CA Identity Manager™

Guida all'implementazione

12.6.5

Riferimenti ai prodotti CA Technologies

Questo documento è valido per i seguenti prodotti di CA Technologies:

- CA CloudMinder™ Identity Management
- Directory CA
- CA Identity Manager ™
- CA Identity Governance (precedentemente CA GovernanceMinder)
- CA SiteMinder®
- CA User Activity Reporting
- CA AuthMinder ™

Contattare il servizio di Supporto tecnico

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

Sommario

Capitolo 1: Gestione di identità e accesso

Questa sezione contiene i seguenti argomenti:

Gestione utenti e accesso alle applicazioni

Tutti i dipartimenti di tecnologia informatica (IT) si trovano davanti alla costante domanda di aggiornamento degli account utente. Gli amministratori IT devono risolvere urgenti necessità degli utenti, come ad esempio reimpostare le password dimenticate, creare nuovi account e occuparsi delle forniture e delle apparecchiature per l'ufficio.

Allo stesso tempo, gli amministratori IT devono fornire agli utenti vari livelli di accesso alle applicazioni. Ad esempio, un manager di dipartimento genera ordini di acquisto e ha bisogno di un account in un'applicazione finanziaria.

Per soddisfare le crescenti richieste del dipartimento IT, CA Identity Manager fornisce un metodo integrato per la gestione degli utenti e il loro accesso alle applicazioni, compresi:

- Assegnazione di privilegi attraverso ruoli. Nello specifico:
  - Ruoli che consentono agli amministratori di creare e gestire account utente
  - Ruoli che forniscono account aggiuntivi agli utenti esistenti (richiede il supporto per il provisioning)
- Delegazione della gestione di utenti e dell'accesso alle applicazioni
- Opzioni self-service per consentire agli utenti di gestire i propri account
- Integrazione di applicazioni aziendali con CA Identity Manager
- Opzioni per la personalizzazione e l'ampliamento di CA Identity Manager

Diritti basati su ruoli

Si attribuiscono privilegi agli utenti con l'assegnazione di ruoli. Un *ruolo* comprende attività che corrispondono a funzionalità in CA Identity Manager, come l'attività Crea utente, a funzionalità in un'applicazione, come la funzionalità di creazione dell'ordine di acquisto, o a modelli account che forniscono account utente, ad esempio un account SAP. Gli utenti ricevono i privilegi corrispondenti al ruolo assegnato.

CA Identity Manager fornisce i seguenti tipi di ruolo:

- Ruoli di gestione utenti, definiti *ruoli di amministrazione*.

  I ruoli di amministrazione possono comprendere, tra le altre, qualsiasi attività visualizzata nella console utente.
- Ruoli di assegnazione account, definiti *ruoli di provisioning*.
- Ruoli di funzionamento delle applicazioni, definiti *ruoli di accesso*.

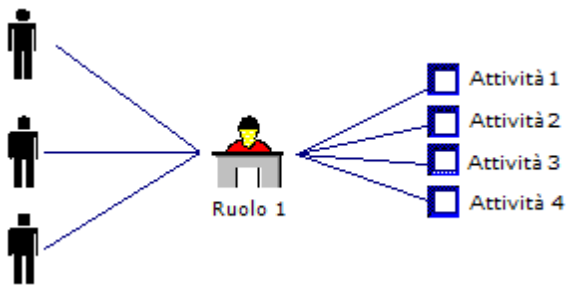
Se si rimuove un'attività o un modello account da un ruolo, l'utente non è più in grado di eseguire quell'attività, utilizzare un account endpoint o far funzionare un'applicazione.

Ruoli di amministrazione

I ruoli di amministrazione controllano le operazioni che possono essere eseguite da un utente in CA Identity Manager. L'amministratore di sistema assegna un ruolo a un utente. Tale ruolo definisce un insieme di attività che l'utente può eseguire. Gli utenti possono eseguire *attività* amministrative negli account utente, ad esempio modificare una password o aggiornare un titolo professionale.

Utenti diversi presentano livelli diversi di accesso a queste attività. Ad esempio, un utente con ruolo di Dipendente può comprendere attività che consentono agli utenti di modificare il proprio nome e indirizzo, mentre il ruolo di Direttore delle risorse umane contiene attività che permettono di modificare il titolo professionale dell'utente e lo stipendio.

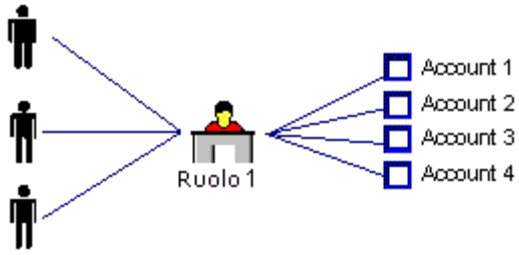
L'immagine riportata di seguito mostra quattro attività combinate in un ruolo di amministrazione e assegnate a tre utenti:



Ruoli di provisioning

Per concedere agli utenti l'accesso agli account nelle applicazioni aggiuntive, ad esempio in un sistema di posta elettronica, è possibile assegnare all'utente i ruoli di provisioning. I ruoli di provisioning contengono esempi di account che definiscono gli attributi esistenti in un tipo di account. Ad esempio, un modello di account per un account Exchange definisce attributi quali le dimensioni della casella di posta elettronica. i modelli di account definiscono inoltre il mapping degli attributi dell'utente di CA Identity Manager sugli account.

L'immagine seguente mostra quattro account combinati in un ruolo di provisioning e assegnati a tre utenti. Quando il ruolo di provisioning viene assegnato, ciascun utente riceve quattro account.



Ruoli di accesso

I ruoli di accesso rappresentano un ulteriore modo per concedere diritti in CA Identity Manager o in un'altra applicazione. Ad esempio, è possibile utilizzare i ruoli di accesso per completare le seguenti operazioni:

- Fornire l'accesso indiretto a un attributo utente
- Creare espressioni complesse
- Impostare un attributo in un profilo utente, utilizzato da un'altra applicazione per determinare i diritti

I ruoli di accesso sono analoghi ai criteri di identità, in quanto applicano un insieme di modifiche aziendali a un utente o a un gruppo di utenti. Tuttavia, quando si utilizza un ruolo di accesso per applicare modifiche aziendali, è possibile visualizzare a quali utenti si applicano le modifiche visualizzando i membri del ruolo di accesso.

Nella maggior parte dei casi, i ruoli di accesso non vengono associati alle attività.

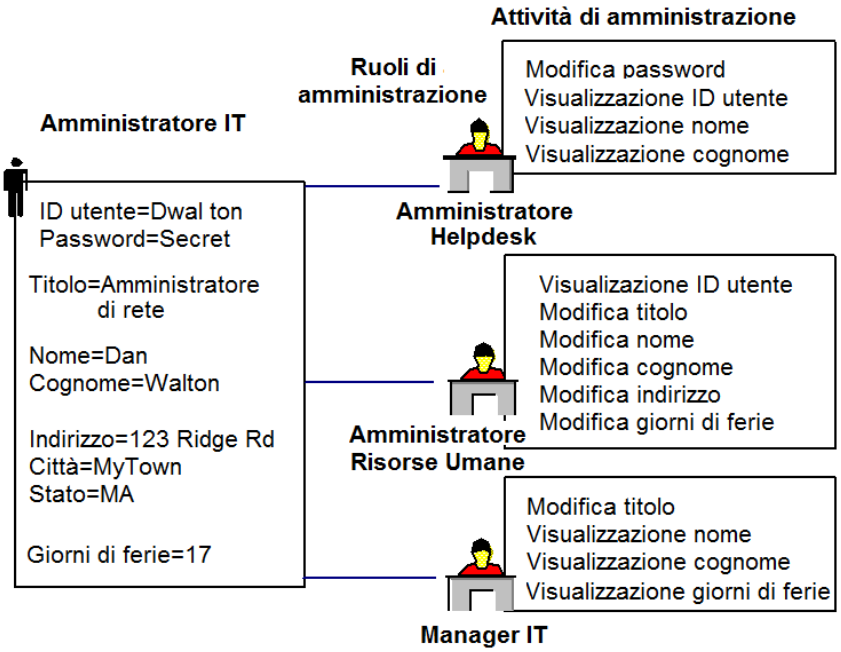
Nota: quando CA Identity Manager si integra con CA SiteMinder, i ruoli di accesso possono anche fornire accesso ad applicazioni protette da CA SiteMinder. In questo caso, i ruoli di accesso comprendono attività di accesso. Per ulteriori informazioni, consultare il capitolo relativo all'integrazione con SiteMinder nella *Guida alla configurazione*.

Ruoli di amministrazione per la gestione degli identificativi degli utenti

In CA Identity Manager, gli oggetti dell'archivio utenti (utenti, gruppi e organizzazioni) vengono gestiti attraverso ruoli di amministrazione. I ruoli di amministrazione vengono utilizzati anche per gestire i ruoli e le attività attraverso cui si gestiscono gli oggetti dell'archivio utenti. Ad esempio, i ruoli di amministrazione vengono utilizzati per modificare gli attributi di profilo degli utenti, fornire agli utenti le opzioni per gestire i propri account e approvare le attività che utilizzano il flusso di lavoro.

Gestione del profilo a livello di attributo

È possibile creare ruoli di amministrazione per diversi amministratori che devono leggere o scrivere diversi attributi di profilo. Ad esempio, un'azienda può avere molti dipendenti che eseguono operazioni sui profili utenti e ciascuno accede ad attributi differenti. La figura seguente mostra tre ruoli e le attività a essi associate. Ciascun ruolo ha un accesso diverso agli attributi di profilo.



In questo esempio, tre ruoli possono gestire attributi differenti per lo stesso utente, Dan Walton:

- Un amministratore dell'Helpdesk visualizza i nomi e gli indirizzi degli utenti e ripristina le password.
- Un amministratore delle Risorse umane modifica gli ID utente, i nomi, gli indirizzi, i titoli e il numero di giorni di ferie degli utenti.
- Un manager IT modifica il titolo degli utenti e ne visualizza il nome e il numero di giorni di ferie.

Qualsiasi ruolo si abbia quando si accede a CA Identity Manager, viene visualizzata una serie di schede, chiamate categorie, in base al ruolo di amministrazione assegnato all'account di CA Identity Manager in uso. Fare clic su una scheda per visualizzare le attività che è possibile eseguire in quella categoria, così come illustrato nella seguente figura:

Le categorie e le attività nelle categorie visualizzate da un utente vengono determinate dai ruoli di amministrazione dell'utente.

Approvazione del flusso di lavoro delle attività di amministrazione

Per semplificare l'automazione dei processi aziendali, è possibile progettare un'attività di amministrazione per generare un processo del flusso di lavoro. Un *processo del flusso di lavoro* automatizza una procedura ben definita che un'azienda ripete frequentemente. CA Identity Manager include il motore del flusso di lavoro WorkPoint.

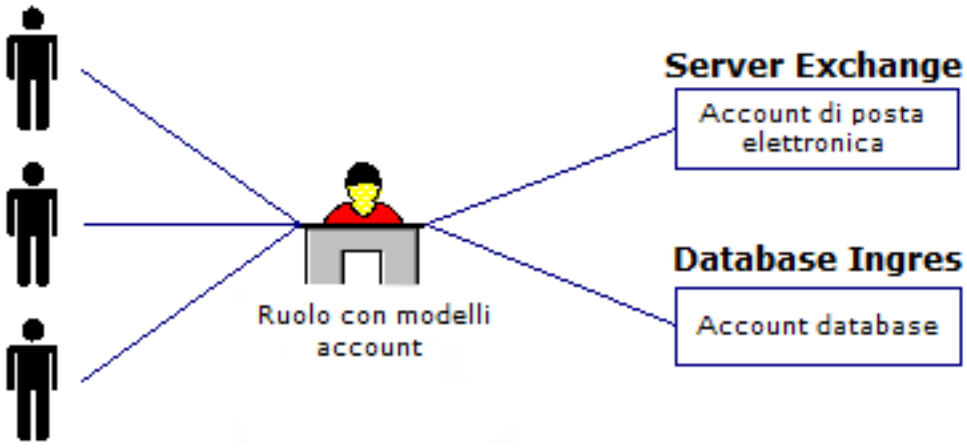
I processi del flusso di lavoro vengono attivati da eventi di CA Identity Manager che fanno parte di un'attività di amministrazione. Ad esempio, l'attività Crea utente include eventi chiamati CreateUserEvent e AddToGroupEvent. Quando si verifica un evento, il motore del flusso di lavoro può:

- Richiedere approvazioni: un responsabile dell'approvazione deve approvare un evento, come ad esempio la modifica di un profilo utente, prima che CA Identity Manager aggiorni un archivio utenti. I responsabili dell'approvazione sono amministratori che hanno il ruolo Responsabile dell'approvazione per un'attività particolare.
- Inviare notifiche: il motore del flusso di lavoro può inviare notifiche agli utenti relative allo stato di un evento nei diversi stadi di un processo, come ad esempio quando un utente avvia un evento o quando un evento viene approvato.
- Generare elenchi di lavoro: gli elenchi di lavoro specificano le attività che un determinato utente deve eseguire. Il motore del flusso di lavoro aggiorna automaticamente gli elenchi di lavoro degli amministratori.

Per eventi comuni, è possibile utilizzare i processi del flusso di lavoro forniti con CA Identity Manager. In alternativa, è possibile creare processi del flusso di lavoro personalizzati.

Ruoli di provisioning per account aggiuntivi

In CA Identity Manager, gli account aggiuntivi vengono forniti agli utenti mediante ruoli di provisioning. I ruoli di provisioning contengono modelli di account che definiscono gli account esistenti negli endpoint gestiti, come ad esempio in un server di posta elettronica. Quando si hanno utenti in CA Identity Manager, è possibile assegnare ruoli di provisioning ad alcuni di quegli utenti. L'utente riceve gli account definiti dai modelli nel ruolo.



I modelli di account definiscono le caratteristiche dell'account. Ad esempio, un modello di account per un account Exchange potrebbe definire la dimensione della casella di posta elettronica. I modelli di account definiscono anche le modalità di mapping degli attributi utente sugli account.

Per poter utilizzare i ruoli di provisioning, è necessario installare il server di provisioning con il server di Identity Manager. Quindi, creare modelli di account nella console utente.

Gestione password

In Identity Manager sono disponibili numerose funzionalità per la gestione delle password degli utenti.

- Criteri di password: questi criteri consentono di gestire le password degli utenti mediante l'applicazione di regole e restrizioni che disciplinano la scadenza, la composizione e l'utilizzo delle password.

  Nota: per i criteri di password avanzati, configurare l'integrazione con SiteMinder. Per ulteriori informazioni, consultare la *Guida all'installazione*.

- Manager password: gli amministratori a cui è stato assegnato il ruolo Manager password possono reimpostare una password quando un utente si rivolge all'Helpdesk.

- Gestione di password self-service: in Identity Manager sono disponibili numerose attività di self-service che consentono agli utenti di gestire le proprie password. Queste attività includono:

  - Registrazione automatica: gli utenti specificano una password quando si registrano presso un sito Web aziendale.

  - Modifica password personale: gli utenti possono modificare la propria password senza l'aiuto del personale tecnico o dell'Helpdesk

  - Password dimenticata: gli utenti possono reimpostare o recuperare una password dimenticata in seguito alla verifica della propria identità in Identity Manager.

  - ID utente dimenticato: gli utenti possono recuperare un ID utente dimenticato in seguito alla verifica della propria identità in Identity Manager.

- Sincronizzazione password (solo per l'uso con il provisioning): le modifiche alle password vengono sincronizzate in Identity Manager e negli account dei sistemi di destinazione chiamati endpoint. Le nuove password vengono verificate in base ai criteri di password di Identity Manager.

Opzioni self-service per gli utenti

Per ridurre ulteriormente il carico di lavoro del dipartimento IT, CA Identity Manager include funzionalità per la registrazione di nuovi utenti e l'invio di una password dimenticata. Queste funzionalità non richiedono l'intervento dell'amministratore. L'utente ottiene l'accesso a CA Identity Manager attraverso una *console pubblica*, che non richiede l'account di accesso. Attraverso questa console, un utente può registrarsi automaticamente a un sito o richiedere un promemoria per una password dimenticata.

Per far risparmiare tempo agli amministratori IT, gli utenti di CA Identity Manager possono gestire i propri account. Poiché gli utenti dispongono di un ruolo di autogestione, possono:

- Gestire le informazioni personali
- Modificare la propria password
- Iscriversi a gruppi auto-sottoscriventi

Personalizzazione ed estendibilità di Identity Manager

È possibile personalizzare le seguenti caratteristiche di CA Identity Manager:

- La directory di Identity Manager, che descrive la struttura di un archivio utenti a CA Identity Manager.
- L'aspetto e la funzionalità dell'interfaccia utente.
- Le schermate delle voci dell'utente, che determinano i campi e il layout di ciascuna schermata di attività.
- La convalida delle voci di dati dell'utente, attraverso l'espressione regolare, JavaScript o le implementazioni di Java.
- Il flusso di lavoro, che definisce i processi automatizzati del flusso di lavoro. Creare o modificare i processi collegando i responsabili dell'approvazione e le azioni in WorkPoint Process Designer.
- I messaggi di posta elettronica, che informano gli utenti dello stato di un'attività.
- L'invio di attività, che può avvenire da un'applicazione di terze parti al Servizio Web per l'esecuzione di attività di Identity Manager (TEWS). TEWS elabora la richiesta di attività remota. Le richieste di attività remote sono conformi agli standard WSDL.

È possibile estendere le funzionalità di CA Identity Manager utilizzando le seguenti API:

- API attributo logico: consente di visualizzare un attributo in maniera diversa rispetto a come è stato archiviato fisicamente in una directory dell'utente.
- API gestore dell'attività di logica aziendale: consente di eseguire la logica aziendale personalizzata durante la convalida dei dati o le operazioni di trasformazione.

- API flusso di lavoro: fornisce le informazioni a uno script personalizzato in un processo del flusso di lavoro. Lo script valuta le informazioni e determina il percorso del processo del flusso di lavoro in maniera corrispondente.
- API resolver partecipante: consente di specificare l'elenco di partecipanti autorizzati ad approvare un'attività del flusso di lavoro.
- API listener di evento: consente di creare un listener di evento personalizzato che ascolta un evento o un gruppo di eventi determinati di Identity Manager. Quando si verifica l'evento, il listener di evento può eseguire la logica aziendale personalizzata.
- API regola di notifica: consente di determinare gli utenti che dovrebbero ricevere una notifica di posta elettronica.
- API modello di posta elettronica: include informazioni specifiche dell'evento in una notifica di posta elettronica.

Nota: per ulteriori informazioni sulle API di CA Identity Manager, consultare la *Programming Guide for Java*.

Quando CA Identity Manager include il provisioning, è possibile estendere le funzionalità di provisioning nel seguente modo:

- Connettori personalizzati: abilitano la comunicazione tra un server di provisioning e un sistema endpoint. Il codice che crea un connettore può includere un plug-in interfaccia utente, un plug-in server e plug-in agente.

  Connector Xpress può generare un connettore dinamico ed è possibile sviluppare un connettore statico personalizzato in Java o C++.
- Uscite programma: consente di fare riferimento al codice personalizzato dal flusso di processo del server di provisioning.

Nota: per ulteriori informazioni sull'estensione della funzionalità di provisioning, consultare la *Programming Guide for Provisioning*.

