanzate, Provisioning.
2. Selezionare Use Session Pool (Usa pool di sessione).
3. Definire il numero minimo di sessioni nel pool all'avvio.
4. Definire il numero massimo di sessioni nel pool.
5. Fare clic su Salva.
6. Riavviare il server applicazioni.

   Il pool di sessione viene abilitato per le impostazioni definite.

Abilitare la sincronizzazione di password

Il server di provisioning consente la sincronizzazione di password tra utenti di CA Identity Manager e gli account degli utenti di endpoint associati. In altre parole, quando un utente che ha ruoli di provisioning viene creato o modificato in CA Identity Manager, l'utente di provisioning viene impostato per consentire le modifiche di password dagli account di endpoint.

Nota: quando si abilita questa funzionalità nella console di gestione, *tutti* gli utenti nell'ambiente vengono impostati per consentire le modifiche di password dagli account di endpoint.

Per abilitare la sincronizzazione di password

1. Nella console di gestione, Selezionare Impostazioni avanzate, Provisioning.
2. Selezionare Enable Password Changes (Abilita modifiche password) da Endpoint Accounts (Account endpoint).
3. Fare clic su Save (Salva).
4. Riavviare il server applicazioni.

Mappature attributi

I mapping di attributo associano gli attributi utente nelle attività di amministrazione relative al provisioning, come Provision Create User (Provisioning - Crea utente), con gli attributi corrispondenti nel server di provisioning. È possibile eseguire il mapping di un singolo attributo di provisioning su più attributi nell'archivio utenti di CA Identity Manager.

I mapping predefiniti esistono per gli attributi nelle attività predefinite, elencate nella sezione Inbound Mappings (Mapping in entrata). Se si modifica una di queste attività di amministrazione in modo tale da utilizzare attributi differenti, aggiornare i mapping di attributo a seconda delle esigenze.

Inbound Mappings (Mapping in entrata)

I mapping in entrata consentono di eseguire il mapping degli eventi, generati dal server di provisioning, su un'attività di amministrazione. Questi mapping sono predefiniti e non possono essere modificati.

Outbound Mappings (Mapping in uscita)

I mapping in uscita consentono di associare gli eventi, che sono generati da attività di amministrazione, a eventi che vengono applicati alla directory di provisioning. Esistono mapping predefiniti per gli eventi che influiscono sugli attributi dell'utente.

Console utente

Si accede a un ambiente di CA Identity Manager mediante la console utente, un'applicazione Web che consente agli utenti di eseguire attività di amministrazione. Si definiscono certe proprietà per la console utente che gli amministratori utilizzano per accedere a un ambiente nella pagina della console utente nella console di gestione.

La pagina Console utente include i campi seguenti:

General Properties (Proprietà generali)

Definire proprietà applicabili a un ambiente.

Show Recently Completed Tasks (Mostra attività completate recentemente)

Stabilisce se viene visualizzato un messaggio di stato in CA Identity Manager quando viene completata un'attività.

Quando questa opzione viene selezionata, gli utenti devono fare clic su OK per cancellare il messaggio di stato visualizzato da CA Identity Manager.

Per disabilitare il messaggio e per fare in modo che gli utenti non debbano fare clic su OK quando viene visualizzato un messaggio di stato, deselezionare questa opzione.

Show About Link (Visualizza collegamento a Informazioni su)

Determina se viene visualizzato un collegamento a Informazioni su nell'angolo in basso a destra della console utente. Quando questa opzione viene selezionata, gli utenti di CA Identity Manager possono fare clic sul collegamento a Informazioni su per visualizzare le informazioni sulla versione di visualizzazione dei componenti di CA Identity Manager.

Abilitazione del cambio di lingua

Determina se in CA Identity Manager viene incluso un elenco a discesa Seleziona lingua nella schermata di accesso e nella console utente. Quando questo campo viene selezionato, gli utenti di CA Identity Manager possono modificare la lingua nella console utente selezionando una nuova lingua dall'elenco.

Nota: per visualizzare il campo Seleziona lingua, assicurarsi di selezionare il campo Enable Language Switching (Abilita cambio di lingua) *e* configurare CA Identity Manager affinché supporti più lingue.

Per ulteriori informazioni, consultare la *User Console Design Guide*.

Job Timeout (Timeout processo)

Determina il periodo di tempo che CA Identity Manager attende dopo che un'attività è stata inoltrata prima che venga visualizzato un messaggio di stato.

Quando l'attività viene completata entro la durata specificata, in CA Identity Manager viene visualizzato il seguente messaggio:

Attività completata

Se l'attività richiede più tempo per il completamento o è sottoposta al controllo del flusso di lavoro, in CA Identity Manager viene visualizzato il seguente messaggio:

Attività inviata per l'elaborazione in *data corrente*

Nota: le modifiche potrebbero non essere applicate immediatamente.

Theme Properties (Proprietà temi)

Consente di personalizzare l'icona e il titolo della console utente in un ambiente. Ad esempio, è possibile aggiungere un logo aziendale e il nome dell'azienda alle schermate della console utente.

Le proprietà dei temi includono le seguenti impostazioni:

Icon (URI) (Icona (URI))

Definisce l'icona mediante un URI a un'immagine disponibile nel server applicazioni.

Esempio: http://myserver.mycompany.com/images/front/logo.gif

Icon Link (URI) (Collegamento icona (URI))

Definisce il collegamento di navigazione all'immagine mediante un URI.

Icon Title (Titolo icona)

Definisce il testo di descrizione del comando che viene visualizzato al passaggio del mouse sull'icona.

Title

Specifica il testo personalizzato che viene visualizzato accanto all'icona nella parte superiore della console utente.

Nota: se è stata definita un'interfaccia personalizzata, è possibile specificare un'icona o un titolo facendo riferimento al file di proprietà dell''interfaccia. Ad esempio, se la voce dell'immagine dell'icona nel file di proprietà di un'interfaccia personalizzata è image/logo.gif, è possibile immettere quella stessa stringa nel campo Icon (Icona).

Login Properties (Proprietà di accesso)

Specificare il metodo di autenticazione e la posizione della pagina di accesso a cui gli utenti vengono indirizzati quando accedono a un ambiente.

Authentication Provider module class name (Nome classe modulo del provider di autenticazione)

Specifica il nome della classe del modulo del provider di autenticazione.

Pagina di accesso

Specifica la pagina a cui gli utenti vengono indirizzati quando accedono a un ambiente.

Servizi Web

Il Servizio Web per l'esecuzione di attività (TEWS, Task Execution Web Service) di CA Identity Managerconsente alle applicazioni client di terze parti di inviare a CA Identity Manager attività di CA Identity Manager per l'esecuzione remota.

La schermata Web Services Properties (Proprietà servizi Web) consente di configurare TEWS per un ambiente. In questa schermata è possibile eseguire le seguenti operazioni:

- Abilitare TEWS per un ambiente di CA Identity Manager.
- Generare documenti Web Services Definition Language (WSDL) specifici dell'attività.
- Consentire l'impersonificazione.
- Specificare che la password amministratore è obbligatoria per l'autenticazione.
- Configurare l'autenticazione di SiteMinder.
- Configurare SiteMinder per proteggere l'URL dei servizi Web se CA Identity Manager è integrato con SiteMinder.
- Specificare l'autenticazione del token del nome utente dei servizi di protezione Web.
- Specificare almeno uno dei tre tipi di autenticazione possibili.

Per informazioni relative all'emissione di richieste remote a CA Identity Manager attraverso TEWS, consultare la *Programming Guide for Java*.

Workflow Properties (Proprietà del flusso di lavoro)

Se abilitata, la funzionalità del flusso di lavoro controlla l'esecuzione di un'attività di CA Identity Manager associata a un processo del flusso di lavoro.

Un processo del flusso di lavoro è un insieme di passaggi eseguiti per raggiungere un obiettivo aziendale, quale la creazione di un account utente. Generalmente, una di queste fasi implica l'approvazione o il rifiuto dell'attività.

Un'attività di amministrazione viene associata a uno o più eventi che possono attivare uno o più processi del flusso di lavoro. Dopo il completamento dei processi del flusso di lavoro, in CA Identity Manager l'attività viene eseguita o rifiutata sulla base dei risultati dei processi del flusso di lavoro.

L'illustrazione seguente mostra la relazione tra un'attività di CA Identity Manager, un evento associato e un processo del flusso di lavoro:

Workflow Properties (Proprietà del flusso di lavoro)

Utilizzare la casella di controllo per abilitare o disabilitare il flusso di lavoro per l'ambiente di CA Identity Manager.

Work Item Delegation (Delega elementi di lavoro)

Se abilitata, la delega degli elementi di lavoro consente a un partecipante (il delegante) di specificare che un altro utente (il delegato) ottenga le autorizzazioni per l'approvazione di attività nell'elenco di lavoro del delegante. Un partecipante può assegnare elementi di lavoro a un altro responsabile dell'approvazione durante i periodi in cui il delegante non è presente in ufficio. I deleganti mantengono l'accesso completo ai loro elementi di lavoro durante il periodo di delega.

La delega utilizza il seguente attributo noto:

%DELEGATORS%

Questo attributo noto archivia i nomi degli utenti che eseguono la delega all'utente con l'attributo, oltre all'ora di creazione della delega.

Nota: per ulteriori informazioni sui criteri di identità preventivi, consultare la *Guida per l'amministratore*.

Workflow Participant Resolvers (Resolver partecipanti al flusso di lavoro)

Le attività in un processo del flusso di lavoro, quali l'approvazione o il rifiuto di un'attività, vengono eseguite dai *partecipanti.*

La schermata Workflow Participant Resolvers (Resolver partecipanti al flusso di lavoro) viene utilizzata per eseguire il mapping di un resolver partecipante personalizzato su una classe Java completa del resolver partecipante.

Un *resolver partecipante* personalizzato è un oggetto di Java che stabilisce i partecipanti di un'attività del flusso di lavoro e restituisce un elenco a CA Identity Manager. Questo elenco viene quindi trasferito da CA Identity Manager al motore del flusso di lavoro.

In genere, un resolver partecipante personalizzato viene scritto solo se nessuno dei resolver partecipanti standard è in grado di fornire l'elenco dei partecipanti richiesto da un'attività.

Nota: per informazioni sullo sviluppo di resolver partecipanti personalizzati, consultare la *Programming Guide for Java*. Per informazioni sui resolver partecipanti standard, consultare la *Guida per l'amministratore*.

Import/Export Custom Settings (Importa/Esporta impostazioni personalizzate)

Dalla schermata Impostazioni avanzate nella console di gestione, è possibile applicare impostazioni avanzate a più ambienti, nel seguente modo:

- Configurare le impostazioni avanzate in un ambiente.
- Esportare le impostazioni avanzate a un file XML.
- Importare il file XML negli ambienti richiesti.

Errori di memoria insufficiente in Java Virtual Machine

Sintomo:

Gli errori di memoria insufficiente in JVM vengono ricevuti durante periodi di stress o di carico elevato che influiscono sulla funzionalità del server di CA Identity Manager.

Soluzione:

Si consiglia di impostare le opzioni di debug in JVM in modo da ricevere notifiche sulle condizioni di memoria insufficiente.

Nota: per ulteriori informazioni sull'impostazione delle opzioni di debug in JVM, consultare Debugging Options in Java HotSpot VM Options all'indirizzo http://www.oracle.com.

Capitolo 8: Verifica

Questa sezione contiene i seguenti argomenti:

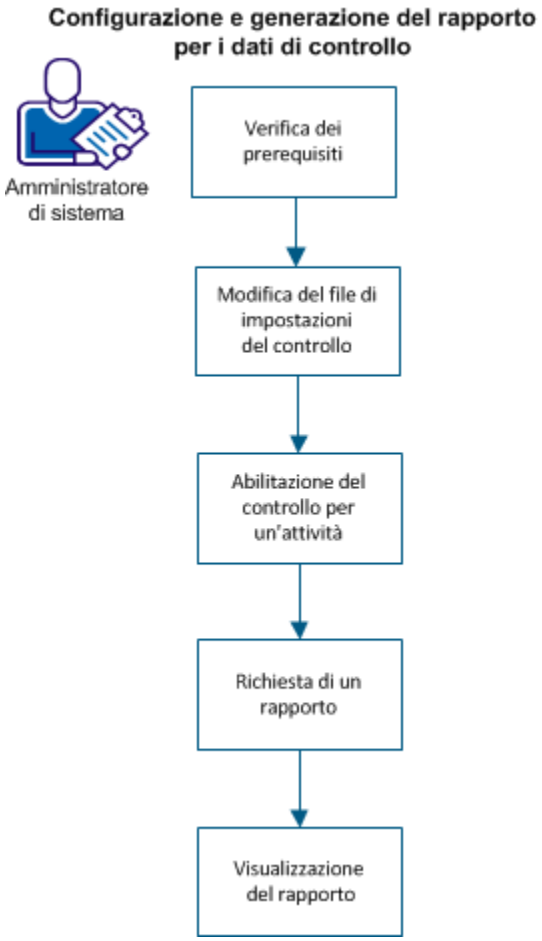
Configurazione e generazione del rapporto per i dati di controllo

I dati di controllo forniscono un record cronologico delle operazioni che si verificano in un ambiente. Quando si configura e si abilita il controllo, il sistema registra informazioni sulle attività in un database di controllo. Le informazioni di controllo possono essere utilizzate per generare rapporti. Alcuni esempi di dati di controllo comprendono i seguenti punti:

- Attività di sistema per un periodo di tempo specificato.
- Eventi di accesso e di disconnessione dell'utente durante l'accesso a un ambiente particolare.
- Attività eseguite da un utente specifico.
- Un elenco di oggetti modificati durante un determinato periodo.
- Ruoli assegnati all'utente
- Operazioni eseguite per un determinato account utente.

I dati di controllo vengono generati per gli *eventi* di CA Identity Manager. Un evento è un'operazione generata da un'attività di CA Identity Manager. Ad esempio, l'attività Crea utente può includere un evento AssignAccessRoleEvent.

Il diagramma seguente descrive la procedura di configurazione del controllo e di generazione di un rapporto sui dati di audit per un amministratore di sistema:



L'amministratore deve completare i passaggi seguenti:

1. Verifica dei prerequisiti (a pagina 249)
2. Modifica del file di impostazioni di audit (a pagina 249)
3. Abilitazione del controllo per un'attività (a pagina 254)
4. Richiesta di un rapporto (a pagina 255)
5. Visualizzazione del rapporto (a pagina 257)

Verifica dei prerequisiti

Verificare che i prerequisiti seguenti siano soddisfatti prima di configurare le impostazioni di audit:

- Un'istanza di database separata viene creata per l'archiviazione dei dati relativi al controllo. Per impostazione predefinita, il file di schema del database di CA Identity Manager si trova nella posizione seguente:
  - **Windows**: C:\Programmi\CA\Identity Manager\IAM Suite\Identity Manager\Identity Manager\tools\db
- Configurare la connessione al server di rapporto per richiedere e visualizzare il rapporto di controllo.
- Aggiungere un oggetto di connessione per il rapporto di controllo. Effettuare i seguenti passaggi:
  a. Accedere alla console utente con privilegi amministrativi.
  b. Passare a Ruoli e attività, Attività di amministrazione, quindi cercare il rapporto di controllo da modificare.
  c. Immettere il nome di connessione seguente nel campo Oggetto di connessione per il rapporto:
  `rptParamConn`

Modifica del file di impostazioni di audit

Configurare le impostazioni di audit nel relativo file per definire il tipo di informazioni da controllare con CA Identity Manager. È possibile configurare un file di impostazioni di audit per l'esecuzione delle seguenti operazioni:

- Controllare alcuni o tutti gli eventi generati dalle attività di amministrazione.
- Registrare le informazioni su un evento in stati specifici, ad esempio quando un evento viene completato o annullato.
- Registrare le informazioni relative agli attributi coinvolti in un evento. Ad esempio, è possibile registrare attributi che vengono modificati durante un evento ModifyUserEvent.

- Impostare il livello di verifica per la registrazione degli attributi.

Il file di impostazioni di audit è un file XML creato mediante l'esportazione delle impostazioni di audit. Il file presenta il seguente schema:

```
<Audit enabled="" auditlevel="" datasource="">
  <AuditEvent name="" enabled="" auditlevel="">
    <AuditProfile objecttype="" auditlevel="">
      <AuditProfileAttribute name="" auditlevel="" />
    </AuditProfile>
    <EventState name="" severity=""/>
  </AuditEvent>
</Audit>
```

Per ulteriori informazioni sullo schema e sugli elementi di controllo, consultare i commenti nel file di impostazioni di audit.

Gli elementi AuditProfileAttribute indicano gli attributi controllati da CA Identity Manager. Gli attributi si applicano all'oggetto specificato nell'elemento AuditProfile.

Nota: Se non è stato specificato alcun attributo del profilo di controllo, per l'oggetto vengono registrati tutti gli attributi specificati nell'elemento AuditProfile.

La tabella seguente mostra gli attributi validi per i tipi di oggetto di CA Identity Manager:

Attributi validi per i tipi di oggetto di CA Identity Manager

Tipo di oggetto	Attributi validi
ACCESS ROLE	■ nome: nome visibile all'utente per il ruolo ■ descrizione: commento facoltativo sullo scopo del ruolo. ■ membri: gli utenti che possono utilizzare il ruolo. ■ amministratori: gli utenti che possono assegnare amministratori o membri del ruolo. ■ titolari: gli utenti che possono modificare il ruolo. ■ attivo: indica se il ruolo è abilitato o no. ■ assegnabile: indica se il ruolo è assegnabile da un amministratore o no. ■ attività: le attività di accesso associate al ruolo.

Attributi validi per i tipi di oggetto di CA Identity Manager	
Tipo di oggetto	**Attributi validi**
ACCESS TASK	■ nome: nome dell'attività visibile all'utente ■ descrizione: commento facoltativo sullo scopo dell'attività. ■ applicazione: l'applicazione associata all'attività. ■ tag: identificatore univoco dell'attività. ■ reserved1, reserved2, reserved3, reserved4: i valori dei campi riservati all'attività
ADMINISTRATIVE ROLE	■ nome: nome visibile all'utente per il ruolo ■ descrizione: commento facoltativo sullo scopo del ruolo ■ membri: gli utenti che possono utilizzare il ruolo. ■ amministratori: gli utenti che possono assegnare amministratori o membri del ruolo. ■ titolari: gli utenti che possono modificare il ruolo. ■ attivo: indica se il ruolo è abilitato o no. ■ assegnabile: indica se il ruolo è assegnabile da un amministratore o no. ■ attività: le attività associate al ruolo.

Attributi validi per i tipi di oggetto di CA Identity Manager

Tipo di oggetto	Attributi validi
ADMINISTRATIVE TASK	■ nome: nome dell'attività visibile all'utente ■ descrizione: commento facoltativo sullo scopo dell'attività. ■ tag: identificatore univoco dell'attività. ■ categoria: la categoria nell'interfaccia utente di CA Identity Manager in cui viene visualizzata l'attività ■ primary_object: l'oggetto con cui opera l'attività ■ azione: l'operazione eseguita sull'oggetto. ■ nascosto: indica se l'attività *non* viene visualizzata nei menu. ■ pubblico: indica se l'attività è disponibile agli utenti che non hanno effettuato l'accesso a CA Identity Manager. ■ controllo: indica se l'attività consente la registrazione di informazioni di verifica. ■ esterno: indica se l'attività è un'attività esterna. ■ url: l'URL a cui l'utente viene reindirizzato da CA Identity Manager durante l'esecuzione di un'attività esterna. ■ flusso di lavoro: indica se gli eventi di CA Identity Manager associati all'attività attivano il flusso di lavoro ■ servizio Web: indica se l'attività è un'attività per la quale l'output WSDL (Web Services Description Language) può essere generato dalla console di gestione di CA Identity Manager.
GROUP	Qualsiasi attributo valido definito per l'oggetto GROUP nel file di configurazione di directory (directory.xml).
ORGANIZATION PARENTORG	Qualsiasi attributo valido definito per l'oggetto ORGANIZATION nel file di configurazione di directory (directory.xml).

Attributi validi per i tipi di oggetto di CA Identity Manager	
Tipo di oggetto	**Attributi validi**
RELATIONSHIP	■ %CONTAINER%: identificatore univoco dell'oggetto padre. Ad esempio, se l'oggetto RELATIONSHIP descrive l'appartenenza al ruolo, il contenitore è il ruolo. ■ %CONTAINER_NAME%: nome del gruppo padre visibile dall'utente. ■ %ITEM%: identificatore univoco dell'oggetto contenuto nell'oggetto padre. Ad esempio, se l'oggetto RELATIONSHIP descrive l'appartenenza al ruolo, gli elementi sono i membri del ruolo. ■ %ITEM_NAME%: nome del gruppo nidificato visibile dall'utente.
USER	Qualsiasi attributo valido definito per l'oggetto USER nel file di configurazione di directory (directory.xml).
NESSUNO	Nessun attributo

Nota: I punti seguenti si applicano alla tabella precedente:

- Attivo, assegnabile, verificabile, flusso di lavoro, nascosto, servizio Web e pubblico sono registrati come true o false.
- Durante la verifica delle attività per i ruoli, viene registrato il nome visibile dell'utente.
- Il database archivia i criteri membri, di amministrazione e di titolarità in formato XML compilato. Questo formato è diverso dall'interfaccia utente in cui ciascun criterio viene visualizzato come espressione.

Procedere come descritto di seguito:

1. Accedere alla console di gestione, selezionare l'ambiente, Impostazioni avanzate, quindi fare clic su Controllo.
2. Fare clic su Esporta.

   Il sistema esporta le impostazioni di audit correnti in un file .xml.

3. Modificare le impostazioni di audit nel file .xml esportato nel passaggio precedente. Compiere le attività seguenti:
   a. Impostare il valore di audit abilitato ="true" e fornire il valore del nome JNDI di "iam_im_<auditdb>.xml" per l'origine dati dell'elemento.
   b. Specificare il seguente nome JNDI:
      `java:/auditDbDataSource`

      Nota: L'origine dati si trova nella posizione seguente:
      `iam/im/jdbc/auditDbDataSource`
   c. Aggiungere, modificare o eliminare gli elementi nel file.
   d. Modificare il livello di informazioni registrate per ciascun evento.
4. Ripetere i passaggi 1 e 2. Fare clic su Importa e caricare il file .xml modificato delle impostazioni di audit.
5. Riavviare l'ambiente.

Il file di impostazioni di audit è stato aggiornato.

Abilitazione del controllo per un'attività

Abilitare il controllo per le attività per cui è stato configurato nel file di impostazioni di audit.

Procedere come descritto di seguito:

1. Accedere alla console utente con privilegi di amministratore di sistema.
2. Creare o modificare l'attività per cui si desidera abilitare il controllo.
3. Nella scheda Profilo, verificare che la casella di controllo Attiva controllo sia selezionata.
4. Fare clic su Inoltra.

Il controllo viene abilitato per l'attività.

Richiesta di un rapporto

Per visualizzare il rapporto, richiederlo a un utente con privilegi di amministratore dei rapporti. Selezionare il rapporto appropriato in cui sono registrati i dati di controllo. Se il rapporto richiesto necessita dell'approvazione, il sistema invia un avviso di posta elettronica.

Prima di pianificare un rapporto, completare i passaggi seguenti:

1. Accedere alla console utente con privilegi amministrativi.
2. Passare a Ruoli e attività, Modifica attività di amministrazione, quindi selezionare il rapporto di controllo da modificare.
3. Selezionare la scheda Schede e fare clic su Utilità di pianificazione server di rapporto IAM per la modifica.
4. Selezionare la casella di controllo Abilita opzione ricorrenza.
5. Fare clic su OK e su Invia.

Procedere come descritto di seguito:

1. Accedere alla console utente con privilegi utente per le attività di rapporto.
2. Selezionare Rapporti, Attività di rapporto, Richiedi un rapporto.

   Viene visualizzato un elenco di rapporti.
3. Selezionare un rapporto basato sul controllo.

   Verrà visualizzato una schermata di parametri.
4. Fare clic su Pianifica rapporto e selezionare una pianificazione per il rapporto.

   Ora

   Consente di specificare che il rapporto deve essere eseguito immediatamente.

   Una volta

   Specifica che il rapporto viene eseguito una volta, durante un determinato periodo di tempo. Selezionare la data di inizio e fine e l'ora di inizio e fine per la generazione del rapporto.

   (Solo rapporti di controllo) Ogni ora

   Specifica che il rapporto viene generato all'ora di inizio e, successivamente, ogni "n" ore, dove "n" denota l'intervallo tra rapporti consecutivi. Selezionare la data di inizio e fine, l'ora di inizio e fine e l'intervallo tra rapporti consecutivi.

   (Solo rapporti di controllo) Ogni giorno

   Specifica che il rapporto viene generato all'ora di inizio e, successivamente, ogni "n" giorni, dove "n" denota l'intervallo tra rapporti consecutivi. Selezionare la data di inizio e fine, l'ora di inizio e fine e l'intervallo tra rapporti consecutivi.

(Solo rapporti di controllo) Ogni settimana

Specifica che il rapporto viene generato ogni settimana nel giorno selezionato, a partire dalla data di avvio. Selezionare la data di inizio e fine e l'ora di inizio e fine per la generazione del rapporto.

(Solo rapporti di controllo) Ogni mese

Specifica che il rapporto viene generato ogni mese a partire dalla data di avvio e, successivamente, ogni "n" mesi, dove "n" indica l'intervallo tra rapporti consecutivi. Selezionare la data di inizio e fine, l'ora di inizio e fine e l'intervallo tra rapporti consecutivi.

(Solo rapporti di controllo) Esegui rapporto il giorno N del mese

Specifica che il rapporto viene generato nel giorno del mese specifico indicato dall'utente. Selezionare la data di inizio e fine e l'ora di inizio e fine per la generazione del rapporto.

(Solo rapporti di controllo) Il primo lunedì

Specifica che il rapporto viene generato ogni primo lunedì del mese. Selezionare la data di inizio e fine e l'ora di inizio e fine per la generazione del rapporto.

(Solo rapporti di controllo) L'ultimo giorno del mese

Specifica che il rapporto viene generato nell'ultimo giorno del mese. Selezionare la data di inizio e fine e l'ora di inizio e fine per la generazione del rapporto.

(Solo rapporti di controllo) Il giorno X della settimana del mese N

Specifica che il rapporto viene generato in giorno specifico e in una settimana specifica di ogni mese. Selezionare la data di inizio e fine e l'ora di inizio e fine per la generazione del rapporto. Ad esempio, è possibile generare un rapporto il venerdì della terza settimana di ogni mese.

5. Fare clic su Inoltra.

   La richiesta di rapporto viene inoltrata. In base alla configurazione del proprio ambiente, la richiesta viene eseguita subito oppure dopo l'approvazione da parte di un amministratore.

   In genere, prima che la richiesta del rapporto sia completata dal sistema, è necessaria l'approvazione di un amministratore di sistema o di un altro utente con privilegi di amministrazione dei rapporti. L'approvazione è obbligatoria perché l'esecuzione di alcuni rapporti può richiedere molto tempo o un numero elevato di risorse di sistema. Se il rapporto richiesto necessita dell'approvazione, il sistema invia un avviso di posta elettronica.

   Nota: Attivare il flusso di lavoro per l'ambiente se è richiesta l'approvazione.

Visualizzazione del rapporto

In base alla configurazione dell'ambiente in uso, è possibile che rapporto non venga visualizzato fino all'approvazione della richiesta da parte di un amministratore. Se il rapporto richiesto è in attesa di approvazione, il sistema invia un avviso di posta elettronica. Il rapporto che si desidera visualizzare non compare nell'elenco di ricerca finché non riceve l'approvazione.

Nota: per visualizzare i rapporti in CA Identity Manager utilizzando l'attività Visualizza rapporti personali, attivare i cookie di sessione di terze parti nel browser.

Procedere come descritto di seguito:

1. In Console utente, passare a Rapporti, Attività di rapporto e fare clic su Visualizza rapporti personali.
2. Individuare il rapporto generato che si desidera visualizzare.

   Verranno visualizzate le istanze del rapporto di ricorrenza generato e del rapporto su richiesta.

   Nota: Se lo stato del rapporto è In sospeso/Ricorrente, il rapporto non viene generato e il suo completamento può richiedere tempi lunghi.
3. Selezionare il rapporto che si desidera visualizzare.
4. (Facoltativo) Fare clic su Esporta questo rapporto nell'angolo superiore sinistro per esportare il rapporto nei formati seguenti:
   - Crystal Reports
   - PDF
   - Microsoft Excel (97-2003)
   - Microsoft Excel (97-2003) - Solo dati
   - Microsoft Excel (97-2003) - Modificabile
   - Rich Text Format (RTF)
   - Separated Values (CSV)
   - XML

Pulizia del database di controllo

Il database di controllo potrebbe accumulare record che non sono più necessari. Per rimuovere questi record, eseguire la seguente procedura di database nella directory db\auditing:

`garbageCollectAuditing12` *`environment-ID MM/DD/YYYY`*

environment-ID

Definisce l'ID dell'ambiente di CA Identity Manager

GG/MM/AAAA

Definisce la data prima della quale è necessario rimuovere i record di verifica.

Capitolo 9: Ambienti di produzione

Questa sezione fornisce descrizioni funzionali dettagliate per l'esecuzione della migrazione di parti specifiche della funzionalità. Assicurarsi che venga utilizzata solamente quando vengono apportate modifiche limitate nell'ambiente di sviluppo e che quelle modifiche vengano ben comprese.

Questa sezione contiene i seguenti argomenti:

Per eseguire la migrazione delle definizioni di attività e ruoli di amministrazione

È possibile personalizzare i ruoli e le attività di CA Identity Manager per soddisfare le esigenze specifiche della propria azienda. La personalizzazione implica la creazione o la modifica di ruoli e di attività di amministrazione o l'utilizzo delle attività Crea o Modifica per un ruolo o un'attività di amministrazione.

Un metodo alternativo, benché *non consigliato*, è la modifica dei ruoli e delle attività nel file roledefinition.xml. Utilizzare questo metodo per modifiche molto limitate a causa del rischio di errori durante la modifica.

Questo processo eseguirà solamente la migrazione delle definizioni di attività e di ruoli di amministrazione. Se i ruoli sono associati a organizzazioni, valutare l'opportunità di migrare l'intero ambiente di CA Identity Manager.

Importante. Se sono state modificate le definizioni di ruoli o di attività nell'ambiente di produzione, tali modifiche vanno perse quando si importano definizioni di ruoli o di attività da un ambiente di sviluppo. L'importazione delle definizioni di ruoli e di attività sovrascrive le definizioni esistenti di ruoli e di attività con gli stessi nomi.

Per esportare le definizioni di ruoli e di attività di amministrazione

Se le modifiche sono state apportate direttamente al file roledefinition.xml, questo file può essere importato direttamente nell'ambiente di produzione. In caso contrario procedere come segue per esportare le definizioni di ruoli e di attività:

1. Se si dispone di un cluster del Policy Server, controllare che sia in esecuzione solamente un Policy Server.
2. Arrestare tutto tranne un nodo di CA Identity Manager.
3. Accedere alla console di gestione.
4. Fare clic su CA Identity Manager environments (Ambienti di CA Identity Manager).
5. Selezionare l'ambiente di CA Identity Manager da cui esportare le definizioni di ruoli e di attività.
6. Fare clic su Ruoli, quindi su Esporta e fornire un nome per il file.
7. Seguire le istruzioni della procedura successiva per importare questo file.

Per importare le definizioni di attività e di ruoli di amministrazione

Procedere come descritto di seguito:

1. Copiare il file creato nella procedura precedente nell'ambiente di produzione.
2. Accedere alla console di gestione nell'ambiente di produzione.
3. Fare clic su CA Identity Manager environments (Ambienti di CA Identity Manager).
4. Selezionare l'ambiente di CA Identity Manager appropriato.
5. Fare clic su Ruoli.
6. Fare clic su Importa e specificare il nome del file XML generato dall'esportazione.
7. Se queste fasi vanno a buon fine, avviare eventuali nodi di CA Identity Manager e Policy Server aggiuntivi arrestati in precedenza.

   Nota: se è necessario apportate nuove modifiche a un ambiente di CA Identity Manager, ripetere la fase 6.

Per verificare l'importazione di ruoli e di attività

Per verificare che i ruoli e le attività siano stati importati correttamente, accedere a CA Identity Manager come account di amministratore che può utilizzare le attività seguenti:

- Modifica ruolo di amministrazione
- Modifica attività di amministrazione

Eseguire queste attività e verificare che i ruoli e le attività rispecchino le definizioni di ruolo appena importate.

Per eseguire la migrazione di interfacce di CA Identity Manager

È possibile personalizzare le interfacce di CA Identity Manager perché l'applicazione abbia l'aspetto desiderato. Se sono state modificate o create nuove interfacce per un set di utenti, utilizzare le fasi seguenti per eseguire la migrazione delle interfacce dall'ambiente di sviluppo all'ambiente di produzione.

Se si sta modificando un'interfaccia, copiare i file modificati.

Procedere come descritto di seguito:

1. Copiare i file nuovi e modificati dal server di sviluppo al server di produzione, come ad esempio i file di immagine, i fogli di stile, i file di proprietà e la pagina della console (index.jsp).
2. Se vengono utilizzate più interfacce, configurare la risposta di SiteMinder.

   Nota: per ulteriori informazioni sull'utilizzo di più interfacce, consultare la *Guida alla configurazione*.

Per verificare la migrazione delle interfacce, accedere alla console utente e controllare che l'interfaccia venga visualizzata correttamente.

Aggiornamento di CA Identity Manager in un ambiente di produzione

Dopo avere eseguito la migrazione di CA Identity Manager dallo sviluppo alla produzione, potrebbe essere necessario eseguire aggiornamenti incrementali. Per eseguire la migrazione di nuove funzionalità di CA Identity Manager dall'ambiente di sviluppo all'ambiente di produzione, eseguire le seguenti fasi:

1. Eseguire la migrazione di ambienti di CA Identity Manager.
2. Copiare iam_im.ear.
3. Eseguire la migrazione di definizioni del processo del flusso di lavoro.

Per eseguire la migrazione di un ambiente di CA Identity Manager

Un ambiente di CA Identity Manager viene creato dalla console di gestione. L'ambiente di CA Identity Manager include un insieme di definizioni di ruoli e di attività, definizioni del flusso di lavoro, funzionalità personalizzate create con le API di CA Identity Manager e una directory di CA Identity Manager.

Procedere come descritto di seguito:

1. Se CA Identity Manager è integrato con SiteMinder e si dispone di un cluster del Policy Server, controllare che sia in esecuzione solamente un Policy Server.
2. Arrestare tutto tranne un nodo di CA Identity Manager.
3. Esportare ambienti di CA Identity Manager dalla console di gestione all'ambiente di sviluppo.
4. Importare gli ambienti esportati nella console di gestione dell'ambiente di produzione.
5. Se CA Identity Manager è integrato con SiteMinder, applicare nuovamente la protezione alle aree di autenticazione di CA Identity Manager nell'interfaccia utente del Policy Server.

   Il dominio di criterio non viene esportato dal Policy Store quando si esporta un ambiente di CA Identity Manager.
6. Riavviare il Policy Server e i nodi di CA Identity Manager che arrestati in precedenza.

Durante la migrazione di un ambiente di CA Identity Manager, si verificano le seguenti attività:

- Se lo stesso oggetto esiste in entrambe le posizioni, le modifiche nel server di sviluppo sovrascrivono le modifiche nel server di produzione.
- Se nell'ambiente di sviluppo vengono creati oggetti nuovi, questi vengono aggiunti al server di produzione.
- Se nel server di produzione vengono creati oggetti nuovi, essi vengono conservati.

Per esportare un ambiente di CA Identity Manager

Per effettuare la distribuzione di un ambiente di CA Identity Manager su un sistema di produzione, si esporta l'ambiente da un sistema di sviluppo o gestione temporanea e lo si importa nel sistema di produzione.

Nota: quando si importa un ambiente precedentemente esportato, CA Identity Manager mostra un registro in una finestra di stato nella console di gestione. Per visualizzare le informazioni di convalida e distribuzione per ciascuno oggetto distribuito e relativi attributi in questo registro, selezionare il campo Enable Verbose Log Output (Abilita output registro dettagliato) nella pagine delle proprietà dell'ambiente *prima* di esportare l'ambiente. La selezione del campo Enable Verbose Log Output (Abilita output registro dettagliato) può causare problemi di prestazioni significativi durante l'importazione.

Procedere come descritto di seguito:

1. Fare clic su Environments (Ambienti) nella console di gestione.

   Viene visualizzata la schermata degli ambienti di CA Identity Manager, in cui è visualizzato un elenco degli ambienti di CA Identity Manager.
2. Selezionare l'ambiente che si desidera esportare.
3. Fare clic sul pulsante Esporta.

   Viene visualizzata la schermata di download file.
4. Salvare il file .zip in una posizione accessibile per il sistema di produzione.
5. Fare clic su Fine.

   Le informazioni di ambiente vengono esportate in un file .zip che è possibile importare in un altro ambiente.

Per importare un ambiente di CA Identity Manager

Dopo avere esportato un ambiente di CA Identity Manager da un sistema di sviluppo, è possibile importarlo in un sistema di produzione.

Procedere come descritto di seguito:

1. Fare clic su Environments (Ambienti) nella console di gestione.

   Viene visualizzata la schermata degli ambienti di CA Identity Manager, in cui è visualizzato un elenco degli ambienti di CA Identity Manager.
2. Fare clic sul pulsante Importa.

   Viene visualizzata la schermata Importa ambiente.

3. Accedere al file .zip richiesto per importare un ambiente.
4. Fare clic su Fine.

L'ambiente viene importato in CA Identity Manager.

Per verificare la migrazione dell'ambiente di CA Identity Manager

Per verificare la migrazione corretta dell'ambiente di CA Identity Manager, confermare che l'ambiente di CA Identity Manager viene visualizzato nell'interfaccia utente del Policy Server per il Policy Server nell'ambiente di produzione.

Nell'interfaccia utente del Policy Server, verificare i seguenti punti:

- Le impostazioni della directory dell'utente di CA Identity Manager sono accurate.
- Il nuovo dominio di CA Identity Manager esiste.
- Gli schemi di autenticazione corretti proteggono le aree di autenticazione di CA Identity Manager.

Anche all'accesso alla console di gestione, verificare che l'ambiente di CA Identity Manager venga visualizzato quando si selezionano gli ambienti.

Migrazione di iam_im.ear per JBoss

Distribuire nuovamente iam_im.ear ogni volta che viene eseguita la migrazione della funzionalità dall'ambiente di sviluppo all'ambiente di produzione. Attraverso la migrazione dell'intero EAR, si garantisce che l'ambiente di produzione sia identico all'ambiente di sviluppo.

Procedere come descritto di seguito:

1. Copiare iam_im.ear dall'ambiente di sviluppo a una posizione accessibile all'ambiente di produzione.
2. Nella copia di iam_im.ear, modificare le informazioni di connessione del Policy Server, perché rispecchino l'ambiente di produzione.

   Per ottenere questa modifica, copiare *jboss_home*/server/default/iam_im.ear/policyserver_rar/META-INF/ra.xml dall'ambiente di produzione a iam_im.ear.

3. Sostituire il file iam_im.ear installato con la copia del file iam_im.ear dell'ambiente di sviluppo dalla fase 2:
   a. Eliminare iam_im.ear dall'ambiente di produzione:

      cluster_node_jboss_home\server\default\deploy\iam_im.ear

   b. Sostituire i file eliminati con la copia modificata di iam_im.ear dall'ambiente di sviluppo.
4. Ripetere queste fasi per ogni nodo del cluster.

Migrazione di iam_im.ear per WebLogic

Distribuire nuovamente iam_im.ear ogni volta che viene eseguita la migrazione della funzionalità dall'ambiente di sviluppo all'ambiente di produzione. Attraverso la migrazione dell'intero EAR, si garantisce che l'ambiente di produzione sia identico all'ambiente di sviluppo.

Procedere come descritto di seguito:

1. Preservare le informazioni di connessione del Policy Server.

   Le informazioni di connessione del Policy Server vengono archiviate nel file ra.xml nella directory policyserver_rar/WEB-INF. Copiare questo file in un'altra posizione, perché sia possibile sostituirlo in iam_im.ear prima di ridistribuirlo.
2. Copiare iam_im.ear in una posizione disponibile al server di gestione di WebLogic.
3. Sostituire le informazioni di connessione del Policy Server.

   Nel file iam_im.ear, sostituire il file policyserver_rar/WEB-INF/ra.xml con il file archiviato dal passaggio 1.
4. Ridistribuire iam_im.ear
   a. Accedere alla console di WebLogic.
   b. Accedere a Deployments, Application, Identity Manager.

Nella scheda Deploy, selezionare Deploy (Re-Deploy), Application.

Migrazione di iam_im.ear per WebSphere

Procedere come descritto di seguito:

1. Copiare lo script *imsInstall.jacl* da *was_im_tools_dir**WebSphere-tools* nella directory *deployment_manager_dir* *bin* directory dove:
   - *was_im_tools_dir* è la directory nel sistema di sviluppo in cui sono installati gli strumenti di CA Identity Manager per WebSphere.
   - *deployment_manager_dir* è la posizione in cui viene installato il Manager di distribuzione.
2. Nel sistema di sviluppo in cui è stata configurata l'applicazione di CA Identity Manager, copiare *was_im_tools_dir* *WebSphere-tools**imsExport.bat* o *imsExport.sh* in *was_home**bin*.
3. Nella riga di comando, accedere a *was_home**bin.*
4. Verificare che il server applicazioni di WebSphere sia in esecuzione.
5. Esportare l'applicazione di CA Identity Manager distribuita nel seguente modo:

   Per Windows, immettere il seguente comando:

   `imsExport.bat "path-to-exported-ear"`

   dove *path-to-exported-ear* è il percorso completo e il nome file creato dall'utilità imsExport.

   Per i sistemi Windows, utilizzare le barre (/) anziché le barre rovesciate (\) quando si specifica il percorso a was_im.ear. Ad esempio:

   ```
   imsExport.bat "c:/program files/CA/CA Identity Manager/
   exported_ear/iam_im.ear"
   ```

   Per UNIX, immettere il seguente comando:

   `./wsadmin -f imsExport.jacl -conntype RMI -port 2809 path to exported ear`

   dove *path-to-exported-ear* è il percorso completo che comprende il nome file del file EAR esportato.
6. Copiare il file EAR esportato dalla posizione nel sistema di sviluppo in cui è stato esportato a una posizione nel sistema su cui è installato il Manager di distribuzione.
7. Sostituire *was_im_tools_dir*/WebSphere-ear/iam_im.ear/policyserver_rar/META-INF/ra.xml con il file dell'ambiente di produzione.

   Il file ra.xml contiene le informazioni di connessione del Policy Server.
8. Nel sistema su cui è installato il Manager di distribuzione, distribuire l'EAR Identity Manager:
   a. Dalla riga di comando, accedere a:

      deployment_manager_dir \bin.

   b. Verificare che il server applicazioni di WebSphere sia in esecuzione.

c. Eseguire lo script imsInstall.jacl nel seguente modo:

Nota: l'esecuzione dello script imsInstall.jacl può richiedere diversi minuti.

Windows:

wsadmin -f imsInstall.jacl *"path-to-copied-ear" cluster_name*

dove *path-to-copied-ear* è il percorso completo che comprende il nome file per l'EAR di Identity Manager copiato nel sistema del Manager di distribuzione.

Ad esempio:

wsadmin -f imsInstall.jacl "c:\Programmi\CA\Identity Manager\WebSphere-tools\was_im.ear" im_cluster

UNIX:

./wsadmin -f imsInstall.jacl *path-to-copied-ear cluster_name*

dove *path-to-copied-ear* è il percorso completo che comprende il nome file per l'EAR di Identity Manager copiato nel sistema del Manager di distribuzione.

Ad esempio:

./wsadmin -f imsInstall.jacl /opt/CA/Identity Manager/WebSphere-tools/was_im.ear im_cluster

9. Se CA Identity Manager è integrato con SiteMinder, verificare i punti seguenti:
   - Gli agenti di SiteMinder possono connettersi al Policy Store.
   - Il Policy Server può connettersi all'archivio utenti.
   - I domini di CA Identity Manager sono stati creati.

Migrazione delle definizioni del processo del flusso di lavoro.

Se si utilizza il flusso di lavoro nell'ambiente di sviluppo, esportare le definizioni del flusso di lavoro e importarle nell'ambiente di produzione. Quindi, configurare il flusso di lavoro in ciascuno dei nodi del server.

Esportazione delle definizioni del processo

Nel sistema dell'ambiente di sviluppo, esportare le definizioni del processo del flusso di lavoro.

Procedere come descritto di seguito:

1. Verificare che il server applicazioni sia in esecuzione.
2. Accedere ad *admin_tools*\Workpoint\bin\ ed eseguire Archive.bat (per Windows) o Archive.sh (per UNIX) nel seguente modo:
   a. Nella finestra di dialogo Importa, selezionare l'oggetto principale.
   b. Fare clic su Aggiungi.
   c. Specificare il nome del file da generare.
   d. Fare clic su Esporta.
   e. Fare clic su Vai.

   admin_tools fa riferimento agli strumenti di amministrazione che vengono installati per impostazione predefinita in uno dei percorsi seguenti:
   - **Windows**: C:\Programmi\CA\Identity Manager\IAM Suite\Identity Manager\tools
   - **UNIX**: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools
3. Seguire le istruzioni nella successiva sezione, per importare le definizioni del processo (a pagina 268).

Importazione delle definizioni del processo

Nel sistema dell'ambiente di produzione, importare le definizioni del processo del flusso di lavoro.

Procedere come descritto di seguito:

1. Riavviare il server applicazioni.
2. In via facoltativa, creare una copia di backup delle definizioni correnti esportando le definizioni mediante la procedura illustrata in precedenza.

3. Accedere ad *admin_tools*\Workpoint\bin\ ed eseguire lo script archivio nel seguente modo:

   a. Nella finestra di dialogo Importa, selezionare tutti gli elementi da importare.

   b. Alla richiesta se utilizzare il formato nuovo o quello precedente, mantenere il formato precedente.

      Il nuovo formato non supporta CA Identity Manager.

   c. Fornire il nome del file generato dall'esportazione.

   d. Fare clic su Vai.

   admin_tools fa riferimento agli strumenti di amministrazione che vengono installati per impostazione predefinita in uno dei percorsi seguenti:

   - **Windows: C:\Programmi\CA\Identity Manager\IAM Suite\Identity Manager\tools**
   - **UNIX**: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

Capitolo 10: Registri di CA Identity Manager

Questa sezione contiene i seguenti argomenti:

Registrazione dei problemi in CA Identity Manager

In CA Identity Manager sono inclusi i seguenti metodi per registrare lo stato e tenere traccia dei problemi:

Attività Visualizza attività inoltrate

Mostra lo stato di tutti gli eventi e di tutte le attività in un ambiente di CA Identity Manager. Gli amministratori utilizzano questa attività nella console utente.

L'attività Visualizza attività inoltrate fornisce i seguenti tipi di informazioni:

- L'elenco di eventi e attività che si verificano nell'ambiente.
- L'elenco di attributi associati a un evento.
- Eventi riusciti e non riusciti
- Eventi in stato in sospeso o bloccato.
- Eventi rifiutati, che includono la ragione del rifiuto
- Stato di sincronizzazione dell'account
- Stato di sincronizzazione del criterio di identità
- Informazioni di provisioning (se il provisioning è abilitato).

Registri del server applicazioni

Contengono le informazioni relative a tutti i componenti di un'installazione di CA Identity Manager e forniscono dettagli su tutte le operazioni in CA Identity Manager.

La posizione e il tipo di file di registro dipendono da quale dei seguenti tipi di server applicazioni viene utilizzato:

- Le informazioni di CA Identity Manager WebLogic vengono scritte in standard out. Per impostazione predefinita, standard out è la finestra della console in cui l'istanza del server è in esecuzione.
- Le informazioni su JBoss di CA Identity Manager vengono scritte nella finestra della console in cui l'istanza del server è in esecuzione e in *jboss_home*\server\log\server.log
- Le informazioni su WebSphere di CA Identity Manager vengono scritte nella finestra della console in cui l'istanza del server è in esecuzione e in *was_home*\AppServer\logs*server_name*\SystemOut

Per ulteriori informazioni, consultare la documentazione del server applicazioni in uso.

File di registro del server di directory

Contiene le informazioni sull'attività che si svolge nella directory dell'utente.

Il tipo di informazioni registrate e la posizione dei file di registro dipendono dal tipo di server di directory utilizzato. Per ulteriori informazioni, consultare la documentazione del server di directory.

File di registro del Policy Server

Quando CA Identity Manager è integrato con SiteMinder vengono visualizzate le seguenti informazioni:

- Problemi di connessione di SiteMinder
- Problemi di autenticazione di SiteMinder
- Le informazioni sugli oggetti gestiti di CA Identity Manager nel Policy Store di SiteMinder.
- Valutazione dei criteri di password

Per informazioni sulla configurazione dei registri di SiteMinder, consultare la *CA SiteMinder Web Access Manager Policy Server Administration Guide*.

Profiler del Policy Server

Se CA Identity Manager è integrato con SiteMinder, è possibile tenere traccia della diagnostica interna del Policy Server e delle funzioni di elaborazione, comprese le funzioni correlate a CA Identity Manager.

Per ulteriori informazioni, consultare la sezione Registrazione dei componenti e dei campi di dati (a pagina 273).

File di registro dell'agente Web

Se CA Identity Manager è integrato con SiteMinder, gli agenti Web scrivono informazioni nei due registri seguenti:

- File di registro degli errori: contiene gli errori del programma e gli errori a livello operativo, ad esempio l'agente Web che non è in grado di comunicare con il Policy Server.
- File di registro di tracce: contiene i messaggi di avviso e informativi, quali ad esempio i messaggi di traccia e i messaggi di stato del flusso. Inoltre, include dati quali ad esempio i dettagli dell'intestazione e le variabili dei cookie.

Nota: per ulteriori informazioni sui file di registro dell'agente Web, consultare la *CA SiteMinder Web Access Manager Web Agent Configuration Guide*.

Registrazione dei componenti e dei campi di dati

Se CA Identity Manager è integrato con SiteMinder, è possibile utilizzare il profiler del Policy Server di SiteMinder per tenere traccia dei componenti e dei campi di dati nelle estensioni di CA Identity Manager per il Policy Server. Il profiler consente di configurare i filtri per l'output di analisi in modo che vengano acquisiti solamente i valori specifici di un componente o di un campo di dati.

Nota: per istruzioni sull'utilizzo del profiler del Policy Server, consultare la *CA SiteMinder Web Access Manager Policy Server Administration Guide*.

È possibile abilitare l'analisi per i seguenti componenti:

Function_Begin_End

Fornisce dichiarazioni di traccia a basso livello quando vengono eseguiti determinati metodi nelle estensioni di CA Identity Manager per il Policy Server.

IM_Error

Tiene traccia degli errori di runtime nelle estensioni di CA Identity Manager per il Policy Server di SiteMinder.

IM_Info

Fornisce informazioni generali di analisi per le estensioni di CA Identity Manager.

IM_Internal

Tiene traccia delle informazioni generali sulle operazioni interne di CA Identity Manager.

IM_MetaData

Fornisce informazioni di analisi quando CA Identity Manager elabora i metadati della directory.

IM_RDB_Sql

Fornisce informazioni di analisi per i database relazionali.

IM_LDAP_Provider

Fornisce informazioni di analisi per le directory LDAP.

IM_RuleParser

Tiene traccia del processo di analisi e valutazione dei criteri membri, di titolarità e di amministrazione definiti in un file XML che viene interpretato al runtime.

IM_RuleEvaluation

Tiene traccia della valutazione delle regole di membri, di amministrazione, di titolarità e di ambiti.

IM_MemberPolicy

Tiene traccia della valutazione dei criteri membri, inclusi appartenenza e ambito.

IM_AdminPolicy

Tiene traccia della valutazione dei criteri di amministrazione.

IM_OwnerPolicy

Tiene traccia della valutazione dei criteri di titolarità.

IM_RoleMembership

Tiene traccia delle informazioni relative all'appartenenza al ruolo, quali l'elenco di ruoli di un utente e l'elenco di membri in un certo ruolo.

IM_RoleAdmins

Tiene traccia delle informazioni relative all'amministrazione dei ruoli, quali l'elenco di ruoli che un utente può amministrare e l'elenco di amministratori per un certo ruolo.

IM_RoleOwners

Tiene traccia delle informazioni relative alla titolarità dei ruoli, quali l'elenco di ruoli di proprietà di un utente e l'elenco di titolari per un certo ruolo.

IM_PolicyServerRules

Tiene traccia della valutazione delle regole membri, quali RoleMember, RoleAdmin, RoleOwner che il Policy Server ha risolto e delle regole di ambito, quali All e le regole AccessTaskFilter per AccessTasks.

IM_LLSDK_Command

Tiene traccia della comunicazione tra l'SDK CA Identity Manager interno e il Policy Server. Il supporto tecnico utilizza questo componente di traccia.

IM_LLSDK_Message

Tiene traccia dei messaggi inviati esplicitamente dal codice Java al Policy Server dall'SDL CA Identity Manager interno. Il supporto tecnico utilizza questo componente di traccia.

IM_IdentityPolicy

Tiene traccia della valutazione e dell'applicazione dei criteri di identità.

IM_PasswordPolicy

Tiene traccia della valutazione dei criteri di password.

IM_Version

Fornisce informazioni sulla versione di CA Identity Manager.

IM_CertificationPolicy

Tiene traccia della valutazione dei criteri di certificazione.

IM_InMemoryEval

Tiene traccia dell'elaborazione dei criteri di CA Identity Manager, inclusi i criteri membri, di amministrazione, di titolarità e di identità. Il supporto tecnico utilizza questo componente di traccia.

IM_InMemoryEvalDetail

Fornisce dettagli aggiuntivi sull'elaborazione dei criteri di CA Identity Manager, inclusi i criteri membri, di amministrazione, di titolarità e di identità. Il supporto tecnico utilizza questo componente di traccia.

I campi di dati per i quali è possibile configurare l'analisi sono elencati nella *CA SiteMinder Web Access Manager Policy Server Administration Guide*.

Capitolo 11: Protezione di CA Identity Manager

Questa sezione contiene i seguenti argomenti:

Protezione della console utente

La console utente è l'interfaccia utente che consente agli amministratori di gestire oggetti quali utenti, gruppi e organizzazioni in un ambiente di CA Identity Manager. Questi oggetti vengono assegnati con un set di ruoli e attività associati. Quando un amministratore accede alla console utente, vengono visualizzate le attività relative all'amministratore in quell'ambiente.