Integrazione di CA Identity Governance

CA Identity Governance è un prodotto di gestione del ciclo di vita dell'identità che consente di sviluppare, gestire e analizzare modelli di ruolo in modo rapido e accurato. Consente, inoltre, un controllo centralizzato dei criteri di conformità ed automatizza i processi associati con le richieste di protezione e di conformità. Mediante CA Identity Governance è possibile eseguire le seguenti operazioni:

- Confermare che i privilegi dell'utente di CA Identity Manager vengono concessi in conformità con i criteri di conformità aziendali
- Ottenere il controllo di conformità e dei ruoli suggeriti durante la creazione o la modifica di utenti, ruoli e account di CA Identity Manager

- Comprendere i ruoli esistenti nell'organizzazione, stabilire un modello di ruolo adatto all'organizzazione e ricreare il modello di ruolo desiderato all'interno di CA Identity Manager
- Analizzare e gestire il modello di ruolo conformemente all'evoluzione delle attività

CA Identity Manager è integrato con CA Identity Governance in due modi:

- Connettore di CA Identity Governance per CA Identity Manager

  Un tipo speciale di connettore che sincronizza automaticamente i dati relativi ai privilegi tra CA Identity Manager e CA Identity Governance. Mediante questo connettore, è possibile importare i dati da CA Identity Manager a CA Identity Governance oppure esportarli da CA Identity Governance a CA Identity Manager.

- Smart Provisioning

  Se CA Identity Manager viene integrato con CA Identity Governance, è possibile configurare funzionalità aggiuntive che consentono di utilizzare informazioni relative ai ruoli e alla conformità, disponibili in un modello di ruolo, per supportare le operazioni quotidiane di gestione dell'identità. Le modifiche effettuate in CA CA Identity Manager aggiornano in modo dinamico il modello di ruolo in CA Identity Governance.

Nota: per ulteriori informazioni sull'integrazione di CA Identity Governance con CA Identity Manager, consultare la *Guida all'integrazione di CA Identity Manager* del Bookshelf di CA Identity Governance.

Integrazione di CA User Activity Reporting

A partire da CA Identity Manager r12.6, CA Enterprise Log Manager viene chiamato CA User Activity Reporting (CA UAR).

CA UAR utilizza CA Common Event Grammar (CEG) per eseguire il mapping in formato standard di eventi che hanno origine in vari sistemi e archivia tutti gli eventi, anche quelli di cui non è stato ancora eseguito il mapping, per la revisione e l'analisi. Inoltre, CA UAR fornisce agli utenti una soluzione in grado di gestire ed eseguire rapporti su grandi volumi di dati raccolti, utilizzando query di database configurabili e/o rapporti per la ricerca di vari tipi di informazioni ed eventi.

CA UAR fornisce una visione più ampia e più approfondita dei sistemi non gestiti o al di fuori dell'ambito e del controllo di CA Identity Manager, consentendo di investigare a fondo nelle identità.

L'integrazione con CA Identity Manager consente di visualizzare i rapporti e/o le query dinamiche incentrati sull'identità nella console utente di CA UAR mediante la console utente di CA Identity Manager. Dalla console utente, è possibile configurare le modalità per visualizzare e modificare i rapporti e/o le query esistenti di CA Identity Manager/CA UAR mentre si eseguono analisi approfondite su una specifica identità.

Rapporti CA UAR

I seguenti rapporti CA UAR vengono forniti per impostazione predefinita con le definizioni di ruolo CA UAR:

Attività	Richiamo rapporto
Tutti gli eventi di sistema per Utente	CA Identity Manager: tutti gli eventi di sistema filtrati per ID utente
Gestione account per Host	Gestione account per Host
Creazioni account per Account	Creazioni account per Account
Eliminazioni account per Account	Eliminazioni account per Account
Blocchi account per Account	Blocchi account per Account
Attività di processo di certificazione per Host	CA Identity Manager: attività di processo per Host
Attività di modifica criterio password	CA Identity Manager: attività di modifica criterio

Capitolo 2: Soddisfazione delle esigenze dell'azienda

Questa sezione contiene i seguenti argomenti:

Elaborazione delle modifiche aziendali

Utilizzando i criteri di identità, è possibile automatizzare l'elaborazione di certe attività di gestione identità. Un criterio di identità è un insieme di modifiche di business che si verifica quando un utente soddisfa una determinata condizione o regola. È possibile utilizzare set di criteri di identità per svolgere le seguenti attività:

- 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 (a pagina 25). Ad esempio, è possibile creare un set di criteri di identità per impedire ai membri del ruolo Firmatario assegni di venire associati al ruolo Approvatore assegni, nonché per impedire ai dipendenti della società di emettere assegni con un importo maggiore di € 10.000.
- Applicazione della conformità. Ad esempio, è possibile sottoporre a revisione gli utenti associati ad uno specifico ruolo e con un reddito superiore a € 100.000.

  I criteri di identità che applicano la conformità vengono definiti *criteri di conformità*.

Le modifiche aziendali associate ad un criterio di identità includono:

- Assegnazione o revoca di ruoli, inclusi i ruoli di provisioning (quando CA Identity Manager include il provisioning)
- Assegnazione o revoca dell'appartenenza a gruppi
- Aggiornamento degli attributi in un profilo utente

Ad esempio, una società può creare un criterio di identità in base al quale tutti i vicepresidenti appartengono al gruppo Membro country club e sono associati al ruolo Approvatore stipendi. Quando il titolo di un utente viene modificato in Vicepresidente e tale utente viene sincronizzato con il criterio di identità, CA Identity Manager aggiunge tale utente al gruppo e al ruolo appropriati. Quando un vicepresidente viene promosso a CEO, non soddisferà più la condizione definita dal criterio di identità Vicepresidente e pertanto le modifiche applicate da tale criterio verranno revocate, mentre verranno applicate le nuove modifiche in base al criterio CEO.

Le azioni di modifica che si verificano in base a un criterio di identità contengono eventi che possono essere inseriti in un controllo a livello di flusso di lavoro e sottoposti a verifica. Nell'esempio precedente, il ruolo Approvatore stipendi assegna privilegi molto significativi ai relativi membri. Per proteggere il ruolo di Approvatore stipendi, l'azienda può creare un processo del flusso di lavoro che richiede una serie di approvazioni prima che il ruolo venga assegnato e configurare CA Identity Manager in modo che verifichi l'assegnazione del ruolo.

Per semplificare la gestione dei criteri di identità, tali criteri vengono raggruppati in set. Ad esempio, i criteri Vicepresidente e CEO possono essere inclusi nel set di criteri di identità Privilegi dirigenti.

Rispetto dei criteri aziendali

La conformità è un controllo aziendale che include un'ampia gamma di procedure per garantire che una società e i relativi dipendenti rispettino i criteri aziendali. Tali procedure di conformità spesso implicano l'attestazione, l'automazione e il controllo dell'assegnazione di diritti ad applicazioni e sistemi.

CA Identity Manager include le seguenti funzionalità, che supportano la gestione della conformità:

- **Smart Provisioning**

  Smart Provisioning è una raccolta di funzionalità che semplifica le operazioni di assegnazione dei ruoli di provisioning quando CA Identity Manager è integrato con CA Identity Governance. La funzionalità include:

  - Ruoli di provisioning consigliati

    CA Identity Manager è in grado di fornire agli amministratori un elenco di ruoli di provisioning assegnabili agli utenti. L'elenco dei ruoli di provisioning è determinato da CA Identity Governance sulla base di criteri immessi dall'amministratore.

    Il suggerimento dei ruoli di provisioning garantisce la corretta assegnazione dei privilegi agli utenti, mantenendo un modello di ruolo conforme a quello aziendale.

- Messaggi di conformità e modello

  Gli amministratori di CA Identity Manager possono convalidare le modifiche proposte a fronte di un modello di ruolo di CA Identity Governance prima di salvare le modifiche. La convalida delle modifiche prima del salvataggio aiuta le aziende a mantenere il modello di ruolo definito per le operazioni.

  Gli utenti possono convalidare le modifiche proposte ai ruoli di provisioning (assegnandoli o rimuovendoli) e agli attributi utente.

  In CA Identity Manager vengono eseguiti due tipi di convalida dei criteri:

  - Conformità

    Le modifiche proposte vengono convalidate a fronte del modello di ruolo CA Identity Governance per verificare che non violino regole di criteri aziendali esplicite di CA Identity Governance.

  - Criterio

    Le modifiche proposte vengono confrontate con il modello di ruolo di CA Identity Governance per verificare se causano l'uscita dal modello da parte dell'oggetto sottoposto a modifica. Inoltre, in CA Identity Manager si verifica che le modifiche non alterino significativamente un modello stabilito nel modello di ruolo.

    È possibile configurare CA Identity Manager in modo da eseguire automaticamente queste convalide quando gli utenti eseguono determinate attività o consentire agli utenti di avviare la convalida manualmente.

  È possibile implementare Smart Provisioning in un ambiente di CA Identity Manager quando in CA Identity Governance è presente un modello di ruolo stabilito sulla base dei dati di CA Identity Manager.

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

- **Criteri di identità**

  È possibile creare un criterio di conformità, un tipo di criterio di identità (a pagina 21), che impedisce la coesistenza di alcuni privilegi per gli utenti. Ad esempio, è possibile impedire l'emissione di assegni agli utenti che possono approvarli.

  I criteri di conformità consentono di esercitare una separazione tra i compiti nell'ambiente.

- **Rapporti di conformità**

  CA Identity Manager include dei rapporti di esempio in cui viene visualizzato lo stato di conformità degli utenti nel proprio ambiente. Utilizzando tali rapporti, è possibile individuare gli utenti che non rispettano i criteri aziendali.

Rapporti di conformità

CA Identity Manager include i report di esempio nella tabella seguente che è possibile utilizzare per monitorare la conformità con i criteri aziendali collettivi.

Rapporto	Descrizione
Membri del ruolo	Consente di visualizzare i ruoli nel database di rapporto ed elenca i membri di quei ruoli
Ruoli	Consente di visualizzare le informazioni seguenti per ogni ruolo presente nel database di rapporto: ■ Attività associate al ruolo ■ Criteri membri e membri del ruolo ■ Criteri amministratori e amministratori del ruolo ■ Criteri di titolarità e titolari del ruolo
Tasks Roles (Ruoli di attività)	Consente di visualizzare le attività nel database di reporting e i ruoli ai quali vengono associate
Ruoli utente	Consente di visualizzare gli utenti nel database di reporting ed elenca i ruoli di ciascun utente
Non-Standard Accounts Trend (Tendenza account non standard)	Consente di visualizzare l'andamento account non standard per account orfani, account di sistema e account di eccezione
Non-Standard Accounts (Account non standard)	Consente di visualizzare tutti gli account orfani, di sistema e di eccezione
Account orfani	Consente di visualizzare tutti gli account di endpoint senza utente globale nel server di provisioning
Criteri	Consente di visualizzare tutti i criteri di identità
Profilo utente	Consente di visualizzare le seguenti informazioni relative agli utenti: ■ Nome ■ ID utente ■ Gruppi dei quali l'utente è membro o amministratore ■ Ruoli in cui l'utente è membro, amministratore o titolare

Rapporto	Descrizione
Endpoint Accounts (Account di endpoint)	Consente di visualizzare gli account per ogni endpoint (è possibile scegliere quale endpoint visualizzare)
Amministratori di ruolo	Consente di visualizzare i ruoli e i relativi amministratori
Proprietari di ruolo	Consente di visualizzare i ruoli e i relativi titolari
Snapshot	Consente di visualizzare tutte le snapshot esportate
Account utente	Consente di visualizzare un elenco di utenti e dei relativi account
User Entitlements (Diritti utente)	Consente di visualizzare i ruoli, i gruppi e gli account dell'utente
User Policy Sync Status (Stato di sincronizzazione criterio utente)	Consente di visualizzare lo stato dell'utente per ogni criterio (quali criteri dovrebbero essere allocati, rilasciati o riallocati)

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

Requisiti per l'applicazione dell'imposizione di mansioni

I requisiti per l'imposizione di mansioni (SOD, Segregation of Duties) impediscono agli utenti di ricevere privilegi che possono dare origine a un conflitto di interessi o a una frode. CA Identity Manager fornisce la funzionalità seguente per supportare SOD:

- **Criteri di identità preventivi**

  Tali criteri, che vengono eseguiti prima dell'inoltro di un'attività, consentono all'amministratore di verificare la presenza di violazioni dei criteri prima di assegnare privilegi o modificare attributi del profilo. Se esiste una violazione, l'amministratore potrà cancellarla prima di inoltrare l'attività.

  Ad esempio, una società può creare un criterio di identità preventivo che proibisce che gli utenti con il ruolo Manager utente dispongano anche del ruolo Responsabile dell'approvazione utente. Se un amministratore utilizza l'attività Modifica utente per assegnare a un Manager utente il ruolo di Responsabile dell'approvazione utente, in CA Identity Manager viene visualizzato un messaggio relativo alla violazione. L'amministratore può modificare le assegnazioni di ruolo per cancellare la violazione prima di inoltrare l'attività.

- **Convalida di criteri attraverso Smart Provisioning**

  Gli amministratori di CA Identity Manager possono convalidare le modifiche proposte per i ruoli di provisioning e gli attributi utente in rapporto alle Regole del processo di business (BPR) in CA Identity Governance prima di salvare le modifiche. I BPR rappresentano vari vincoli per i privilegi. Ad esempio, una regola di processo aziendale potrebbe impedire agli utenti che dispongono di un ruolo dell'ufficio acquisti, che consente di ordinare merci ai fornitori, di disporre anche di un ruolo per il pagamento dei fornitori. Un amministratore di sistema, un manager aziendale, un revisore o un ingegnere del ruolo crea i BPR in CA Identity Governance.

  Nota: Per ulteriori informazioni sui BPR, consultare la *CA Identity Governance Sage DNA User Guide*.

Nota: per ulteriori informazioni sui criteri di identità preventivi e lo Smart Provisioning, consultare la *Guida per l'amministratore* di *CA Identity Manager*.

Trasformazione dei dati nell'archivio utenti

In alcuni casi, può essere opportuno che CA Identity Manager trasformi i dati prima che vengano dell'archiviazione nell'archivio utenti. Ad esempio, potrebbe essere necessario archiviare informazioni in un formato differente rispetto al formato di immissione oppure applicare delle modifiche quando sono presenti certi tipi di informazioni.

CA Identity Manager include le caratteristiche seguenti per la trasformazione dei dati:

- Criteri di identità
- Gestori attributi logici

Nota: è anche possibile utilizzare i criteri di identità e i gestori di attributi logici per implementare una logica aziendale personalizzata.

Gestori attributi logici

I gestori di attributi logici sono codice Java personalizzato che trasformano i valori attributo dell'utente utilizzati in schermate di attività di CA Identity Manager. Utilizzando i gestori di attributi logici, è possibile controllare la modalità di visualizzazione di un attributo fisico in una schermata di attività. È anche possibile utilizzare i gestori di attributi logici per trasformare un valore di visualizzazione, come ad esempio il costo, nella schermata di attività in uno o più attributi fisici, come ad esempio prezzo unitario e quantità, archiviati nell'archivio utenti.

Nota: per ulteriori informazioni sui gestori di attributi logici, consultare la *Programming Guide for Java*.

Applicazione della logica aziendale personalizzata

È possibile personalizzare CA Identity Manager per implementare la logica aziendale richiesta dall'azienda. CA Identity Manager include le seguenti opzioni per implementare la logica aziendale personalizzata:

- Criteri di identità: è possibile utilizzare i criteri di identità per definire un insieme di modifiche aziendali che si verificano quando un utente soddisfa una determinata condizione o regola. Ad esempio, i criteri di identità possono automatizzare certe attività di gestione delle identità, come ad esempio l'assegnazione di ruoli o l'applicazione di regole aziendali, ad esempio per impedire agli utenti di firmare e di approvare assegni oltre $ 20.000.

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

- Gestori attributi logici: questi gestori possono essere associati a schermate di attività di CA Identity Manager per controllare la visualizzazione e la modifica di valori attributi.

  Per ulteriori informazioni, consultare la *Programming Guide for Java.*

- Gestori dell'attività di logica aziendale: consentono di eseguire una logica aziendale personalizzata, come ad esempio la seguente, durante le operazioni di convalida dei dati per un'attività di CA Identity Manager:

  - Applicazione di regole aziendali personalizzate (ad esempio, non è possibile consentire a un amministratore di gestire più di cinque gruppi).
  - Conferma di campi di schermate di attività specifici del cliente (ad esempio, il valore di un campo ID dipendente deve esistere nel database principale di Risorse umane).

  È possibile implementare i gestori dell'attività di logica aziendale in Java o JavaScript.

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

- Flusso di lavoro: consente di creare definizioni di processo personalizzate che vengono associate a un evento di CA Identity Manager.

Nota: prima di decidere se implementare la logica aziendale in un gestore dell'attività di logica aziendale o in un processo del flusso di lavoro, consultare le sezioni seguenti:

- Considerazioni sul gestore dell'attività di logica aziendale (a pagina 28)
- Considerazioni sui processi del flusso di lavoro (a pagina 28)

Considerazioni sul gestore dell'attività di logica aziendale

I gestori dell'attività di logica aziendale eseguono la convalida della logica aziendale durante la fase di elaborazione sincrona dell'attività, che si verifica prima della generazione di eventi. Questo consente di:

- Eseguire la convalida a livello di attività. Ad esempio, è possibile aggiungere o rimuovere membri di un gruppo sulla base della posizione dell'ufficio, specificata nella schermata del profilo utente.
- Impedire a un'attività di essere inviata se la convalida non riesce.
- Prima dell'invio dell'attività, trasformare automaticamente tutte le informazioni di una schermata di attività affinché corrisponda ai criteri aziendali

Nota: in un gestore dell'attività di logica aziendale è opportuno non implementare attività che richiedano tempi lunghi di completamento. Le attività a lunga esecuzione ritardano l'invio dell'attività e non sono adatte alla fase sincrona in cui si verifica l'interazione dell'utente. Si consiglia di utilizzare un processo del flusso di lavoro, che viene eseguito durante la fase asincrona dell'attività.

Considerazioni sui processi del flusso di lavoro

I processi del flusso di lavoro vengono chiamati durante la fase asincrona dell'attività e sono associati all'esecuzione di eventi singoli. Questo consente di:

- Eseguire attività di approvazione basate sui dati dell'evento singolo
- Eseguire attività di logica aziendale personalizzate a lunga esecuzione

Mentre l'API flusso di lavoro consente di ottenere dati a livello di attività da un'attività del flusso di lavoro, di norma si opera nel contesto di quell'evento specifico nel flusso di lavoro.

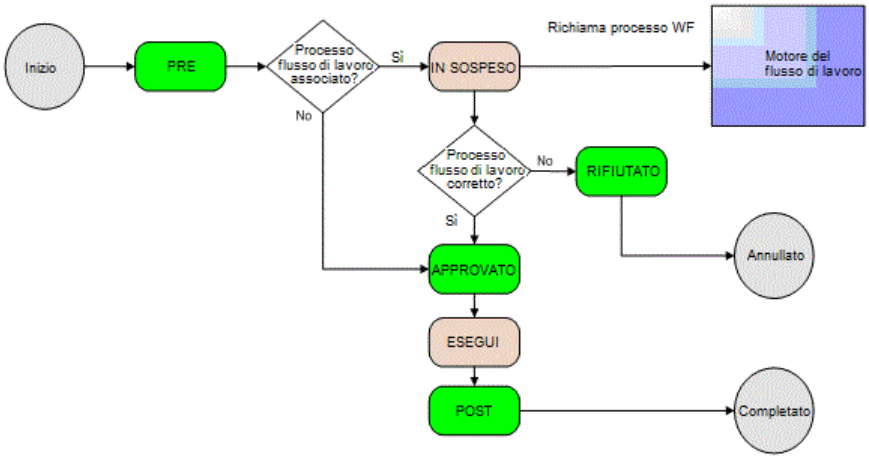
Approvazione delle modifiche aziendali

Il flusso di lavoro descrive un processo che consiste in una o più fasi che devono essere eseguite per raggiungere un obiettivo aziendale, come ad esempio eseguire una procedura di assunzione o ottenere l'affidabilità creditizia di un utente da un sistema esterno. Generalmente, una delle fasi di un processo del flusso di lavoro consiste nell'approvazione o nel rifiuto della modifica aziendale.