Per impostazione predefinita, CA Identity Manager protegge l'accesso alla console utente con l'autenticazione nativa. Gli amministratori di CA Identity Manager immettono un nome utente e una password validi per accedere a un ambiente di CA Identity Manager. CA Identity Manager autentica il nome e la password nell'archivio utenti gestito da CA Identity Manager.

Se CA Identity Manager è integrato con SiteMinder, CA Identity Manager utilizza *automaticamente* l'autenticazione di base di SiteMinder per proteggere l'ambiente. Non viene richiesta alcuna configurazione aggiuntiva per utilizzare l'autenticazione di base. Mediante l'Interfaccia di amministrazione di SiteMinder, è possibile configurare metodi di autenticazione avanzati.

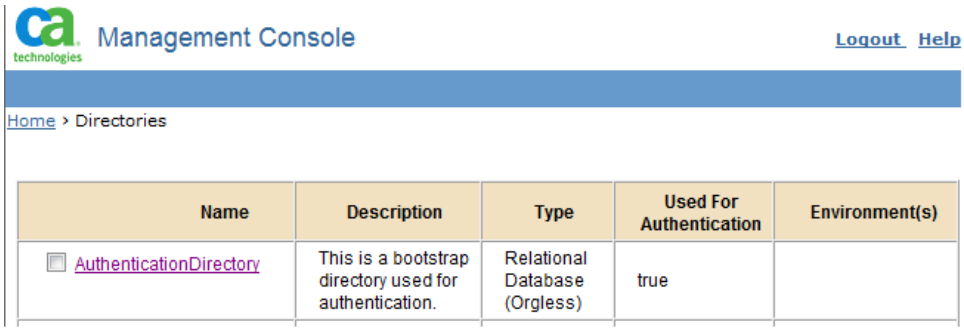
Nota: per ulteriori informazioni, consultare la *CA SiteMinder Web Access Manager Policy Server Configuration Guide*.

Protezione della console di gestione

La console di gestione consente agli amministratori di creare e gestire directory e ambienti di CA Identity Manager. Gli amministratori possono utilizzare la console di gestione anche per configurare funzionalità personalizzate per un ambiente.

L'installazione di CA Identity Manager include un'opzione per la protezione della console di gestione. Questa opzione è selezionata per impostazione predefinita. Durante l'installazione, specificare le credenziali utilizzate da CA Identity Manager per autenticare un amministratore con accesso alla console di gestione. CA Identity Manager crea un utente con le credenziali fornite in una directory di avvio chiamata AuthenticationDirectory. È possibile visualizzare questa directory nella console di gestione.

Nota: non è possibile utilizzare la protezione nativa per proteggere la console di gestione se CA Identity Manager è integrato con CA SiteMinder.



Aggiunta di amministratori aggiuntivi della console di gestione

Per impostazione predefinita, una console di gestione con protezione di CA Identity Manager nativa dispone di un account di amministratore, creato in una nuova directory di CA Identity Manager durante l'installazione.

Per aggiungere ulteriori amministratori, specificare una directory di CA Identity Manager contenente utenti che devono accedere alla console di gestione. L'utilizzo di una directory esistente consente di concedere l'accesso alla console di gestione agli utenti della propria organizzazione senza dovere creare nuovi account.

È possibile specificare soltanto una directory per l'autenticazione. Non è possibile eliminare una directory durante la configurazione per l'autenticazione.

Procedere come descritto di seguito:

1. Accedere alla console di gestione con le credenziali utente fornite durante l'installazione.
2. Aprire le directory e fare clic sulla directory che contiene gli utenti che richiedono l'accesso alla console di gestione.
3. Fare clic su Update Authentication (Aggiorna autenticazione).
4. Selezionare l'opzione Used for Authentication (Utilizzato per l'autenticazione).
5. Immettere il nome di accesso per il primo utente e fare clic su Aggiungi.
6. Continuare ad aggiungere gli utenti che richiedono l'accesso alla console di gestione finché tutti gli utenti sono stati aggiunti. Quindi fare clic su Salva.

   Gli utenti specificati possono ora utilizzare il proprio nome utente e la propria password per accedere alla console di gestione.

Disattivazione della protezione nativa per la console di gestione

Se la protezione nativa è stata abilitata per la console di gestione e ora si desidera utilizzare un'applicazione diversa per proteggerla, disabilitare la protezione nativa prima di implementare un altro metodo di protezione.

Procedere come descritto di seguito:

1. Disabilitare la protezione nativa per la console di gestione nel file web.xml nel seguente modo:
   a. Aprire *CA Identity Manager_installation*\iam_im.ear\management_console.war\WEB-INF\web.xml in un editor di testo.
   b. Impostare il valore del parametro Attiva per ManagementConsoleAuthFilter su false nel seguente modo:
   ```
   <filter>
   <filter-name>ManagementConsoleAuthFilter</filter-name>
   <filter-
   class>com.netegrity.ims.manage.filter.ManagementConsoleAuth
   Filter</filter-class>
   <init-param>
   <param-name>Enable</param-name>
   <param-value>false</param-value>
   </init-param>
   </filter>
   ```
   c. Salvare il file web.xml.
2. Riavviare il server di CA Identity Manager.

   La console di gestione non è più protetta dalla protezione nativa.

Utilizzo di SiteMinder per la protezione della console di gestione

Per proteggere inizialmente la console di gestione, è possibile creare un criterio di SiteMinder.

Un criterio di SiteMinder identifica una risorsa da proteggere, come ad esempio la console di gestione, e concede a un set di utenti l'accesso a tale risorsa.

Procedere come descritto di seguito:

1. Disabilitare la protezione nativa (a pagina 280) per la console di gestione.
2. Accedere a una delle seguenti interfacce come amministratore con privilegi di dominio:
   - Per CA SiteMinder versione 12 o successiva, accedere all'interfaccia di amministrazione.
   - Per CA SiteMinder 6.0 SP*x*, accedere all'interfaccia utente del Policy Server.

   Nota: per informazioni sull'utilizzo di queste interfacce, consultare la documentazione relativa alla versione di SiteMinder in uso.
3. Individuare il dominio del criterio per l'ambiente di CA Identity Manager appropriato.

   Questo dominio viene creato automaticamente quando CA Identity Manager è integrato con SiteMinder. Il formato del nome dominio è il seguente:

   *Identity Manager-environment*Domain

   In questo formato, *Identity Manager-environment* specifica il nome dell'ambiente in corso di modifica. Ad esempio, se il nome è *employee*, il nome di dominio è *employees*Domain.
4. Creare un'area di autenticazione con il seguente filtro risorse:

   /iam/immanage/
5. Creare una regola per l'area di autenticazione. Specificare un asterisco (*) come filtro per proteggere tutte le pagine della console di gestione.
6. Creare un nuovo criterio e associarlo alla regola creata nella fase precedente.

   Assicurarsi di associare al criterio gli utenti che possono accedere alla console di gestione.
7. Riavviare il server applicazioni.

Protezione di un ambiente esistente dopo l'aggiornamento

Dopo che è stato eseguito l'aggiornamento a CA Identity Manager versione 12.6 o successiva, è possibile proteggere la console di gestione mediante la protezione nativa.

Nota: non è possibile utilizzare la protezione nativa di CA Identity Manager per proteggere la console di gestione quando CA Identity Manager è integrato con CA SiteMinder.

Procedere come descritto di seguito:

1. Abilitare la protezione nativa per la console di gestione nel file web.xml nel seguente modo:
   a. Aprire *CA Identity Manager_installation*\iam_im.ear\management_console.war\WEB-INF\web.xml in un editor di testo.
   b. Impostare il valore del parametro Attiva per ManagementConsoleAuthFilter su true nel seguente modo:
   ```
   <filter>
   <filter-name>ManagementConsoleAuthFilter</filter-name>
   <filter-
   class>com.netegrity.ims.manage.filter.ManagementConsoleAuth
   Filter</filter-class>
   <init-param>
   <param-name>Enable</param-name>
   <param-value>true</param-value>
   </init-param>
   </filter>
   ```
   c. Salvare il file web.xml.
2. Creare la tabella IM_AUTH_USER nell'archivio oggetti di CA Identity Manager.

   La tabella IM_AUTH_USER archivia informazioni sugli amministratori della console di gestione.
   a. Accedere a CA\Identity Manager\IAM Suite\Identity Manager\tools\db\objectstore
   b. Eseguire uno dei seguenti script per l'archivio oggetti:
      - sql_objectstore.sql
      - oracle_objectstore.sql

   Nota: per informazioni sull'esecuzione di uno script per un database esistente, consultare la documentazione del fornitore relativa a quel database.

3. Utilizzare lo strumento di password per crittografare la password utente.

   Lo strumento di password viene installato con gli strumenti di CA Identity Manager nella posizione seguente:

Windows: C:\Programmi\CA\Identity Manager\IAM Suite\Identity Manager\tools\PasswordTool

UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools/PasswordTool

   PasswordTool

   Eseguire lo strumento di password mediante il comando seguente:
   `pwdtools -JSAFE -p anypassword`

   L'opzione JSAFE crittografa un valore di testo normale mediante l'algoritmo PBE.

1. Inserire le informazioni dell'utente bootstrap nella tabella IM_AUTH_USER. Specificare i valori per tutte le colonne nella tabella IM_AUTH_USER.

   Ad esempio:

   USER_NAME: admin1

   PASSWORD: *anypassword*

   DISABLED: 0

   ID:1

2. Riavviare il server di CA Identity Manager.

   La console di gestione è protetta dalla protezione nativa.

Protezione dagli attacchi CSRF

CA Identity Manager è stato migliorato per rafforzare la resistenza agli attacchi di richieste intersito false (CSRF, Cross-Site Request Forgery). Per impostazione predefinita, il miglioramento è disabilitato in CA Identity Manager.

Per abilitare il miglioramento:

1. Aprire il file web.xml disponibile nella seguente posizione:

   `application-server/iam_im.ear/user_console.war/WEB-INF`

2. Trovare l'elemento <context-param> con <param-name> csrf-prevention-on.
3. Impostare <param-value> su true.
4. Riavviare il server applicazioni.

Capitolo 12: Integrazione di CA SiteMinder

Questa sezione contiene i seguenti argomenti:

SiteMinder e CA Identity Manager

Se CA Identity Manager è integrato con CA SiteMinder, in CA SiteMinder è possibile aggiungere le seguenti funzionalità a un ambiente di CA Identity Manager:

Autenticazione avanzata

Per impostazione predefinita, in CA Identity Manager è inclusa l'autenticazione nativa per gli ambienti di CA Identity Manager. Gli amministratori di CA Identity Manager immettono un nome utente e una password validi per accedere a un ambiente di CA Identity Manager. CA Identity Manager autentica il nome e la password nell'archivio utenti gestito da CA Identity Manager.

Quando CA Identity Manager è integrato con CA SiteMinder, CA Identity Manager utilizza l'autenticazione di base di CA SiteMinder per proteggere l'ambiente. Quando si crea un ambiente di CA Identity Manager, in CA SiteMinder vengono creati un dominio di criterio e uno schema di autenticazione per proteggere quell'ambiente.

Quando CA Identity Manager è integrato con CA SiteMinder, è anche possibile utilizzare l'autenticazione di SiteMinder per proteggere la console di gestione.

Ruoli e attività di accesso

I ruoli di accesso consentono agli amministratori di CA Identity Manager di assegnare privilegi in applicazioni protette da CA SiteMinder. I ruoli di accesso rappresentano una singola azione che un utente può eseguire in un'applicazione business, come la generazione di un ordine di acquisto in un'applicazione finanziaria.

Mapping di directory

Un amministratore può aver bisogno di gestire utenti i cui profili esistono in un archivio utenti differente da quello che viene utilizzato per autenticare l'amministratore. Quando accede all'ambiente di CA Identity Manager, l'amministratore viene autenticato utilizzando una directory, quindi viene utilizzata una directory differente per autorizzare l'amministratore a gestire utenti.

Quando CA Identity Manager è integrato con CA SiteMinder, è possibile configurare un ambiente di CA Identity Manager per utilizzare directory differenti per l'autenticazione e l'autorizzazione.

Interfacce per diversi set di utenti

Un'interfaccia modifica l'aspetto della console utente. Se CA Identity Manager è integrato con CA SiteMinder, è possibile abilitare diversi set di utenti per la visualizzazione di interfacce diverse. Per ottenere questa modifica, utilizzare una risposta di SiteMinder per associare un'interfaccia a un set di utenti. La risposta viene abbinata a una regola in un criterio, che viene associata a un set di utenti. L'attivazione della regola avvia la risposta per il trasferimento delle informazioni sull'interfaccia a CA Identity Manager per la creazione della console utente.

Nota: per ulteriori informazioni, consultare la *User Console Design Guide*.

Preferenze di impostazioni internazionali per un ambiente localizzato

Se CA Identity Manager è integrato con CA SiteMinder, è possibile definire una preferenza per le impostazioni internazionali per un utente utilizzando un'intestazione HTTP imlanguage. Nel Policy Server di SiteMinder, impostare questa intestazione all'interno di una risposta di SiteMinder e specificare un attributo utente come valore dell'intestazione. Questa intestazione imlanguage funge da preferenza di massima priorità per le impostazioni internazionali per un utente.

Nota: per ulteriori informazioni, consultare la *User Console Design Guide*.

Ulteriori informazioni:

Raccolta delle credenziali utente mediante uno schema di autenticazione personalizzato (a pagina 340)

Modalità di protezione delle risorse

L'autenticazione avanzata richiede l'utilizzo di un Policy Server di SiteMinder nell'implementazione in uso. Il server applicazioni in cui risiede il server di CA Identity Manager è un ambiente operativo diverso dal server Web. Per fornire servizi di inoltro, il server Web richiede:

- Un plug-in messo a disposizione dal fornitore del server applicazioni.
- Un agente di SiteMinder per proteggere le risorse di CA Identity Manager, quali le funzionalità della console utente, di registrazione automatica e di password dimenticata.

L'agente Web controlla l'accesso di utenti che richiedono le risorse di CA Identity Manager. Una volta che gli utenti sono autenticati e autorizzati, l'agente Web consente al server Web di elaborare le richieste.

Quando il server Web riceve la richiesta, il plug-in del server applicazioni lo inoltra al server applicazioni in cui risiede il server di CA Identity Manager.

L'agente Web protegge le risorse di CA Identity Manager visualizzate da utenti e amministratori.

Panoramica dell'integrazione di SiteMinder e CA Identity Manager

Quando l'amministratore dei criteri e l'amministratore di identità lavorano insieme per integrare SiteMinder in un'installazione di CA Identity Manager esistente, l'architettura di CA Identity Manager si espande per includere i seguenti componenti:

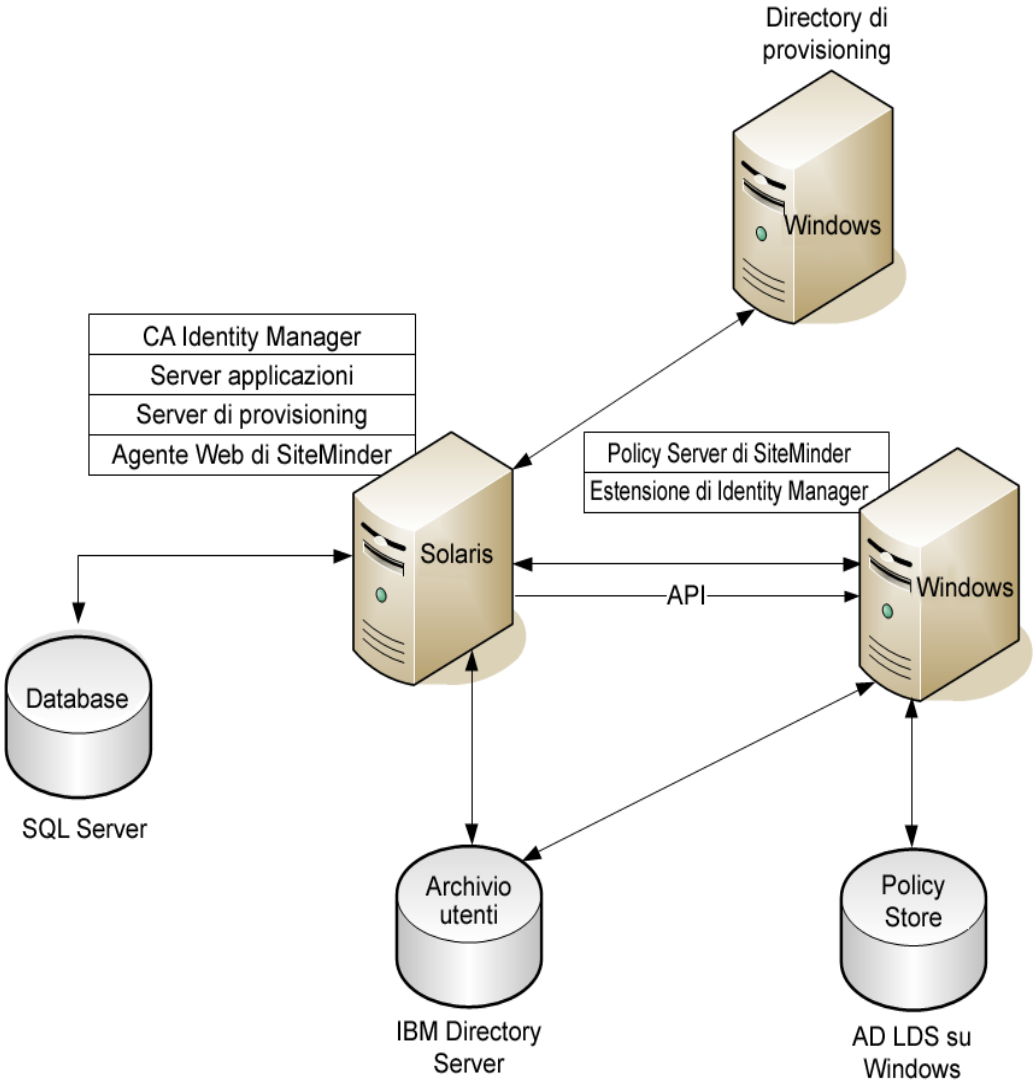
Agente Web di SiteMinder

Protegge il server di CA Identity Manager. L'agente Web viene installato nel sistema con il server di CA Identity Manager.

Policy Server di SiteMinder

Fornisce autenticazione e autorizzazione avanzate per CA Identity Manager.

La figura seguente è un esempio di un'installazione di CA Identity Manager con un agente Web e un Policy Server di SiteMinder:

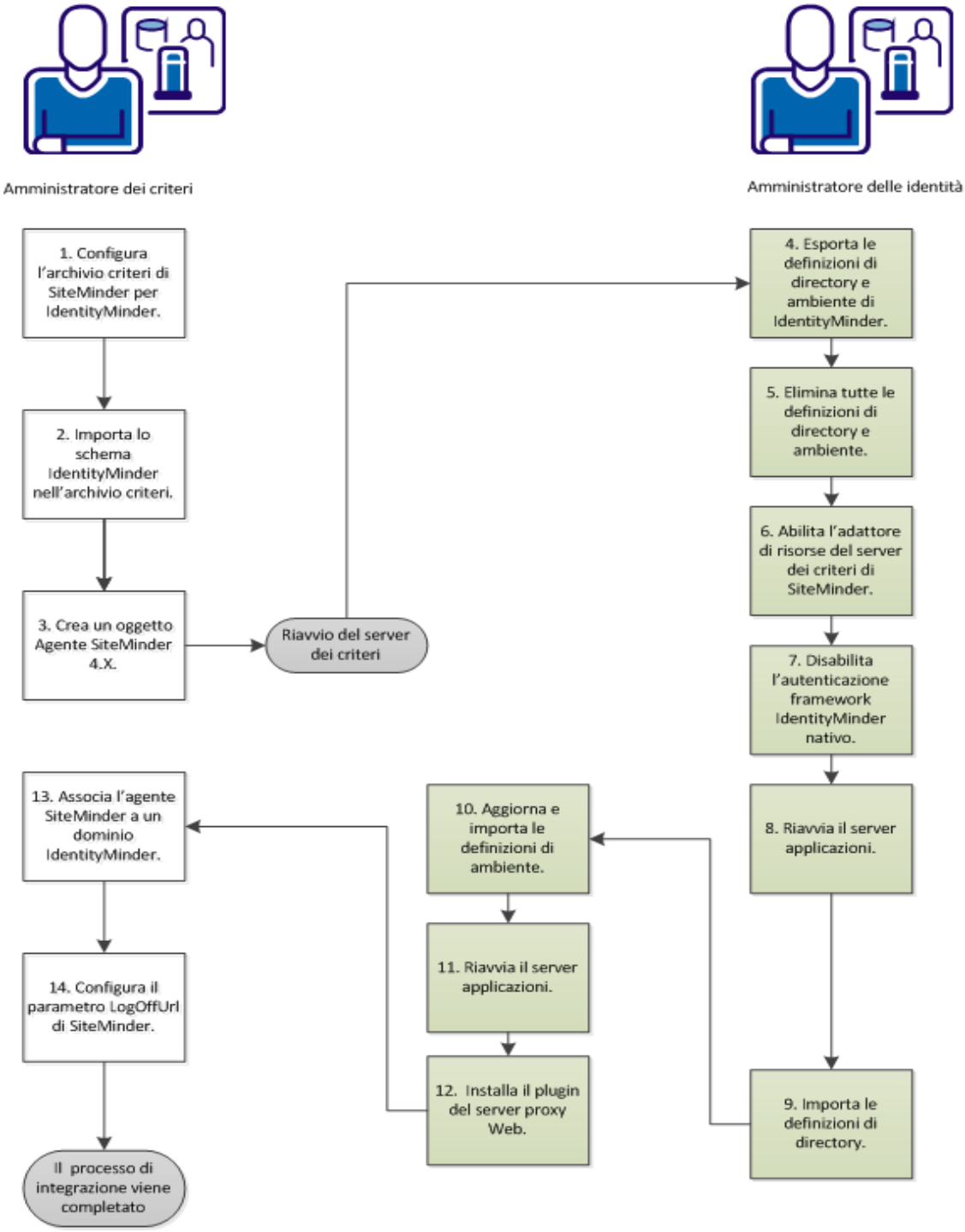


Nota: i componenti vengono installati su piattaforme diverse, a titolo di esempio. Tuttavia, è possibile scegliere altre piattaforme. I database di CA Identity Manager si trovano in Microsoft SQL Server e l'archivio utenti si trova in IBM Directory Server. Il Policy Store di SiteMinder si trova in AD LDS su Windows.

Il completamento di questo processo richiede due ruoli: l'amministratore di identità di CA Identity Manager e l'amministratore dei criteri di SiteMinder. In alcune organizzazioni, una sola persona svolge entrambi i ruoli. Quando sono coinvolte due persone, è richiesta una stretta collaborazione per completare le procedure in questo scenario. L'amministratore dei criteri avvia e conclude questo processo. L'amministratore di identità svolge tutte le fasi intermedie.

Importante. Per le installazioni di CA Identity Manager a partire dalla versione 12.5 SP7, sono obbligatori i Java Cryptography Extension Unlimited Strength Jurisdiction Policy Files (librerie JCE). Scaricare queste librerie dal sito Web di Oracle. Caricarle nella seguente cartella: <Java_path>\<jdk_version>\jre\lib\security\.

Il diagramma seguente illustra il processo completo di integrazione di SiteMinder in CA Identity Manager:



Procedere come descritto di seguito:

1. Configurazione del Policy Store di SiteMinder per CA Identity Manager. (a pagina 293)
2. Importazione dello schema di CA Identity Manager nel Policy Store. (a pagina 299)
3. Creare un oggetto agente di SiteMinder 4.X. (a pagina 299)
4. Esportazione delle directory e degli ambienti di CA Identity Manager. (a pagina 301)
5. Eliminazione di tutte le definizioni di directory e ambiente. (a pagina 302)
6. Attivazione dell'adattatore di risorse del Policy Server di SiteMinder. (a pagina 303)
7. Disattivazione del filtro di autenticazione framework di CA Identity Manager nativo. (a pagina 304)
8. Riavviare il server applicazioni. (a pagina 305)
9. Configurazione di un'origine dati per SiteMinder. (a pagina 305)
10. Importazione delle definizioni di directory. (a pagina 306)
11. Aggiornamento e importazione delle definizioni di ambiente. (a pagina 307)
12. Riavviare il server applicazioni. (a pagina 305)
13. Installazione del plug-in del server proxy Web. (a pagina 307)
14. Associazione dell'agente di SiteMinder a un dominio di CA Identity Manager. (a pagina 326)
15. Configurazione del parametro LogOffUrl di SiteMinder. (a pagina 326)

Configurazione del Policy Store di SiteMinder per CA Identity Manager

Come amministratore dei criteri, si utilizzano gli strumenti di amministrazione di CA Identity Manager per accedere agli script SQL o al testo dello schema LDAP per aggiungere lo schema IMS al Policy Store. L'amministratore di identità avrà installato questi strumenti nella cartella Admin Tools (Strumenti di amministrazione). Attenersi a *una* delle seguenti procedure per configurare il Policy Store:

Configurazione di un database relazionale (a pagina 293)

Configurazione di Sun Java Systems Directory Server o di IBM Directory Server (a pagina 294)

Configurazione di Microsoft Active Directory (a pagina 294)

Configurazione di Microsoft ADAM (a pagina 295)

Configurazione di CA Directory Server (a pagina 296)

Configurazione del server di Novell eDirectory (a pagina 297)

Configurazione di Oracle Internet Directory (OID) (a pagina 298)

Configurazione di un database relazionale

Dopo la configurazione, è possibile utilizzare il proprio database relazionale come Policy Store di SiteMinder.

Procedere come descritto di seguito:

1. Configurare il database come Policy Store supportato di SiteMinder.

   Nota: per le istruzioni di configurazione, consultare la *SiteMinder Policy Server Installation Guide.*

2. Eseguire lo script appropriato per il proprio database:

   - **SQL:** C:\Programmi\CA\Identity Manager\IAM Suite\Identity Manager\tools\policystore-schemas\MicrosoftSQLServer\ims8_mssql_ps.sql
   - **Oracle:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools/policystore-schemas/OracleRDBMS/ims8_oracle_ps.sql

   I percorsi precedenti sono le posizioni di installazione predefinite. La posizione per la propria installazione può essere diversa.

Configurazione di Sun Java Systems Directory Server o di IBM Directory Server

Per configurare un server di directory Java o IBM, applicare il file di schema appropriato.

Procedere come descritto di seguito:

1. Configurare la directory come un Policy Store di SiteMinder supportato.

   Nota: per istruzioni di configurazione, consultare la *Guida all'installazione del Policy Server di CA SiteMinder*.

2. Aggiungere il file di schema LDIF appropriato alla directory. Il percorso predefinito di Windows per i file LDIF è C:\Programmi\CA\Identity Manager\IAM Suite\Identity Manager\tools\policystore-schemas.

   Aggiungere i seguenti file di schema per la directory in uso:

   - **IBM Directory Server:**

     IBMDirectoryServer\V3.identityminder8

   - **Sun Java Systems Directory Server (iPlanet):**

     SunJavaSystemDirectoryServer\sundirectory_ims8.ldif

Configurazione di Microsoft Active Directory

Per configurare un Policy Store di Microsoft Active Directory, applicare lo script activedirectory_ims8.ldif.

Procedere come descritto di seguito:

1. Configurare la directory come un Policy Store di SiteMinder supportato.

   Nota: per istruzioni di configurazione, consultare la *Guida all'installazione del Policy Server di CA SiteMinder*.

2. Modificare il file di schema activedirectory_ims8.ldif nel seguente modo:

   a. In un editor di testo, aprire il file activedirectory_ims8.ldif. Il percorso predefinito di Windows è:

      C:\Programmi\CA\Identity Manager\IAM Suite\Identity Manager\tools\policystore-schemas\MicrosoftActiveDirectory

   b. Sostituire tutte le istanze di {root} dall'organizzazione principale per la directory.

      L'organizzazione principale deve corrispondere all'organizzazione principale specificata quando è stato configurato il Policy Store nella console di gestione del Policy Server.

Ad esempio, se la root è dc=myorg,dc=com, sostituire
dn: CN=imdomainid6,CN=Schema,CN=Configuration,{root} con dn:
CN=imdomainid6,CN=Schema,CN=Configuration,dc=myorg,dc=com

c. Salvare il file.

3. Aggiungere il file di schema così come descritto nella documentazione per la directory in uso.

Configurazione di Microsoft ADAM

Per configurare un Policy Store di Microsoft ADAM, applicare lo script adam_ims8.ldif.

Procedere come descritto di seguito:

1. Configurare la directory come un Policy Store di SiteMinder supportato.

   Nota: per istruzioni di configurazione, consultare la *Guida all'installazione del Policy Server di CA SiteMinder*.

   Prendere nota del valore CN (il guid).

2. Modificare il file di schema adam_ims8.ldif nel seguente modo:

   a. Aprire il file adam_ims8.ldif\.ldif in un editor di testo. Il percorso predefinito di Windows è:

      C:\Programmi\CA\Identity Manager\IAM Suite\Identity Manager\tools\policystore-schemas\MicrosoftActiveDirectory

   b. Sostituire ogni riferimento a cn={guid} con la stringa trovata durante la configurazione del Policy Store di SiteMinder nella fase 1 di questa procedura.

      Ad esempio, se la stringa guid è CN={39BC711D-7F27-4311-B6C0-68FDEE2917B8}, sostituire ogni riferimento a cn={guid} con CN={39BC711D-7F27-4311-B6C0-68FDEE2917B8}.

   c. Salvare il file.

3. Aggiungere il file di schema così come descritto nella documentazione per la directory in uso.

Configurazione di CA Directory Server

Per configurare CA Directory Server, creare un file di schema personalizzato. Nelle fasi riportate di seguito, *dxserver_home* è la directory di installazione di CA Directory. Il percorso di origine predefinito per questo file in Windows è C:\Programmi\CA\Identity Manager\IAM Suite\Identity Manager\tools\policystore-schemas\eTrustDirectory.

Procedere come descritto di seguito:

1. Configurare la directory come un Policy Store di SiteMinder supportato.

   Nota: per istruzioni di configurazione, consultare la *Guida all'installazione del Policy Server di CA SiteMinder*.

2. Copiare etrust_ims8.dxc a *dxserver_home*\config\schema.

3. Creare un file di configurazione dello schema personalizzato nel seguente modo:

   a. Copiare il file *dxserver_home*\config\schema\default.dxg nel file *dxserver_home*\config\schema*company_name*-schema.dxg.

   b. Modificare il file *dxserver_home*\config\schema*company_name*-schema.dxg aggiungendo le seguenti righe in basso nel file:

   ```
   # Identity Manager Schema
   source "etrust_ims8.dxc";
   ```

4. Modificare il file *dxserver_home*\bin\schema.txt aggiungendo i contenuti di etrust_ims_schema.txt alla fine del file. Il percorso di origine predefinito per questo file in Windows è C:\Programmi\CA\Identity Manager\IAM Suite\Identity Manager\tools\policystore-schemas\eTrustDirectory.

5. Creare un file di configurazione dei limiti personalizzato nel seguente modo:

   a. Copiare il file *dxserver_home*\config\limits\default.dxc nel file *dxserver_home*\config\limits*company_name*-limits.dxc.

   b. Aumentare il limite di dimensione predefinito a 5000 nel file *dxserver_home*\config\limits*company_name*-limits.dxc nel seguente modo:

   ```
   set max-op-size=5000
   ```

   Nota: l'aggiornamento di CA Directory sovrascrive il file limits.dxc. Pertanto, assicurarsi di ripristinare max-op-size su 5000 una volta completato l'aggiornamento.

6. Modificare il file *dxserver_home*\config\servers*dsa_name*.dxi nel seguente modo:

   ```
   # schema
   source "company_name-schema.dxg";

   #service limits
   source "company_name-limits.dxc";
   ```

   dove *dsa_name* è il nome del DSA che utilizza i file di configurazione personalizzati.

7. Eseguire l'utilità dxsyntax.
8. Arrestare e riavviare il DSA come utente DSA per applicare le modifiche apportate allo schema, nel seguente modo:
   ```
   dxserver stop dsa_name
   dxserver start dsa_name
   ```

Configurazione del server di Novell eDirectory

Per configurare un Policy Store del server di Novell eDirectory, applicare lo script novell_ims8.ldif.

Procedere come descritto di seguito:

1. Configurare la directory come un Policy Store di SiteMinder supportato.

   Nota: per istruzioni di configurazione, consultare la *Guida all'installazione del Policy Server di CA SiteMinder*.

2. Cercare il nome distinto (DN) del NCPServer per il server di Novell eDirectory immettendo le informazioni seguenti in una finestra di comando del sistema su cui è installato il Policy Server:
   ```
   ldapsearch -h hostname -p port -b container -s sub
   -D admin_login -w password objectClass=ncpServer dn
   ```

   Ad esempio:
   ```
   ldapsearch -h 192.168.1.47 -p 389 -b "o=nwqa47container" -s sub -D
   "cn=admin,o=nwqa47container" -w password objectclass=ncpServer dn
   ```

3. Aprire il file novell_ims8.ldif.
4. Sostituire ogni variabile NCPServer con il valore trovato nella fase 2.

   Il percorso predefinito per novell_ims8.ldif su Windows è:

   C:\Programmi\CA\Identity Manager\IAM Suite\Identity Manager\tools\policystore-schemas\NovelleDirectory

   Ad esempio, se il valore di DN è cn=servername,o=servercontainer, si sostituirà ogni istanza di *NCPServer* con cn=servername,o=servercontainer.

5. Aggiornare il server eDirectory con il file novell_ims8.ldif.

   Per istruzioni, consultare la documentazione Novell eDirectory.

Configurazione di Oracle Internet Directory (OID)

Per configurare Oracle Internet Directory, aggiornare il file oracleoid ldif.

Procedere come descritto di seguito:

1. Configurare la directory come un Policy Store di SiteMinder supportato.

   Nota: per istruzioni di configurazione, consultare la *Guida all'installazione del Policy Server di CA SiteMinder*.

2. Aggiornare il server di Oracle Internet Directory con il file oracleoid_ims8.ldif. Il percorso di installazione predefinito per questo file su Windows è:

   install_path\policystore-schemas\OracleOID\

   Per istruzioni, consultare la documentazione di Oracle Internet Directory.

Verifica del Policy Store

Per verificare il Policy Store, confermare i seguenti punti:

- Il registro del Policy Server non contiene una sezione di avvisi che inizia con il codice seguente:
  `*** IMS NO SCHEMA BEGIN`

  Questo avviso viene visualizzato solamente se sono state installate le estensioni per il Policy Server di SiteMinder, ma non ne è stato ampliato lo schema.

- Gli oggetti di CA Identity Manager sono presenti nel database o nella directory del Policy Store. Gli oggetti di CA Identity Manager iniziano con un prefisso ims.

Importazione dello schema di CA Identity Manager nel Policy Store

L'amministratore dei criteri importa lo schema di CA Identity Manager nel Policy Store. Questa attività consente a CA Identity Manager di creare, aggiornare ed eliminare oggetti di criterio. Gli esempi includono oggetti di directory, domini, aree di autenticazione, regole, criteri e gli oggetti di criterio che abilitano ruoli e attività di accesso.

Procedere come descritto di seguito:

1. Nel Policy Server di SiteMinder, chiudere il servizio del Policy Server.
2. Eseguire il programma di installazione di CA Identity Manager per la versione in uso.
3. Quando viene richiesto quali componenti installare, selezionare le estensioni per SiteMinder (se SiteMinder è installato localmente).
4. Prima di continuare, verificare che il servizio del Policy Server venga riavviato.

Creazione di un oggetto agente di SiteMinder 4.X

L'amministratore dei criteri crea un agente Web di SiteMinder 4.x. Questa attività consente la comunicazione tra SiteMinder e CA Identity Manager. L'amministratore di identità fa riferimento a questo agente durante la configurazione di CA Identity Manager.

Procedere come descritto di seguito:

1. Accedere all'interfaccia di amministrazione di SiteMinder.

   Vengono visualizzate le schede corrispondenti per i privilegi di amministratore.
2. Fare clic su Infrastruttura, Agenti, Agente, Crea agente.

   Viene visualizzata la finestra di dialogo Crea agente.
3. Selezionare Create a new object of type Agent (Crea un nuovo oggetto di tipo Agente), quindi fare clic su OK.

   Viene visualizzata la finestra di dialogo Crea agente.
4. Immettere un nome e una descrizione facoltativa.

   Nota: utilizzare un nome che è possibile associare facilmente alla procedura guidata Connessione SharePoint corrispondente.

5. Scegliere SiteMinder.
6. Selezionare Agente Web dall'elenco a discesa.
7. Abilitare le funzionalità di 4.x tramite le seguenti fasi:
   a. Selezionare la casella di controllo Supporta gli agenti 4.x.

      Vengono visualizzati i campi di impostazioni di attendibilità.

   b. Aggiungere le impostazioni di attendibilità completando i seguenti campi:

      Indirizzo IP

      Specifica l'indirizzo IP del Policy Server.

      Segreto condiviso

      Specifica una password associata all'oggetto Agente di 4.x. La procedura guidata Connessione SharePoint richiede anche questa password.

      Conferma segreto

      Conferma una password associata all'oggetto Agente di 4.x. La procedura guidata Connessione SharePoint richiede anche la conferma di questa password.
8. Fare clic su Inoltra.

   L'attività Create Agent Object (Crea oggetto agente) viene inoltrata per l'elaborazione e viene visualizzato il messaggio di conferma.

Esportazione delle directory e degli ambienti di CA Identity Manager

Il processo di integrazione rimuove tutte le definizioni correnti di ambienti e directory. Per garantire che queste informazioni non vengano perse, l'amministratore di identità esporta gli ambienti utilizzando la console di gestione di CA Identity Manager. Dopo aver completato l'integrazione, queste definizioni ripristinano le directory e gli ambienti.

Procedere come descritto di seguito:

1. Aprire la console di gestione di CA Identity Manager.
2. Fare clic su Directory.
3. Fare clic sulla prima directory nell'elenco, quindi su Esporta.
4. Salvare e archiviare il file XML di directory.
5. Ripetere questa procedura per le directory rimanenti.
6. Fare clic su Pagina principale, quindi su Environments (Ambienti).
7. Selezionare il primo ambiente.
8. Fare clic su Esporta.
9. Ripetere questa procedura per gli ambienti rimanenti.

   Nota: questo processo può richiedere alcuni minuti per ciascun ambiente.

Eliminazione di tutte le definizioni di directory e ambiente

Per preparare la protezione di CA Identity Manager da parte di SiteMinder, l'amministratore di identità elimina le definizioni di directory e ambiente mediante la console di gestione di CA Identity Manager.

Procedere come descritto di seguito:

1. Aprire la console di gestione di CA Identity Manager.
2. Fare clic su Environments (Ambienti).
3. Selezionare il primo ambiente
4. Fare clic su Elimina.
5. Ripetere questo processo per ciascuno degli ambienti rimanenti.

   Nota: eliminare gli ambienti prima delle directory perché gli ambienti fanno riferimento alle directory.
6. Tornare alla sezione Directory.
7. Selezionare tutte le directory elencate.
8. Fare clic su Elimina.

Attivazione dell'adattatore di risorse del Policy Server di SiteMinder.

L'amministratore di identità abilita l'adattatore di risorse del Policy Server di SiteMinder. Lo scopo dell'adattatore è la convalida del cookie SMSESSION. Dopo la convalida, SiteMinder crea il contesto dell'utente.

Procedere come descritto di seguito:

1. Accedere alla cartella \policysever.rar\META-INF disponibile nel file iam_im.ear del server applicazioni che esegue CA Identity Manager.
2. Aprire il file ra.xml in un editor.
3. Cercare la proprietà Enabled config-property, quindi modificare il valore config-property-value su true, così come illustrato nel seguente esempio:

```
        <config-property-name>validateSmHeadersWithPS</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>true</config-property-value>
    </config-property>
    <config-property>
        <config-property-name>Enabled</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>true</config-property-value>
    </config-property>
    <!-- Set FIPS Mode to true if SiteMinder is in FIPS Only Mode -->
    <config-property>
        <config-property-name>FIPSMode</config-property-name>
```

4. Individuare la proprietà ConnectionURL e fornire il nome host del Policy Server di SiteMinder. Utilizzare un nome dominio completo (FQDN).
5. Individuare la proprietà UserName e specificare l'account da utilizzare per la comunicazione con SiteMinder. SiteMinder è il valore predefinito per questo account.
6. Individuare la proprietà AdminSecret. Fornire la password crittografata. Copiare la password dal file directory.xml esportato e incollarla in ra.xml. Se non si è sicuri di disporre di una password comune, crittografare la propria password utilizzando lo strumento Password di CA Identity Manager.
7. Incollare la password crittografata nel file ra.xml.
8. Specificare il nome agente 4.x creato dall'amministratore dei criteri durante la configurazione di SiteMinder.
9. Specificare la password crittografata. Utilizzare lo strumento Password per crittografare la password, se necessario.
10. Salvare le modifiche al file ra.xml.

L'adattatore di risorse del Policy Server di SiteMinder è abilitato.

Ulteriori informazioni:

Modifica di una password o di un segreto condiviso di SiteMinder (a pagina 358)

Disattivazione del filtro di autenticazione framework di CA Identity Manager nativo

Una volta attivato l'adattatore di SiteMinder, il filtro di autenticazione framework non è più necessario. L'amministratore di identità può disabilitare il filtro.

Procedere come descritto di seguito:

1. Individuare e modificare il file web.xml nella cartella \user_console.war\WEB-INF nel iam_im.ear.
2. Individuare il FrameworkAuthFilter e modificare il valore del parametro Enable init-param su false.

   Se si sta utilizzando CA Identity Manager versione 12.5 SP7 o successiva, verificare che i Java Cryptographic Extension Unlimited Strength Jurisdiction Policy Files (JCE) siano stati scaricati in \<Java_path>\<jdk_version>\jre\lib\security nell'ambiente di CA Identity Manager. Questi file consentono a CA Identity Manager di connettersi a SiteMinder.

   Se le librerie JCE sono installate, vengono visualizzati i seguenti messaggi durante l'avvio dell'applicazione di CA Identity Manager:

   ```
   2012-07-06 11:23:56,079 WARN  [ims.default] (main) * Fase di avvio 2: Tentativo di avvio di PolicyServerService
   2012-07-06 11:23:56,081 WARN  [ims.default] (main) Attendibilità illimitata Java Crypto Extensions attivata: TRUE
   ```

   In caso contrario, il valore è false per la voce Attendibilità illimitata Java Crypto Extensions attivata. CA Identity Manager non è in grado di stabilire la connessione al Policy Server.

Riavvio del server applicazioni

Il riavvio aggiorna il server applicazioni con le modifiche. L'amministratore di identità conferma che il passaggio è avvenuto correttamente e che esiste una connessione corretta al Policy Server di SiteMinder.

Procedere come descritto di seguito:

1. Utilizzare il pannello Servizi per riavviare CA Identity Manager quando il server applicazioni è in esecuzione come servizio.
2. Fare riferimento a server.log per convalidare la connessione

Configurazione di un'origine dati per SiteMinder

Se l'ambiente di CA Identity Manager utilizza un database relazionale per l'archivio di identità, l'amministratore di identità deve completare un processo aggiuntivo sul Policy Server di SiteMinder. SiteMinder richiede che un'origine dati locale comunichi con il database.

Procedere come descritto di seguito:

1. Per i server di Windows, aprire la console Amministratore origine dati ODBC che si trova in Administrative Tools (Strumenti di amministrazione).
2. Fare clic sulla scheda System DSN (DSN di sistema).
3. Fare clic su Aggiungi e selezionare il driver di SiteMinder corrispondente al database.
4. Fornire le informazioni necessarie per fare riferimento all'archivio utenti del database relazionale.
5. Verificare la connettività prima di continuare.

Importazione delle definizioni di directory

Per prepararsi all'importazione degli ambienti, l'amministratore di identità importa le directory a cui gli ambienti fanno riferimento. L'importazione della definizione di directory in CA Identity Manager aggiunge anche le informazioni sulle directory al Policy Store di SiteMinder.

Procedere come descritto di seguito:

1. Assicurarsi che CA Identity Manager sia in esecuzione e connettersi a SiteMinder.
2. Accedere alla console di gestione di CA Identity Manager.
3. Fare clic su Directory, quindi su Create or Update from XML (Crea o aggiorna da XML).
4. Selezionare il file di configurazione di directory (directory.xml). Questo file è quello che è stato esportato in Esportazione delle directory e degli ambienti di CA Identity Manager (a pagina 301).
5. Fare clic su Avanti.
6. Fare clic su Fine e rivedere l'output di carico. Verificare che la directory sia presente in CA Identity Manager e SiteMinder.
7. Ripetere queste fasi per l'archivio di provisioning ed eventuali directory rimanenti.
8. Accedere all'interfaccia di amministrazione di SiteMinder per convalidare la creazione delle directory utente.

Aggiornamento e importazione delle definizioni di ambiente

L'amministratore di identità importa nuovamente gli ambienti aggiornati in CA Identity Manager.

Procedere come descritto di seguito:

1. A differenza delle esportazioni delle directory, l'esportazione di ambienti avviene sotto forma di file .zip. Trascinare una copia del file *name*.xml dal file .zip.
2. Copiare il file *name*.xml. Inserire un riferimento all'agente di protezione (non l'agente di 4.x SM) alla fine dell'elemento ImsEnvironment, prima della parentesi uncinata di chiusura />: *agent="idmadmin"*
3. Salvare e incollare nuovamente il file nel file .zip.
4. Aprire la console di gestione di CA Identity Manager e fare clic su Environments (Ambienti), quindi su Importa.
5. Immettere il nome del file .zip dell'ambiente aggiornato.
6. Fare clic su Fine e rivedere l'input di carico.
7. Ripetere questo processo per tutti gli ambienti rimanenti.
8. Riavviare il server applicazioni.

Installazione del plug-in del server proxy Web

A seconda dell'applicazione installata, l'amministratore di identità installa uno dei seguenti plug-in che il server Web utilizza per inoltrare le richieste al server applicazioni:

- WebSphere (a pagina 308)
- JBoss (a pagina 315)
- WebLogic (a pagina 319)

Installazione del plug-in proxy su WebSphere

Il server Web in cui è stato installato l'agente Web inoltra le richieste al server applicazioni in cui risiede il server di CA Identity Manager. Il plug-in proxy del server Web messo a disposizione dal fornitore offre questo servizio.

Utilizzare le procedure applicabili alla distribuzione in uso:

1. Configurazione di IBM HTTP Server (a pagina 308) (tutti i server Web)
2. Configurazione del plug-in proxy (a pagina 309) (tutti i server Web)
3. Uno dei seguenti elementi:
   - Completamento della configurazione su IIS (a pagina 312)
   - Completamento della configurazione su iPlanet o Apache (a pagina 314)

Configurazione di IBM HTTP Server

Per tutti i server Web, installare il plug-in proxy e utilizzare il comando configurewebserver.

Procedere come descritto di seguito:

1. Installare il plug-in proxy da WebSphere Launch Pad.
2. Aggiungere il server Web alla cella di WebSphere eseguendo il comando configurewebserver1.bat nel seguente modo:
   a. Modificare *websphere_home*\Plugins\bin\configurewebserver1.bat/.sh in un editor di testo.
   b. Aggiungere un nome utente e una password alla fine di wsadmin.bat/.sh nel seguente modo:
   ```
   wsadmin.bat -user wsadmin -password password -f
   configureWebserverDefinition.jacl
   ```
   c. Eseguire configurewebserver1.bat/.sh.

   Nota: per ulteriori informazioni sul comando configurewebserver, consultare la documentazione di IBM WebSphere.
3. Continuare con la procedura per la Configurazione del plug-in proxy (a pagina 309).

Configurazione del plug-in proxy

Per tutti i server Web, aggiornare il plug-in utilizzando il comando GenPluginCfg di WebSphere:

Procedere come descritto di seguito:

1. Eseguire l'accesso al sistema su cui è installato WebSphere.
2. Dalla riga di comando, accedere a *websphere_home*\bin, dove *websphere_home* è il percorso di installazione di WebSphere.

   Ad esempio:

   - **Windows:**

     C:\Programmi\WebSphere\AppServer\profile\AppSrv01\bin

   - **UNIX:**

     /*home_dir*/WebSphere/AppServer/profile/AppSrv01/bin

3. Eseguire il comando GenPluginCfg.bat o GenPluginCfg.sh.

   L'esecuzione di questo comando genera un file plugin-cfg.xml nel seguente percorso:

   websphere_home\AppServer\profiles\AppSrv01\config\cells

4. Continuare con una delle procedure seguenti:

   - Completamento della configurazione su IIS (a pagina 312)
   - Completamento della configurazione su iPlanet o Apache (a pagina 314)

Completamento della configurazione su IIS (7.x)

Prima di avviare questa procedura, verificare che la versione utilizzata corrisponda alla versione 6.1.0.9 o successiva del plug-in del server Web. Le versioni precedenti del plug-in non supportano il sistema operativo Windows Server 2008.

Procedere come descritto di seguito:

1. Installare IIS versione 7.x con i componenti di Compatibilità di gestione con IIS versione 6.0. I componenti di Compatibilità di gestione con IIS versione 6.0 non vengono installati per impostazione predefinita.
2. Completare le seguenti fasi per visualizzare la finestra Server Manager in Windows Server 2008:
    1. Fare clic su Start, Administrative Tools, Server Managers.
    2. Fare clic su Action, Add Roles, quindi su Next.
    3. Selezionare il ruolo Web Server (IIS) nella pagina Select Server Roles, quindi fare clic su Next.
    4. Fare clic su Add Feature, Next, quando viene visualizzato un prompt per la funzionalità Windows Process Activation Service
    5. Fare clic su Next nella pagina di introduzione di IIS.
3. Quando viene visualizzata la finestra Role Services, verificare che oltre alle opzioni predefinite già selezionate siano selezionate anche le opzioni seguenti.
    - Internet Information Services: Management Tools
    - Compatibilità di gestione con IIS versione 6.0: IIS Version 6.0 Management Console, IIS Version 6.0 Scripting Tools, IIS Version 6.0 WMI Compatibility e IIS Metabase compatibility
    - Sviluppo di applicazioni: ISAPI Extensions, ISAPI Filters
4. Fare clic su Next per abilitare le opzioni selezionate, quindi su Install nella finestra successiva per eseguire l'installazione.
5. Al termine dell'installazione, fare clic su Close nella finestra dei risultati dell'installazione.
6. Aprire il prompt dei comandi e accedere a:\Programmi\IBM\WebSphere\AppServer\profiles\Dmgr01\bin.
7. Eseguire questo comando: GenPluginCfg.bat.

    Il file plugin-cfg.xml verrà generato in questo percorso: C:\Programmi\IBM\WebSphere\AppServer\profiles\Dmgr01\config\cells.
8. Creare una directory in c:\, ad esempio, c:\plugin.
9. Copiare il file plugin-cfg.xml nella directory c:\plugin.
10. Copiare il file iisWASPlugin_http.dll nella directory c:\plugin.

11. Selezionare Start, All Programs, Administrative Tools, Internet Information Services (IIS) Manager su un sistema operativo di Windows Server 2008. Questa azione avvia l'applicazione IIS e crea una nuova directory virtuale per l'istanza del sito Web. Queste istruzioni suppongono che si stia utilizzando il sito Web predefinito.
12. Espandere la struttura a sinistra finché non viene visualizzato il sito Web predefinito.
13. Fare clic con il tasto destro del mouse sul sito Web predefinito, su Add Virtual Directory per creare la directory con un'installazione predefinita.
14. Immettere setPlugins nel campo Alias in Virtual Directory Alias della procedura guidata Virtual Directory Creation.
15. Accedere alla directory c:\plugin directory nel campo Physical Path della finestra Web Site Content Directory della procedura guidata, quindi fare clic su OK.
16. Fare clic sul pulsante Test Settings. Se la verifica delle impostazioni non riesce, è possibile modificare le autorizzazioni della directory fisica. In alternativa, selezionare Connect As e consentire a IIS di connettersi come account utente di Windows con autorità sui file in quel percorso fisico.
17. Fare clic su OK per aggiungere la directory virtuale setPlugins al sito Web.
18. Selezionare la directory virtuale setPlugins appena creata nella struttura di navigazione.
19. Fare doppio clic su Handler Mappings, quindi su Edit Feature Permissions nel pannello Actions.
20. Selezionare Script and Execute, se non sono già stati selezionati.
21. Fare clic su OK.
22. Tornare alla finestra di IIS Manager ed espandere la cartella dei siti Web nella struttura di navigazione a sinistra in quella finestra.
23. Selezionare Default Web Site nella struttura di navigazione.
24. Completare le seguenti fasi nel pannello Default Web Site Properties per aggiungere il filtro ISAPI:
    1. Fare doppio clic sulla scheda ISAPI Filters.
    2. Per aprire la finestra di dialogo Add/Edit Filter Properties, selezionarla.
    3. Nel campo Filter name, immettere iisWASPlugin.
    4. Fare clic su Browse per selezionare il file di plug-in disponibile nella directory c:\plugin\iisWASPlugin_http.dll.
    5. Fare clic su OK per chiudere la finestra di dialogo Add/Edit Filter Properties.
25. Selezionare il nodo server di livello più alto nella struttura di navigazione.

26. Fare doppio clic su ISAPI and CGI Restrictions nel pannello Features.

    Per determinare il valore da specificare per la proprietà ISAPI or CGI Path , passare allo stesso file di plug-in selezionato nella fase precedente e selezionarlo. Ad esempio: c:\plugin\iisWASPlugin_http.dll.

27. Fare clic su Add nel pannello Actions.

28. Immettere WASPlugin nel campo Description , selezionare Allow extension path to execute, quindi fare clic su OK per chiudere la finestra di dialogo ISAPI and CGI Restrictions .

29. Creare il nuovo file plugin-cfg.loc nella posizione c:\plugin. Impostare il valore nel file plugin-cfg.loc nella posizione del file di configurazione. La posizione predefinita è C:\plugin\plugin-cfg.xml.

Aggiornamento dell'agente Web

Dopo aver configurato IIS 7.x, apportare le modifiche seguenti all'agente Web:

1. Fare clic su Application pools e modificare il pool di applicazioni predefinito nella modalità Classic.
2. Fare clic su Inoltra.
3. Verificare che l'agente occupi una posizione più alta nell'elenco delle priorità dei filtri ISAPI rispetto al plug-in del server applicazioni utilizzato da CA Identity Manager.
4. Riavviare IIS versione 7.x e il profilo di WebSphere Application Server.