In CA Identity Manager, un processo del flusso di lavoro viene associato a un evento, un'azione che si verifica durante l'elaborazione di un'attività. Quando un evento entra nello stato In sospeso durante il suo ciclo di vita, CA Identity Manager richiama eventuali processi del flusso di lavoro associati e interrompe l'esecuzione dell'evento fino al completamento del processo. CA Identity Manager quindi esegue o rifiuta l'evento sulla base dei risultati del processo del flusso di lavoro.

Questa sequenza è illustrata nel diagramma seguente:

Ciclo di vita dell'evento ed elaborazione del flusso di lavoro



CA Identity Manager include il motore del flusso di lavoro InSession WorkPoint per creare e gestire i processi del flusso di lavoro.

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

Capitolo 3: Architettura di CA Identity Manager

Questa sezione contiene i seguenti argomenti:

Componenti di CA Identity Manager

Un'implementazione di CA Identity Manager può includere alcuni dei componenti seguenti oppure tutti:

- Server
- Archivi utenti
- Database
- Connettori

Server

Un'implementazione di CA Identity Manager include uno o più tipi di server, a seconda della funzionalità richiesta.

Server di CA Identity Manager (obbligatorio)

Esegue attività all'interno di CA Identity Manager. L'applicazione J2EE di CA Identity Manager include la console di gestione e la console utente.

Server di provisioning di CA Identity Manager

Gestisce account nei sistemi endpoint.

Questo server è necessario se l'installazione di CA Identity Manager supporterà il provisioning di account.

Nota: è necessario che la directory di provisioning sia installata in remoto (o in locale solo per un ambiente dimostrativo) su un server di CA Directory prima dell'installazione del server di provisioning.

Policy Server di SiteMinder

Fornisce l'autenticazione avanzata per CA Identity Manager, nonché l'accesso alle funzionalità di SiteMinder, quali Password Services e Single Sign-On.

Questo server è facoltativo.

Archivio utenti e directory di provisioning

CA Identity Manager coordina due archivi utenti:

- L'*archivio utenti di CA Identity Manager*, l'archivio utenti gestito da CA Identity Manager. Generalmente, questo è un archivio esistente che contiene le identità degli utenti che un'azienda deve gestire.

  L'archivio utenti può essere una directory LDAP o un database relazionale.

  Nella console di gestione, si crea un oggetto di directory di CA Identity Manager per la connessione all'archivio utenti e la descrizione degli oggetti dell'archivio utenti che verranno gestiti da CA Identity Manager.

- La *directory di provisioning*, l'archivio utenti gestito dal server di provisioning.

  È un'istanza di CA Directory e include utenti globali, che associano gli utenti della directory di provisioning agli account su endpoint, come ad esempio Microsoft Exchange, Active Directory e SAP.

  Solo alcuni utenti di CA Identity Manager dispongono di un utente globale corrispondente. Quando un utente di CA Identity Manager riceve un ruolo di provisioning, il server di provisioning crea un utente globale.

Separazione dell'archivio utenti dalla directory di provisioning

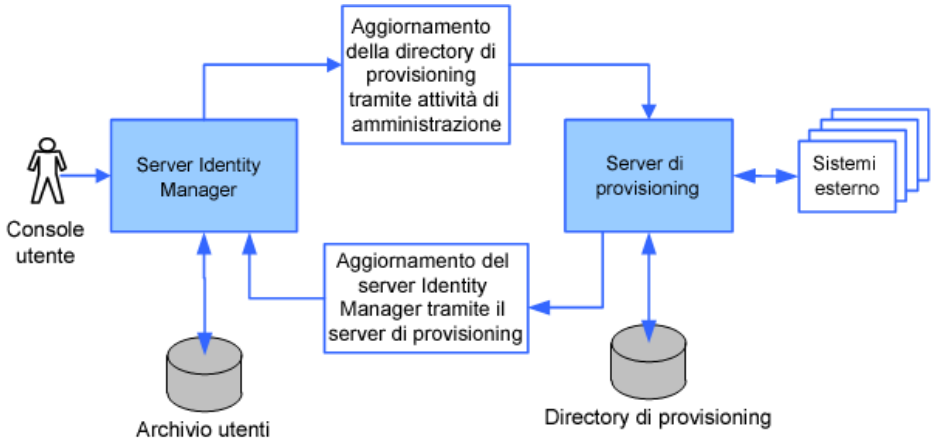
La figura seguente mostra un archivio utenti separato e una directory di provisioning che corrispondono allo scenario supportato per una nuova installazione di CA Identity Manager. In questa figura:

- Un amministratore di CA Identity Manager utilizza un'attività di amministrazione per la modifica di un utente nell'archivio utenti, la quale influisce sulla directory di provisioning.

  Questa modifica può anche aggiornare un endpoint (come ad esempio un server di messaggi di posta elettronica) che ha un connettore al server di provisioning.

  Una modifica apportata al server di provisioning (o a un endpoint con un connettore al server di provisioning) aggiorna l'archivio utenti di CA Identity Manager e la directory di provisioning.

Ad esempio, un endpoint, come ad esempio un'applicazione di Risorse umane, potrebbe aggiornare gli indirizzi di posta elettronica degli utenti.



Database

CA Identity Manager utilizza origini dati per connettersi a database che archiviano informazioni necessarie per supportare le funzionalità di CA Identity Manager. Questi database possono risiedere in un'unica istanza fisica di un database o in istanze separate.

Database di oggetti (obbligatorio)

Contiene informazioni di configurazione di CA Identity Manager.

Database di persistenza delle attività (obbligatorio)

Gestisce le informazioni sulle attività di CA Identity Manager e sui relativi eventi associati nel tempo. Questo consente al sistema di tenere accuratamente traccia delle attività di CA Identity Manager, anche se il server di CA Identity Manager viene riavviato.

Database di archiviazione (obbligatorio)

Archivia i dati provenienti dal database di persistenza delle attività.

Database del flusso di lavoro

Archivia le definizioni del processo del flusso di lavoro, processi, script e altri dati necessari al motore del flusso di lavoro.

Database di controllo

Fornisce un record cronologico delle operazioni che si verificano in un ambiente di CA Identity Manager.

Nota: è possibile configurare la quantità e il tipo di informazioni che CA Identity Manager archivia nel database di controllo. Per ulteriori informazioni, consultare la guida *Configuration Guide*.

Database di reporting

Archivia i dati delle snapshot che rispecchiano lo stato corrente degli oggetti in CA Identity Manager al momento in cui viene acquisita la snapshot. Da queste informazioni, è possibile generare rapporti per visualizzare la relazione tra gli oggetti, come ad esempio utenti e ruoli.

Quando si utilizza il programma di installazione, CA Identity Manager configura una connessione a un singolo database, chiamato database di CA Identity Manager, che contiene le tabelle per ciascun tipo di database.

Nota: è possibile creare un archivio dati per la persistenza delle attività, il flusso di lavoro, la verifica o il rapporto in un database separato e configurare CA Identity Manager affinché vi si connetta. Per ulteriori informazioni, consultare la *Guida all'installazione*.

Componenti del connettore

Un connettore è l'interfaccia software di un endpoint. Il server di provisioning utilizza il connettore per comunicare con l'endpoint. Questo traduce le azioni del server di provisioning in modifiche all'endpoint, quali ad esempio “Crea un nuovo account di posta in un endpoint Microsoft Exchange.”

Gli endpoint possono essere, ad esempio, workstation UNIX, PC di Windows o un'applicazione quale Microsoft Exchange (per la posta elettronica).

Server di connessione

Un server di connessione è un server di provisioning che gestisce i connettori. È possibile installarlo sul sistema di server di provisioning o su un sistema remoto.

Un server di connessione utilizza endpoint multipli. Ad esempio, se si dispone di numerosi endpoint di workstation UNIX, potrebbe essere presente un server di connessione che gestisce tutti i connettori che a loro volta gestiscono gli account UNIX. Un altro server di connessione potrebbe gestire tutti i connettori che richiedono account di Windows.

Il server di connessione distribuito utilizza server di connessione multipli. Esso fornisce il bilanciamento del carico quando un server di connessione è occupato e disponibilità elevata quando un server di connessione è inattivo.

Esistono due tipi di server di connessione:

- Il server di connessione IAM CA (CA IAM CS) gestisce connettori scritti in Java
- Il server di connessione C++ (CCS) gestisce connettori scritti in C++

Server di connessione C++

Il *server di connessione C++* è un server di connessione che gestisce i connettori C++. Può essere installato sul server di provisioning o su un sistema remoto. Il server di connessione C++ fornisce un framework di applicazione orientato all'oggetto che semplifica lo sviluppo di connettori, i quali sono responsabili della comunicazione tra il server di connessione C++ e l'endpoint.

CA IAM CS

CA IAM CS è un componente server che gestisce l'hosting di connettori Java, il routing verso questi ultimi e la loro gestione. CA IAM CS fornisce un'alternativa Java al server di connessione C++. Dal punto di vista architettonico e funzionale, è simile al server di connessione C++, tranne per il fatto che ha un'API Java anziché un'API C++, la quale consente ai connettori di essere implementati in Java. Inoltre, CA IAM CS è basato sui dati piuttosto che sul codice, il che consente al contenitore (o CA IAM CS), piuttosto che agli stessi connettori, di gestire più funzionalità.

Il server di provisioning gestisce il provisioning di utenti, quindi delega ai connettori (che utilizzano il server di connessione C++ o CA IAM CS) la gestione di account e gruppi di endpoint.

Connettori e agenti

I connettori di CA Identity Manager vengono eseguiti come parte della più ampia architettura del server di provisioning e comunicano con i sistemi gestiti nell'ambiente in uso. Un connettore funge da gateway per una tecnologia di sistema di tipo endpoint nativa. Ad esempio, i computer che eseguono i servizi Active Directory (ADS) possono essere gestiti solo se il connettore ADS è installato su un server di connessione con cui il server di provisioning può comunicare. I connettori gestiscono gli oggetti che risiedono nei sistemi. Gli oggetti gestiti includono account, gruppi e, in via facoltativa, oggetti specifici di tipo endpoint.

I connettori vengono installati sul server di connessione e alcuni componenti vengono installati sul server di provisioning (ad esempio, plug-in del server) o sul Manager di provisioning (plug-in dell'interfaccia utente).

Alcuni connettori richiedono un agente sui sistemi che gestiscono in modo da completare il ciclo di comunicazione, nel qual caso è possibile installarli utilizzando il programma di installazione di provisioning. È possibile suddividere gli agenti nelle seguenti categorie:

Agenti remoti

Installati su sistemi endpoint gestiti

Agenti di ambiente

Installati su sistemi quali CA ACF2, CA Top Secret e RACF

Alcuni componenti funzionano su UNIX e Windows, comprese le seguenti opzioni basate su server del connettore C++:

- UNIX (ETC, NIS)
- Access Control (ACC)

  Nota: il connettore ACC di UNIX può gestire solamente endpoint ACC di UNIX. Il connettore ACC di Windows deve gestire gli endpoint ACC di Windows, ma può gestire anche endpoint ACC di UNIX.
- CA ACF2
- RACF
- CA Top Secret

È possibile accedere agli altri connettori basati su server di connessione C++ dal server di provisioning Solaris facendo affidamento sulla struttura del server di connessione (ConneCSF). La CSF consente a un server di provisioning su Solaris di comunicare con i connettori in esecuzione su Windows.

Nota: per poter utilizzare questi connettori, la CSF deve essere eseguita su Windows.

Connector Xpress

Connector Xpress è un'utilità di CA Identity Manager per gestire connettori dinamici, eseguire il mapping di connettori dinamici sugli endpoint e stabilire regole di routing per gli endpoint. È possibile utilizzarlo per configurare connettori dinamici in modo da consentire il provisioning e la gestione di database SQL e directory LDAP.

Connector Xpress consente di creare e distribuire connettori personalizzati senza la perizia tecnica generalmente necessaria per la creazione di connettori gestiti dal Manager di provisioning.

Utilizzando Connector Xpress, è anche possibile installare, modificare e rimuovere una configurazione del server di connessione (sia Java che C++).

L'input primario in Connector Xpress è lo schema nativo di un sistema endpoint. Ad esempio, è possibile utilizzare Connector Xpress per connettersi a un RDBMS e recuperare lo schema SQL del database. Quindi, è possibile utilizzare Connector Xpress per costruire mapping dalle aree dello schema nativo rilevanti per il provisioning e la gestione di identità. Un mapping descrive come il livello di provisioning rappresenti un elemento dello schema nativo.

Connector Xpress genera metadati che descrivono a un connettore dinamico i mapping di runtime su un sistema di destinazione.

L'output di Connector Xpress è un documento di metadati prodotto al completamento dei mapping. Il documento di metadati è un file XML che descrive la struttura del connettore a CA IAM CS.

Tale documento descrive le classi e gli attributi del server di provisioning e la loro modalità di mapping sullo schema nativo.

I metadati vengono utilizzati per creare tipi di endpoint dinamici su uno o su più server di provisioning.

Nota: per ulteriori informazioni sull'utilizzo di Connector Xpress, consultare la *Connector Xpress Guide*, nel *bookshelf* di *CA Identity Manager*.

Componenti aggiuntivi

CA Identity Manager include alcuni componenti aggiuntivi che supportano le funzionalità di CA Identity Manager. Alcuni di questi componenti vengono installati con CA Identity Manager, mentre altri devono essere installati separatamente.

Flusso di lavoro WorkPoint

Il motore del flusso di lavoro di WorkPoint e WorkPoint Designer vengono installati automaticamente quando si installa CA Identity Manager.

Questi componenti consentono di mettere un'attività di CA Identity Manager sotto il controllo del flusso di lavoro e di modificare le definizioni esistenti del processo del flusso di lavoro o di crearne di nuove.

Nota: per ulteriori informazioni sul flusso di lavoro, consultare la *Guida per l'amministratore*.

Gestione provisioning

Il Manager di provisioning di CA Identity Manager gestisce il server di provisioning attraverso un'interfaccia grafica utilizzata per attività amministrative, quali la gestione delle opzioni del server di provisioning. In alcuni casi, il Manager di provisioning può essere utilizzato anche per gestire certi attributi dell'endpoint che non è possibile gestire nella console utente di CA Identity Manager.

Il Manager di provisioning viene installato come parte degli strumenti di amministrazione di CA Identity Manager.

Nota: questa applicazione viene eseguita soltanto su sistemi Windows.

Per ulteriori informazioni sul Manager di provisioning, consultare la *Provisioning Reference Guide*.

Server di rapporto

CA Identity Manager fornisce rapporti che è possibile utilizzare per monitorare lo stato di un ambiente di CA Identity Manager. Per utilizzare i rapporti forniti con CA Identity Manager, installare il server di rapporto incluso in CA Identity Manager.

Il server di rapporto utilizza la tecnologia Business Objects Enterprise XI. Se si dispone di un server Business Objects esistente, è possibile utilizzarlo al posto del server di rapporto per generare rapporti CA Identity Manager.

Nota: per le istruzioni di installazione, consultare la *Guida all'installazione*.

Installazioni di esempio di CA Identity Manager

Con CA Identity Manager, è possibile controllare le identità dell'utente e il loro accesso ad applicazioni e account su sistemi endpoint. Selezionare i componenti di CA Identity Manager da installare sulla base della funzionalità richiesta.

In tutte le installazioni di CA Identity Manager, il server di CA Identity Manager viene installato su un server applicazioni. Per installare gli altri componenti richiesti, utilizzare il programma di installazione di CA Identity Manager.

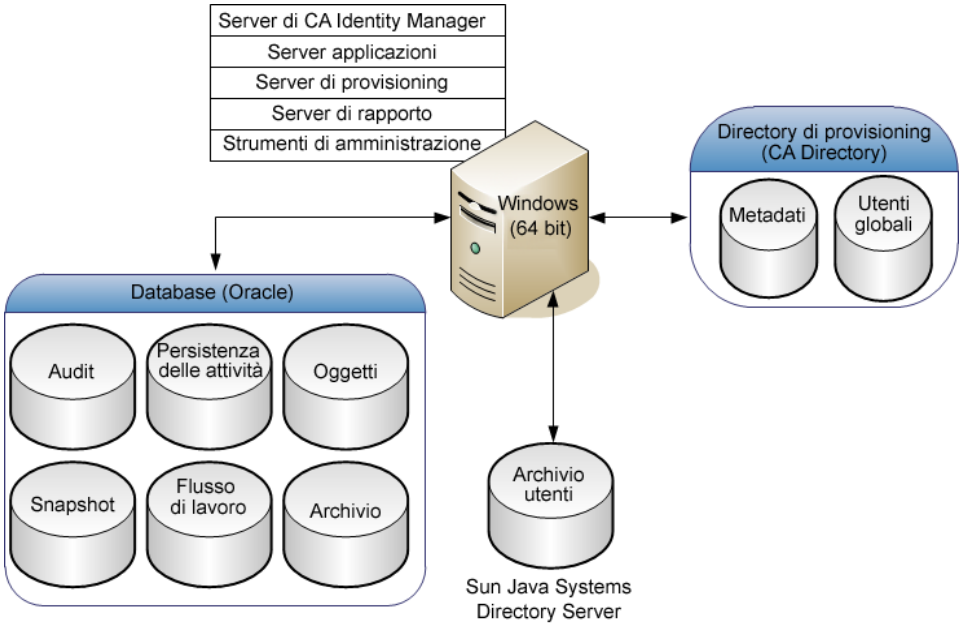
Le seguenti sezioni illustrano alcuni esempi di implementazioni di CA Identity Manager ad alto livello.

Installazione con componenti di provisioning

Il provisioning di CA Identity Manager consente di creare un ambiente che si connette a un server di provisioning per gli account di provisioning a vari sistemi endpoint. È possibile assegnare ruoli di provisioning a utenti creati mediante CA Identity Manager. I ruoli di provisioning sono ruoli con modelli di account che definiscono gli account che gli utenti possono ricevere su sistemi endpoint. Gli account forniscono agli utenti l'accesso a risorse aggiuntive, come ad esempio un account di posta elettronica.

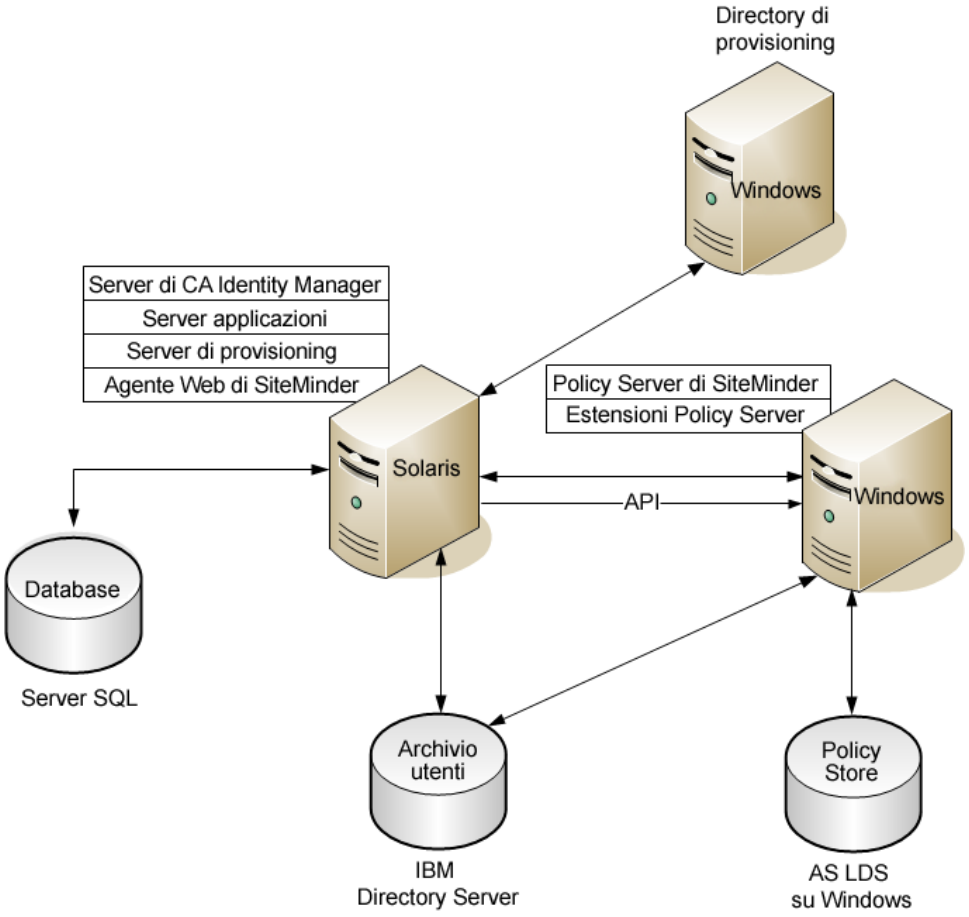
Quando si assegna un ruolo di provisioning a un utente, tale utente riceve gli account definiti dai modelli di account nel ruolo. I modelli di account definiscono anche le modalità di mapping degli attributi utente sugli account. Gli account vengono creati in endpoint gestiti definiti dai modelli di account.