Completamento della configurazione su IIS

Dopo avere configurato IBM HTTP Server e il plug-in proxy, assicurarsi che il proxy plugin-cfg.xml sia nella posizione giusta ed eseguire fasi per configurare un file di plugin aggiuntivo.

Procedere come descritto di seguito:

1. Copiare il file plugin-cfg.xml nel seguente modo:
   a. Accedere al sistema su cui è installato l'agente Web.
   b. Creare una cartella senza spazi nell'unità C:. Ad esempio: C:\plugin.
   c. Copiare il file plugin-cfg.xml nella cartella C:\plugin.
2. Creare un file chiamato plugin-cfg.loc nella cartella C:\plugin e aggiungere la seguente riga nel file:

   C:\plugin\plugin-cfg.xml

3. Scaricare il programma di installazione di Websphere Plugin da www.ibm.com al sistema in cui WebSphere viene installato.
4. Accedere alla posizione del programma di installazione di WebSphere Plugin.
5. Generare il file iisWASPlugin_http.dll mediante questo comando:

   ```
   install is:javahome "c:\IBM\WebSphere\AppServer\Java
   ```

   Rispondere alle domande presentate in base alla propria configurazione.

   Al termine della procedura guidata, il file iisWASPlugin_http.dll viene salvato nella cartella C:\IBM\WebSphere\Plugs\bin. Cercare una sottocartella a 32 bit o a 64 bit.
6. Copiare il file iisWASPlugin_http.dll nella cartella C:\plugin nel sistema con l'agente Web.
7. Creare una directory virtuale nel seguente modo:
   a. Aprire IIS Manager.
   b. Fare clic con il tasto destro del mouse su Default web sites.
   c. Fare clic su New virtual directory e fornire questi valori:

      Alias: sePlugins (fa distinzione maiuscole/minuscole).

      Percorso: c:\plugin

      Autorizzazione: lettura + esecuzione (ISAPI o CGI)
8. Aggiungere un filtro ISAPI nel modo seguente:
   a. Fare clic con il tasto destro del mouse su Default Web Site.
   b. Fare clic su Properties.
   c. Fare clic su Add nella scheda del filtro ISAPI.
   d. Fornire questi valori:

      Nome filtro: sePlugins

      Eseguibile: c:\plugin\ iisWASPlugin_http.dll
9. Creare un'estensione del servizio Web nel seguente modo:
   a. In IIS6 Manager, espandere il nome computer.
   b. Creare un'estensione del servizio Web e impostarla su Allowed.

      Nome di estensione: WASPlugin

      Percorso: c:\plugin\ iisWASPlugin_http.dll
   c. Fare clic con il tasto destro del mouse su ciascuna estensione del servizio Web per impostarla sullo stato Allowed.

10. Riavviare il server Web IIS.

    Nel servizio WWW principale, assicurarsi che il plug-in di WebSphere (sePlugin) venga visualizzato dopo il plug-in dell'agente Web di SiteMinder e che il plug-in di WebSphere sia stato avviato correttamente.

Completamento della configurazione su iPlanet o Apache

Dopo avere configurato IBM HTTP Server e il plug-in proxy, assicurarsi che il proxy plugin-cfg.xml sia nella posizione giusta e riavviare il server Web.

Procedere come descritto di seguito:

1. Copiare il file plugin-cfg.xml dal sistema in cui è stato installato il plug-in proxy nel seguente percorso:

   websphere_home\AppServer\profiles*server_name*\config\cells*websphere_cell*\nodes\webserver1_node\servers\webserver1\

2. Assicurarsi che il plug-in di WebSphere (libns41_http.so) venga caricato dopo il plug-in dell'agente Web di SiteMinder (NSAPIWebAgent.so) su tutti i server Web di iPlanet.

3. Controllare l'ordine dei plug-in in *iplanet_home*/https-*instance*/config/magnus.conf per i server Web di IPlanet 6.0.

4. Copiare le seguenti righe da *iplanet_home*/https-*instance*/config/magnus.conf in *iplanet_home*/https-*instance*/config/obj.conf (server Web di IPlanet 5.x):

   ```
   Init fn="load-modules" funcs="as_init,as_handler,as_term"
   shlib="/export/WebSphere/AppServer/bin/libns41_http.so"

   Init fn="as_init"
   bootstrap.properties="/export/WebSphere/AppServer/config/cells/plugin-cfg.xml"
   ```

   Aggiungere il seguente codice dopo AuthTrans fn="SiteMinderAgent" nel file obj.conf:

   ```
   Service fn="as_handler"
   ```

5. Assicurarsi che il plug-in dell'agente Web di SiteMinder (mod2_sm.so) venga caricato prima del plug-in di WebSphere (mod_ibm_app_server_http.so) sui server Web di Apache. Questo comando si trova nella sezione Dynamic Shared Object (DSO) Support di *apache_home*/config/httpd.conf,

6. Riavviare il server Web.

Installazione del plug-in proxy per JBoss

Dopo che l'agente Web di SiteMinder autentica e autorizza una richiesta per una risorsa di CA Identity Manager, il server Web inoltra la richiesta al server applicazioni in cui risiede il server di CA Identity Manager. Per inoltrare queste richieste, installare e configurare un connettore JK nel sistema su cui è installato l'agente Web di SiteMinder. Per ulteriori informazioni sul connettore JK, consultare il seguente sito Web di Jakarta Project:

http://community.jboss.org/wiki/usingmodjk12withjboss

Gli strumenti di amministrazione di CA Identity Manager includono i file di configurazione di esempio che possono essere utilizzati per configurare il connettore JK. Per istruzioni, consultare il file readme.txt nella directory indicata nella tabella seguente:

Piattaforma	Posizione
Server Web IIS su un sistema Windows	C:\Programmi\CA\Identity Manager\IAM Suite\Identity Manager\tools\samples\ConnectorConfiguration\windows\IIS_JBoss*
Server Web di Sun Java System su un sistema Solaris	/opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools/samples/ConnectorConfiguration/solaris/Iplanet_JBoss*
Server Web di Apache su un sistema Solaris	/opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools/samples/ConnectorConfiguration/solaris/apache_JBoss*

Installazione e configurazione di un plug-in dell'applicazione JBoss (IIS 7.x)

Questa procedura descrive la configurazione del plug-in JBoss Apache a partire da IIS 7.0

Procedere come descritto di seguito:

1. Distribuire e aggiornare i filtri ISAPI nel file system.

   Distribuire la cartella ISAPI alla root dell'unità C.

2. Modificare il file jakarta.reg della cartella decompressa.

   Se la cartella ISAPI è stata collocata nella root di C:\, non modificare questo file. Se è stata collocata in una cartella differente, specificare la cartella nelle righe 9, 11 e 12.

3. Salvare le modifiche e fare doppio clic per aggiornare il registro.

4. Modificare il file workers.properties specificando la posizione del server applicazioni di JBoss. La porta e il tipo non devono essere modificati.

5. Installare IIS7 o IIS7.5 su Windows 2008.

6. Aprire il manager di sistema e verificare che il filtro ISAPI di IIS e l'estensione ISAPI siano stati installati.

7. Avviare inetmgr nella finestra Run.
8. Selezionare il nome m/c e fare doppio clic su ISAPI and CGI Restriction.
9. Fare clic sul pulsante Add nel pannello a destra.
10. Viene visualizzata la finestra Add ISAPI or CGI Restrictions.
11. Selezionare isapi_redirect.dll e immettere la descrizione come ISAPI.
12. Selezionare Allow Extension path to execute.
13. Fare clic su OK nella finestra Add ISAPI or CGI Restrictions.
14. Espandere i siti nella sezione Connection, selezionare il sito Web predefinito, quindi fare clic con il tasto destro del mouse su Add Virtual Directory.
15. Immettere l'alias "jakarta" e la posizione del file isap_redirect.dll (c:\ajp) nel percorso fisico.
16. Fare clic sul pulsante Test Settings:
    - Se l'autenticazione e l'autorizzazione sono andate a buon fine, fare clic su OK.
    - Se l'autorizzazione non riesce, fare clic sul pulsante Connect As.
17. Selezionare l'utente specifico e fornire il nome utente e la password dell'amministratore.
18. Fare clic nuovamente sul pulsante Test Settings. Questa volta l'autorizzazione va a buon fine.
19. Fare clic sul sito Web predefinito sulla sinistra e doppio clic sul filtro ISAPI.
20. Fare clic sul pulsante Add nel pannello a destra.
21. Immettere il nome e fornire la posizione del file isapi_redirect.dll.
22. Fare clic su OK.
23. Espandere il sito Web predefinito e fare clic sulla directory virtuale jakarta.
24. Fare doppio clic su Handler Mapping.
25. Selezionare il file ISAPI-dll e fare clic su Edit Feature Permission.

26. Verificare che siano selezionate tutte le autorizzazioni (lettura, script ed esecuzione).
27. Fare clic su OK.

Aggiornamento dell'agente Web

Dopo aver configurato IIS 7.x, apportare le modifiche seguenti all'agente Web:

1. Fare clic su Application pools e modificare il pool di applicazioni predefinito nella modalità Classic.
2. Fare clic su Inoltra.
3. Verificare che l'agente occupi una posizione più alta nell'elenco delle priorità dei filtri ISAPI rispetto al plug-in del server applicazioni utilizzato da CA Identity Manager.

Il plug-in di JBoss è stato configurato.

Installazione e configurazione di un plug-in dell'applicazione JBoss (IIS 6.0)

Questa integrazione suppone che un utente in SiteMinder venga autenticato e autorizzato prima di raggiungere CA Identity Manager. Un utente deve avere un cookie SMSESSION prima di raggiungere CA Identity Manager. Utilizzare un plug-in dell'applicazione (reindirizzamento di proxy) protetto da un agente Web di SiteMinder. Attraverso questa configurazione, un utente viene autenticato da SiteMinder, quindi reindirizzato a CA Identity Manager dopo che è stato creato un cookie SMSESSION.

Questa procedura è valida per la distribuzione e la configurazione del plug-in di Apache JBoss per IIS 6.0:

Procedere come descritto di seguito:

1. Distribuire e aggiornare il filtro ISAPI nel file system.

   Assicurarsi di distribuire la cartella ISAPI alla root dell'unità C.
2. Modificare il file jakarta.reg della cartella decompressa.

   Se la cartella ISAPI è stata collocata nella root di C:\, non modificare questo file. Se viene collocata in una cartella differente, specificare la cartella nelle righe 9, 11 e 12.
3. Salvare le modifiche e fare doppio clic per aggiornare il registro.
4. Modificare il file workers.properties specificando la posizione del server applicazioni di JBoss. La porta e il tipo non devono essere modificati.
5. Distribuire il filtro ISAPI in IIS.
6. Aprire Internet Information Services Manager da Administrative Tools.
7. Espandere i livelli fino a che il sito Web predefinito non diventa visibile. Fare clic con il tasto destro del mouse e selezionare New, Virtual Directory.

8. Immettere *jakarta* come alias.
9. Fare riferimento al percorso in cui è stato installato il plug-in ISAPI.
10. Selezionare Read, Run scripts (quali ASP) ed Execute (quali applicazioni ISAPI o CGI).
11. Fare clic su Next per continuare e completare la procedura guidata.
12. Fare clic con il tasto destro del mouse sul sito Web predefinito e selezionare le proprietà, selezionare la scheda ISAPI Filters, quindi fare clic su Add.
13. Immettere *jakarta* come nome filtro, quindi fare clic su Browse per selezionare il file isapi_redirect.dll. Quindi fare clic su OK due volte.
14. Per IIS 6.0, abilitare questo filtro nelle estensioni del servizio Web.
15. Selezionare la cartella Web Service Extensions. Fare clic sul collegamento azzurro a sinistra per aggiungere una nuova estensione del servizio Web.
16. Indicare Jakarta-Tomcat come nome. Fare clic su Add and browse per la stessa dll indicata sopra. Fare clic su OK, quindi impostare Set extension status su Allowed e fare clic su OK.
17. Riavviare il server IIS.

Con il proxy ora attivato, è possibile accedere a CA Identity Manager attraverso IIS. Ad esempio, di seguito vengono elencati i collegamenti per accedere a CA Identity Manager prima e dopo la configurazione del proxy:

Prima

http://identitymgr.forwardinc.ca:8080/idmmange
http://identitymgr.forwardinc.ca:8080/idmmange

Dopo

http://smserver.forwardinc/idmmanage http://smserver.forwardinc/idmmanage

Nota: potrebbe essere necessario aggiungere una barra "/" alla fine di questo URL perché il proxy funzioni. Fare riferimento ai registri del proxy se non si viene indirizzati alla console di gestione.

Installazione del plug-in proxy su WebLogic

Dopo che l'agente Web autentica e autorizza una richiesta per una risorsa di CA Identity Manager, il server Web inoltra la richiesta al server applicazioni in cui risiede il server di CA Identity Manager.

1. Installare il plug-in proxy di WebLogic per il server Web così come descritto nella documentazione di WebLogic.

   Nota: per gli utenti di IIS, quando si installa il plug-in proxy, occorre assicurarsi di configurare l'inoltro dei dati in base all'estensione del file e al percorso. Quando si configura l'inoltro di dati in base all'estensione del file, aggiungere un mapping di applicazione sulla scheda App Mapping con le seguenti proprietà:
   Eseguibile: IISProxy.dll
   Estensione: .wlforward

2. Configurare il plug-in proxy per CA Identity Manager così come descritto in una delle sezioni seguenti:

   - Plug-in proxy di IIS (a pagina 321)
   - Plug-in proxy di iPlanet (a pagina 323)
   - Plug-in di proxy di Apache (a pagina 325)

Configurazione del plug-in proxy per IIS (7.x)

La seguente procedura illustra la distribuzione e la configurazione del plug-in proxy di WebLogic per IIS 7.x.

Nota: queste istruzioni valgono per gli ambienti operativi a 32 bit. Le stesse istruzioni si applicano ad ambienti operativi a 64 bit. Il percorso del file di installazione .dll è differente:

- %WL_HOME%server\plugin\win\32\
- %WL_HOME%server\plugin\win\64\

Procedere come descritto di seguito:

1. Installare l'agente Web e configurarlo su IIS7.
2. Creare una cartella con il nome Plugin nell'unità C.
3. Copiare i file seguenti nella cartella plugin:

   - lisforward.dll
   - lisproxy.dll
   - iisproxy.ini

   È possibile trovare questi file in \\lodimmaple.ca.com\RegressionHarness\thirdparty\weblogic\Weblogic_Proxy_Files_IIS7.

4. Installare i servizi ruolo Application Development (Sviluppo di applicazioni) e Management Tools (Strumenti di gestione) su IIS7.
5. Aprire Inet Manager e selezionare il sito Web predefinito.
6. Fare clic su Handler Mappings.
7. Fare doppio clic su Static File e modificare il percorso di richiesta in *.*.
8. Fare clic sul pulsante Request Restrictions.
9. Sulla scheda Mapping selezionare Invoke handler only if the request is mapped to a File or folder.
10. Nella finestra di dialogo Handler Mappings, fare clic su Add Script Map… nelle opzioni di menu sul lato destro. Immettere i seguenti valori:
    - Request path: *
    - Executable: iisProxy.dll
    - Name: proxy
11. Fare clic sul pulsante Request Restrictions.
12. Annullare la selezione di Invoke handler only if the request is mapped to.
13. Fare clic su Yes alla richiesta se consentire questa estensione IASPI.
14. Fare clic sul nodo principale (nome computer) della struttura di IIS Manager e fare clic su ISAPI and CGI Restrictions.
15. Fare clic su Add nel pannello Actions e immettere i seguenti valori:
    - ISAPI or CGI Path: C: C:\plugin\ iisproxy.dll.
    - Description: Weblogic
    - Selezionare Allow Extension path to execute.
16. Fare clic sul nodo principale (nome computer) della struttura di Gestione IIS e fare clic su ISAPI and CGI Restrictions. Selezionare l'opzione Weblogic e fare clic su Edit Feature Settings nel riquadro sulla destra.
17. Selezionare Allow unspecified ISAPI modules e Allow unspecified CGI modules.
18. Fare lo stesso per Webagent.
19. In Features View, nel sito Web predefinito, fare doppio clic su Handler Mappings.
20. Nella pagina Handler Mappings, nel riquadro Actions, fare clic su Add Script Map e sui valori seguenti:
    - Request path: .jsp
    - Executable: iisproxy.dll
    - Name: JSP
21. Fare clic su Request restrictions.

22. Sulla scheda Mapping, selezionare Invoke handler only if request is mapped to File.
23. Fare clic su OK.
24. Fare clic su Add Script Map e sui valori seguenti:
    - Request path: .do
    - Executable: C:\plugin\iisproxy.dll
25. Fare clic su Request restrictions. Le impostazioni sono uguali a quelle per .jsp.
26. Fare clic su OK.
27. Fare clic su Add Script Map e immettere i valori seguenti:
    - Request path: .wlforward
    - Executable: C:\plugin\iisproxy.dll
28. Fare clic su Request restrictions. Le impostazioni sono uguali a quelle per .jsp.
29. Fare clic su Default Web Site e fare doppio clic su ISAPI Filters.
30. Fare clic su View Order List nel riquadro sulla destra.
31. Collocare l'eseguibile dell'agente di SiteMinder al secondo posto nell'elenco. Dopo questa voce, nell'elenco si trova solamente l'eseguibile di Weblogic.

    Nota: se l'eseguibile dell'agente di SiteMinder viene visualizzato dopo l'eseguibile di Weblogic, spostare l'agente di SiteMinder utilizzando l'azione MOVE UP.
32. Fare clic su Application pools e modificare il pool di applicazioni predefinito nella modalità Classic.

Il plug-in di WebLogic è stato configurato.

(WL) Configurazione del plug-in proxy IIS 6.0

Questa procedura si applica a configurazioni del plug-in proxy di WebLogic per IIS 6.0.x:

Procedere come descritto di seguito:

1. Creare una cartella nel sistema in cui è stato installato l'agente Web. Ad esempio: c:\weblogic_proxy.
2. Accedere al sistema in cui è in esecuzione il server di CA Identity Manager.
3. Accedere alla cartella: *Weblogic_Home*\wlserver_11\server\plugin
4. Copiare i seguenti file nella cartella proxy weblogic creata nella fase 1.
    - iisforward.dll
    - iisproxy.dll

5. Creare un file denominato iisproxy.ini nella stessa cartella e includere il contenuto seguente:

```
# This file contains initialization name/value pairs
# for the IIS/WebLogic plug-in.
WebLogicHost=host-name
WebLogicPort=7001
ConnectTimeoutSecs=20
ConnectRetrySecs=2
WlForwardPath=/castylesr5.1.1,/iam,/im , /ca/Odata/
WLLogFile= c:\weblogic_proxy \proxy.log
DebugConfigInfo=ON
```

   Sostituire *hostname* con il nome host effettivo.

6. Avviare IIS Manager.
7. Espandere i siti Web.
8. Fare clic con il tasto destro del mouse su Default Web Site.
9. Selezionare Properties.
10. Aggiungere un filtro come segue:
    a. Fare clic su ISAPI Filters.
    b. Fare clic su Add e completare la finestra di dialogo nel seguente modo:

       Per il nome filtro: WebLogic

       Per l'eseguibile: percorso di iisforward.dll
11. Fornire la posizione del file iisproxy.dll nel seguente modo:
    a. Fare clic su Home Directory.
    b. Fare clic su Configurazione.
    c. Fare clic su Aggiungi.
    d. Immettere il percorso del file iisproxy.dll.
    e. Immettere .jsp nel campo Estensione.
    f. Deselezionare l'opzione Verify that file exists.
12. Ripetere la fase 11 per le estensioni .do e .wlforward.
13. Aggiungere un'estensione del servizio Web per wlforward (in lettere minuscole) puntando alla posizione di iisforward.dll.

    Impostare lo stato dell'estensione su Allowed.
14. Fare clic con il tasto destro del mouse su ciascuna estensione del servizio Web per impostarla sullo stato Allowed.
15. Riavviare il server Web IIS.

Configurazione del plug-in proxy iPlanet

Per configurare il plug-in, modificare i seguenti file di configurazione di iPlanet:

- magnus.conf
- obj.conf

I file di configurazione di iPlanet hanno regole rigide sulla posizione del testo. Per evitare problemi, occorre notare quanto segue:

- Eliminare gli spazi iniziali e finali estranei. Gli spazi extra possono causare la non riuscita del server di iPlanet.
- Se occorre immettere più caratteri di quanti possano essere inseriti in una riga, aggiungere una barra rovesciata (\) alla fine di quella riga e continuare a digitare nella riga seguente. La barra rovesciata congiunge direttamente la fine della prima riga con l'inizio della riga seguente. Se è necessario uno spazio tra le parole alla fine della prima riga e l'inizio della seconda, assicurarsi di utilizzare uno spazio o alla fine della prima riga (prima della barra rovesciata) o all'inizio della seconda riga.
- Non suddividere gli attributi su diverse righe.

I file di configurazione di iPlanet per l'istanza di iPlanet in uso si trovano nella seguente posizione:

iplanet_home/https-*instance_name*/config/

dove *iplanet_home* è la directory principale dell'installazione di iPlanet e *instance_name* è la configurazione specifica del server in uso.

Procedere come descritto di seguito:

1. Dalla directory *weblogic_home*/server/lib, copiare il file libproxy.so che corrisponde alla versione del server Web di iPlanet nel file system in cui è stato installato iPlanet.
2. In un editor di testo, modificare il file magnus.conf di iPlanet.

   Per far sì che iPlanet carichi il file libproxy.so come modulo di iPlanet, aggiungere le seguenti righe all'inizio del file magnus.conf:

   ```
   Init fn="load-modules" funcs="wl_proxy,wl_init"\
   shlib=path in file system from step 1/libproxy.so
   Init fn="wl_init"
   ```

   Ad esempio:

   ```
   Init fn="load-modules" funcs="wl_proxy,wl_init"\
   shlib=/usr/local/netscape/plugins/libproxy.so
   Init fn="wl_init"
   ```

   La funzione load-modules segnala la libreria condivisa per il caricamento durante l'avvio di iPlanet. I valori wl_proxy e wl_init identificano le funzioni eseguite dal plug-in.

3. In un editor di testo, modificare il file obj.conf di iPlanet nel seguente modo:
   a. Dopo l'ultima riga che inizia con il testo seguente:

      NameTrans fn=....

      Aggiungere la seguente direttiva di servizio nella sezione Object name="default":

      ```
      Service method="(GET|HEAD|POST|PUT)" type=text/jsp fn="wl-proxy"
      ```

      Nota: è possibile aggiungere questa direttiva in una riga dopo le direttive di servizio esistenti.

   b. Aggiungere il seguente codice alla fine del file:

      ```
      <Object name="idm" ppath="*/iam/*">">
      Service fn="wl-proxy" WebLogicHost="hostname" WebLogicPort="portnumber"
      PathTrim="/weblogic"
      </Object>
      <Object name="weblogic1" ppath="*/console*">
      Service fn="wl-proxy" WebLogicHost="hostname" WebLogicPort="portnumber"
      PathTrim="/weblogic"
      </Object>
      ```

      dove *hostname* è il nome server e il dominio del sistema in cui è stato installato WebLogic e *portnumber* è la porta di WebLogic (il valore predefinito è 7001).

      È possibile che vi sia più di una voce Object.

      Ad esempio:

      ```
      <Object name="idm" ppath="*/iam/*">">
      Service fn="wl-proxy" WebLogicHost="MyServer.MyCompany.com"
      WebLogicPort="7001" PathTrim="/weblogic"
      <Object name="weblogic1" ppath="*/console*">
      Service fn="wl-proxy" WebLogicHost="MyServer.MyCompany.com"
      WebLogicPort="7001" PathTrim="/weblogic"
      </Object>
      ```

4. Salvare i file di configurazione di iPlanet.
5. Riavviare l'istanza del server Web in uso.

IM_12.8--Configurazione del plug-in proxy Apache

La configurazione del plug-in proxy di Apache richiede la modifica del file http.conf.

Procedere come descritto di seguito:

1. Arrestare il server Web di Apache dopo avere installato un agente Web su Solaris e copiare il file mod_wl_20.so dalla posizione seguente:

   weblogic_home/server/lib/solaris

   nella posizione

   apache_home/modules

2. Modificare il file http.conf (che si trova in *apache_home*/conf) e apportarvi le seguenti modifiche:

   a. Nella sezione load-module, aggiungere il seguente codice:
   ```
   LoadModule weblogic_module modules/mod_wl_20.so
   ```

   b. Modificare il nome server con il nome del sistema server di Apache.

   c. Aggiungere un blocco If alla fine del file nel seguente modo:
   ```
   <IfModule mod_weblogic.c>
     WebLogicHost weblogic_server.com
     WebLogicPort 7001
     MatchExpression /iam
     MatchExpression /castylesr5.1.1
     MatchExpression /ca/Odata
   </IfModule>
   ```

3. Salvare il file http.conf.

4. Riavviare il server Web Apache.

Associazione dell'agente di SiteMinder a un dominio di CA Identity Manager

L'amministratore dei criteri esegue questa attività dopo avere completato le attività di CA Identity Manager. Durante il caricamento degli ambienti in CA Identity Manager, fare riferimento all'agente 4.X. SiteMinder utilizza quell'agente durante la creazione di dominio/area di autenticazione nel Policy Server di SiteMinder. Questo agente convalida i cookie SMSESSION. Aggiornare il dominio o l'area di autenticazione e fare riferimento all'agente funzionante nel server Web utilizzato per accedere a CA Identity Manager. Questo server Web funge da punto di accesso a CA Identity Manager e crea i cookie SMSESSION.

Procedere come descritto di seguito:

1. Accedere all'interfaccia di amministrazione di SiteMinder.
2. Accedere a Criteri, Domini.
3. Modificare il dominio per l'ambiente.
4. Nella scheda Aree di autenticazione, modificare la prima area di autenticazione elencata: XXX_ims_realm.
5. Cercare e selezionare l'agente nel proxy.

   Nota: Se non si dispone di un agente proxy (agente del server Web), crearne uno. Verificare di disporre di un server Web e un proxy per CA Identity Manager.
6. Fare clic su OK due volte, quindi ripetere questo processo per l'area di autenticazione Public XXX_pub_realm.
7. Dopo avere aggiornato ambedue le aree di autenticazione, fare clic su Invia.
8. Attendere che l'agente venga aggiornato o riavviare il server Web in cui si trova l'agente proxy.

Configurazione del parametro LogOffUrI di SiteMinder

Dopo aver aggiunto SiteMinder all'ambiente, la disconnessione in CA Identity Manager non ha alcun effetto. Per riabilitare questa funzionalità, aggiornare l'oggetto Configurazione agente (ACO) per l'agente sul proxy.

Procedere come descritto di seguito:

1. Accedere all'interfaccia di amministrazione di SiteMinder. Fare clic sulla scheda Infrastruttura, Agenti, Expand Agent Configuration (Espandi configurazione agente), quindi fare clic su Modifica configurazione agente.
2. Individuare l'ACO. Individuare il parametro #LogoffUri. Fare clic sul pulsante di riproduzione (freccia verso destra) a sinistra del parametro.

3. Rimuovere il segno del cancelletto (#) dal nome nel campo Valore e immettere /idm/logout.jsp.
4. Fare clic su OK, quindi su Invia per aggiornare l'oggetto Configurazione agente.

   La volta successiva che l'agente recupera la propria configurazione dal Policy Server, la nuova impostazione viene propagata.

Risoluzione dei problemi

I seguenti argomenti descrivono gli errori comuni che possono verificarsi. Dove possibile, all'errore è stata associata una soluzione per fornire assistenza durante l'integrazione.