La seguente figura è un esempio di un'installazione di CA Identity Manager con il provisioning:



Installazione con Policy Server di SiteMinder

Un Policy Server di SiteMinder fornisce la protezione e l'autenticazione avanzata per l'ambiente di CA Identity Manager. La seguente figura è un esempio di un'installazione di CA Identity Manager con un Policy Server di SiteMinder:



Un'implementazione di CA Identity Manager che include SiteMinder include tutti i componenti dell'installazione di base o dell'installazione con provisioning, oltre ai seguenti componenti aggiuntivi:

Agente Web di SiteMinder

Collabora con il Policy Server di SiteMinder per proteggere la console utente. L'agente Web viene installato nel sistema con il server di CA Identity Manager.

Policy Server di SiteMinder

Fornisce l'autenticazione avanzata e l'autorizzazione per CA Identity Manager, nonché altre funzionalità come Password Services e Single-Sign On.

Estensioni per Policy Server di SiteMinder

Consente a un Policy Server di SiteMinder di supportare CA Identity Manager. Installare le estensioni su ciascun sistema di Policy Server di SiteMinder nell'implementazione di CA Identity Manager.

Policy Store di SiteMinder

Archivia le informazioni necessarie a SiteMinder per gestire l'accesso alle risorse Web.

Quando CA Identity Manager si integra con SiteMinder, il Policy Store include anche informazioni sulle directory e sugli ambienti di CA Identity Manager, in modo che SiteMinder possa fornire l'autenticazione avanzata.

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, mentre l'archivio utenti si trova in IBM Directory Server. Il Policy Store di SiteMinder si trova in AD LDS su Windows.

Capitolo 4: Pianificazione dell'implementazione

Per pianificare un'implementazione di CA Identity Manager, è necessario stabilire la modalità di gestione degli utenti da parte di CA Identity Manager e le funzionalità necessarie per raggiungere i propri obiettivi aziendali. Alcune domande da considerare sono:

- Come gestire gli utenti?
- Il provisioning degli account è necessario?
- Quali sono i requisiti aziendali personalizzati ed è necessario implementarli utilizzando il flusso di lavoro?

Sulla base delle decisioni prese, è possibile stabilire il modo migliore per implementare CA Identity Manager nell'ambiente in uso.

Questa sezione contiene i seguenti argomenti:

Definizione degli elementi da gestire

La definizione degli elementi che si desidera gestire consente di stabilire i componenti da installare. CA Identity Manager consente di gestire i seguenti elementi:

- Identità degli utenti
- Accesso agli account su sistemi endpoint

Identità degli utenti

Le identità degli utenti rappresentano le persone che un'azienda deve gestire, quali dipendenti, terze parti, fornitori e altri.

Per gestire le identità degli utenti, è necessario installare solamente il server di CA Identity Manager e gli strumenti di amministrazione.

Configurazione del supporto della gestione utenti

In CA Identity Manager, gli utenti vengono gestiti con ruoli di amministrazione, che determinano le attività di CA Identity Manager che possono essere eseguite dagli amministratori.

Nota: prima di implementare la gestione utenti in CA Identity Manager, è necessario stabilire le funzionalità richieste e sviluppare un piano (a pagina 58) per implementare tali funzionalità in fasi.

Per configurare il supporto della gestione utenti, completare le seguenti fasi di alto livello:

1. Installare il server di CA Identity Manager e gli strumenti di amministrazione.

   Per eseguire il provisioning degli account per gestire gli utenti, sarà anche necessario installare il supporto per il provisioning (a pagina 45).

   Nota: per istruzioni, consultare la *Guida all'installazione*.

2. Nella console di gestione di CA Identity Manager, creare i seguenti elementi:

   - **Directory di CA Identity Manager**

     Descrive un archivio utenti a CA Identity Manager. Include le informazioni seguenti:

     - 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 rappresentati in CA Identity Manager.

   - **Ambiente di CA Identity Manager**

     Fornisce uno spazio dei nomi di gestione che consente agli amministratori di CA Identity Manager di gestire oggetti, quali utenti, gruppi e organizzazioni, con un insieme di ruoli e attività associati. L'ambiente di CA Identity Manager controlla la gestione e la presentazione grafica di una directory.

   Per ulteriori informazioni sulle directory e gli ambienti di CA Identity Manager, consultare la *Guida alla configurazione*.

3. Modificare le attività e i ruoli di amministrazione predefiniti perché rispondano ai propri requisiti aziendali.

   Le tipiche modifiche di ruolo includono l'aggiunta o la rimozione di attività predefinite nei ruoli di amministrazione esistenti o la creazione di nuovi ruoli di amministrazione basati sui ruoli predefiniti.

Le modifiche standard apportate alle attività includono la personalizzazione delle schede dei profili utente predefinite in modo che includano solamente le informazioni da gestire. (Le schede dei profili predefiniti includono tutti gli attributi definiti per gli utenti).

Per informazioni sulla modifica delle attività e dei ruoli di amministrazione predefiniti, consultare la *User Console Design Guide*.

4. Assegnare i ruoli di amministrazione agli utenti che eseguiranno attività di gestione dell'utente.

Account di provisioning da altre applicazioni

La decisione di implementare il provisioning dipende dal tipo di informazioni che è necessario gestire. Se si sta gestendo una directory utente centrale e non si intende gestire account utenti in altri sistemi, il provisioning non è necessario. Se si desidera gestire account utenti su vari sistemi, il supporto del provisioning deve essere implementato.

Le capacità di provisioning vengono fornite attraverso il server di provisioning, che viene integrato con CA Identity Manager. Il server di provisioning fornisce la seguente funzionalità per il provisioning degli account:

- Gestione endpoint
- Sincronizzazione account
- Modelli di account
- Funzionalità Esplora e Correla

Nota: le informazioni sul provisioning vengono archiviate in una directory di provisioning. Se CA Identity Manager gestisce gli utenti in un altro tipo di directory, la distribuzione includerà un archivio utenti e una directory di provisioning di CA Identity Manager.

Gestione endpoint

Per eseguire il provisioning degli account, definire e gestire gli endpoint nella console utente di CA Identity Manager. Un *endpoint* è un sistema per cui gli utenti necessitano dell'accesso. Gli endpoint sono, ad esempio, database Oracle, server UNIX NIS, server di Windows e server di Microsoft Exchange. Utilizzare *modelli di account* (a pagina 46) per creare account e determinare le capacità degli utenti in endpoint gestiti.

Nota: per definire e gestire gli endpoint, è anche possibile utilizzare il Manager di provisioning. Benché si consigli di utilizzare la console utente per la maggior parte delle attività di gestione di endpoint, alcune attività, quali la gestione di determinati attributi di endpoint e di oggetti endpoint che non siano account, richiedono l'uso del Manager di provisioning. Per ulteriori informazioni sul Manager di provisioning, consultare la *Provisioning Reference*.

Sincronizzazione account

È possibile sincronizzare account utenti in multipli endpoint gestiti. Quando la sincronizzazione account è abilitata, le modifiche apportate a un profilo utente nel server di provisioning vengono propagate a tutti gli endpoint in cui quell'utente possiede un account.

Nota: specificare le impostazioni di sincronizzazione account nella scheda Profilo per un'attività di CA Identity Manager. Per ulteriori informazioni sulla configurazione della sincronizzazione account, consultare la *Guida per l'amministratore*.

Modelli di account

I modelli di account definiscono la modalità di rappresentazione di un utente in un endpoint gestito. Ad esempio, un modello per un account di Exchange potrebbe definire il formato dell'indirizzo di posta elettronica di un utente, quale ad esempio <prima iniziale><cognome>@lamiaazienda.com.

I modelli di account determinano anche i privilegi di un utente all'interno di un sistema gestito. Ad esempio, oltre alla definizione del formato di un indirizzo di posta elettronica, un modello di un account di Exchange potrebbe anche limitare la dimensione della casella di posta elettronica di un utente.

I modelli di account vengono creati e gestiti nella console utente.

Funzionalità Esplora e Correla

Le funzionalità Esplora e Correla semplificano la gestione degli endpoint rilevando e sincronizzando le modifiche nei sistemi gestiti.

La funzionalità Esplora trova gli oggetti negli endpoint, compresi gli account, e archivia i riferimenti a tali oggetti nella directory di provisioning. È possibile utilizzare la funzionalità Esplora per individuare nuovi oggetti da gestire. Ad esempio, se si esegue il provisioning di account in una directory LDAP e in quella directory vengono aggiunte nuove organizzazioni, è possibile utilizzare la funzionalità Esplora per introdurre tali nuove organizzazioni da utilizzare in modelli di account.

La funzionalità Correla associa un account in un endpoint gestito a un utente globale nella directory di provisioning. Quando si apporta una modifica all'account attraverso l'endpoint, la funzionalità Correla può sincronizzare tali modifiche con l'account utente globale.

Nota: per ulteriori informazioni sulle funzionalità Esplora e Correla, consultare la *Guida per l'amministratore*.

Configurazione del supporto del provisioning

Dopo avere deciso di implementare il provisioning, si completano le seguenti fasi di alto livello.

1. Utilizzare il programma di installazione del server di CA Identity Manager per installare il server di CA Identity Manager, il server di provisioning, l'inizializzazione della directory di provisioning e gli strumenti di amministrazione.

   Nota: per ulteriori informazioni sull'installazione di componenti di CA Identity Manager, consultare la *Guida all'installazione*.

2. Configurare il Manager di provisioning per connettersi al server di CA Identity Manager.

3. Configurazione del provisioning nella console di gestione di CA Identity Manager:

   a. Abilitare il provisioning.

   b. Configurare un ambiente per il provisioning completando le seguenti operazioni:

      - Importazione delle definizioni di ruolo personalizzate
      - Configurazione di un amministratore in entrata
      - Connessione dell'ambiente al server di provisioning.

   Nota: per ulteriori informazioni, consultare la *Guida alla configurazione.*

4. Creare endpoint nella console utente.

   Questo consente a CA Identity Manager di gestire l'endpoint.

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

5. Esplorare e correlare l'endpoint.

   Quando si esplora un endpoint, CA Identity Manager trova gli oggetti nell'endpoint e archivia le istanze di tali oggetti nella directory di provisioning. Questa azione popola la directory di provisioning con gli account e gli altri oggetti trovati nell'endpoint.

   Quando si correlano gli account in un endpoint, CA Identity Manager li associa a un utente globale nella directory di provisioning. Si può scegliere se la funzione Correla creerà eventuali utenti globali non presenti o se assocerà gli account senza utente globale corrispondente all'utente globale [utente predefinito].

6. Creare e aggiornare account di endpoint utilizzando i modelli di account contenenti gli attributi utilizzati per creare gli account.

7. Associare i modelli di account ai ruoli di provisioning.

   Quando si assegnano ruoli di provisioning agli utenti, CA Identity Manager crea account negli endpoint associati per quegli utenti.

   Nota: per informazioni sui modelli di account e i ruoli di provisioning, consultare la *Guida per l'amministratore*.

Determinazione dei requisiti di verifica

CA Identity Manager include capacità di verifica che consentono di monitorare le attività in un ambiente di CA Identity Manager.

Queste informazioni vengono archiviate in un database di controllo. È possibile configurare la quantità e il tipo di informazioni archiviate nel database di controllo.

I dati di verifica vengono visualizzati nella console utente attraverso un'attività chiamata Visualizza attività inviate. Questa attività permette agli amministratori di cercare e visualizzare le attività che si verificano nel sistema. Gli amministratori possono visualizzare le informazioni sulle attività ad alto livello o visualizzare i dettagli relativi alle attività e agli eventi.

Considerazioni sulla verifica in CA Identity Manager

I dati di controllo forniscono un record cronologico delle operazioni che si verificano in un ambiente di CA Identity Manager. Per verificare i dati in CA Identity Manager, sono necessari i seguenti elementi:

- Un database di controllo
- Un file di impostazioni di audit

Database di controllo

Quando si utilizza il programma di installazione di CA Identity Manager, CA Identity Manager configura una connessione a un database singolo, chiamato database di CA Identity Manager, e crea un'origine dati per connettersi alle tabelle di database per la verifica.

Nota: il database di CA Identity Manager include anche dati che vengono utilizzati da altre funzionalità di CA Identity Manager, incluse la persistenza di attività, il flusso di lavoro e la creazione di rapporti. Ai fini della scalabilità, è possibile creare una nuova istanza separata di un database di controllo.

Nota: per ulteriori informazioni sul database di controllo, consultare la *Guida all'installazione*.

Impostazioni di audit

Le impostazioni di audit vengono configurate in un file di impostazioni di audit. Un file di impostazioni di audit determina la quantità e il tipo di informazioni sottoposte a verifica da parte di CA Identity Manager. È possibile configurare un file di impostazioni di audit per eseguire le seguenti operazioni:

- Abilitare la verifica di un ambiente di CA Identity Manager.
- Abilitare la verifica di alcuni o tutti gli eventi di CA Identity Manager generati da attività di amministrazione.
- Registrare informazioni 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.

Nota: per ulteriori informazioni sulla configurazione della verifica, consultare la *Guida alla configurazione*.

Considerazioni su CA Audit

CA Audit è un sistema di gestione della verifica che consente di raccogliere e archiviare dati relativi alla protezione per il controllo la creazione di rapporti, la verifica della conformità e il monitoraggio di eventi.

Per l'integrazione con CA Audit, installare il componente iRecorder al momento dell'installazione del server di CA Identity Manager. iRecorder recupera gli eventi da CA Identity Manager. Sulla base dei criteri presenti nel gestore dei criteri di CA Audit, iRecorder ignora l'evento o lo indirizza a CA Audit.

Definizione dei requisiti dell'archivio utenti

Un'implementazione di CA Identity Manager deve includere un archivio utenti che contiene le identità degli utenti gestiti da CA Identity Manager. Generalmente, si tratta di un archivio utenti esistente che un'azienda utilizza per archiviare informazioni sui propri utenti, quali ad esempio dipendenti e clienti.

Se l'implementazione in uso include il provisioning, CA Identity Manager richiede inoltre una directory di provisioning che include utenti globali, i quali vengono associati ad account in endpoint quali Microsoft Exchange, Active Directory e Oracle.

Gestione di archivi utenti multipli

Un'azienda può gestire archivi utenti multipli. In ciascun archivio utenti, l'identità dell'utente permette l'accesso a diverse risorse aziendali. È possibile utilizzare uno dei seguenti metodi per gestire archivi utenti multipli:

- Utilizzare CA Identity Manager per gestire direttamente la directory di provisioning e utilizzare il server di provisioning per gestire indirettamente gli utenti e gli account nei diversi archivi utenti.

  Questo approccio consente di:

  - Gestire in maniera centralizzata utenti a cui è possibile assegnare varie risorse aziendali da una posizione
  - Implementare una protezione comune e regole di business a tutte le risorse dell'azienda. Questo può includere quanto segue:
    - Controllo degli accessi basato sui ruoli
    - Amministrazione delegata
    - Attività e schermate personalizzate in base al tipo di identità aziendale che gestiscono

- Criteri di identità per la gestione di identità basata sulle regole
- Personalizzazione ed estendibilità

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

- Creare un ambiente di CA Identity Manager separato per gestire ciascun archivio utenti

  Con questo metodo, le informazioni non vengono condivise tra gli ambienti.

Selezione dei componenti da installare.

La seguente tabella elenca i componenti da installare per supportare la funzionalità da implementare.

Nota: per le istruzioni sull'installazione di questi componenti, consultare la *Guida all'installazione*.

Se si intende...	Installare questi componenti
Gestire le identità degli utenti in un archivio utenti aziendale esistente	■ Server di CA Identity Manager
Eseguire il provisioning degli account in sistemi endpoint	■ Server di provisioning ■ Directory di provisioning ■ Gestione provisioning ■ Connettori ■ Server di connessione **Nota**: per le istruzioni sull'installazione di connettori, consultare la *Guida al connettore* per il tipo di connettori da installare.

Se si intende...	Installare questi componenti
Implementare una o più delle seguenti funzionalità: ■ Autenticazione avanzata ■ Criteri di password avanzati ■ Interfacce di console diverse per diverse serie di utenti ■ Configurazione delle preferenze delle impostazioni internazionali per gli utenti	■ Policy Server di SiteMinder ■ Policy Store ■ Agente Web di SiteMinder ■ Estensioni di CA Identity Manager al Policy Server **Nota**: per istruzioni sull'installazione del Policy Server e del Policy Store di SiteMinder, consultare la *Guida all'installazione dei server di criteri per Web Access Manager di CA SiteMinder* .Per istruzioni sull'installazione dell'agente Web, consultare la *Guida all'installazione dell'agente Web di Web Access Manager di CA SiteMinder* .
Generare rapporti sulle attività di CA Identity Manager	Server di rapporto

Decisione sui requisiti hardware

L'hardware necessario per l'installazione di CA Identity Manager dipende dalla funzionalità che si intende implementare e dalla dimensione della distribuzione.

Le seguenti sezioni descrivono implementazioni più frequenti di CA Identity Manager e il relativo hardware necessario.

Tipi di distribuzione

Durante la pianificazione dell'hardware necessario per una distribuzione di CA Identity Manager, considerare le funzionalità da implementare e la dimensione iniziale della distribuzione. Utilizzare una delle categorie seguenti per effettuare una stima della dimensione della distribuzione.

Nota: il tipo di distribuzione selezionato determina la dimensione del file DxGrid utilizzato dalla directory di provisioning. Il tipo di distribuzione viene specificato quando si installa il server di CA Identity Manager.

Dimostrazione

Una distribuzione di server singolo per l'uso in dimostrazioni o la verifica di base in un ambiente di sviluppo. Una distribuzione dimostrativa supporta fino a 10.000 account con provisioning.

Nota: questo tipo di implementazione non supporta le implementazioni di produzione.

Di base

Un'implementazione a disponibilità elevata adatta alla maggior parte delle implementazioni di piccole e medie dimensioni. Una distribuzione di base supporta fino a 400.000 account con provisioning.

Questo tipo di implementazione richiede due server per eseguire l'applicazione di CA Identity Manager e i relativi componenti e due server per eseguire il database di CA Identity Manager e l'archivio utenti.

Intermedia

Un'implementazione a disponibilità elevata adatta alle implementazioni di medie dimensioni. Una distribuzione intermedia supporta fino a 600.000 account con provisioning.

Grande azienda

Un'implementazione a disponibilità elevata che include cluster di server aggiuntivi per indirizzare utenti aggiuntivi e un numero crescente di transazioni. Una grande distribuzione supporta oltre 600.000 account con provisioning.

Nota: per ulteriori informazioni sulle implementazioni a disponibilità elevata, consultare la *Guida all'installazione*.

Requisiti aggiuntivi per il provisioning

Oltre ai componenti richiesti per un'implementazione di CA Identity Manager di base, sono necessari i seguenti componenti aggiuntivi se CA Identity Manager include il provisioning:

- Server di provisioning

  Può essere installato sullo stesso computer del server di CA Identity Manager.

- Inizializzazione della directory di provisioning

  Importante. È necessario installare l'inizializzazione della directory di provisioning in CA Directory.

- Gestione provisioning

  Può essere installato su qualsiasi computer con Windows che può accedere al server di provisioning.

Nota: in un ambiente di sviluppo, è possibile installare questi componenti su un computer che include anche i componenti di installazione di base.

Requisiti aggiuntivi per l'integrazione di SiteMinder

Quando CA Identity Manager integra SiteMinder, l'implementazione deve includere i componenti nell'installazione di CA Identity Manager di base, più i seguenti componenti aggiuntivi:

- **Server di criteri**

  Fornisce i servizi per la contabilità e la gestione, l'autenticazione e l'autorizzazione di criteri.

  È possibile installare il Policy Server sullo stesso computer del server di CA Identity Manager, se il Policy Server è dedicato a CA Identity Manager. Se il Policy Server sta proteggendo altre applicazioni, per assicurare le massime prestazioni si consiglia di installarlo su un computer separato.

- **Policy Store**

  Contiene tutti i dati del Policy Server. È possibile configurare un Policy Store in un database relazionale o LDAP supportato. Per le implementazioni a disponibilità elevata, si consiglia di installare il Policy Store su un server separato.

- **Estensioni del Policy Server**

  Consente a un Policy Server di SiteMinder di supportare CA Identity Manager. Installare le estensioni su ciascun sistema di Policy Server di SiteMinder nell'implementazione di CA Identity Manager.

- **Agente Web di SiteMinder**

  Collabora con il Policy Server di SiteMinder per proteggere la console utente. Installato sul sistema con il server di CA Identity Manager.

Selezione di un metodo per l'importazione di utenti

Se è necessario importare utenti in un archivio utenti esistente, basare il metodo selezionato sui requisiti aziendali.

Le seguenti sezioni descrivono le opzioni per l'importazione di utenti.

Importazione di utenti in un nuovo archivio utenti

Dopo aver stabilito la modalità di archiviazione dei dati degli utenti, potrebbe essere necessario importare gli utenti da un archivio a un altro. A seconda dell'implementazione in uso, è possibile utilizzare diversi modalità di importazione degli utenti.

Nota: dopo avere importato gli utenti in un nuovo archivio utenti, è possibile utilizzare criteri di identità (a pagina 56) per applicare le modifiche agli utenti importati.

Importazione di utenti utilizzando CA Identity Manager

CA Identity Manager fornisce i seguenti metodi per aggiungere utenti a un archivio utenti gestito direttamente da CA Identity Manager.

di autenticazione	Funzionalità	Limitazioni
Bulk Loader	Consente di utilizzare l'attività dell'Utilità di caricamento in blocco nella console utente per caricare i file di alimentatore utilizzati per gestire simultaneamente un grande numero di oggetti gestiti. Il vantaggio del metodo Utilità di caricamento in blocco consiste nella possibilità di automatizzare il processo di gestione di un grande numero di oggetti gestiti utilizzando un file (alimentatore) di informazioni. Inoltre, è possibile mappare l'attività Bulk Loader su un processo del flusso di lavoro.	Se si sta utilizzando l'Utilità di caricamento in blocco, potrebbero presentarsi eccezioni di memoria insufficiente a seconda del numero di utenti che si sta importando. Per risolvere questo problema, aumentare le impostazioni di memoria di JVM.
Chiamata di attività remota mediante il Servizio Web per l'esecuzione di attività (TEWS, Task Execution Web Service)	Consente l'esecuzione di qualsiasi attività di CA Identity Manager abilitata per i servizi Web, compresa l'attività Crea utente. Se l'attività viene configurata per la sincronizzazione utente, CA Identity Manager eseguirà qualsiasi criterio di identità applicabile.	Le caratteristiche delle prestazioni del modello di servizio Web potrebbero non essere adatte ai requisiti di velocità elevata delle operazioni di importazione in blocco

API IM	■ Fornisce API basate sull'utente che è possibile richiamare direttamente per creare utenti attraverso un client di Java ■ Fornisce le capacità di velocità più elevate.	■ Ignora i meccanismi di verifica e di protezione forniti dal server di attività. ■ Non supporta l'esecuzione di criteri di identità.

Nota: per ulteriori informazioni sull'Utilità di caricamento in blocco, consultare la *Guida per l'amministratore*. Per ulteriori informazioni su TEWS e sull'API IM, consultare la guida *Programming Guide for Java*.

Esecuzione di criteri di identità su utenti importati

Un *criterio di identità* è un insieme di modifiche di business che si verificano quando un utente soddisfa una determinata condizione o regola. Queste modifiche possono includere l'assegnazione o la revoca di ruoli (inclusi ruoli di provisioning per utenti nella directory di provisioning), l'assegnazione o la revoca dell'appartenenza a un gruppo e l'aggiornamento di attributi in un profilo utente.

È possibile utilizzare criteri di identità per applicare modifiche ad account utenti dopo la loro importazione in un nuovo archivio utenti.

Questa sezione descrive i metodi per eseguire i criteri di identità per utenti importati in una o due fasi.

Approccio a una fase

È possibile utilizzare i seguenti metodi di importazione per eseguire criteri di identità su utenti importati in un nuovo archivio utenti in una singola fase:

- Utilità di caricamento in blocco nella console utente
- Esecuzione dell'attività Crea utente tramite TEWS
- Sincronizzazione in entrata

Approccio a due fasi

Utilizzando un approccio a due fasi, innanzitutto si importano gli utenti, quindi si eseguono i criteri di identità su tali utenti. È possibile utilizzare questo metodo quando CA Identity Manager gestisce gli utenti nel server di provisioning. Questo metodo può fornire una maggiore flessibilità, a seconda dei requisiti di importazione.

1. Per aggiungere utenti nella directory di provisioning, utilizzare uno degli strumenti di importazione.
2. Richiamare l'attività di CA Identity Manager Sincronizza utente attraverso TEWS in ciascuno degli utenti importati.

Importazione di utenti attraverso il server di provisioning

Il server di provisioning include opzioni di importazione in blocco per aggiungere e gestire gli utenti nella directory di provisioning. Le seguenti tabelle descrivono i metodi per importare gli utenti nella directory di provisioning.

di autenticazione	Funzionalità	Limitazioni
Utilità batch (etautil)	Un'utilità dell'interfaccia della riga di comando che consente di gestire oggetti nella directory di provisioning	■ Attualmente supportata solo per sistemi Windows
Esplora e Correla	■ Scopre nuovi oggetti che il server di provisioning può gestire in un endpoint noto (inclusi gli utenti) ■ Fornisce capacità correlate per le istanze di oggetti che esistono nell'endpoint e nel server di provisioning. Ulteriori informazioni sono disponibili in Funzionalità Esplora e Correla.	■ Per impostazione predefinita, la funzionalità Esplora e Correla è disponibile per i connettori attualmente supportati. Può essere ampliata con connettori personalizzati ■ L'opzione Correla può influire sulla scalabilità se si utilizzano set risultanti di utenti di grandi dimensioni. Se si seleziona questa opzione di importazione, assicurarsi di valutare le implicazioni in termini di prestazioni e scalabilità.

Sincronizzazione di utenti globali con l'archivio utenti di CA Identity Manager

Dopo aver importato gli utenti nel server di provisioning, è possibile utilizzare i seguenti metodi per aggiungere quegli utenti all'archivio utenti di CA Identity Manager:

- **Sincronizzazione in entrata**

  La sincronizzazione in entrata mantiene gli utenti di CA Identity Manager aggiornati rispetto alle modifiche effettuate nella directory di provisioning. Le modifiche alla directory di provisioning includono quelle apportate utilizzando il Manager di provisioning o i sistemi con connettori al server di provisioning.

  Quando si utilizza la sincronizzazione in entrata per importare utenti, è opportuno considerare quanto segue:

  - Nella console di gestione di CA Identity Manager, è possibile personalizzare la modalità di mapping degli attributi dalla richiesta in entrata agli attributi nell'attività di CA Identity Manager.

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

  - Considerare quali modifiche al server di provisioning richiedano la sincronizzazione con l'archivio utenti aziendale. La sincronizzazione di un grande numero di modifiche può avere un impatto negativo su prestazioni e scalabilità.

- **Ruoli di provisioning e modelli di account**

  Il server di provisioning può gestire account nell'archivio utenti di CA Identity Manager mediante ruoli di provisioning e modelli di account. Questo richiede che un endpoint gestito, che punta all'archivio utenti di CA Identity Manager, sia stato acquisito e che i ruoli e i modelli di account appropriati esistano. In questo caso, agli utenti globali creati attraverso una delle opzioni descritte in Importazione di utenti attraverso il server di provisioning può essere assegnato un ruolo di provisioning che crea l'account utente nell'archivio utenti di CA Identity Manager.

Sviluppo di un piano di distribuzione

Durante la pianificazione di un'implementazione di grandi dimensioni, la distribuzione di funzionalità di CA Identity Manager dovrebbe avvenire in fasi. Il seguente ordine di distribuzione consente di ottenere rapidamente un valore significativo da CA Identity Manager, valutare le mutevoli esigenze dell'implementazione in uso nel tempo e costruire attentamente l'ambiente per le migliori prestazioni e la perfetta scalabilità:

- Self-service e Gestione password
- Criteri di identità
- Approvazioni del flusso di lavoro

- Amministrazione delegata per utente, gruppo e oggetti di organizzazione
- Amministrazione delegata per l'amministrazione di ruoli

Dopo ogni fase di distribuzione, assicurarsi di valutare le prestazioni e di effettuare adeguamenti prima di passare alla fase successiva. L'ottimizzazione di CA Identity Manager (a pagina 69) fornisce informazioni su prestazioni, ottimizzazione e scalabilità.

Distribuzione di Self-service e Gestione password

Effettuare la distribuzione di attività di self-service e gestione password prima di distribuire altre funzionalità di CA Identity Manager per le seguenti ragioni:

- Le attività di self-service e gestione password sono facili da distribuire e forniscono rapidamente un valore significativo.
- Queste funzionalità sono indipendenti dal modello di amministrazione delegato e possono essere riconfigurate in base alle necessità per affrontare le mutevoli esigenze aziendali.
- Queste funzionalità generalmente generano il volume più alto di attività che CA Identity Manager elabora su base regolare. Di conseguenza, forniscono un modo per verificare la scalabilità dell'implementazione prima della distribuzione di funzionalità aggiuntive.

Per distribuire le attività self-service, completare le seguenti fasi:

1. Configurazione dell'attività di registrazione automatica.

   Questa è un'attività pubblica, che viene abilitata per impostazione predefinita durante l'installazione. Per configurare questa attività, aggiungere o rimuovere campi dall'attività di registrazione automatica predefinita, in base alle necessità.

2. Distribuzione del ruolo Gestione automatica.

   La regola membri per questo ruolo deve essere configurata perché possa essere applicata a tutti gli utenti o deve includere una regola membri che assegna automaticamente il ruolo a nuovi utenti. Ad esempio, è possibile creare una regola membri che assegni il ruolo Self Manager (Manager automatico) a tutti i dipendenti a tempo pieno. Quando un utente effettua la registrazione automatica, CA Identity Manager può impostare il tipo di dipendente su Full-time (A tempo pieno) (utilizzando un gestore attributo logico o un gestore di attività di business). L'utente soddisfa i criteri della regola membri e riceve automaticamente il ruolo Self Manager (Manager automatico).

   Nota: quando si configurano regole membri per il ruolo Self Manager (Manager automatico), non consentire agli amministratori di aggiungere o rimuovere membri dei ruoli. Poiché il ruolo viene assegnato automaticamente, non è necessario che un amministratore assegni il ruolo esplicitamente.

Per effettuare la distribuzione di capacità di gestione password, completare le seguenti fasi:

1. Configurare le attività pubbliche di gestione password, quali l'attività di Password dimenticata.
2. Creare criteri di password che stabiliscono la modalità di creazione e la scadenza delle password.
3. Effettuare la distribuzione del ruolo Manager password, che abilita i membri del ruolo a ripristinare le password utenti.

Nota: per informazioni su ruoli, attività e gestione password, consultare la *Guida per l'amministratore*.

Distribuzione dei criteri di identità

Un criterio di identità è un insieme di modifiche di business che si verifica quando un utente soddisfa una determinata condizione o regola. È possibile utilizzare criteri di identità per fornire diritti guidati dal business prima della distribuzione di un modello di delegazione completo. Ad esempio, è possibile creare un criterio di identità che assegna il ruolo di provisioning di Responsabile delle vendite, il quale concede l'accesso ad applicazioni di vendita, a tutti gli utenti il cui titolo è Responsabile delle vendite. Quando un rappresentante viene promosso a responsabile delle vendite, riceve automaticamente l'accesso a tutti i sistemi necessari per svolgere il proprio lavoro senza il coinvolgimento dell'amministratore.

Per effettuare la distribuzione dei criteri di identità, completare le seguenti fasi:

1. Configurare criteri di identità che vengono attivati da modifiche agli attributi del profilo utente.
2. Configurare il ruolo Manager utente per consentire a un numero limitato di amministratori di utilizzare attività utente, quali Crea Utente e Modifica utente, per modificare gli attributi che attivano i criteri di identità.

   Assicurarsi di configurare le regole di ambito nei criteri membri di Manager utente per determinare il set di utenti che può essere gestito dai membri del ruolo.

Quando si distribuiscono i criteri di identità, osservare quanto segue:

- Potrebbe essere opportuno creare innanzitutto criteri di identità che concedono diritti che *non* richiedono approvazioni del flusso di lavoro. Questo consente di distribuire criteri di identità senza dovere definire processi del flusso di lavoro, moduli di approvazione e modelli di responsabile dell'approvazione.
- Prima di creare criteri di identità, occorre avere familiarità con altri metodi di implementazione delle regole di business in CA Identity Manager, quali ad esempio le regole di convalida dei dati, gli attributi logici, i gestori di attività di logica aziendale e i processi del flusso di lavoro, per determinare quale metodo fornisce la soluzione migliore.

  Nota: per ulteriori informazioni su questi metodi, consultare la *Guida per l'amministratore* e la *Programming Guide for Java*.
- I criteri di identità sono un modo efficace di assegnare diritti in CA Identity Manager, ma possono avere un impatto significativo sulle prestazioni (a pagina 85).
- Per la distribuzione iniziale di attività utente, considerare l'opportunità di rimuovere o nascondere le schede di relazione, quali le schede Ruoli, che gestiscono gli stessi diritti dei criteri di identità. Questo previene il rischio di diritti non autorizzati e l'impatto di ruoli costruiti in modo improprio sulle potenziali prestazioni.

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

Distribuzione di approvazioni del flusso di lavoro

Le approvazioni del flusso di lavoro possono aggiungere un livello di protezione e automazione supplementare all'implementazione di CA Identity Manager.

La distribuzione delle approvazioni del flusso di lavoro richiede le seguenti attività:

1. Decidere quali eventi o quali attività richiedano approvazioni.
2. Definire l'insieme di responsabili dell'approvazione, chiamati partecipanti, per ciascun processo del flusso di lavoro.

   Nota: tutti i partecipanti vengono determinati in modo dinamico da resolver partecipanti. Per mantenere buone prestazioni, limitare il numero dei partecipanti a trenta utenti.
3. Configurare moduli di approvazione.
4. Definire i processi del flusso di lavoro personalizzati, se necessario.

Approvazioni del flusso di lavoro a livello di ambiente e attività

CA Identity Manager supporta due tipi di approvazioni: approvazioni a livello di ambiente e approvazioni a livello di attività. Le approvazioni a livello di ambiente vengono definite per tutte le istanze di un evento, a prescindere dalle attività alle quali sono associate. Le approvazioni a livello di attività vengono definite per un evento specifico associato a una determinata attività. Le approvazioni a livello di attività hanno la priorità rispetto alle approvazioni a livello di ambiente.

La maggior parte delle approvazioni viene definita a livello di ambiente per assicurare che per un evento si verifichino le stesse attività del flusso di lavoro, indipendentemente dall'attività alla quale è associato. Tuttavia, nelle seguenti situazioni, considerare l'opportunità di implementare il flusso di lavoro a livello di attività:

- Attività specializzate che eseguono specifiche modifiche di business che generano eventi che non richiedono approvazioni.
- Azioni di modifica, attivate da criteri di identità, che generano eventi che non richiedono approvazione del flusso di lavoro.
- Si necessita della flessibilità per associare processi specifici del flusso di lavoro a modifiche specifiche dell'attività.

Le approvazioni a livello di ambiente possono richiedere una crescente quantità di risorse di sistema e di elaborazione con l'aumentare del volume delle transazioni. Questo può infine comportare problemi di prestazioni e scalabilità. L'utilizzo di approvazioni a livello di attività, laddove necessario, può ridurre o eliminare questi problemi.

Distribuzione dell'amministrazione delegata per utenti, gruppi e organizzazioni

L'amministrazione delegata è la gestione degli utenti e dei relativi diritti in cui vari utenti di CA Identity Manager eseguono le funzioni di modifica, assegnazione e utilizzo di un ruolo.

Nota: i modelli di delegazione devono essere creati attentamente per garantire buone prestazioni e scalabilità nell'implementazione di CA Identity Manager.

La delegazione viene applicata da regole di ambito, definite in criteri membri e di amministrazione per i ruoli di amministrazione. Una regola di ambito determina gli oggetti in cui un membro del ruolo può utilizzare il ruolo. Ad esempio, una regola di ambito può abilitare un manager utente per la gestione di utenti nel proprio dipartimento, ma non in altri dipartimenti.

Generalmente, le regole di ambito dovrebbero riflettere la struttura logica dell'archivio utenti. Ad esempio, in un archivio utenti LDAP gerarchico, l'ambito può essere definito da organizzazioni. In un database relazionale, l'ambito può essere definito mediante attributi, quali l'ID dipartimento.

Quando si distribuisce l'amministrazione delegata per utenti, gruppi e organizzazioni, occorre tenere presente quanto segue:

- Durante le attività relative agli utenti, limitare l'accesso alle schede di relazione, quali Ruoli di amministrazione e Ruoli di provisioning. Queste schede di relazione vengono incluse in attività utente predefinite, quali Crea utente e Modifica utente. Considerare l'opportunità di rimuoverle dalle attività predefinite e utilizzarle solamente in attività specializzate associate a un numero limitato di ruoli di amministrazione.
- CA Identity Manager valuta ogni regola di ambito in modo dinamico. Le informazioni di ambito non vengono memorizzate nella cache. Valutare la possibilità di creare regole di ambito che contengano query di directory semplici per garantire buone prestazioni.
- Valutare le prestazioni delle regole di ambito determinando il tempo impiegato da CA Identity Manager per restituire gli oggetti che un amministratore può gestire.

Distribuzione dell'amministrazione delegata per i ruoli

L'amministrazione delegata di ruoli concede i privilegi più significativi in CA Identity Manager e può avere l'effetto più significativo (a pagina 70) sulle prestazioni. Per queste ragioni, è opportuno valutare la possibilità di distribuire l'amministrazione delegata per i ruoli dopo aver distribuito tutte le altre funzionalità.

Durante la distribuzione dell'amministrazione delegata per i ruoli, occorre notare quanto segue:

- Limitare il numero di ruoli di amministrazione, membri del ruolo di amministrazione e amministratori di ruolo di amministrazione per proteggere l'ambiente e garantire buone prestazioni.
- Una volta distribuita l'amministrazione delegata per i ruoli, condurre verifiche su prestazioni e scalabilità. Ottimizzare l'ambiente in base alle necessità.

Capitolo 5: Integrazione con 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:

Installazione con Policy Server di SiteMinder (a pagina 41)

Autenticazione SiteMinder

CA Identity Manager include le seguenti console, che devono essere protette:

Console utente

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

Console di gestione

Consente agli amministratori di CA Identity Manager di creare e configurare una directory di CA Identity Manager, una directory di provisioning e un ambiente di CA Identity Manager.