DLL Windows mancante

Sintomo:

DLL Windows mancante (MSVCP71.dll)

È stato rilevato che dopo che l'abilitazione della connessione di SiteMinder, JBoss ha generato un errore java relativo a un DLL mancante (MSVCP71.dll).

Nota: questo errore potrebbe non essere visualizzato se JBoss è in esecuzione come servizio. Se possibile, verificare la propria configurazione senza che JBoss sia in esecuzione come servizio.

Soluzione:

Procedere come descritto di seguito:

1. Individuare MSVCP71.dll sul Policy Server di SiteMinder, se in esecuzione su Windows.
2. Copiare questo DLL (MSVCP71.dll) nella cartella \Windows\system32.
3. Dopo avere collocato questo file nella posizione corretta, registrarlo nel sistema operativo.
4. Da una finestra di comando, eseguire il comando regsvr32. Se il file è stato caricato, il problema dovrebbe essere risolto.
5. Riavviare il server applicazioni.

Posizione del Policy Server di SiteMinder errata

Sintomo:

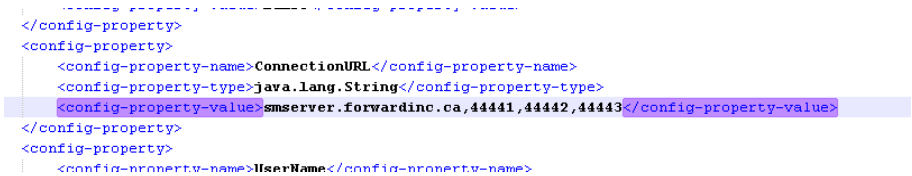
Posizione del Policy Server di SiteMinder errata.

Soluzione:

Nel file ra.xml si fa riferimento a una posizione errata e viene visualizzato il messaggio di errore "Cannot connect to policy server: xxx" (Impossibile connettersi al Policy Server: xxx).

Procedere come descritto di seguito:

1. Verificare il nome host fornito in ra.xml.



2. Nella proprietà ConnectionURL, specificare il nome host del Policy Server di SiteMinder. Utilizzare un FQN (nome completo).

Nome amministratore errato

Sintomo:

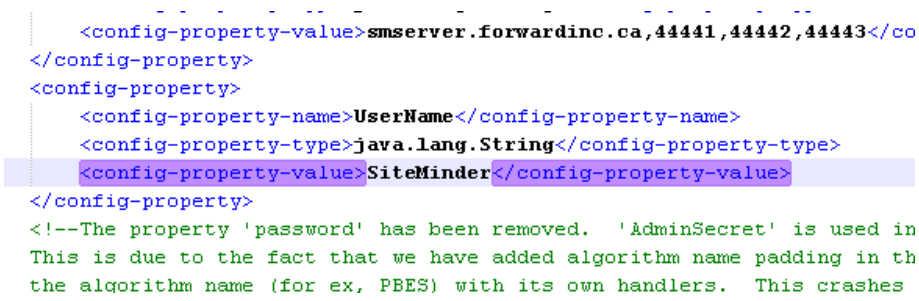
Nome amministratore errato

Soluzione:

Nel file ra.xml si fa riferimento a un amministratore errato e viene visualizzato il messaggio di errore "Unknown administrator" (Amministratore sconosciuto).

Procedere come descritto di seguito:

1. Controllare la proprietà UserName in ra.xml.



2. Nella proprietà UserName, specificare l'account utilizzato per comunicare con CA SiteMinder. Ad esempio, utilizzare l'account di SiteMinder (valore predefinito).

Segreto amministratore errato

Sintomo:

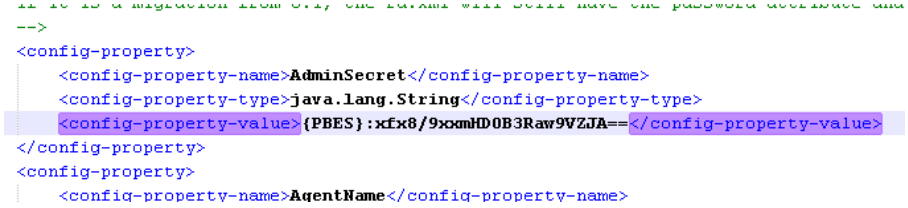
Segreto amministratore errato

Soluzione:

Nel file ra.xml viene utilizzato un segreto amministratore errato e viene visualizzato il messaggio di errore "Cannot connect to the policy server: Invalid credentials" (Impossibile connettersi al Policy Server: credenziali non valide).

Procedere come descritto di seguito:

1. Controllare la proprietà AdminSecret in ra.xml.




```
<config-property>
    <config-property-name>AdminSecret</config-property-name>
    <config-property-type>java.lang.String</config-property-type>
    <config-property-value>{PBES}:xfx8/9xxmHD0B3Raw9VZJA==</config-property-value>
</config-property>
<config-property>
    <config-property-name>AgentName</config-property-name>
```

2. Nella proprietà AdminSecret, specificare la password crittografata per il nome utente a cui si fa riferimento nella proprietà UserName.

Ulteriori informazioni:

Modifica di una password o di un segreto condiviso di SiteMinder (a pagina 358)

Nome agente errato

Sintomo:

Nome agente errato

Soluzione:

Nel file ra.xml viene utilizzato un nome agente errato e viene visualizzato il messaggio di errore "Cannot connect to the policy server: Failed to init Agent API: -1" (Impossibile connettersi al Policy Server: impossibile inizializzare l'API agente: -1).

Procedere come descritto di seguito:

1. Controllare la proprietà AgentName in ra.xml.

```
</config-property>
<config-property>
    <config-property-name>AgentName</config-property-name>
    <config-property-type>java.lang.String</config-property-type>
    <config-property-value>idmagent</config-property-value>
</config-property>
<config-property>
```

2. Specificare il nome dell'Agente 4.X creato durante la terza fase delle configurazioni di SiteMinder.

Segreto agente errato

Sintomo:

Segreto agente errato

Soluzione:

Nel file ra.xml viene utilizzato un segreto agente errato e viene visualizzato il messaggio di errore "Cannot connect to the policy server: Failed to init Agent API: -1" (Impossibile connettersi al Policy Server; impossibile inizializzare l'API agente: -1) con un errore del gestore crittografia precedente.

Procedere come descritto di seguito:

1. Controllare la proprietà AgentSecret in ra.xml.

```
<config-property>
    <config-property-name>AgentSecret</config-property-name>
    <config-property-type>java.lang.String</config-property-type>
    <config-property-value>{PBES}:xfx8/9xxmHD0B3Raw9VZJA==</config-property-value>
</config-property>
<config-property>
```

2. Specificare la password crittografata utilizzata durante la creazione di quell'agente.

Ulteriori informazioni:

Modifica di una password o di un segreto condiviso di SiteMinder (a pagina 358)

Nessun contesto utente in CA Identity Manager

Sintomo:

Nessun contesto utente in CA Identity Manager.

Se un utente prova ad accedere a CA Identity Manager senza un cookie SMSESSION, CA Identity Manager non può autenticare l'utente. In questo caso, è possibile attendersi un'interfaccia utente CA Identity Manager vuota.

Se il flusso di lavoro è abilitato per l'ambiente in uso, verrà visualizzato un errore simile a questo.

```
Exception during page display:

java.lang.IllegalArgumentException
        at com.netegrity.webapp.bean.WorkList.(WorkList.java:84)
        at com.netegrity.webapp.bean.WorkList.(WorkList.java:70)
        at com.netegrity.webapp.bean.WorkList.getConsoleWorkListFromRequest(WorkList.java:109)
        at com.netegrity.taglib.skin.TagUtilLocal.getWorkItems(TagUtilLocal.java:660)
        at com.netegrity.taglib.skin.TagUtilLocal.hasWorkItems(TagUtilLocal.java:846)
        at com.netegrity.taglib.skin.IfWorkItemsTag.doStartTag(IfWorkItemsTag.java:73)
        at idm_jsp.app.ca12.home_jsp._jspService(Unknown Source)
        at org.apache.jasper.runtime.HttpJspBase.service(HttpJspBase.java:70)
        at javax.servlet.http.HttpServlet.service(HttpServlet.java:803)
        at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:290)
        at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:206)
        at org.apache.catalina.core.ApplicationDispatcher.invoke(ApplicationDispatcher.java:654)
        at org.apache.catalina.core.ApplicationDispatcher.doInclude(ApplicationDispatcher.java:557)
        at org.apache.catalina.core.ApplicationDispatcher.include(ApplicationDispatcher.java:481)
        at org.apache.jasper.runtime.JspRuntimeLibrary.include(JspRuntimeLibrary.java:968)
        at idm_jsp.app.ca12.index_jsp._jspx_meth_skin_ifhomepage_0(Unknown Source)
        at idm_jsp.app.ca12.index_jsp._jspService(Unknown Source)
        at org.apache.jasper.runtime.HttpJspBase.service(HttpJspBase.java:70)
        at javax.servlet.http.HttpServlet.service(HttpServlet.java:803)
        at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:290)
        at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:206)
        at org.apache.catalina.core.ApplicationDispatcher.invoke(ApplicationDispatcher.java:654)
        at org.apache.catalina.core.ApplicationDispatcher.processRequest(ApplicationDispatcher.java:445)
        at org.apache.catalina.core.ApplicationDispatcher.doForward(ApplicationDispatcher.java:379)
        at org.apache.catalina.core.ApplicationDispatcher.forward(ApplicationDispatcher.java:292)
        at com.netegrity.webapp.filter.ConsolePageFilter.doFilter(ConsolePageFilter.java:521)
        at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:235)
        at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:206)
        at com.netegrity.webapp.page.jsf.FacesFilter.doFilter2(FacesFilter.java:180)
```

Soluzione:

Questo errore può essere causato da alcune situazioni, ma di solito è una delle seguenti:

- È stato eseguito un accesso diretto a CA Identity Manager.
- L'agente di SiteMinder nel proxy viene disabilitato (ovvero, nessun elemento è protetto e il cookie SMSESSION non viene creato).
- Il dominio di SiteMinder per l'ambiente di CA Identity Manager non è configurato correttamente.

Le prime due cause sono piuttosto semplici. Assicurarsi di essere instradati attraverso il server Web con l'agente Web completo abilitato. Tuttavia, se si sta passando attraverso il server Web e l'agente è abilitato, è necessario modificare il dominio.

Procedere come descritto di seguito:

1. Accedere all'interfaccia di amministrazione di SiteMinder.
2. Individuare il dominio di CA Identity Manager in uso e fare clic sui livelli per modificarlo. Fare clic sulla scheda Area autenticazione, quindi sulla prima area di autenticazione nell'elenco.
3. La posizione predefinita della barra è sotto l'area di autenticazione. Eliminarla.
4. Fare clic sulla regola in questa area di autenticazione.

   La risorsa effettiva predefinita per la regola è un asterisco "*".
5. Aggiungere la barra "/" prima dell'asterisco.

   La barra è stata spostata dall'area di autenticazione alla regola. La protezione è la stessa, ma in SiteMinder viene considerata in maniera diversa.

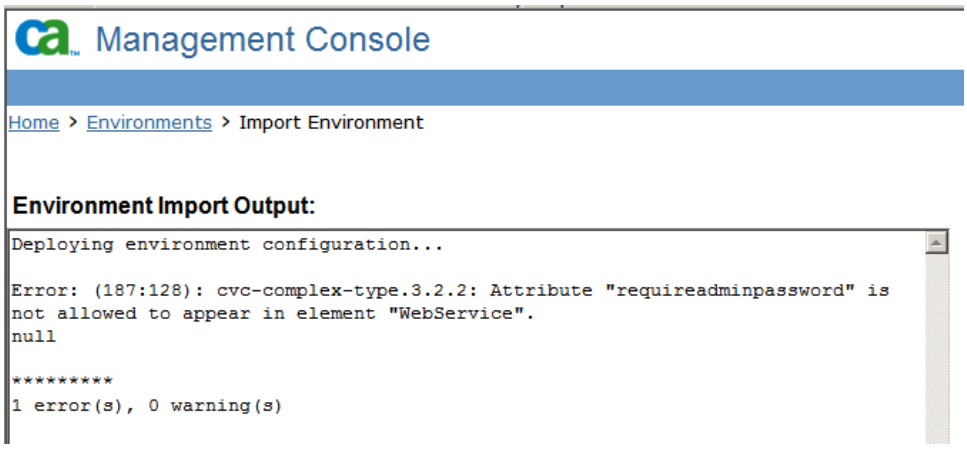
   Ora è possibile eseguire correttamente l'accesso a CA Identity Manager attraverso SiteMinder. Per convalidare la protezione adeguata, rivedere i registri dell'agente di SiteMinder.

Errore durante il caricamento degli ambienti

Sintomo:

Durante la reimportazione dell'ambiente in CA Identity Manager dopo l'integrazione con SiteMinder, viene visualizzato un errore relativo all'attributo requireadminpassword e all'elemento WebService.

Nota: questo problema può verificarsi anche quando SiteMinder non fa parte della distribuzione.



Soluzione:

Questo errore consente la distribuzione parziale dell'ambiente. La distribuzione parziale può creare elementi vuoti nell'archivio oggetti di CA Identity Manager. Correggere uno degli XML dell'ambiente ed eseguire nuovamente l'importazione.

Procedere come descritto di seguito:

1. Individuare il file .zip archiviato ed esplorarlo.
2. Creare una copia del file XXX_environment_settings.xml.
3. Modificare questo file e individuare l'elemento WebService.
4. Eliminare il tag "requireadminpassword="false."

   Nota: rimuovere il tag *e* il valore, non soltanto il valore.
5. Salvare le modifiche e collocare il file nuovamente nel file .zip.
6. Reimportare il file .zip dell'ambiente archiviato.

   Non è necessario eliminare l'ambiente creato dal tentativo non riuscito. La nuova importazione di un file corretto corregge gli errori del tentativo non riuscito.

Impossibile creare una directory o un ambiente di CA Identity Manager

Sintomo:

Non è possibile creare una directory o un ambiente di CA Identity Manager quando l'integrazione con SiteMinder è abilitata.

Soluzione:

Questo problema può essere causato da una voce mancante nel registro.

Verificare che la seguente impostazione di registro esista sul computer del Policy Server di SiteMinder:

- Solaris o Linux:

  Verificare che la voce seguente esista in sm.registry:
  ImsInstalled=8.0; REG_SZ

- Windows:

  Verificare che l'impostazione ImsInstalled=8.0; REG_SZ esista nella posizione seguente:
  HKLM\SOFTWARE\Netegrity\SiteMinder\CurrentVersion

  Nota: se il percorso del registro \Netegrity\SiteMinder\CurrentVersion non esiste, crearlo manualmente.

Se si modifica il registro, assicurarsi di riavviare il Policy Server perché le modifiche abbiano effetto.

Importante. Prima di modificare il registro, eseguire un backup completo del sistema.

L'utente non può accedere

Sintomo:

Un nuovo utente non riesce ad accedere a un ambiente con una password di testo non crittografato.

Soluzione:

Verificare che la seguente classificazione di dati non sia inclusa nella definizione dell'attributo password nel file di configurazione di directory (directory.xml):

<DataClassification name="AttributeLevelEncrypt"/>

In ambienti che includono i componenti seguenti, l'abilitazione della crittografia a livello di attributo impedisce agli utenti di accedere a:

- CA SiteMinder e
- Un database relazionale

Configurazione delle impostazioni dell'agente di CA Identity Manager

Quando CA Identity Manager è integrato con SiteMinder, in CA Identity Manager viene utilizzato un agente di CA Identity Manager incorporato per comunicare con il Policy Server di SiteMinder. Per ottimizzare le prestazioni, configurare le seguenti impostazioni di connessione per l'agente di CA Identity Manager.

1. Completare una delle operazioni indicate di seguito:
   - Se CA Identity Manager è in esecuzione su un server applicazioni WebSphere o WebLogic, modificare l'adattatore di risorse nel descrittore del connettore policyserver_rar nella console del server applicazioni.
   - Se CA Identity Manager è in esecuzione su un server applicazioni JBoss, aprire policyserver-service.xml da <JBoss_home>\server\default\deploy\iam_im.ear\policyserver_rar\META-INF.
2. Configurare le impostazioni nel seguente modo:

   ConnectionMax

   Imposta il numero massimo di connessioni al Policy Server, ad esempio, 20.

   ConnectionMin

   Imposta il numero minimo di connessioni al Policy Server, ad esempio, 2.

   ConnectionStep

   Imposta il numero di connessioni aggiuntive da aprire quando tutte le connessioni di agente sono in uso.

   ConnectionTimeout

   Specifica la durata (in secondi) dell'attesa dell'agente per connettersi a SiteMinder prima del timeout.
3. Riavviare il server applicazioni.

Configurazione della disponibilità elevata di SiteMinder

Se è stato creato un cluster del Policy Server di SiteMinder, è possibile configurare un cluster del server applicazioni per utilizzarlo per il bilanciamento del carico e il failover.

Procedere come descritto di seguito:

1. Modificare il file ra.xml in questa posizione:
   WebSphere:
   WAS_PROFILE/config/cells/*CELL_NAME*/applications/iam_im.ear/deployments/IdentityMinder/policyserver_rar/META-INF
   Jboss:*jboss_home*/server/all/deploy/iam_im.ear/policyserver_rar/META-INF
   WebLogic: *wl_domain*/applications/iam_im.ear/policyserver_rar/META-INF
2. Modificare questi elementi, che verranno spiegati nelle sezioni seguenti:
   - Impostazioni di connessione per il Policy Server
   - Il numero del Policy Server
   - La selezione di bilanciamento del carico o del failover per il cluster.
3. Ripetere queste fasi per ogni server di CA Identity Manager del cluster.
4. Riavviare il server applicazioni per rendere effettive le modifiche.

Nota: durante la creazione di una directory o di un ambiente di CA Identity Manager oppure durante la modifica delle impostazioni di directory o di ambiente, impostare FailoverServers e Failover di SiteMinder su false. In caso contrario, l'oggetto di directory potrebbe essere creato ma non replicato in tempo per essere utilizzato. Ad esempio, si crea una directory nel server 1. Quindi, si crea un attributo utilizzando l'ID oggetto di quella directory sul server 2, ma la seconda directory non esiste ancora. Si riceve un errore Oggetto non trovato.

Modifica delle impostazioni di connessione del Policy Server

Le informazioni di connessione del Policy Server devono rispecchiare il server primario per l'ambiente di produzione. Queste informazioni sono composte da ConnectionURL, dal nome utente e dalla password per l'account di amministratore di SiteMinder e dal nome e dal segreto condiviso dell'agente.

Nell'esempio seguente, i valori modificabili vengono mostrati in LETTERE MAIUSCOLE.

```
<config-property>
        <config-property-name>ConnectionURL</config-property-name>
   <config-property-type>java.lang.String</config-property-type>
        <config-property-
value>DEVELOPMENT.SEVERCOMPANY.COM,VALUE,VALUE,VALUE</config-
                property-value>
</config-property>
```

```
<config-property>
        <config-property-name>UserName</config-property-name>
   <config-property-type>java.lang.String</config-property-type>
        <config-property-value>SITEMINDER-ADMIN-NAME</config-property-
                value>
</config-property>

<config-property>
        <config-property-name>AdminSecret</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>ENCRYPTED-PASSWORD</config-
                property-value>
</config-property>
<config-property>
        <config-property-name>AgentName</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>DEVELOPMENT-AGENT-NAME</config-property-
                value>
</config-property>

<config-property>
        <config-property-name>AgentSecret</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>ENCRYPTED-AGENT-SECRET</config-
                property-value>
</config-property>
```

Nota: per i valori che richiedono testo crittografato, utilizzare lo strumento Password di CA Identity Manager. Per ulteriori informazioni, consultare la *Guida alla configurazione*.

Aggiunta di più Policy Server

Per aggiungere più Policy Server all'istanza di installazione di CA Identity Manager, modificare la voce FailoverServers nel file ra.xml.

Nota: includere il Policy Server primario e tutti i server di failover nella voce FailoverServers.

Per ciascun Policy Server, immettere un indirizzo IP e i numeri di porta per i servizi di autenticazione, autorizzazione e contabilità. Utilizzare un punto e virgola per separare voci, così come illustrato di seguito:

```
<config-property>
        <config-property-name>FailoverServers</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>
                172.123.123.123,44441,44442,44443;172.123.123.124,33331,
                33332,33333
        </config-property-value>
</config-property>
```

Selezione del bilanciamento del carico o del failover

Il comportamento predefinito di CA Identity Manager è l'utilizzo del bilanciamento del carico round-robin mediante i server identificati da ConnectionURL e FailoverServers. Il bilanciamento del carico si verifica se FailOver rimane impostato su false.

Per selezionare il failover, impostare FailOver su true:

```
<config-property>
        <config-property-name>FailOver</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>true</config-property-value>
</config-property>
```

Rimozione di SiteMinder da una distribuzione di CA Identity Manager esistente

Questa sezione fornisce istruzioni dettagliate per rimuovere CA SiteMinder da un ambiente di CA Identity Manager esistente.

Procedere come descritto di seguito:

Importante. Le informazioni di cronologia password non saranno accessibili dopo la migrazione.

1. Arrestare il server applicazioni.
2. Disabilitare il Policy Server nel file ra.xml che si trova in \iam_im.ear\policyserver.rar\META-INF impostando il valore config-property Attivo su false.
3. Modificare il file web.xml che si trova in \iam_im.ear\User_console.war/WEB-INF e impostare la proprietà FrameworkAuthFilter su Attivo = true.

   Nota: per WebSphere, il file web.xml si trova in *WebSphere_home*/AppServer/profiles/*Profile_name*/config/cells/*Cell_name*/applications/iam_im.ear/deployments/IdentityMinder/user_console.war/WEB-INF.

4. Avviare il server applicazioni.
5. (Solo WebSphere) Aggiornare l'oggetto policyServer nella console di amministrazione con lo stesso valore del file ra.xml.

Operazioni SiteMinder

Le sezioni seguenti illustrano la modalità di modifica delle funzionalità di SiteMinder, compresi i domini di criteri e gli schemi di autenticazione per supportare CA Identity Manager:

Raccolta delle credenziali utente mediante uno schema di autenticazione personalizzato (a pagina 340)

Modifica il metodo utilizzato da CA Identity Manager per raccogliere credenziali per gli utenti che provano ad accedere a un ambiente di CA Identity Manager.

Configurazione dei ruoli di accesso (a pagina 341)

Fornisce l'accesso a funzioni in un'applicazione.

Configurazione dell'URL LogOff (a pagina 356)

Previene l'accesso non autorizzato a un ambiente di CA Identity Manager applicando una disconnessione completa.

Aggiornamento di un alias nelle aree di autenticazione di SiteMinder (a pagina 357)

Aggiorna le aree di autenticazione che proteggono un ambiente di CA Identity Manager quando si modifica l'alias dell'ambiente.

Password di SiteMinder (a pagina 358)

Consente di modificare la password dell'account di amministratore che CA Identity Manager utilizza per comunicare con SiteMinder e il segreto condiviso per l'agente di SiteMinder che protegge un ambiente di CA Identity Manager.

Configurazione delle impostazioni dell'agente di CA Identity Manager (a pagina 335)

Ottimizza le prestazioni dell'agente di CA Identity Manager che comunica con il Policy Server di SiteMinder.

Utilizzo di diverse directory per l'autenticazione e l'autorizzazione (a pagina 360)

Consente agli amministratori con profili in una directory di gestire utenti in una directory diversa.

Miglioramento delle prestazioni delle operazioni di directory LDAP (a pagina 362)

Aumenta la velocità delle richieste di CA Identity Manager all'archivio utenti configurando SiteMinder per l'apertura di connessioni multiple alla stessa directory.

Raccolta delle credenziali utente mediante uno schema di autenticazione personalizzato

SiteMinder utilizza uno schema di autenticazione per raccogliere le credenziali utente e determinare l'identità di un utente al momento dell'accesso. Una volta che un utente viene identificato, in CA Identity Manager viene generata una console utente personalizzata sulla base dei privilegi dell'utente.

È possibile implementare uno schema di autenticazione di SiteMinder qualsiasi per proteggere un ambiente di CA Identity Manager.

Ad esempio, è possibile implementare un schema di autenticazione di moduli HTML che raccoglie le credenziali in un modulo HTML. Un modulo HTML consente di creare una pagina di accesso che può includere elementi di personalizzazione, quale ad esempio un logo aziendale, e di collegarsi alle pagine di registrazione automatica e di password dimenticata.

Nota: per informazioni sugli schemi di autenticazione, consultare la *CA SiteMinder Policy Server Configuration Guide*.

Procedere come descritto di seguito:

1. Accedere a una delle seguenti interfacce:
   - Per CA SiteMinder Web Access Manager r12 o successive, accedere all'interfaccia utente di amministrazione.
   - Per CA eTrust SiteMinder 6.0 SP5, accedere all'interfaccia utente del Policy Server.

   Nota: per informazioni sull'utilizzo di queste interfacce, consultare la documentazione per la versione di SiteMinder in uso.
2. Creare uno schema di autenticazione così come descritto nella *CA SiteMinder Policy Server Configuration Guide.*.
3. Modificare l'area di autenticazione che protegge l'ambiente di CA Identity Manager appropriato per utilizzare lo schema di autenticazione creato nella fase 1.

   Il formato del nome dell'area di autenticazione è il seguente:

   *Identity Manager-environment*_ims_realm

   Nota: se è stato configurato il supporto per le attività pubbliche, viene visualizzata un'area di autenticazione aggiuntiva, *Identity Manager-environment*_pub_realm. Quest'area di autenticazione utilizza uno schema di autenticazione anonimo per abilitare gli utenti sconosciuti a utilizzare le funzionalità di registrazione automatica e password dimenticata senza fornire credenziali. Non modificare gli schemi di autenticazione per queste aree di autenticazione.

Importazione di definizioni dei dati nel Policy Store

È possibile controllare l'accesso di un utente a funzioni dell'applicazione utilizzando i criteri di SiteMinder. L'installazione del Policy Server include le definizioni dei dati obbligatorie per consentire questo controllo. Importare il file IdmSmObjects.xdd da questa posizione:

siteminder_home\xps\dd

siteminder_home è il percorso di installazione del Policy Server.

Pianificazione dei ruoli di accesso

Per controllare l'accesso alle applicazioni, vengono creati ruoli e attività di accesso. Un'attività di accesso fornisce l'accesso a una funzione in un'applicazione. Un ruolo di accesso contiene una o più attività di accesso per una o più applicazioni. Se a un utente è stato assegnato un ruolo di accesso, l'utente può utilizzare le funzioni che esistono in quel ruolo.

Ruoli di accesso per l'accesso alle applicazioni fornisce ulteriori dettagli sull'obiettivo dei ruoli di accesso.

I ruoli di accesso richiedono la configurazione in Identity Manager e SiteMinder. Devono essere coinvolti due amministratori:

- Amministratore di Identity Manager: deve essere in grado di creare ruoli e attività di accesso in Identity Manager. I ruoli predefiniti di Manager di sistema e Manager del ruolo di accesso includono queste attività.
- Amministratore di SiteMinder: deve avere accesso all'intero ambito del sistema ed essere in grado di gestire oggetti di sistema e di dominio. Per ulteriori informazioni, consultare la guida *CA eTrust SiteMinder Policy Design* .