CA Identity Manager include l'autenticazione nativa, che protegge la console utente per impostazione predefinita. La console di gestione non viene protetta per impostazione predefinita, ma è possibile configurare CA Identity Manager per proteggerla. Anche CA SiteMinder può essere utilizzato per proteggere la console di gestione.

Per configurare altri tipi di autenticazione per la console utente, quali il certificato o l'autenticazione chiave, è necessario che CA Identity Manager sia integrato con SiteMinder.

Nota: per ulteriori informazioni, consultare la *Guida alla configurazione.*

Capitolo 6: Ottimizzazione di CA Identity Manager

Questa sezione contiene i seguenti argomenti:

Prestazioni di CA Identity Manager

Le prestazioni di CA Identity Manager dipendono dalle prestazioni individuali delle varie funzionalità e dei vari componenti.

È possibile ottimizzare le seguenti funzionalità in un ambiente di CA Identity Manager:

- Ruoli
- Attività
- Appartenenza al gruppo e relativa gestione
- Criteri di identità

Per un ulteriore miglioramento delle prestazioni, è possibile ottimizzare anche i seguenti componenti:

- Archivio utenti
- Componenti di provisioning
- Componenti di runtime, compresi i database, quali il database di persistenza delle attività e le impostazioni del server applicazioni

Per garantire le migliori prestazioni, configurare le funzionalità di CA Identity Manager seguendo le linee guida nelle seguenti sezioni. Quindi, misurare i componenti di prestazione e ottimizzazione, in base alle necessità. Perché i componenti collaborino, potrebbero occorrere numerose iterazioni prima di trovare le migliori impostazioni di ottimizzazione per l'ambiente.

Ottimizzazioni dei ruoli

CA Identity Manager include tre tipi di ruoli:

- Ruoli di amministrazione

  Stabilire i privilegi di cui un utente dispone nella console utente.

  Quando un utente si collega a un ambiente di CA Identity Manager, l'account utente possiede uno o più ruoli di amministrazione. Ciascun ruolo di amministrazione contiene attività, quali Crea utente, che un utente può completare in quell'ambiente di CA Identity Manager. I ruoli di amministrazione di un utente determinano la presentazione della console utente, pertanto gli utenti vedono solamente le attività associate ai loro ruoli.

- Ruoli di provisioning

  Dare agli utenti account in endpoint gestiti, ad esempio in un sistema di posta elettronica.

- Ruoli di accesso

  Offrire un altro modo di fornire diritti in CA Identity Manager.

I ruoli includono criteri che determinano quanto segue:

- Chi può utilizzare il ruolo (solo per i ruoli di amministrazione e di accesso) e dove tale ruolo può essere utilizzato
- Chi può gestire i membri e gli amministratori dei ruoli
- Chi può modificare la definizione del ruolo

La valutazione dei ruoli e dei privilegi ad essi associati può avere un impatto significativo sulle prestazioni di CA Identity Manager.

Come la valutazione dei ruoli influisce sulle prestazioni in fase di accesso

Quando un utente di CA Identity Manager tenta di accedere alla console utente, si verificano le seguenti azioni:

1. CA Identity Manager richiede all'utente di fornire le credenziali, quali nome utente e password.
2. Le credenziali dell'utente vengono autenticate mediante uno dei metodi seguenti:
   - Autenticazione nativa di CA Identity Manager
   - Autenticazione di SiteMinder, se l'implementazione di CA Identity Manager include SiteMinder

3. CA Identity Manager valuta ogni criterio membri per ogni ruolo di amministrazione nell'ambiente, per determinare quali ruoli di amministrazione si applicano all'utente.

   Nota: questa valutazione viene effettuata una volta sola per un determinato utente. Dopo la valutazione iniziale, CA Identity Manager memorizza i risultati nella cache. CA Identity Manager utilizza le informazioni memorizzate nella cache finché non viene apportata una modifica all'utente o all'insieme di criteri membri, che fa sì che CA Identity Manager aggiorni le informazioni nella cache.

4. La console utente di CA Identity Manager visualizza le categorie che l'utente può visualizzare in base ai propri ruoli.

Questo processo si verifica per ogni utente che accede alla console utente. Se un ambiente di CA Identity Manager contiene un grande numero di ruoli o criteri membri inefficienti, la valutazione di appartenenza a un ruolo può avere un impatto significativo sulle prestazioni. In questo caso, la schermata iniziale visualizzata dagli utenti che accedono alla console utente può comparire lentamente.

Nota: CA Identity Manager non valuta i criteri membri quando un utente accede a un'attività pubblica per effettuare la registrazione automatica o richiedere una password dimenticata. In questi casi, CA Identity Manager non ha bisogno di un elenco dei ruoli dell'utente perché non visualizza l'intera console utente.

Prestazioni e oggetti di ruolo

Per supportare ciascun ruolo, CA Identity Manager crea un numero di oggetti nell'archivio oggetti (a pagina 33) di CA Identity Manager, a seconda della configurazione del ruolo.

CA Identity Manager crea un oggetto di base per ciascun ruolo. In aggiunta all'oggetto di base, CA Identity Manager crea un oggetto per ciascun criterio.

Un grande numero di oggetti di ruolo possono avere un impatto negativo sulle prestazioni delle ricerche nell'archivio oggetti e sulle valutazioni dei criteri.

Prestazioni dell'archivio oggetti

CA Identity Manager archivia le informazioni necessarie per la gestione di utenti e diritti in un archivio oggetti. Un grande numero di oggetti di ruolo nell'archivio oggetti può causare i seguenti problemi:

- Le ricerche di oggetti gestiti nelle schermate delle attività CA Identity Manager possono richiedere più tempo.

  Per ridurre l'impatto sulle ricerche, indicizzare gli attributi utilizzati nelle ricerche (a pagina 90).

- È possibile che le attività di gestione dei ruoli vengano eseguite lentamente.

  Quelli che seguono sono alcuni esempi di attività di gestione dei ruoli su cui influiscono le grandi dimensioni di un archivio oggetti:

  - Un'attività Crea ruolo di amministrazione è lenta perché CA Identity Manager deve confermare che il nome del ruolo è univoco nell'archivio oggetti.
  - L'attività Elimina ruolo di amministrazione deve rimuovere tutti gli oggetti creati per supportare il ruolo e la cache di oggetti deve essere aggiornata.

- CA Identity Manager richiede molto tempo per valutare i criteri di ruolo.

CA Identity Manager memorizza le informazioni nella cache dell'archivio oggetti per migliorare le prestazioni.

Ottimizzazione della valutazione dei criteri di ruolo

Per ciascun ruolo di amministrazione, è possibile creare tre tipi di criteri:

- Criteri membri

  Definire una regola membri che stabilisce gli utenti che ricevono il ruolo e le regole di ambito che determinano gli oggetti che i membri del ruolo possono gestire

- Criteri di amministrazione

  Definire regole di amministrazione, regole di ambito e privilegi di amministratore per un ruolo

- Criteri di titolarità

  Definire l'utente che può modificare un ruolo

Per ottimizzare le prestazioni durante la valutazione dei criteri di ruolo da parte di CA Identity Manager, considerare quanto segue:

- Limitare il numero dei ruoli di amministrazione in un ambiente di CA Identity Manager.
- Seguire le linee guida per la creazione delle regole dei criteri (a pagina 73).
- Ottimizzare l'archivio utenti.
- Ottimizzare il Policy Store, se CA Identity Manager include SiteMinder.

Linee guida per la creazione delle regole dei criteri

Uno dei fattori chiave nella determinazione delle prestazioni complessive delle valutazioni dei criteri di ruolo è il tempo impiegato per la valutazione di ogni singola regola di criterio. Per migliorare il tempo di valutazione delle regole dei criteri, durante la creazione di un criterio osservare quanto segue:

- Quando possibile, ridurre il numero di oggetti di criterio creati da CA Identity Manager e il numero di ricerche nell'archivio utenti eseguite creando regole dei criteri con espressioni complesse.

  Una regola singola con un'espressione complessa è più efficiente di regole multiple con espressioni semplici.
- Quando possibile, selezionare il tipo più efficiente e scalabile di regola di criterio.
- Abilitare l'opzione di valutazione in memoria per le regole dei criteri.

  L'opzione di valutazione in memoria riduce significativamente il tempo di valutazione dei criteri perché recupera informazioni su un utente da valutare da parte dell'archivio utenti e archivia una rappresentazione di quell'utente nella memoria. CA Identity Manager utilizza la rappresentazione in memoria per confrontare i valori di attributo con le regole dei criteri.

  Nota: per ulteriori informazioni sull'opzione di valutazione in memoria, consultare la *Guida alla configurazione*.
- Ottimizzare l'archivio utenti.
- Ottimizzare il Policy Store, se l'implementazione di CA Identity Manager include SiteMinder.

Riduzione degli oggetti di criterio e delle ricerche di archivio utenti

Ciascuna regola in un criterio di ruolo richiede un insieme di oggetti nell'archivio oggetti. Quando CA Identity Manager valuta una regola, carica questi oggetti ed esegue eventuali ricerche richieste nell'archivio utenti.

Il seguente esempio mostra un criterio membri che include tre regole membri. Ciascuna regola include quattro regole di ambito.

In questo esempio, CA Identity Manager crea gli oggetti ed esegue le ricerche nell'archivio utenti descritte nella tabella seguente durante la valutazione e l'applicazione del criterio membri.

Regola	Oggetti di criterio	Ricerche potenziali nell'archivio utenti
■ Regola membri: where (Department = "Administration") ■ Ambito utente: City = "Boston" ■ Ambito gruppo: Name = "Product Team" ■ Ambito ruolo di provisioning: Name = "Employee" ■ Ambito attività di accesso: Name = "Development"	5	5 (uno per ciascun oggetto di definizione della regola)
■ Regola membri: where (Department = "Engineering") ■ Ambito utente: City = "Boston" ■ Ambito gruppo: Name = "Product Team" ■ Ambito ruolo di provisioning: Name = "Employee" ■ Ambito attività di accesso: Name = "Development"	5	5
■ Regola membri: where (Department = "Human Resources") ■ Ambito utente: City = "Boston" ■ Ambito gruppo: Name = "Product Team" ■ Ambito ruolo di provisioning: Name = "Employee" ■ Ambito attività di accesso: Name = "Development"	5	5

In questo esempio, CA Identity Manager crea 15 oggetti ed esegue 15 ricerche di directory per determinare appartenenza e ambito.

Per ridurre il numero di oggetti di criterio e di ricerche nell'archivio utenti eseguite da CA Identity Manager, combinare le regole in espressioni complesse. L'esempio seguente specifica gli stessi diritti del primo esempio come una regola membri.

Member Policies

Member Rule	Scope Rules
where (Department = "Administration" or Department = "Engineering" or Department = "Human Resources")	**Access Role** where (Name = "Development") **Group** where (Group Name = "Product Team") **Provisioning Role** where (Name = "Employee") **User** where (City = "Boston")

In questo esempio, CA Identity Manager crea solamente dieci oggetti di criterio ed esegue solo cinque ricerche nell'archivio utenti.

Regola	Oggetti di criterio	Ricerche potenziali nell'archivio utenti
■ Regola membri: where (Department = "Administration") OR where (Department = "Engineering") OR where (Department = "Human Resources") ■ Ambito utente: City = "Boston" ■ Ambito gruppo: Name = "Product Team" ■ Ambito ruolo di provisioning: Name = "Employee" ■ Ambito attività di accesso: Name = "Development"	5	5

Selezione dei tipi di regola di criterio scalabili

Oltre al numero di regole dei criteri, anche il tipo di regola di criterio può avere un impatto sulle prestazioni. Generalmente, le regole dei criteri vengono costruite in base alla struttura dell'archivio utenti e alla modalità di determinazione dei diritti. Ad esempio, si possono creare regole dei criteri basate sull'appartenenza a un gruppo, sull'organizzazione o sugli attributi utente. Tuttavia, quando vi sono più modi per costruire regole dei criteri, esaminare le linee guida relative alle prestazioni nella seguente tabella prima di decidere quale tipo di regola costruire.

Nota: i tipi di regola di criterio nella tabella seguente vengono classificati in ordine di prestazioni, iniziando dal tipo di regola più efficiente.

Tipo di regola di criterio	Note sulle prestazioni
Organizzazione	■ Prestazioni complessive migliori ■ Non richiede una ricerca nelle directory LDAP. CA Identity Manager utilizza il DN dell'utente in fase di valutazione e il DN dell'organizzazione nella regola di criterio
Ruolo	■ CA Identity Manager archivia informazioni sugli oggetti di ruolo e sulle valutazioni precedenti nella cache dell'archivio oggetti ■ Nella maggior parte dei casi, le prestazioni saranno tanto buone quanto le regole dei criteri dell'organizzazione
Attributo utente	■ Fornisce le migliori prestazioni di ricerca nell'archivio utenti ed è il meno interessato da gruppi risultanti di utenti di grandi dimensioni ■ Consente di abilitare la valutazione in memoria per migliorare le prestazioni in maniera significativa

Tipo di regola di criterio	Note sulle prestazioni
Appartenenza gruppo	■ Le prestazioni dipendono dalla dimensione del gruppo e dal tipo di archivio utenti

Ottimizzazioni di attività

In CA Identity Manager, le attività visualizzate da un utente nella console utente dipendono dai privilegi specifici di quell'utente. Per visualizzare ed eseguire attività, CA Identity Manager deve eseguire numerose valutazioni di protezione, che possono avere un impatto significativo sulle prestazioni quando applicate su tutti gli utenti in un ambiente di CA Identity Manager.

CA Identity Manager esegue valutazioni di protezione quando si verificano le seguenti azioni:

- Un utente accede alla console utente

  In questo caso, CA Identity Manager deve valutare i ruoli di un utente per determinare le attività alle quali quell'utente può accedere nella console utente.

- Un utente richiama un'attività

  Quando viene richiamata un'attività, CA Identity Manager deve determinare gli oggetti che utente può gestire con quell'attività.

- Un utente accede a una scheda di relazione

  Una scheda di relazione è una qualsiasi scheda in cui un utente può visualizzare o gestire una relazione uno-a-molti tra il soggetto dell'attività e un insieme di diritti. Un esempio di scheda di relazione è la scheda Ruoli di amministrazione, che visualizza i ruoli di un utente.

- Un utente aggiunge oggetti a una scheda di relazione

  Ad esempio, CA Identity Manager esegue controlli di protezione aggiuntivi quando un utente aggiunge ruoli supplementari a un altro utente nella scheda Ruoli di amministrazione.

Le prestazioni di attività vengono influenzate da quanto segue:

- L'ambito attività, che stabilisce dove un amministratore può utilizzare un'attività
- Le schede di relazione, che visualizzano la relazione di un oggetto con altri oggetti

Valutazione dell'ambito di attività e prestazioni

Quando un amministratore utilizza un'attività di amministrazione che implica la ricerca di un oggetto gestito, quale un utente, un gruppo, un'organizzazione, un'attività o un ruolo, CA Identity Manager valuta e applica regole di ambito attività. Queste regole possono avere un impatto significativo sulla quantità di tempo richiesta da CA Identity Manager per visualizzare l'elenco di oggetti da selezionare per l'attività.

Nota: a differenza delle valutazioni di criteri di membri, amministrazioni e titolarità, le informazioni sulle valutazioni delle regole di ambito non vengono memorizzate in una cache.

L'ambito attività viene determinato dai seguenti elementi:

- Il tipo di oggetto che l'attività gestisce.
- Le regole di ambito applicabili al ruolo di amministrazione che include l'attività. Le regole di ambito vengono definite nei criteri di membri, titolarità e amministrazione.
- Tutti i criteri di ricerca definiti dall'utente.

Ad esempio, esaminare un'attività Modifica utente, che viene inclusa nel ruolo Manager utente. Il ruolo Manager utente ha un criterio membri con una regola di ambito che consente ai Manager utente di gestire gli utenti nell'organizzazione di dipendenti. Un amministratore apre l'attività Modifica utente e immette i criteri di ricerca: il cognome inizia con A. In questo caso, l'ambito dell'attività Modifica utente è relativo a tutti gli utenti nell'organizzazione di dipendenti il cui cognome inizia con A.

Modalità di esecuzione del rendering delle schede di relazione da parte di CA Identity Manager

Una scheda di relazione consente agli utenti di visualizzare e gestire la relazione del soggetto di un'attività con un insieme di diritti. Ad esempio, la scheda Ruoli di provisioning mostra i ruoli di provisioning di un utente.

Per determinare gli oggetti che vengono visualizzati in una scheda di relazione, CA Identity Manager esegue numerose valutazioni di protezione, che possono avere un impatto significativo sulle prestazioni.

L'esempio seguente mostra le operazioni effettuate da CA Identity Manager per eseguire il rendering della scheda Ruoli di provisioning:

1. Un amministratore fa clic sulla scheda Ruoli di provisioning nell'attività Modifica utente.
2. CA Identity Manager recupera i ruoli di provisioning di cui l'utente selezionato è membro.

3. Se la scheda è configurata per consentire la gestione di amministratori di ruolo, CA Identity Manager fa una seconda chiamata per recuperare l'elenco dei ruoli di provisioning in cui l'utente selezionato è un amministratore.
4. CA Identity Manager valuta ogni ruolo di provisioning dell'utente per verificare se l'amministratore che ha avviato l'attività può gestire l'appartenenza per quel ruolo.

   Se l'amministratore può gestire membri del ruolo, CA Identity Manager mostra una casella di controllo attiva nella colonna Appartenenza per quel ruolo nell'elenco di ruoli nella scheda.
5. CA Identity Manager valuta ogni ruolo di provisioning dell'utente per verificare se l'amministratore che ha avviato l'attività può gestire i diritti di amministrazione per quel ruolo.

   Se l'amministratore può gestire diritti di amministrazione, CA Identity Manager mostra una casella di controllo attiva nella colonna Amministratore per quel ruolo nell'elenco di ruoli nella scheda.

   CA Identity Manager deve completare le fasi da 2 a 5 per visualizzare i ruoli di provisioning correnti dell'utente. Se l'amministratore deve assegnare un nuovo ruolo di provisioning, sono necessarie le seguenti fasi aggiuntive.
6. L'amministratore fa clic sul pulsante Aggiungi per individuare nuovi ruoli di provisioning da assegnare.
7. CA Identity Manager visualizza una schermata di ricerca che può essere utilizzata dall'amministratore per cercare il ruolo da aggiungere.
8. L'amministratore immette un filtro di ricerca per trovare il ruolo da aggiungere.
9. CA Identity Manager restituisce l'elenco dei ruoli di provisioning che soddisfano i seguenti criteri:
   - I ruoli corrispondono al filtro di ricerca immesso dall'amministratore.
   - L'amministratore può gestire l'appartenenza per i ruoli.
   - L'utente è nell'ambito amministrativo dell'amministratore per i ruoli.
   - L'utente non dispone ancora di ruoli di provisioning.
10. CA Identity Manager ripete la fase 9 per determinare i ruoli in cui l'amministratore può gestire i privilegi amministrativi.

Schede di relazione e prestazioni

A causa del numero di valutazioni di protezione eseguite da CA Identity Manager, il rendering di una scheda di relazione può avere un impatto significativo sulle prestazioni. I fattori che determinano le prestazioni variano a seconda del tipo di scheda.

Per le schede di relazione di ruolo, i seguenti fattori possono avere un impatto sulle prestazioni:

- Numero di ruoli in cui il soggetto dell'attività è un membro
- Numero di ruoli in cui il soggetto dell'attività è un amministratore
- Numero di oggetti totali nel sistema che CA Identity Manager richiede per calcolare i ruoli del soggetto
- Numero di criteri membri/amministrazione per ciascun ruolo
- Complessità delle regole di ambito dei criteri membri/amministrazione
- La capacità di gestire autorizzazioni memorizzate nella cache perché gli invoker di attività limitino l'effetto dell'applicazione della protezione

Per determinare l'appartenenza a un gruppo e i privilegi amministrativi in schede di relazione di gruppo, CA Identity Manager deve effettuare una ricerca in tutti i gruppi nell'archivio utenti. Le prestazioni di queste ricerche dipendono dai fattori seguenti:

- Numero di oggetti di gruppo nell'archivio utenti
- Numero di membri in qualsiasi gruppo
- Prestazioni del database o della directory in cui si trova l'archivio utenti

Elaborazione di attività e prestazioni

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 sua aggiunta a un gruppo e l'assegnazione di ruoli.

Quando CA Identity Manager elabora un'attività, elabora ogni evento associato all'attività. Durante l'elaborazione dell'evento, CA Identity Manager salva ogni evento quattro volte. Questo consente a CA Identity Manager di proteggere azioni in corso in caso di un'interruzione imprevista del sistema.

Quando CA Identity Manager elabora più eventi contemporaneamente, gli eventi vengono aggiunti a una coda. Quando il primo evento completa la prima fase del suo ciclo di vita, viene salvato, quindi spostato alla fine della coda per attendere l'avvio della seconda fase di elaborazione. CA Identity Manager completa quindi la prima fase di elaborazione per l'evento successivo nella coda e quell'evento viene spostato alla fine della coda. Il processo continua finché tutti gli eventi nella coda hanno completato la prima fase di elaborazione. Quindi, il primo evento nella coda inizia la seconda fase di elaborazione. Questo processo continua finché tutti gli eventi nella coda completano tutte e quattro le fasi di elaborazione.

In condizioni di carico normali, questo comportamento non influisce sulle prestazioni. Tuttavia, se il sistema sta elaborando un numero elevato di attività e di eventi, ad esempio durante il caricamento in blocco di un set risultante di utenti di grandi dimensioni, tutti gli eventi e le attività devono attendere più a lungo nella coda e, pertanto, presentano un tempo di completamento più lungo.

Per evitare problemi di prestazioni in condizioni di carico, prendere in considerazione le seguenti azioni:

- Utilizzare l'impostazione Priorità attività nella scheda Profilo di un'attività.

  L'impostazione Priorità attività consente di impostare la priorità di un'attività su Alta, Media o Bassa.

  Le attività che devono essere elaborate immediatamente devono essere impostate su Alta. Le attività coinvolte in un caricamento in blocco devono essere impostate su Bassa.

  Se viene impostata una priorità di attività, gli eventi associati all'attività vengono elaborati con altre attività con la stessa priorità. Ad esempio, se l'attività Modifica utente è impostata sulla priorità Alta e un amministratore modifica un profilo utente, CA Identity Manager elabora quell'attività prima delle attività con priorità Media o Bassa. Se sono presenti altre attività con priorità Alta, CA Identity Manager completa la prima fase di elaborazione per il primo evento con priorità Alta, quindi sposta l'evento alla fine dell'elenco degli altri eventi con priorità Alta.

- Installare un server di CA Identity Manager separato e dedicato per gestire le operazioni di caricamento in blocco

Linee guida per l'ottimizzazione delle attività

Le attività predefinite, che CA Identity Manager distribuisce quando si crea un ambiente di CA Identity Manager, vengono configurate in modo che supportino una vasta gamma di scenari di utilizzo amministrativo. La maggior parte delle implementazioni di CA Identity Manager non richiede tutte le funzionalità fornite nelle attività predefinite. Dopo avere creato un ambiente di CA Identity Manager, modificare queste attività per soddisfare specifiche esigenze amministrative.

Le seguenti operazioni forniscono le linee guida per modificare le attività:

- **Creare attività di gestione utenti specializzate**

  Le attività predefinite Crea utente, Modifica utente e Visualizza utente forniscono capacità amministrative complete. Nella maggior parte delle implementazioni, solo un numero ridotto di amministratori ha bisogno di tutte le capacità disponibili.

  Creare nuove attività che includono soltanto le capacità richieste. Ad esempio, se la maggior parte delle attività di gestione utenti coinvolge solamente la gestione di profilo e gruppo, creare una nuova attività Modifica utente che includa solamente le schede Profilo e Gruppo. Rimuovere le schede Ruoli di amministrazione, Ruoli di accesso e Ruoli di provisioning che sono disponibili nell'attività predefinita Modifica utente.

  Le schede inutilizzate possono causare un sovraccarico significativo se vengono lasciate in attività utilizzate di frequente, soprattutto quando si utilizza il client Servizio Web per l'esecuzione di attività (TEWS), in cui queste schede potrebbero essere state attivate involontariamente attraverso la classe java schede fornita con CA Identity Manager.

  Le attività specializzate create devono corrispondere al modello di amministrazione delegata (a pagina 63) definito per l'ambiente in uso.

- **Disattivare Gestione amministratori nelle schede di relazione**

  Per impostazione predefinita, tutte le schede di relazione forniscono la capacità di gestire i diritti amministrativi per l'oggetto gestito dalla scheda, quali ruoli e gruppi. La maggior parte delle implementazioni non deve fornire questa funzionalità agli amministratori.

Per eliminare il sovraccarico aggiuntivo che si verifica quando CA Identity Manager valuta i diritti amministrativi, cancellare l'opzione Gestione amministratori dalle seguenti schede, se questa funzionalità non è necessaria:

- Ruoli di amministrazione
- Ruoli di provisioning
- Ruoli di accesso
- Gruppi

Per abilitare gli utenti alla gestione dei diritti amministrativi in schede specifiche, creare copie delle schede predefinite, abilitare l'opzione Gestione amministratori e disattivare l'opzione Gestione membri. Aggiungere le nuove schede alle attività specializzate, che vengono utilizzate solamente dagli amministratori che ne hanno bisogno.

- **Abilitare le ricerche per ambito in schede di relazione di ruolo**

  È possibile configurare ogni scheda dei ruoli in modo da includere ricerche che consentano agli amministratori di specificare criteri per i nuovi ruoli da assegnare a un utente. Le ricerche dei ruoli limitano il numero di regole dei criteri membri e amministrazione che CA Identity Manager deve valutare per determinare i ruoli che possono essere assegnati a un utente da un amministratore.

- **Impostazione delle opzioni di sincronizzazione delle attività**

  Per ciascuna attività di CA Identity Manager, è possibile specificare un'opzione di sincronizzazione utente, che sincronizza gli utenti con i criteri di identità e un'opzione di sincronizzazione account di provisioning, che sincronizza gli utenti con account con provisioning. Le opzioni consentono di sincronizzare gli utenti al completamento di un'attività o di un evento.

  Per eliminare il tempo di valutazione ed elaborazione, impostare la sincronizzazione in modo che avvenga al completamento di un'attività, anziché al completamento di eventi.

Linee guida per le ottimizzazioni di membri del gruppo/amministratori

Per migliorare le prestazioni delle ricerche di membri del gruppo e amministratori, considerare quanto segue:

- Definire attributi noti nel file di configurazione di directory (directory.xml), che descrive la struttura e i contenuti dell'archivio utenti a CA Identity Manager.

  Un attributo noto è un attributo che ha un significato speciale in CA Identity Manager.

  Per migliorare le ricerche di membri del gruppo\amministratori, definire i seguenti attributi noti per l'oggetto utente:

  %MEMBER_OF%

  Identifica un attributo nell'oggetto utente che archivia un elenco di gruppi di cui l'utente è membro.

  Quando definito, questo attributo può impedire a CA Identity Manager di effettuare la ricerca di tutti i membri in tutti i gruppi nell'archivio utenti. Le ricerche di gruppi possono influire in maniera significativa sulle prestazioni di gruppi molto grandi.

  %ADMINISTRATOR_OF%

  Identifica un attributo nell'oggetto utente che archivia un elenco di gruppi di cui l'utente è amministratore.

  Così come l'attributo %MEMBER_OF%, questo attributo noto può eliminare lunghe ricerche di gruppi.

- Specificare il tipo di gruppo nei file di configurazione di directory

  CA Identity Manager supporta tre tipi di gruppi: gruppi standard, gruppi nidificati e gruppi dinamici.

  Quando si definisce l'oggetto di gruppo nel file di configurazione di directory, è possibile specificare il tipo di gruppi supportato dall'archivio utenti. Se l'implementazione in uso non supporta gruppi dinamici o nidificati, impostare l'attributo Tipo gruppo nel seguente modo:

  GroupType = NONE

  L'impostazione NONE specifica il supporto dei gruppi standard.

  L'impostazione del tipo di gruppo predefinita è ALL, che può avere un impatto sulle prestazioni.

  Nota: per ulteriori informazioni su attributi noti e tipi di gruppo nel file di configurazione di directory, consultare la *Guida alla configurazione*.

- Per migliorare le prestazioni del GlobalGroup, impostare gli indici della cache della directory di provisioning

  Per le implementazioni di CA Identity Manager che includono un archivio utenti insieme a una directory di provisioning, è possibile ottimizzare l'appartenenza al GlobalGroup per la valutazione delle regola dei criteri per i criteri di ruolo e di identità.

  Per abilitare questa ottimizzazione, indicizzare i seguenti attributi utilizzati dal server di provisioning per risolvere l'appartenenza al gruppo nella cache della directory di provisioning:

  eTID

  L'attributo dell'ID oggetto univoco. Per le ricerche dell'appartenenza al gruppo, il valore è un utente o un gruppo specifico coinvolto nella ricerca.

  eTPID

  L'ID padre dell'oggetto utilizzato durante la ricerca di relazioni di appartenenza.

  eTCID

  L'ID figlio dell'oggetto utilizzato durante la ricerca di relazioni di appartenenza.

  Inoltre, aggiungere le seguenti voci hash:

  eTSuperiorClass

  Il tipo di oggetto padre in una ricerca di appartenenza

  eTSubordinateClass

  Il tipo di oggetto figlio in una ricerca di appartenenza

  Nota: per ulteriori informazioni sulla cache della directory di provisioning, consultare la *Guida all'installazione*.

Ottimizzazioni dei criteri di identità

Un *criterio di identità* è un insieme di modifiche di business che si verifica quando un utente soddisfa una determinata condizione o regola. Queste modifiche possono includere l'assegnazione o la revoca di ruoli, l'assegnazione o la revoca dell'appartenenza al gruppo e l'aggiornamento di attributi in un profilo utente.

CA Identity Manager valuta i criteri di identità quando viene effettuata la sincronizzazione utente.

Le prestazioni dei criteri di identità vengono influenzate da quanto segue:

- La modalità di configurazione dei criteri di identità
- La frequenza della sincronizzazione utente

Modalità di sincronizzazione di utenti e criteri di identità

Quando vengono utilizzati i criteri di identità, è importante comprendere in che modo i criteri vengono valutati e applicati agli utenti in CA Identity Manager. Senza una corretta comprensione del processo di sincronizzazione degli utenti, c'è il rischio di configurare set di criteri di identità che restituiscono risultati imprevisti.

La procedura seguente descrive la valutazione e l'applicazione dei criteri di identità in CA Identity Manager:

1. Il processo di sincronizzazione degli utenti viene avviato:
   - **Automaticamente**: è possibile configurare le attività di CA Identity Manager in modo che attivino automaticamente la sincronizzazione degli utenti.
   - **Manualmente**: utilizzare l'attività Sincronizza utente nella console utente per sincronizzare un utente.
2. CA Identity Manager determina il set di criteri di identità che si applicano ad un utente.
3. Il set di criteri viene quindi confrontato con l'elenco di criteri già applicati a tale utente.

   Nota: l'elenco di criteri applicati ad un utente è archiviato nell'attributo %IDENTITY_POLICY% nel profilo utente. Per ulteriori informazioni sulla configurazione di questo attributo, consultare la *Guida alla configurazione*.
   - Se un criterio di identità è presente nell'elenco di criteri applicabili *e non* è stato applicato precedentemente all'utente, tale criterio viene aggiunto a un elenco di assegnazione.
   - Se un criterio di identità si trova nell'elenco di criteri applicabili, è stato precedentemente applicato all'utente e l'impostazione Applicare una volta per il criterio è disattivata, tale criterio viene aggiunto a un elenco di riallocazione.
   - Se un criterio di identità non è presente nell'elenco di criteri applicabili, è stato applicato all'utente e l'utente non soddisfa più la condizione prevista, tale criterio viene aggiunto a un elenco di annullamento assegnazione.
4. Dopo la valutazione di tutti i criteri per un utente, questi vengono applicati nell'ordine seguente:
   a. Criteri di identità dall'elenco di annullamento assegnazione
   b. Criteri di identità dall'elenco di assegnazione
   c. Criteri di identità dall'elenco di riassegnazione

5. Una volta applicati, i criteri di identità vengono rivalutati per controllare se è necessario applicare ulteriori modifiche in base alle modifiche già apportate nel primo processo di sincronizzazione (passaggi 2-4).

   Tale operazione serve a garantire che le modifiche apportate applicando i criteri di identità non attivino altri criteri di identità.

6. La valutazione e l'applicazione dei criteri di identità continuano finché l'utente non viene sincronizzato in base a tutti i criteri applicabili oppure finché in CA Identity Manager non viene raggiunto il livello massimo di ricorrenza, definito nella console di gestione.

   Ad esempio, con un criterio di identità il dipartimento di un utente potrebbe essere modificato quando all'utente viene assegnato un ruolo. Il nuovo dipartimento attiva un altro criterio di identità. Tuttavia, se il livello di ricorrenza è impostato a 1, la modifica successiva non viene apportata fino alla nuova sincronizzazione dell'utente.

   Per ulteriori informazioni sull'impostazione del livello di ricorrenza, consultare la Guida in linea della console di gestione.

Progettazione di criteri di identità efficienti

Utilizzare le seguenti linee guida durante la creazione dei criteri di identità:

- **Limitare il numero di oggetti di criterio**

  CA Identity Manager crea oggetti nell'archivio oggetti che supportano i criteri di identità. Per ridurre il numero di oggetti nell'archivio oggetti, creare criteri di identità con espressioni complesse.
  Un approccio simile viene consigliato per i criteri di ruolo (a pagina 74).

- **Limitare le iterazioni di set di criteri di identità**

  È possibile configurare il livello di ricorsione per un criterio di identità, che determina il numero di volte in cui CA Identity Manager valuta e applica i criteri di identità durante la sincronizzazione di un utente. Ad esempio, con un criterio di identità il dipartimento di un utente potrebbe essere modificato quando all'utente viene assegnato un ruolo. Il nuovo dipartimento attiva un altro criterio di identità. Tuttavia, se il livello di ricorsione è impostato a 1, la modifica successiva non viene apportata fino alla nuova sincronizzazione dell'utente.

  L'impostazione dei limiti del livello di ricorsione limita il numero di volte in cui CA Identity Manager deve valutare i criteri di identità.

- **Limitare le dipendenze tra le regole di criteri di identità**

  È possibile creare un criterio di identità in cui l'azione di modifica (Azione su Applica criteri o Azione su Rimuovi criteri) di un criterio viene utilizzata nella condizione del criterio di identità di un altro criterio, così come illustrato nella tabella seguente.

Condizione criterio di identità	Azione su Applica criteri	Azione su Rimuovi criteri
where (codice processo = "100")	Rendere membro di (ruolo di provisioning "Account Manager")	Rimuovere membro di (ruolo di provisioning "Account Manager")
Utenti membri di (ruolo di provisioning "Account Manager")	Rendere membro di (gruppo "Account Manager")	Rimuovere membro di (gruppo "Account Manager")

  Quando CA Identity Manager valuta questo tipo di criterio, deve valutare e applicare le modifiche almeno due volte per assicurare che entrambe le condizioni vengano soddisfatte. Il livello di ricorsione, impostato per un intero ambiente di CA Identity Manager, deve essere maggiore di 1, il che causa quindi valutazioni aggiuntive per ciascun set di criteri di identità.

Riduzione delle attività che avviano la sincronizzazione utente

I criteri di identità vengono valutati e applicati durante il processo di sincronizzazione utente. È possibile configurare la sincronizzazione automatica specificando una delle seguenti opzioni di sincronizzazione utente per un'attività:

Al completamento dell'attività

CA Identity Manager avvia il processo di sincronizzazione utente dopo il completamento di tutti gli eventi in un'attività.

A ogni evento

CA Identity Manager avvia il processo di sincronizzazione utente dopo il completamento di ogni evento di un'attività.

Per le migliori prestazioni, limitare il numero di attività che attivano la sincronizzazione utente automatica.

Durante la configurazione della sincronizzazione utente, prendere in considerazione quanto segue:

- **Disabilitare la sincronizzazione utente per attività di password**

  Nella maggior parte dei casi, le password non vengono utilizzate nelle condizioni dei criteri di identità.

- **Disabilitare la sincronizzazione utente per l'attività Sincronizza utente**

  Poiché l'attività Sincronizza utente avvia valutazioni dei criteri di identità, CA Identity Manager esegue nuovamente le valutazioni se l'opzione di sincronizzazione utente è abilitata per questa attività.

- **Creare attività specializzate**

  Quando è possibile, creare attività che eseguono modifiche che avviano le condizioni dei criteri di identità e abilitano sincronizzazioni utenti solamente per quelle attività.

Ottimizzazione della valutazione delle regole dei criteri di identità

Per ridurre il tempo necessario alla valutazione delle condizioni dei criteri di identità che includono attributi utente, è possibile abilitare 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 condizioni dei criteri. Questa operazione limita il numero di chiamate effettuate direttamente da CA Identity Manager all'archivio utenti.

Nota: per ulteriori informazioni sull'opzione di valutazione in memoria, consultare la *Guida alla configurazione*.

Ottimizzazione dell'archivio utenti

L'ottimizzazione dell'archivio utenti coinvolge una serie di fasi, compreso quanto segue:

- Ottimizzazione della struttura dell'archivio utenti
- Ottimizzazione degli archivi sottostanti
- Implementazione della replica e del bilanciamento del carico

Queste fasi dipendono dal tipo di archivio utenti utilizzato. Per informazioni sull'ottimizzazione in queste aree, consultare la documentazione per il database o la directory contenente l'archivio utenti.

Oltre alle considerazioni generali sull'ottimizzazione, le seguenti considerazioni sull'ottimizzazione sono specifiche di CA Identity Manager:

- **Misurazione delle prestazioni di ricerca nell'archivio utenti**

  Per prestazioni ottimali, le ricerche di valutazione dei criteri di CA Identity Manager dovrebbero essere completate entro 10-20 millisecondi.

  Per garantire che CA Identity Manager possa completare coerentemente queste ricerche nel tempo consigliato, valutare l'opportunità di verificare le prestazioni di ricerca in condizioni di carico multiple.

  È anche possibile utilizzare questa misurazione per stabilire quando un archivio utenti raggiunge i suoi limiti fisici e sono necessari server aggiuntivi per il bilanciamento del carico.

- **Indicizzazione degli attributi**

  Indicizzare ogni attributo utilizzato in un criterio di ruolo o criterio di identità. L'indicizzazione degli attributi può fornire significativi miglioramenti delle prestazioni.

  Nota: per informazioni sull'indicizzazione degli attributi, consultare la documentazione relativa alla directory LDAP o al database relazionale che contiene l'archivio utenti.

- **Memorizzazione in cache dei binding LDAP**

  In CA Identity Manager, tutti i binding di directory LDAP vengono eseguiti dall'utente proxy definito nell'oggetto directory di CA Identity Manager. Per ciascuna connessione, lo stesso binding LDAP si verifica ripetutamente per questo stesso utente.

  Se si sta utilizzando una directory LDAP come archivio utenti, configurare la directory in modo che memorizzi in cache i binding (o le sessioni) LDAP, se la directory lo supporta.

- **Abilitazione delle cache dell'archivio utenti**

  Quando CA Identity Manager valuta le decisioni sui criteri per un utente, quelle informazioni vengono memorizzate in una cache di autorizzazione. Quando le informazioni memorizzate nella cache scadono, CA Identity Manager valuta nuovamente tutti i criteri per quell'utente.

  Per migliorare le prestazioni delle ricerche nell'archivio utenti in valutazioni successive delle regole dei criteri, abilitare l'archivio utenti affinché memorizzi nella cache i dati cercati, se l'archivio utenti lo supporta.