Nota: l'Interfaccia utente di Policy Design utilizza il termine *ambiente di Identity Manager* per riferirsi a un *ambiente di Identity Manager*. Inoltre, la documentazione di SiteMinder fornita con questo prodotto utilizza il termine *Identity Manager*. A partire da r8.1, il nuovo nome del prodotto è *Identity Manager*.

La procedura seguente delinea le fasi per creare un ruolo di accesso:

1. Un amministratore di Identity Manager con il ruolo di Manager del ruolo di accesso:
   a. Crea attività di accesso.
   b. Crea un ruolo di accesso.
   c. Comunica informazioni sui ruoli e le attività all'amministratore di SiteMinder.

2. Un amministratore di SiteMinder crea un criterio di controllo di accessi basato sui ruoli attraverso le seguenti azioni:

   a. Assegnazione di una directory utente associata a uno o più ambienti di Identity Manager a un dominio di criteri.

   b. Associazione di uno o più ambienti di Identity Manager al dominio di criteri della fase 1.

   c. Creazione di aree di autenticazione e regole nel dominio di criteri (se non esistono già). Le aree di autenticazione e le regole dovrebbero corrispondere alle risorse a cui i ruoli di accesso concederanno l'accesso.

   d. Creazione di criteri e loro associazione ai ruoli dell'ambiente di Identity Manager.

   e. (facoltativo) Specificazione delle risposte che forniscono informazioni sui diritti alle risorse protette.

   Per istruzioni sulle fasi precedenti, consultare la guida *CA eTrust SiteMinder Policy Design*.

Abilitazione di ruoli di accesso per l'uso con SiteMinder

Per utilizzare i ruoli di accesso con CA SiteMinder, CA Identity Manager rispecchia tutti gli oggetti nell'archivio oggetti di CA Identity Manager correlati ai ruoli di accesso nell'archivio criteri di SiteMinder. Per abilitare questa azione, configurare una proprietà nella console di gestione di CA Identity Manager.

Per abilitare i ruoli di accesso all'uso con SiteMinder

1. Aprire la console di gestione.
2. Selezionare Ambiente, *Your Environment (Ambiente personale)*, Impostazioni avanzate, Varie.
3. Aggiungere una nuova proprietà fornendo le seguenti informazioni:
   - Nel campo Proprietà, immettere quanto segue:

     EnableSMRBAC
   - Nel campo Valore, immettere quanto segue:

     true

4. Fare clic su Aggiungi. Quindi fare clic su Salva.

   Viene visualizzato un messaggio che indica che l'ambiente deve essere riavviato.

5. Fare clic su Riavvia ambiente.

   In CA Identity Manager vengono ora supportati i ruoli e le attività di accesso per l'utilizzo in CA SiteMinder.

Una volta abilitati i ruoli di accesso all'utilizzo in CA SiteMinder, occorre notare quanto segue:

- Se sono stati utilizzati ruoli di accesso in CA Identity Manager r8x, è necessario eseguire una fase di migrazione aggiuntiva per gestire quei ruoli di accesso nella versione attuale di CA Identity Manager. Per ulteriori informazioni, consultare la *Guida all'aggiornamento*.
- Per disabilitare il supporto per i ruoli di accesso in SiteMinder, eliminare gli oggetti ruolo e attività di accesso di CA Identity Manager dal Policy Store di SiteMinder. Quindi, rimuovere la proprietà EnableSMRBAC dall'elenco Miscellaneous Properties (Proprietà varie) e riavviare l'ambiente.

Aggiunta di attività di accesso al ruolo di amministrazione

Per impostazione predefinita, le attività di Attività di accesso non vengono visualizzate nella scheda Ruoli e attività, pertanto è necessario aggiungere le Attività di accesso al ruolo di amministrazione dell'utente che ha effettuato l'accesso.

Procedere come descritto di seguito:

1. Accedere all'account di CA Identity Manager con un ruolo che include un'attività per la creazione dei ruoli di accesso.
2. Fare clic su Ruoli e attività, Modifica ruolo di amministrazione.
3. Selezionare il ruolo di amministrazione dell'utente che ha effettuato l'accesso.
4. Fare clic sulla scheda Attività, nel campo Filtra per categoria, Select Roles (Seleziona ruoli) e Attività dall'elenco a discesa.
5. Selezionare Crea attività di accesso dall'elenco a discesa Aggiungi attività.
6. Fare clic su Inoltra.

Creazione di un'attività di accesso

Un'attività di accesso è una azione singola che un utente può eseguire in un'applicazione aziendale, come ad esempio la generazione di un ordine di acquisto in un'applicazione finanziaria. Gli utenti possono eseguire quell'azione quando viene loro assegnato un ruolo di accesso che include l'attività di accesso.

Importante. Per creare un'attività di accesso, è necessario aggiungere le attività di accesso (a pagina 343) al ruolo di amministrazione dell'utente che ha effettuato l'accesso.

Procedere come descritto di seguito:

1. Selezionare Ruoli e attività, Attività di accesso, Crea attività di accesso.
2. Selezionare una delle seguenti opzioni:
   - Crea un'attività di accesso
   - Crea una copia di un'attività di accesso.
3. Completare questi campi:

   Nome

   Un nome univoco che è possibile assegnare all'attività, come Genera ordine di acquisto.

   Tag

   Un tag univoco per l'attività. Questo tag deve iniziare con una lettera o un carattere di sottolineatura e deve contenere solo lettere, numeri o caratteri di sottolineatura.

   Descrizione

   Nota facoltativa relativa allo scopo dell'attività.

   ID applicazione

   Un identificatore per un'applicazione, quale ad esempio il nome dell'applicazione, associato all'attività. L'ID applicazione non può contenere spazi o caratteri non alfanumerici.

   Annotare questo ID in quanto verrà richiesto al momento dell'abilitazione del ruolo in SiteMinder.
4. Per completare l'attività di accesso, fare clic su Invia.

Creazione di un ruolo di accesso

Un ruolo di accesso contiene attività di accesso, le quali forniscono l'accesso alle funzioni in un'applicazione. Ad esempio, un ruolo può contenere attività che abilitano i membri del ruolo a inserire un ordine in un'applicazione di acquisto e ad aggiornare le quantità in un'applicazione di controllo dell'inventario.

Completare le seguenti fasi per creare un ruolo di accesso:

1. Inizio della creazione del ruolo di accesso. (a pagina 345)
2. Definizione delle proprietà di base per il ruolo di accesso nella scheda Profilo. (a pagina 345)
3. Selezione delle attività di accesso per il ruolo. (a pagina 346)
4. Definizione dei criteri membri per il ruolo. (a pagina 347)
5. Definizione dei criteri di amministrazione per il ruolo. (a pagina 347)
6. Definizione dei criteri di titolarità per il ruolo. (a pagina 348)

Inizio della procedura di creazione del ruolo di accesso

1. Accedere ad Identity Manager utilizzando un account con un ruolo associato ad attività finalizzate alla creazione di ruoli di accesso.
2. Fare clic su Ruoli di accesso, Crea ruolo di accesso.

   Scegliere le opzioni desiderate per creare un nuovo ruolo oppure una copia di un ruolo esistente. Se si seleziona Copia, cercare il ruolo desiderato.
3. Continuare con la sezione Definizione del profilo di un ruolo di accesso.

Definizione del profilo di un ruolo di accesso

Per definire il profilo di un ruolo di accesso

1. Immettere un nome ed una descrizione, quindi aggiungere eventuali attributi personalizzati definiti per il ruolo.

   Nota: nella scheda Profilo è possibile definire attributi personalizzati con i quali specificare informazioni aggiuntive sui ruoli di accesso. Tali informazioni aggiuntive sono utili per facilitare le ricerche di ruoli in ambienti che presentano un numero elevato di ruoli.
2. Selezionare Attivato per rendere disponibile il ruolo subito dopo la creazione.
3. Continuare con la sezione Definizione dei criteri membri per un ruolo di accesso.

Selezione delle attività di accesso per il ruolo

Nella scheda Attività:

1. Selezionare le attività da includere in questo ruolo. Innanzitutto selezionare le applicazioni, quindi l'attività. È possibile includere attività da diverse applicazioni.

   Nota: se un altro ruolo dispone delle attività necessarie, fare clic su Copia attività da un altro ruolo. È possibile modificare l'elenco visualizzato.

   Durante la creazione di un ruolo o un'attività, vengono visualizzate le icone per aggiungere, modificare e rimuovere elementi:

   Procedere o selezionare l'elemento corrente da visualizzare o modificare.

   Se JavaScript è disabilitato, premere il pulsante di avanzamento per effettuare una selezione da un elenco a discesa.

   Tornare indietro o annullare una selezione precedente.

   Inserire un elemento, quali un'attività o una regola.

   Eliminare l'attività corrente o, in una regola, l'espressione che segue.

   Spostare l'elemento corrente in alto nell'elenco.

   Spostare l'elemento corrente in basso nell'elenco.

2. Procedere con la sezione successiva, Definizione dei criteri membri per un ruolo di accesso.

Definizione dei criteri membri per un ruolo di accesso

Un criterio membri definisce una regola membri e regole di ambito per un ruolo. È possibile definire numerosi criteri membri per un ruolo. Per ciascun criterio, gli utenti che soddisfanno la condizione nella regola membri dispongono dell'ambito per utilizzare il ruolo definito nel criterio.

Procedere come descritto di seguito:

1. Fare clic sulla scheda Membri.
2. Selezionare Aggiungi per definire i criteri membri.
3. (Facoltativo) Nella pagina Criterio membri definire una regola membri per chi deve essere in grado di utilizzare questo ruolo.

   La definizione di una regola membri assegna automaticamente il ruolo agli utenti che corrispondono ai criteri nel criterio membri.

   Nota: definire i criteri membri che utilizzano solamente attributi di directory, ad esempio: title=Manager. Se si definiscono criteri membri che fanno riferimento agli oggetti non archiviati nella directory utente, quali i ruoli di amministrazione, SiteMinder non è in grado di risolvere il riferimento.
4. Verificare che il criterio membri venga visualizzato nella scheda Membri.

   Per modificare un criterio, fare clic sulla freccia a sinistra. Per rimuoverlo, fare clic sull'icona con il segno meno.
5. Nella scheda Membri, abilitare la casella di controllo Gli amministratori possono aggiungere e rimuovere i membri di questo ruolo.

   Una volta abilitata questa funzionalità, definire Aggiungi azione e Azione di rimozione. Queste azioni definiscono le operazioni eseguite quando un utente viene aggiunto o rimosso come membro del ruolo.

Definizione dei criteri di amministrazione per un ruolo di accesso

Un criterio di amministrazione definisce le regole di amministrazione, le regole di ambito e i privilegi di amministratore per un ruolo. È possibile definire numerosi criteri di amministrazione per un ruolo. Ciascun criterio indica che se un amministratore soddisfa la condizione nella regola di amministrazione disporrà dei privilegi di amministratore e dell'ambito definiti per il criterio.

Procedere come descritto di seguito:

1. Selezionare la scheda Amministratori per il ruolo di accesso.
2. Se si desidera rendere disponibile l'opzione Gestione amministratori, selezionare la casella di controllo Gli amministratori possono aggiungere e rimuovere gli amministratori di questo ruolo.

   Una volta abilitata questa funzionalità, definire le azioni da eseguire quando un utente viene aggiunto o rimosso come amministratore del ruolo.

3. Sulla scheda Amministratori, aggiungere i criteri di amministrazione che includono le regole di amministrazione e di ambito e i privilegi di amministratore. Ciascun criterio ha bisogno almeno di un privilegio (Gestione membri o Gestione amministratori).

   È possibile aggiungere molti criteri di amministrazione con regole e privilegi differenti per gli amministratori che soddisfano la regola.

   Nota: definire i criteri di amministrazione che utilizzano solamente attributi di directory, ad esempio: title=Manager. Se si definiscono criteri membri che fanno riferimento agli oggetti non archiviati nella directory utente, quali i ruoli di amministrazione, non sarà possibile risolvere il riferimento in SiteMinder.

4. Per modificare un criterio, fare clic sulla freccia a sinistra. Per rimuoverlo, fare clic sull'icona con il segno meno.

5. Procedere con la sezione successiva, Definizione delle regole di titolarità per un ruolo di accesso.

Definizione delle regole proprietari per un ruolo di accesso

Una regola di titolarità stabilisce l'utente che può modificare un ruolo. È possibile definire numerose regole di titolarità per un ruolo.

Procedere come descritto di seguito:

1. Selezionare la scheda Titolari per il ruolo di accesso.

2. Definire le regole di titolarità, che determinano quali utenti possono modificare il ruolo.

   Nota: definire regole di titolarità che utilizzano solo attributi di directory, ad esempio: title=Manager. Se si definiscono regole di titolarità che fanno riferimento agli oggetti non archiviati nella directory utente come ruoli di amministrazione, non sarà possibile risolvere il riferimento in SiteMinder.

3. Fare clic su Invia.

   Un messaggio sembra indicare che l'attività è stata inviata. Può verificarsi un ritardo momentaneo prima che un utente possa utilizzare il ruolo.

Attivazione di ruoli di accesso in SiteMinder

Un amministratore di SiteMinder associa ruoli a criteri di protezione che definiscono le modalità di interazione degli utenti con le risorse. I criteri possono collegare i seguenti oggetti:

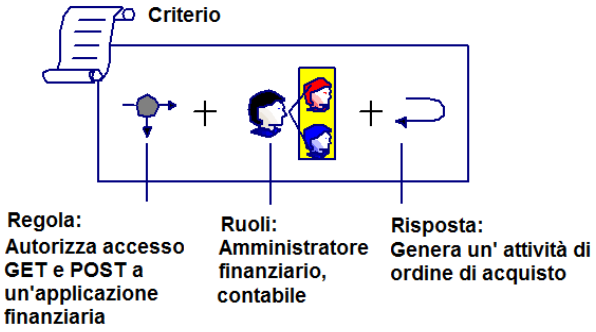
- Utenti e gruppi di utenti: identificare un set di utenti interessati da un criterio.
- Ruoli: identificano gli utenti a cui è stato assegnato un insieme di privilegi in Identity Manager.
- Regole: identificano una risorsa e le azioni consentite o negate per la risorsa. La risorsa è generalmente un URL, un'applicazione o uno script.

- Risposte: determinano una reazione a una regola. Quando una regola viene attivata, le risposte vengono restituite a un agente SiteMinder.

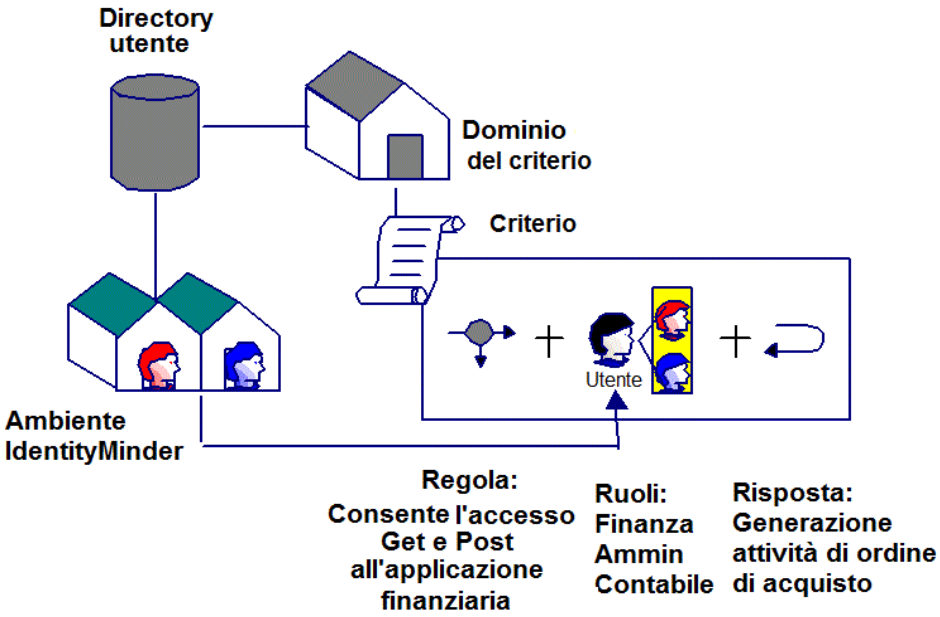
  Identity Manager utilizza le risposte di SiteMinder per fornire informazioni specifiche su ruoli e attività a una risorsa protetta.

È possibile associare i criteri di SiteMinder a utenti, a ruoli o a utenti *e* ruoli. Quando un utente o un membro del ruolo tenta di accedere a una risorsa protetta, SiteMinder utilizza le informazioni nel criterio per decidere se concedere l'accesso e attivare le risposte.

La seguente figura illustra la relazione degli oggetti di criterio in un criterio basato su ruoli.



I criteri di SiteMinder vengono creati in domini di criterio, che legano logicamente le directory utente a risorse protette. La seguente figura illustra la relazione degli oggetti di criterio in un criterio basato su ruoli.



Per fornire i diritti dell'utente a un'applicazione protetta, un amministratore di SiteMinder associa una regola nel criterio dell'applicazione a una risposta. La risposta contiene un attributo di risposta generato da SiteMinder che recupera le informazioni sui diritti da Identity Manager.

Quando SiteMinder autorizza un membro del ruolo per una risorsa protetta, si verificano i seguenti eventi:

1. La regola del criterio viene eseguita in SiteMinder e attiva la risposta associata.
2. Il Policy Server ottiene da Identity Manager informazioni sui diritti da includere in una risposta.
3. Il Policy Server trasferisce l'attributo di risposta all'agente Web.
4. L'agente Web rende disponibili all'applicazione le informazioni sui diritti come variabile di intestazione HTTP o cookie.

Attributi di risposta generati da SiteMinder

Identity Manager trasferisce le informazioni sui diritti alle applicazioni attraverso le risposte dell'agente Web di SiteMinder. Queste risposte contengono variabili di intestazione HTTP negli attributi di risposta, i quali possono essere utilizzati dall'applicazione per determinare i privilegi di accesso di un utente. Le risposte vengono incluse nei criteri di SiteMinder, che determinano le modalità di interazione degli utenti con una risorsa protetta.

Gli amministratori di SiteMinder possono configurare una risposta che include due tipi di attributi di risposta per trasferire informazioni a un'applicazione:

- SM_USER_APPLICATION_ROLES[:*application id*]: restituisce un elenco di ruoli assegnati a un utente
- SM_USER_APPLICATION_TASKS[:*application id*]: restituisce un elenco di attività che possono essere eseguite da un utente sulla base dei ruoli a lui assegnati

L'ID applicazione limita l'insieme di ruoli e attività necessari a un'applicazione specifica. Ad esempio, se si crea il seguente attributo di risposta:

SM_USER_APPLICATION_ROLES:Finance_application

SiteMinder restituisce i ruoli che hanno attività nell'applicazione finanziaria all'agente Web, il quale trasferisce quindi le informazioni all'applicazione finanziaria.

Nota: l'*ID applicazione* fornito dovrebbe corrispondere a un *ID applicazione* fornito quando è stato utilizzato Crea attività di accesso in Identity Manager. Se l'attività non è stata ancora creata, l'ID applicazione può essere qualsiasi nome a scelta, ma non può contenere alcuno spazio, né caratteri non alfanumerici.

È possibile specificare più ID applicazioni in un elenco delimitato da virgole per restituire l'insieme di ruoli e attività da più applicazioni in un singolo attributo di risposta. Ad esempio, per restituire l'elenco di ruoli di un utente nelle applicazioni finanziarie e per gli acquisti, specificare quanto segue:

SM_USER_APPLICATION_ROLES:Finance, Purchasing

Elenco di controllo per l'attivazione dei ruoli di accesso in SiteMinder

Nota: le seguenti fasi presuppongono che l'applicazione a cui si applica il ruolo di accesso che si sta creando venga già protetta da SiteMinder. Se si sta creando un ruolo di accesso per un'applicazione non protetta da SiteMinder, consultare la *CA eTrust SiteMinder Policy Design* per istruzioni sulla configurazione dell'applicazione in SiteMinder.

✓	Passaggio	Argomento
	1. Nell'interfaccia utente del Policy Server, assegnare la directory utente associata all'ambiente di Identity Manager a un dominio di criterio.	*CA eTrust SiteMinder Policy Design*
	2. Aggiungere l'ambiente di Identity Manager al dominio di SiteMinder che protegge l'applicazione alla quale si applica il ruolo di accesso.	*CA eTrust SiteMinder Policy Design*
	3. Nel dominio di criterio, creare aree di autenticazione e regole (se non esistono già) che corrispondano alle risorse alle quali il ruolo di accesso concederà l'accesso.	*CA eTrust SiteMinder Policy Design*
	4. Creare una risposta per trasferire le informazioni sui diritti alla risorsa.	Creazione di una risposta di SiteMinder (a pagina 353)
	5. Creare un criterio e associarlo a: ■ Il ruolo creato in Identity Manager ■ Le aree di autenticazione e le regole create nella fase 2. ■ Le risposte create nella fase 4.	*CA eTrust SiteMinder Policy Design*

Aggiunta di ambienti di Identity Manager a un dominio di criterio

Per abilitare il supporto dei ruoli di accesso in SiteMinder, associare un ambiente di CA Identity Manager a una directory utente e a un dominio di criterio in SiteMinder.

Nota: *prima* di poter aggiungere l'ambiente di CA Identity Manager al dominio di criterio, aggiungere a quest'ultimo l'archivio utenti associato all'ambiente di CA Identity Manager.

Per aggiungere un ambiente di CA Identity Manager a un dominio di criterio

1. Nella finestra di dialogo Policy Domain (Dominio di criterio) nell'interfaccia utente del Policy Server, aggiungere l'archivio utenti associato all'ambiente di CA Identity Manager a un dominio di criterio nel seguente modo:
   a. Selezionare la scheda Directory utente.
   b. Dalla casella di elenco a discesa nella parte inferiore della scheda, selezionare la directory utente da includere nel dominio di criterio.
   c. Fare clic sul pulsante Aggiungi.

      L'interfaccia utente del Policy Server aggiunge la directory all'elenco visualizzato nella scheda Directory utente.
   d. Fare clic su Applica.
2. Aggiungere l'ambiente di CA Identity Manager al dominio di criterio nel seguente modo:
   a. Selezionare la scheda CA Identity Manager Environments (Ambienti di CA Identity Manager).
   b. Selezionare l'ambiente di CA Identity Manager che si desidera associare al dominio di criterio dall'elenco a discesa nella parte inferiore della scheda.
   c. Fare clic su Aggiungi.

      L'interfaccia utente del Policy Server aggiunge la selezione all'elenco di ambienti di CA Identity Manager in alto nella scheda.
3. Fare clic su OK per salvare le selezioni e chiudere la finestra di dialogo.

   Gli ambienti di CA Identity Manager selezionati sono disponibili al momento della creazione dei criteri.

Creazione di una risposta di SiteMinder

1. Accedere all'interfaccia utente del Policy Server.
2. A seconda dei propri privilegi amministrativi, effettuare una delle seguenti azioni:
   - Se si dispone del privilegio Gestisci oggetti di sistema e di dominio:
     a. Nel riquadro Oggetto, fare clic sulla scheda Domini.
     b. Selezionare il dominio di criterio a cui si desidera aggiungere una risposta.
   - Se si dispone del privilegio Manage Domain Objects (Gestisci oggetti di dominio), selezionare il dominio di criterio a cui si desidera aggiungere una risposta nel riquadro Oggetto.
3. Dalla barra dei menu, selezionare Modifica, <nome dominio>, Crea risposta.

   Si apre la finestra di dialogo Risposta di SiteMinder (consultare la finestra di dialogo Risposta).
4. Immettere un nome e una descrizione per la nuova risposta.

5. Nella casella di gruppo Tipo di agente, selezionare il pulsante di opzione SiteMinder.
6. Selezionare l'opzione dell'agente Web nell'elenco a discesa della casella del gruppo Tipo di agente e fare clic su Applica per salvare le modifiche.
7. Fare clic su Crea.

   Si apre la finestra di dialogo Response Attribute Editor (Editor attributi di risposta) di SiteMinder.
8. Dall'elenco a discesa Attributo, selezionare l'attributo di risposta WebAgent-HTTP-Header-Variable.
9. Nella scheda Attribute Setup (Configurazione attributo), selezionare il pulsante di opzione Attributo utente.
10. Nel campo Variabile, immettere il nome della variabile che verrà trasferita all'applicazione.

    Ad esempio, se si specifica la variabile TASKS, all'applicazione viene restituita la seguente intestazione:

    HTTP_TASKS
11. Nel campo Nome attributo, specificare l'attributo di risposta nel seguente modo:
    - SM_USER_APPLICATION_ROLES[:*application id1, application_id2, ...application_idn*]: restituisce un elenco di ruoli assegnati ad un utente
    - SM_USER_APPLICATION_TASKS[:*application id1, application_id2, ...application_idn*]

    Per ulteriori informazioni, consultare la sezione Attributi di risposta generati da SiteMinder (a pagina 351).
12. Fare clic su OK per salvare le modifiche e tornare alla finestra Amministrazione di SiteMinder.

Aggiunta di ruoli a un criterio di SiteMinder

Quando un utente a cui è stato assegnato il ruolo di accesso appropriato prova ad accedere a una risorsa protetta, il Policy Server di SiteMinder verifica che all'utente sia stato assegnato il ruolo di accesso, quindi attiva le regole incluse nel criterio per verificare se l'utente è autorizzato ad accedere alla risorsa.

Per aggiungere ruoli di accesso a un criterio di SiteMinder

1. Nella finestra di dialogo Criterio di SiteMinder, fare clic sulla scheda Utenti.

   La scheda Utenti contiene schede per ciascuna directory utente e ciascun ambiente di CA Identity Manager inclusi nel dominio di criterio.
2. Selezionare l'ambiente di CA Identity Manager che contiene i ruoli che si desidera aggiungere al criterio.

3. Fare clic sul pulsante Add/Remove (Aggiungi/Rimuovi).

   Si apre la finestra di dialogo SiteMinder Policy Identity Manager Role (Ruolo di Identity Manager al criterio di SiteMinder).

4. Per aggiungere ruoli al criterio, selezionare una voce dall'elenco di Available Members (Membri disponibili) e spostarla nell'elenco Current Members (Membri correnti).

5. Fare clic su OK per salvare le modifiche e tornare alla finestra di dialogo Criterio di SiteMinder.

Esclusione di ruoli da un criterio

Oltre a utilizzare ruoli di accesso per concedere l'accesso ad applicazioni, è anche possibile utilizzare i ruoli di accesso per impedire ai membri di ruoli di accesso di accedere a un'applicazione. Per impedire ai membri del ruolo di accesso di accedere a un'applicazione, escludere i ruoli dai criteri di SiteMinder. Quando un utente a cui è stato assegnato il ruolo di accesso escluso in CA Identity Manager prova ad accedere a una risorsa protetta, il Policy Server verifica l'esclusione del ruolo di CA Identity Manager all'utente assegnato. A seguito della verifica, blocca l'accesso alla risorsa.

Procedere come descritto di seguito:

1. Nella finestra di dialogo SiteMinder Policy (Criterio di SiteMinder), fare clic sulla scheda Utenti.

   La scheda Utenti contiene schede per ciascuna directory utente e ciascun ambiente di CA Identity Manager inclusi nel dominio di criterio.

2. Fare clic sull'ambiente di CA Identity Manager che contiene i ruoli che si desidera escludere dal criterio.

3. Fare clic sul pulsante Add/Remove (Aggiungi/Rimuovi).

   Si apre la finestra di dialogo SiteMinder Policy CA Identity Manager Role (Ruolo di CA Identity Manager al criterio di SiteMinder).

4. Per aggiungere ruoli al criterio, selezionare una voce dall'elenco Available Members (Membri disponibili) e fare clic sul pulsante con la freccia a sinistra che punta all'elenco Current Members (Membri correnti).

   La procedura contraria rimuove i ruoli dall'elenco di Current Members (Membri correnti).

5. Nell'elenco Current Members (Membri correnti), selezionare i ruoli da escludere, quindi fare clic sul pulsante Escludi sotto l'elenco.

   A sinistra dei ruoli esclusi, viene visualizzato un cerchio rosso con una barra.

6. Fare clic su OK per salvare le modifiche e tornare alla finestra di dialogo Criterio di SiteMinder.

Configurazione dell'URI LogOff

Per proteggere un ambiente di CA Identity Manager, configurare l'agente Web di SiteMinder che protegge l'ambiente per concludere una sessione dell'utente dopo la sua disconnessione da CA Identity Manager.

L'agente Web conclude una sessione utente eliminando la sessione di SiteMinder e i cookie di autenticazione del browser Web e istruendo il Policy Server di rimuovere qualsiasi informazione di sessione.

Per concludere la sessione di SiteMinder, configurare la funzionalità di disconnessione nel campo LogOffURI nell'oggetto Configurazione agente per l'agente di SiteMinder che protegge l'ambiente di CA Identity Manager.

Note:

- Un agente di SiteMinder ha un URI LogOff. Tutte le applicazioni protette dall'agente utilizzano la stessa pagina di disconnessione.
- Quando si configurano pagine di disconnessione personalizzate nella console di gestione, così come descritto in Configurazione di pagine di disconnessione, CA Identity Manager invia la richiesta di disconnessione alla pagina di disconnessione personalizzata *e* all'URI LogOff. Tuttavia, in CA Identity Manager l'utente visualizza solamente la pagina di disconnessione personalizzata.

Procedere come descritto di seguito:

1. Accedere a una delle seguenti interfacce:
   - Per CA SiteMinder versione 12 o successiva, accedere all'interfaccia di amministrazione.
   - Per CA eTrust SiteMinder 6.0 SP5, accedere all'interfaccia utente del Policy Server.

   Nota: per informazioni sull'utilizzo di queste interfacce, consultare la documentazione relativa alla versione di SiteMinder in uso.
2. Modificare la proprietà #LogOffUri nell'oggetto Configurazione agente per l'agente che protegge l'ambiente di CA Identity Manager nel seguente modo:
   - Rimuovere il segno del cancelletto (#)
   - Nel campo Valore, specificare l'URI seguente:

     /iam/im/logout.jsp

   Nota: selezionare un oggetto Configurazione agente quando si installa l'agente Web. Per ulteriori informazioni, consultare la *CA SiteMinder Web Access Manager Policy Server Installation Guide*.
3. Salvare le modifiche.
4. Riavviare il server Web.

Alias nelle aree di autenticazione di SiteMinder

Un *alias* è una stringa univoca che viene aggiunta all'URL per accedere a un ambiente di CA Identity Manager. Ad esempio, quando l'alias di un ambiente è *employees* (dipendenti), l'URL per accedere a quell'ambiente è il seguente:

`http://myserver.mycompany.org/iam/im/employees`

myserver.mycompany.org

Definisce il nome di dominio completo del server su cui è installato CA Identity Manager.

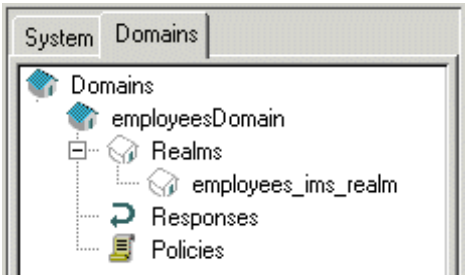
Specificare almeno un alias quando si crea un ambiente di CA Identity Manager nella console di gestione (si può specificare anche un alias pubblico).

In SiteMinder viene utilizzato il nome dell'ambiente per nominare gli oggetti che lo proteggono. Ad esempio, quando si specifica il nome *employees* (dipendenti), in SiteMinder vengono creati oggetti denominati *employeesobject_type*.

object_type

Definisce l'oggetto di SiteMinder, come ad esempio employees_ims_realm.

L'illustrazione seguente mostra due degli oggetti creati da SiteMinder:



Aggiornamento di un alias nelle aree di autenticazione di SiteMinder

Se si modifica l'alias protetto o pubblico nella console di gestione, in CA Identity Manager viene effettuato un tentativo di aggiornamento dei nomi alias nel Policy Server. Se non è possibile aggiornare i nomi in CA Identity Manager, è possibile aggiornarli manualmente in una delle interfacce seguenti:

- Per CA SiteMinder Web Access Manager versione 12 o successiva, utilizzare l'interfaccia di amministrazione.
- Per CA eTrust SiteMinder 6.0 SP5, utilizzare l'interfaccia utente del Policy Server.

Procedere come descritto di seguito:

1. Individuare le aree di autenticazione per l'ambiente di CA Identity Manager.

   Queste aree di autenticazione vengono create automaticamente (insieme ad altri oggetti di SiteMinder obbligatori) quando CA Identity Manager viene integrato con SiteMinder.

   Le aree di autenticazione utilizzano la seguente convenzione di denominazione:

   - *Identity Manager-environment*_ims_realm: protegge la console utente.
   - *Identity Manager-environment*_pub_realm: consente il supporto per le attività pubbliche, come ad esempio le attività di registrazione automatica e password dimenticata. Quest'area di autenticazione viene visualizzata solamente se è stato configurato un alias pubblico.

     Nota: se si sta utilizzando l'interfaccia utente del Policy Server per modificare l'area di autenticazione, individuare innanzitutto il dominio di criterio (*Identity Manager-environment*Domain) per l'ambiente di CA Identity Manager. Le aree di autenticazione si trovano sotto il dominio.

2. Modificare la risorsa per l'area di autenticazione nel seguente modo:

   /iam/im/*new_alias*

   Non rimuovere il /iam/im/ che precede l'alias nel filtro di risorsa.

3. Salvare le modifiche.

Nota: Modify CA Identity Manager Properties (Modifica proprietà di CA Identity Manager) fornisce istruzioni sulla modifica dell'alias nella console di gestione.

Modifica di una password o di un segreto condiviso di SiteMinder

Quando si installano le estensioni di CA Identity Manager al Policy Server, fornire la password per l'account di amministratore di SiteMinder utilizzata in CA Identity Manager per comunicare con il Policy Server.

È possibile modificare la password, tuttavia la password deve essere crittografata. Per crittografare una password, utilizzare lo strumento Password fornito con CA Identity Manager.

Nota: prima di modificare la password di SiteMinder, assicurarsi che la variabile JAVA_HOME sia stata definita per l'ambiente.

Procedere come descritto di seguito:

1. Crittografare la password nel seguente modo:
   a. Dalla riga di comando, accedere a *admin_tools*\PasswordTool, dove *admin_tools* è la posizione di installazione degli strumenti di amministrazione, come illustrato negli esempi seguenti:
      - **Windows:** C:\Programmi\CA\Identity Manager\IAM Suite\Identity Manager\tools\PasswordTool
      - **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools/PasswordTool
   b. Digitare il seguente comando:

      pwdtools *new_password*

      In questo comando, *new_password* è la password da crittografare.

      Nota: per informazioni sulle opzioni per l'utilità pwdtools, immettere il seguente comando:

      pwdtools help
   c. Copiare la password crittografata.
2. Completare la fase rilevante nel seguente modo:
   - Se CA Identity Manager è in esecuzione su un server applicazioni WebLogic, eseguire le seguenti attività:
     a. Nella console di WebLogic, modificare l'adattatore di risorse di WebLogic nel descrittore del connettore di policyserver_rar.
     b. Aggiungere la password crittografata come valore della proprietà Password.
   - Se CA Identity Manager è in esecuzione su un server applicazioni JBoss, eseguire le seguenti attività:

     a. Aprire ra.xml da *JBoss_home*\server\default\deploy\iam_im.ear\policyserver_rar\META-INF.

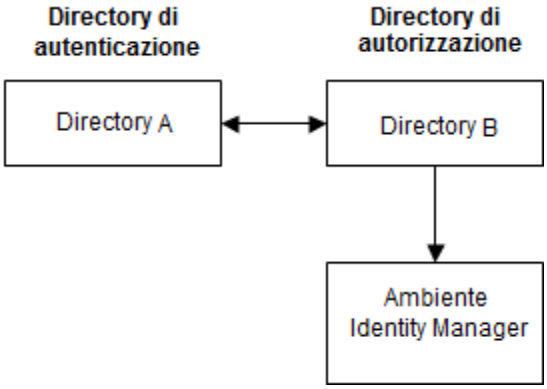
     b. Aggiungere la password crittografata come valore della proprietà Password config-property.
   - Se CA Identity Manager è in esecuzione su un server applicazioni WebSphere, eseguire le seguenti attività:

     a. Nella console di WebSphere, aprire ra.xml.

     b. Aggiungere la password crittografata come valore della proprietà Password config-property.
3. Riavviare il server applicazioni.

Configurazione di un ambiente di CA Identity Manager per utilizzare diverse directory per l'autenticazione e l'autorizzazione

Un amministratore può aver bisogno di gestire utenti i cui profili esistono in un archivio utenti differente da quello che viene utilizzato per autenticare l'amministratore. In altre parole, quando si accede all'ambiente di CA Identity Manager, l'amministratore deve essere autenticato in una directory e autorizzato a gestire utenti in una seconda directory, così come mostrato nell'illustrazione seguente:



Procedere come descritto di seguito:

1. Accedere a una delle seguenti interfacce:
   - Per CA SiteMinder Web Access Manager r12 o successive, accedere all'interfaccia utente di amministrazione.
   - Per CA eTrust SiteMinder 6.0 SP5, accedere all'interfaccia utente del Policy Server.

   Nota: per informazioni sull'utilizzo di queste interfacce, consultare la documentazione per la versione di SiteMinder in uso.
2. Creare due directory utente.

   Una directory fa riferimento ai dati di autenticazione (profili di amministratore), l'altra directory fa riferimento ai dati di autorizzazione (profili utenti).
3. Nella console di gestione, creare un ambiente di CA Identity Manager.

   Selezionare la directory di autorizzazione come directory di CA Identity Manager.

4. Nell'interfaccia per la versione di SiteMinder in uso, aggiungere la directory di autenticazione al dominio per l'ambiente di CA Identity Manager creato nella fase precedente.

   Il dominio e gli altri oggetti necessari per SiteMinder vengono creati automaticamente quando si crea un ambiente e SiteMinder viene integrato con CA Identity Manager.

   Il dominio utilizza la seguente convenzione di denominazione:

   *Identity Manager-environment*Domain

5. Assicurarsi che questa directory venga visualizzata in cima all'elenco di directory associate al dominio.
6. Individuare *Identity Manager-environment*_ims_realm.
7. Eseguire il mapping della directory di autorizzazione sulla directory di autenticazione nella sezione Opzioni avanzate della definizione dell'area di autenticazione.
8. Individuare la seguente risposta *Identity Manager-environment*response_ims.
9. Aggiungere attributi di risposta alle risposte nel seguente modo:

Campo	Valore
Attributo	WebAgent-HTTP-Header-Variable
Tipo di attributo	attributo utente
Nome variabile	sm_userdn
Nome attributo	SM_USERNAME

10. Salvare le modifiche.

    CA Identity Manager utilizza ora directory diverse per l'autenticazione e l'autorizzazione.

Miglioramento delle prestazioni delle operazioni di directory LDAP

Le operazioni di directory possono richiedere più tempo per l'elaborazione perché tutte le richieste di CA Identity Manager per la directory utente LDAP vengono instradate attraverso un insieme prestabilito di connessioni.

Per aumentare la velocità delle richieste di CA Identity Manager all'archivio utenti, configurare SiteMinder per l'apertura di connessioni multiple alla stessa directory. A tal fine, aggiungere il server LDAP più volte nella finestra di dialogo di LDAP Directory Failover and Load Balancing Setup (Configurazione failover e bilanciamento del carico della directory LDAP) nell'interfaccia utente del Policy Server.

Il numero di volte in cui si inserisce il server LDAP (e il numero di connessioni da creare) dipende dal carico su CA Identity Manager.

Appendice A: Conformità FIPS 140-2

Questa sezione contiene i seguenti argomenti:

Panoramica su FIPS

Il Federal Information Processing Standard (FIPS) 140-2 è uno standard di sicurezza per le librerie di crittografia e gli algoritmi da utilizzare per la crittografia. La crittografia FIPS 140-2 interessa la trasmissione di tutti i dati sensibili tra i componenti dei prodotti CA e tra i prodotti CA e i prodotti di terze parti. Lo 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.

CA Identity Manager utilizza lo standard AES (Advanced Encryption Standard) adattato dal governo degli U.S.A. CA Identity Manager incorpora le librerie di crittografia RSA Crypto-J v3.5 e Crypto-C ME v2.0, che sono state convalidate come conformi ai requisiti di sicurezza FIPS 140-2 per i moduli di crittografia.

Comunicazioni

La crittografia FIPS copre tutte le comunicazioni di dati tra CA Identity Manager e i seguenti componenti:

- Server di CA Identity Manager
- Server di provisioning
- Client e Manager di provisioning
- Server di connessione C++
- Endpoint dei server di connessione C++ (se supportati dall'endpoint)
- Server di connessione IAM CA (CA IAM CS)
- Endpoint di CA IAM CS (se supportati dall'endpoint)
- Connector Xpress (se supportato dall'endpoint)
- Agenti di sincronizzazione delle password di Windows
- Java Identity and Access Management (JIAM)

Installazione

Il programma di installazione di Identity Manager consente di configurare CA Identity Manager in modo da soddisfare i requisiti di conformità FIPS 140-2.

Tutti i componenti di un ambiente di Identity Manager devono essere abilitati per FIPS 140-2 perché Identity Manager supporti FIPS 140-2. Per abilitare FIPS 140-2 durante l'installazione è necessaria una chiave di crittografia FIPS. Lo strumento di password pwdtools.bat/pwdtools.sh necessario per generare una chiave FIPS si trova nella posizione seguente:

```
C:\Programmi\CA\Identity Manager\IAM Suite\Identity
Manager\PasswordTool\pwdtools.bat
```

Importante. Utilizzare la stessa chiave di crittografia FIPS 140-2 in tutte le installazioni e assicurarsi di proteggere il file della chiave generato dallo strumento di password.

Connessione a SiteMinder

Quando si esegue la connessione a CA SiteMinder durante l'installazione di Identity Manager, tenere presente che sono supportate solo la modalità FIPS e le configurazioni della versione di prodotto elencate nella tabella seguente:

Identity Manager r12	SiteMinder	Versione SiteMinder
Modalità FIPS-only	Modalità FIPS-only	r12
Modalità FIPS-only	Modalità FIPS-compatible	r12
Modalità Non-FIPS	Modalità FIPS-compatible	r12
Modalità Non-FIPS	Modalità Non-FIPS	r6

Archiviazione file di chiave

CA Identity Manager utilizza il file system per l'archiviazione della chiave di crittografia FIPS. L'amministratore di CA Identity Manager è responsabile per la protezione dei file da accessi non autorizzati e imposta le autorizzazioni di accesso alle directory per tipi di gruppo o utente specifici, come ad esempio l'utente che è autorizzato ad eseguire CA Identity Manager.

La tabella seguente mostra un elenco dei file di chiave FIPS per ciascun componente di CA Identity Manager.

Componente	Posizione di installazione
Server di CA Identity Manager	*IdentityMinder.ear*\config\com\netegrity\config\keys\FIPSkey.dat *IdentityMinder.ear* è la posizione di installazione di CA Identity Manager nel server applicazioni.
Server di provisioning	*Provisioning Server install*\data\tls\keymgmt\imps_datakey
Server di connessione C++	*Provisioning Server install*\data\tls\keymgmt\imps_datakey

Lo strumento Password

L'utilità dello strumento Password conforme a FIPS, pwdtools.bat (o pwdtools.sh), può generare la chiave di crittografia durante l'installazione di CA Identity Manager dalla riga di comando.

Modificare il file pwdtools.bat/pwdtools.sh prima di utilizzare lo strumento Password e di impostare la variabile JAVA_HOME così come richiesto.

Importante. CA Identity Manager non supporta la migrazione dei dati o la ripetizione della crittografia. Pertanto, verificare che non venga apportata alcuna modifica alle chiavi di crittografia dopo l'installazione.

Questo comando presenta la sintassi seguente:

```
pwdtools -{FIPSKEY|JSAFE|FIPS|RC2} -p plain text [-k <key file location>] [-f
<encrypting parameters file>]
```

JSAFE

Crittografare un valore di testo normale mediante l'algoritmo PBE.

Esempio:

```
pwdtools -JSAFE –p mypassword
```

Nota: Nelle versioni precedenti, la password per l'amministratore di bootstrap era archiviata in testo non crittografato. In caso di eseguendo l'aggiornamento o migrazione a CA Identity Manager r12.6 SP1 o versione successiva, è necessario eseguire la crittografia manuale della password in testo non crittografato. Verificare che l'opzione JSAFE sia specificata quando si utilizza tale strumento, quindi completare i passaggi seguenti:

1. Dopo l'aggiornamento o la migrazione a CA Identity Manager r12.6 SP1 e versioni successive, accedere al database dell'archivio oggetti di CA Identity Manager e cercare la tabella seguente:
   `IM_AUTH_USER`
2. Crittografare la password in testo non crittografato mediante lo strumento di password con JSAFE.
3. Sostituire il testo non crittografato con la password crittografata nella tabella.

FIPSKEY

Per il programma di installazione, creare un file di chiave FIPS. Generare la chiave prima di installare CA Identity Manager.

Esempio:

```
pwdtools -FIPSKEY -k C:\keypath\FIPSkey.dat
```

dove *keypath* è il percorso completo alla posizione in cui si desidera archiviare la chiave FIPS.

Lo strumento Password crea la chiave FIPS nella posizione specificata. Durante l'installazione, fornire la posizione del file di chiave FIPS al programma di installazione.

Nota: assicurarsi di proteggere la chiave impostando le autorizzazioni di accesso alla directory per determinati tipi di gruppi o di utenti, come ad esempio l'utente autorizzato a eseguire CA Identity Manager.

FIPS

Crittografare un valore di testo normale mediante un file di chiave FIPS. FIPS utilizza il file di chiave FIPS.

Esempio:

```
pwdtools -FIPS –p firewall -k C:\keypath\FIPSkey.dat
```

dove *keypath* è il percorso completo alla directory della chiave FIPS.

Nota: utilizzare lo stesso file di chiave FIPS specificato durante l'installazione.

RC2

Crittografare un valore di testo normale mediante l'algoritmo RC2.

Importante. CA Identity Manager utilizza il file di chiave FIPS per verificare se l'applicazione viene avviata in modalità FIPS o in modalità non FIPS. Pertanto, verificare che il file di chiave sia denominato FIPSKey.dat e abbia il seguente percorso di distribuzione del server applicazioni:

```
iam_im.ear\config\com\netegrity\config\keys\FIPSkey.dat
```

dove iam_im.ear è nella directory di distribuzione del server applicazioni, ad esempio:

```
jboss_home\server\default\deploy
```

Rilevazione modalità FIPS

Per determinare se CA Identity Manager sta operando in modalità FIPS o in modalità non FIPS, utilizzare la pagina di stato Ambiente di CA Identity Manager.

Per accedere alla pagina di stato, immettere l'URL seguente in un browser:

```
http://server_name/idm/status.jsp
```

server_name

Determina il nome di dominio completo del server in cui CA Identity Manager è installato, ad esempio, myserver.mycompany.com. In questo esempio, l'URL completo è:

http://myserver.mycompany.com/idm/status.jsp

Lo stato FIPS viene visualizzato in fondo alla pagina.

Nota: è possibile controllare anche se CA Identity Manager sta operando in modalità FIPS individuando il file di chiave seguente:

```
/config/com/netegrity/config/keys/FIPSkey.dat
```

Se questo file esiste, CA Identity Manager sta operando in modalità FIPS.

Il file di chiave FIPSkey.dat viene creato dall'utilità strumento di password pwdtools.bat (o pwdtools.sh), durante l'installazione di <CA idmgr>.

Formati di testo crittografati

Il nome dell'algoritmo viene aggiunto al testo crittografato come prefisso e comunica a CA Identity Manager l'algoritmo che è stato utilizzato per la crittografia.

In modalità FIPS, il prefisso è {AES}. Ad esempio, se si crittografa il testo "password", il testo crittografato è simile all'esempio seguente:

{AES}:eolQCTq1CGPyg6qe++0asg==

In modalità non FIPS (o modalità JSAFE), a seconda dell'algoritmo, il prefisso (tag di algoritmo) è {PBES} o {RC2}. Ad esempio, se si crittografa il testo "password", il testo crittografato è simile a quanto segue:

{PBES}:gSex2/BhDGzEKWvFmzca4w==

È possibile creare chiavi dinamiche utilizzando l'attività Chiavi segrete in Sistema. Se si definiscono chiavi dinamiche, l'ID chiave viene inserito tra un tag di algoritmo e un delimitatore di tag (':'). L'assenza di un ID chiave nei dati crittografati indica che per la crittografia è stata utilizzata la chiave hardcoded. Questa può essere utilizzata per la compatibilità con le versioni precedenti oppure se non è stata definita alcuna chiave dinamica per l'algoritmo dato.

Informazioni crittografate

Le informazioni di CA Identity Manager seguenti vengono crittografate:

- Password nella configurazione dell'origine dati per JBoss
- Informazioni di recupero di password dimenticate
- Segreto di richiamata del server di provisioning
- Informazioni sulla sessione del flusso di lavoro
- Informazioni di connessione relative al Policy Server

Registrazione in modalità FIPS

I componenti di CA Identity Manager seguenti indicano nei file di registro se la modalità FIPS è abilitata:

- Server di Identity Manager
- Server di provisioning
- Server di connessione C++
- Server di connessione Java
- Gestione provisioning
- Agente di sincronizzazione password

In tutti i casi, la voce di registro che indica che la modalità FIPS è abilitata termina con la stringa seguente:

FIPS 140-2 MODE: ON

Appendice B: Sostituzione dei certificati di CA Identity Manager con i certificati SSL SHA-2 firmati

L'hash dei certificati SSL SHA-2 è un algoritmo crittografico sviluppato dal National Institute of Standards and Technology (NIST) e dalla National Security Agency (NSA). I certificati SHA2 sono più protetti di tutti gli algoritmi precedenti. In CA Identity Manager, è possibile configurare certificati SSL SHA-2 firmati al posto di certificati firmati con la funzione hash SHA-1.

Nota: per ulteriori informazioni sulla configurazione dei certificati SSL, consultare la *Guida all'installazione*.

La seguente tabella mostra la posizione del percorso sul server di CA Identity Manager in cui è possibile collocare i certificati SHA-2 firmati:

Certificati	Posizione di installazione	Descrizione
Certificato del server di provisioning	[Provisioning Server install dir]/data/tls/server/eta2_servercert.pem [Provisioning Server install dir]/data/tls/server/eta2_serverkey.pem *cs_install*/ccs/data/tls/server/eta2_servercert.pem *cs_install*/ccs/data/tls/server/eta2_serverkey.pem *cs_install*/jcs/conf/eta2_server.p12	Utilizzato dal server di provisioning in formato .pem e da CA IAM CS in formato .p12 (inclusi certificato firmato, chiave privata e certificato autorità di certificazione root). **Nota**: importare il keystore eta2_server.p12 into *cs_install*/jcs/conf/ssl.keystore con l'alias eta2_server e rimuovere la voce esistente. La password del ssl.keystore è la password del server di connessione fornita durante l'installazione.

Certificati	Posizione di installazione	Descrizione
Certificato del client di provisioning	[Provisioning Server install dir]/data/tls/client/eta2_clientcert.pem [Provisioning Server install dir]/data/tls/client/eta2_clientkey.pem [Provisioning Manager install dir]/data/tls/client/eta2_clientcert.pem [Provisioning Manager install dir]/data/tls/client/eta2_clientkey.pem *cs_install*/ccs/data/tls/client/eta2_clientcert.pem *cs_install*/ccs/data/tls/client/eta2_clientkey.pem *cs_install*/jcs/conf/eta2_client.p12	Utilizzato dal server di provisioning in formato .pem e da CA IAM CS in formato .p12 (inclusi certificato firmato, chiave privata e certificato autorità di certificazione root).
Certificato attendibile della directory di provisioning	*cadir_install*/config/ssld/impd_trusted.pem	Utilizzato da CA Directory in formato .pem. Deve presentare contenuto di certificato nella seguente struttura: -----BEGIN CERTIFICATE----- Contenuti del certificato -----END CERTIFICATE-----
Certificato di personalità della directory di provisioning	*cadir_install*/config/ssld/personalities/impd-co.pem *cadir_install*/config/ssld/personalities/impd-inc.pem *cadir_install*/config/ssld/personalities/impd-main.pem *cadir_install*/config/ssld/personalities/impd-notify.pem *cadir_install*/config/ssld/personalities/impd-router.pem	Utilizzato da CA Directory in formato .pem.

Certificati	Posizione di installazione	Descrizione
Certificato autorità di certificazione root	[Provisioning Server install dir]/data/tls/et2_cacert.pem [Provisioning Manager install dir]/data/tls/et2_cacert.pem *cs_install*/ccs/data/tls/ et2_cacert.pem *conxp_install*/lib/jiam.jar [Application Server install dir]/iam_im.ear/library/jiam.jar	Il certificato viene importato nel KeyStore di Connector Xpress che si trova in [Connector Xpress install dir]/conf/ssl.keystore. È necessario importare anche il certificato nel KeyStore jiam.jar. Per importare, estrarre il file .jar, importare il certificato in admincacerts.jks, quindi aggiungere nuovamente i contenuti del file .jar. La password del KeyStore di admincacerts.jks è "changeit". Verificare che tutte le copie di jiam.jar vengano sostituite.

Comandi utili

Il programma OpenSSL è uno strumento della riga di comando che consente l'utilizzo delle varie funzioni di crittografia della libreria di OpenSSL. Questo strumento viene fornito con IMPS, che si trova in [Provisioning Server install dir]/bin.

La seguente tabella mostra alcuni comandi utili del programma OpenSSL per l'esecuzione dei vari comandi relativi alla gestione di certificati:

Comandi	Descrizione
`openssl x509 -in cert.pem -text -noout`	Stampa i contenuti del certificato .pem.
`openssl.exe pkcs12 -in my.pkcs12 -info`	Stampa i contenuti del file .p12.
`openssl.exe pkcs12 -export -chain -inkey key.pem -in cert.pem -CAfile cacert.pem -out my.p12`	Converte .pem cert/keypair in .p12.
`keytool -list -v -keystore my.keystore`	Stampa i contenuti di un KeyStore di java.
`keytool –list –v –alias myalias –keystore my.keystore`	Stampa i contenuti di un alias specifico in un KeyStore di java

Comandi		Descrizione
	`keytool –delete –alias myalias –keystore my.keystore`	Elimina un alias da un KeyStore di java
	`keytool –importkeystore –destkeystore my.keystore –srckeystore src.p12 –srcstoretype PKCS12 –srcalias 1 –destalias myalias`	Importa un file .p12 in un KeyStore di java.
	`keytool -import -trustcacerts -alias myrootca -file rootcacert.pem -keystore my.keystore`	Importa un certificato autorità di certificazione root .pem in un KeyStore di java.