  CA Directory include una cache, chiamata dxCache, che è un'implementazione del database in memoria che può effettuare la ricerca tra i dati memorizzati nella cache.

  Nota: per ulteriori informazioni su CA Directory, consultare la guida *CA Directory Administrator Guide*.

Ottimizzazione per i componenti di provisioning

Quando un'implementazione di CA Identity Manager include il provisioning, utilizzare le seguenti ottimizzazioni per garantire le migliori prestazioni:

- Ottimizzare la connessione tra il server di CA Identity Manager e il server di provisioning

  CA Identity Manager comunica con il server di provisioning mediante l'API Java IAM (JIAM). Per migliorare le prestazioni di comunicazione, configurare quanto segue:

  - Pool di sessione JIAM per connessioni multiple al server di provisioning

    Nota: CA consiglia di impostare il valore iniziale delle sessioni su 8 e il valore massimo delle sessioni su 128.

  - Cache JIAM per gli oggetti recuperati dal server di provisioning

  Nota: per informazioni sulle impostazioni di configurazione di JIAM, consultare la *Guida per l'amministratore*.

- Impostare la sincronizzazione di account affinché venga eseguita alla fine di un'attività (a pagina 82), anziché alla fine di ciascun evento
- Ottimizzare il server di provisioning

  Nota: per ulteriori informazioni, consultare la *Guida per l'amministratore* e la *Guida all'installazione.*

Ottimizzazione dei componenti di runtime

Le modifiche di business in CA Identity Manager vengono apportate attraverso attività. Un'attività include uno o più eventi, che rappresentano le attività eseguite da CA Identity Manager per completare l'attività. Ad esempio, un'attività Crea utente può includere gli eventi CreateUserEvent e AddToGroupEvent.

CA Identity Manager include i seguenti componenti, che elaborano attività ed eventi in runtime:

- Database di CA Identity Manager che supportano le funzionalità di CA Identity Manager
- Messaggi JMS, responsabili dell'elaborazione degli eventi

Ottimizzazione dei database di CA Identity Manager

Durante l'esecuzione di attività, CA Identity Manager utilizza i seguenti database:

- Persistenza delle attività

  Gestisce le informazioni sulle attività e gli eventi di CA Identity Manager nel tempo. Questo consente a CA Identity Manager di ripristinare l'ultimo stato noto di eventi e attività in caso di errore di sistema.

  Nota: questo database ha l'impatto più significativo sulle prestazioni di CA Identity Manager, perché l'attività e i relativi eventi vengono salvati e recuperati dal database durante le transizioni di stato.

- Controllo

  Fornisce un record cronologico delle operazioni che si verificano in un ambiente di CA Identity Manager.

- Flusso di lavoro

  Archivia le definizioni del processo del flusso di lavoro, processi, script e altri dati necessari al motore del flusso di lavoro.

- Rapporti

  Archivia i dati delle snapshot che rispecchiano lo stato corrente degli oggetti in CA Identity Manager al momento in cui viene acquisita la snapshot.

CA Identity Manager comunica con ogni database attraverso un pool di connessione JDBC. Creare e configurare un pool di connessione JDBC nel server applicazioni in cui risiede CA Identity Manager. Quando si configura il pool di connessione JDBC, osservare quanto segue:

- Considerare il numero di attività simultanee eseguite in un dato momento.
- Considerare gli altri componenti di runtime quando si configura la dimensione del pool di connessione JDBC. Ciascun componente di runtime funziona insieme agli altri componenti di runtime.

  Nota: CA consiglia di impostare il valore iniziale del pool di connessione su 128.
- Per il database di persistenza delle attività, il numero di connessioni del database nel pool deve consentire a ciascuna attività in esecuzione di recuperare e aggiornare i dati di attività ed eventi lungo tutta la durata dell'attività.
- Il database di persistenza delle attività utilizza istruzioni preparate. Assicurarsi di configurare la cache delle istruzioni preparate per il database utilizzato per memorizzare i dati di persistenza delle attività.

  Nota: per informazioni sulla configurazione della cache delle istruzioni preparate, consultare la documentazione per il database utilizzato per la persistenza delle attività.

Impostazioni JMS

Un'attività di CA Identity Manager include eventi e azioni eseguite da CA Identity Manager per completare un'attività.

Durante il ciclo di vita di un evento, esso passa attraverso i seguenti stati:

- BEGIN
- APPROVATO
- EXECUTING (IN ESECUZIONE)
- COMPLETATO
- INVALID (NON VALIDO)

Gli eventi controllati dal flusso di lavoro possono avere anche i seguenti stati:

- IN SOSPESO
- RIFIUTATO

Per controllare queste transizioni di stato, CA Identity Manager utilizza messaggi JMS.

Controllo delle transizioni di eventi da parte dei messaggi JMS

CA Identity Manager utilizza messaggi JMS per controllare le transizioni di stato di un evento. La procedura seguente descrive le fasi corrispondenti:

1. Un utente inoltra un'attività.
2. L'attività genera uno o più eventi.
3. Quando un evento è pronto per l'elaborazione, CA Identity Manager imposta lo stato dell'evento su BEGIN (INIZIO) e l'evento viene trasmesso al database di persistenza delle attività.
4. CA Identity Manager crea un messaggio JMS che contiene l'ID evento e registra quel messaggio nella coda dei messaggi di evento.
5. Alla ricezione del messaggio, JMS richiama quindi un'istanza del bean guidato da messaggi di evento, che è un'implementazione del controller di eventi.
6. Il controller di eventi utilizza l'ID evento nel messaggio per recuperare l'evento dal database di persistenza delle attività ed esegue le azioni per lo stato attuale dell'evento.
7. Al completamento di tale stato, l'evento viene impostato sullo stato successivo e trasmesso al database di persistenza delle attività; quindi, viene registrato un nuovo messaggio JMS per elaborare lo stato successivo.

   Questo ciclo continua finché l'evento non ha completato il suo computer di stato.

Messaggi JMS e prestazioni

Per ogni evento, ci sono da tre a cinque stati che richiedono messaggi JMS per la transizione di stato:

- BEGIN
- IN SOSPESO (solamente nel controllo del flusso di lavoro)
- APPROVATO o RIFIUTATO
- EXECUTING (IN ESECUZIONE)
- COMPLETATO o INVALID (NON VALIDO)

Per elaborare un singolo evento, si verificano le seguenti azioni:

- Da tre a cinque registrazioni nella coda dei messaggi di evento
- Da tre a cinque chiamate del bean guidato da messaggi
- Da sei a dieci connessioni al database di persistenza delle attività (un'azione di lettura e una di scrittura per ogni stato)

Queste azioni possono avere un impatto sulla quantità di tempo necessaria a CA Identity Manager per elaborare un'attività.

Per garantire le migliori prestazioni durante le transizioni di stato, ottimizzare le risorse JMS nel server applicazioni in cui risiede CA Identity Manager, in modo che vi siano adeguate risorse JMS disponibili.

Ottimizzazione delle impostazioni JMS

I seguenti parametri di ottimizzazione di JMS del server applicazioni definiscono le connessioni di coda e i pool di istanze del bean guidato da messaggi.

- **Ottimizzazione di JMS WebSphere**

  WebSphere fornisce due parametri della factory di connessione coda che è possibile configurare per migliorare le prestazioni. Utilizzare la console di amministrazione di WebSphere per impostare le seguenti proprietà:

  - In Risorse, individuare le seguenti factory di connessione coda: iam-im-neteQCF e iam-im-wpConnectionFactory.
  - Per ciascuna, modificare le proprietà del pool di connessione per impostare il numero massimo di connessioni su 128.

- **Ottimizzazione di WebLogic**

  Nei server applicazioni di WebLogic, le factory di connessione coda ottengono thread di gestione della connessione dal pool di thread JMS del server o dal pool di esecuzione predefinito, a seconda della dimensione del pool di thread JMS. Se la dimensione del pool di thread JMS è 0, WebLogic utilizza i thread nel pool di esecuzione.

  Si consiglia di impostare il numero di thread del pool di thread JMS su un valore uguale alla dimensione massima del pool di bean per il bean guidato da messaggi di evento di CA Identity Manager, che per impostazione predefinita equivale a 128.

  Utilizzare la console di WebLogic Server per impostare la dimensione del pool di thread JMS nelle proprietà dei servizi JMS per il dominio e il server su cui è installato CA Identity Manager.

La dimensione del pool di bean guidati da messaggi di evento di CA Identity Managerviene impostata modificando l'impostazione max-beans-in-free-pool nel file del descrittore nel seguente percorso:

WebLogic_home\domain\applications\iam_im.ear\identityminder_ejb.jar\META-INF\weblogic-ejb-jar.xml

```
<weblogic-enterprise-bean>
        <ejb-name>SubscriberMessageEJB</ejb-name>
        <message-driven-descriptor>
            <pool>
                <max-beans-in-free-pool>128</max-beans-in-free-pool>
                <initial-beans-in-free-pool>16</initial-beans-in-free-pool>
            </pool>
            <destination-jndi-name>com.netegrity.ims.msg.queue</destination-
jndi-name>
        </message-driven-descriptor>
    </weblogic-enterprise-bean>
```

- **Ottimizzazione di JBoss**

  Nei server applicazioni JBoss, le factory di connessione coda ottengono thread di gestione delle connessioni dalla factory di sessioni del pool JMS standard del server. Per impostazione predefinita, il numero di thread massimi viene impostato su 15.

  Si consiglia di impostare questo valore in modo che corrisponda al valore della dimensione massima del contenitore di bean di messaggi standard.

  La factory di sessioni del pool JMS è impostata nell'elemento MaximumSize del JMSContainerInvoker nel seguente file:

  jboss_home\server\default\conf\standardjboss.xml

```
<invoker-proxy-binding>
         <name>message-driven-bean</name>
         …
         <proxy-factory-config>

<JMSProviderAdapterJNDI>DefaultJMSProvider</JMSProviderAdapterJNDI>

<ServerSessionPoolFactoryJNDI>StdJMSPool</ServerSessionPoolFactoryJNDI>
            <MaximumSize>128</MaximumSize>
            <MaxMessages>1</MaxMessages>
            …
         </proxy-factory-config>
     </invoker-proxy-binding>
```

La dimensione del bean guidato da messaggi di evento di CA Identity Manager viene impostata modificando il valore relativo alla dimensione massima nel file del descrittore seguente:

jboss_home\server\default\conf\standardjboss.xml

```
<container-configuration>
         <container-name>Standard Message Driven Bean</container-name>
         <call-logging>false</call-logging>
         <invoker-proxy-binding-name>message-driven-bean</invoker-proxy-
binding-name>
        ……
         <container-pool-conf>
            <MaximumSize>128</MaximumSize>
         </container-pool-conf>
   </container-configuration>
```

Ottimizzazione delle prestazioni di JBoss 5

In un'installazione predefinita di JBoss 5, lo scanner di distribuzione a caldo di JBoss viene eseguito ogni 5 secondi. Questa operazione influisce sulle prestazioni di JBoss. È possibile disattivare questa funzionalità, se non è necessaria, o modificare la frequenza di esecuzione.

Per disattivare o modificare la distribuzione a caldo

1. Modificare il file hdscanner-jboss-beans.xml in questo percorso:

   Nodo singolo: *jboss_home*/server/default/deploy

   Cluster: *jboss_home*/server/all/deploy

2. Per disattivare questa funzionalità, aggiungere la seguente riga nel bean HDScanner:
   `<attribute name="ScanEnabled">False</attribute>`

3. Per modificare la frequenza di scansione, aumentare il valore dell' attributo scanPeriod oltre i 5000 (millisecondi).

Nota: per ulteriori informazioni, consultare questo collegamento: http://community.jboss.org/wiki/JBossASTuningSlimming.

Per risolvere i problemi di memoria insufficiente

Se la dimensione heap di Java è troppo piccola, possono essere rilevate eccezioni di memoria insufficiente. Si consiglia una dimensione iniziale di 1024.

Capitolo 7: Creazione di un piano di ripristino di emergenza

Questa sezione contiene i seguenti argomenti:

Interruzione del servizio a causa di un'emergenza

In caso di emergenza, è possibile che i servizi fondamentali ai processi degli utenti vengano interrotti. Di conseguenza, questi utenti non possono fornire servizi ad altri utenti.

L'urgenza di ripristinare l'accesso ai servizi dipende dall'uso effettivo di CA Identity Manager. In alcune organizzazioni, gli utenti richiedono un accesso ininterrotto ai servizi forniti da CA Identity Manager, mentre altri utenti richiedono il ripristino del sistema entro un giorno. In entrambi i casi, si consiglia di preparare una protezione per l'implementazione di CA Identity Manager da un evento che causa un'interruzione parziale o totale dei sistemi.

Mediante la configurazione di un'architettura ridondante per CA Identity Manager, è possibile assicurare che i servizi siano costantemente disponibili per gli utenti. Quando si verifica un errore in un componente primario, il componente alternativo continua a fornire lo stesso servizio. Inoltre, è possibile eseguire regolarmente il backup dei sistemi e del software fondamentali, in modo da poter ripristinare i sistemi o i dati che vengono completamente persi.

Questo documento fornisce linee guida generali per la pianificazione di questi scenari. Si consiglia di utilizzare queste linee guida per sviluppare procedure specifiche di ripristino di emergenza che soddisfino le necessità dell'organizzazione.

Pianificazione del ripristino di emergenza

Per sviluppare un piano efficace di ripristino di emergenza, applicare le fasi descritte dettagliatamente in questo capitolo.

✓	Fase
	1. Definizione dei requisiti del ripristino di emergenza (a pagina 101) Sulla base delle esigenze dell'organizzazione, identificare i tipi di emergenza da prevedere e la velocità necessaria di ripristino dei servizi.
	2. Progettazione di un'architettura ridondante (a pagina 101) In base ai requisiti, progettare un'architettura con componenti ridondanti in una posizione remota.
	3. Sviluppo di piani di backup (a pagina 103) Per proteggere l'installazione, sviluppare piani per eseguire il backup dei componenti.
	4. Sviluppo di procedure di ripristino (a pagina 105) Sviluppare procedure per ripristinare i componenti persi.
	5. Documentazione del piano di ripristino (a pagina 107) Documentare i piani per ripristinare CA Identity Manager dopo un'emergenza.
	6. Verifica del piano di ripristino (a pagina 108) Sulla base delle procedure di ripristino di emergenza, verificare di poter ripristinare l'implementazione di CA Identity Manager così com'era prima dell'evento.
	7. Formazione sul piano di ripristino (a pagina 109) Completare gli sforzi assicurandosi che le persone responsabili del ripristino dei sistemi dopo un'emergenza siano formate per farlo.

Definizione dei requisiti del ripristino di emergenza

Quelle che seguono sono alcune linee guida generali da prendere in considerazione durante la definizione dei requisiti di un piano di ripristino di emergenza:

1. Creare un team con le seguenti conoscenze:
   - Conoscenza dell'architettura e dei sistemi che supportano CA Identity Manager
   - Conoscenza delle procedure di backup dei database relazionali e degli archivi utenti LDAP utilizzati da CA Identity Manager
2. Identificare scenari di emergenze potenziali da risolvere, compresa la perdita parziale o totale dei sistemi in uno o più siti.
3. Elencare i sistemi che devono necessariamente essere disponibili per supportare l'installazione.
4. Definire il tempo massimo consentito di inattività per ciascuno di questi sistemi.

   Ad esempio, i sistemi che supportano un server alternativo possono richiedere un ripristino con una priorità inferiore.

Progettazione di un'architettura ridondante

Per proteggersi dall'errore di un componente fondamentale, prendere in considerazione le seguenti azioni protettive utilizzando componenti alternativi (server e directory) e database ridondanti in posizioni remote.

Configurare la ridondanza per CA Identity Manager utilizzando la *Guida all'installazione.* Includere i seguenti componenti:

- Nodi ridondanti del server applicazioni di CA Identity Manager come parte di un cluster
- Un cluster del Policy Server fornisce il failover (se si sta utilizzando CA SiteMinder per proteggere CA Identity Manager)
- Alternare server di provisioning, directory di provisioning e server di connessione. Se un componente primario viene perso, il sistema passa al componente alternativo.

Configurare la ridondanza per i database includendo quanto segue:

- Uno qualsiasi dei database di runtime che fanno parte di CA Identity Manager, come ad esempio il database del flusso di lavoro o di controllo.

  Consultare la documentazione fornita con ORACLE o Microsoft SQL Server.
- Il database di BusinessObjects, se si sta utilizzando il server di rapporto.

  Consultare la documentazione relativa a BusinessObjects Enterprise, versione 2 e versione 2 SP 4 nel sito Web della documentazione SAP.

Server di CA Identity Manager alternativi

Il provisioning di nodi ridondanti del server applicazioni per il server di CA Identity Manager offre vantaggi in termini di scalabilità e prestazioni, nonché il ripristino di emergenza se si verifica un errore dei singoli server. Il metodo più comune per fornire il failover per un server applicazioni è la creazione di un cluster. Le procedure per creare il cluster vengono illustrate nella sezione Cluster della *Guida all'installazione*.

Nota: per CA Identity Manager versione 12.0 e successive, un cluster del server applicazioni è l'unico metodo valido per implementare una distribuzione di nodi multipli. Gli ambienti di CA Identity Manager richiedono l'architettura cluster J2EE standard del settore, che utilizza code JMS per il backbone. Di conseguenza, l'unico metodo valido per utilizzare nodi multipli in una configurazione di CA Identity Manager è un cluster del server applicazioni.

Per ulteriori informazioni su questa modifica, consultare il documento TechDoc 545594.

Componenti di provisioning alternativi

Molti componenti di provisioning presentano l'opzione di un componente alternativo per fornire una disponibilità elevata. Il componente alternativo deve trovarsi in un sito remoto per la massima protezione.

Per dettagli sulla configurazione di server e directory alternativi, consultare il capitolo Provisioning a disponibilità elevata della *Guida all'installazione*.

Directory di provisioning in più siti

È possibile creare directory di provisioning primarie e alternative con le directory alternative in una posizione remota. CA Directory consiglia di installare tre directory di provisioning, una primaria e due alternative.

Server di provisioning in più siti

Per proteggersi dall'errore del server di provisioning primario, è possibile configurare un server di provisioning alternativo. La differenza fra server di provisioning primari e alternativi è che l'installazione del server primario popola le voci del contenitore della directory di provisioning. Inoltre, la disinstallazione di un server primario rimuove quelle voci. Tranne che per l'installazione e la disinstallazione, i server primari e alternativi funzionano nella stessa maniera.

Server di connessione in più siti

Per il server di connessione Java o C++, è possibile configurare server di connessione multipli per servire lo stesso endpoint o il tipo di endpoint.

Per ciascun server di connessione configurato, è necessario configurare un server di connessione alternativo in una posizione remota per gestire gli stessi endpoint. Se si verifica un errore nel server di connessione, il server alternativo gestisce immediatamente la comunicazione con gli endpoint.

Database ridondanti

Il software di database supportato, Microsoft SQL Server e Oracle, offre la capacità di fornire database ridondanti. Se si verifica un errore nel database principale, il database ridondante è immediatamente disponibile. Il database ridondante deve trovarsi in un sito remoto qualora l'intero sito venga interessato dall'emergenza.

Sviluppo di piani di backup

Per proteggere dalla perdita di uno o di tutti i sistemi, utilizzare l'archivio remoto per tutti i dati di cui si esegue il backup e una pianificazione di backup che soddisfi i requisiti relativi al tempo massimo di inattività. Le procedure di backup e di ripristino utilizzano applicazioni differenti, pertanto dovrebbero essere coordinate per il ripristino del sistema di CA Identity Manager nel suo complesso.

Nei piani di backup, includere i seguenti componenti:

Componente	Descrizione	Metodo di backup
Archivio utenti di CA Identity Manager	Una directory utente LDAP o un database relazionale contenente i record per gli utenti di CA Identity Manager	Consultare la documentazione fornita con il software del database o LDAP.
Database di CA Identity Manager	I database di persistenza delle attività, di flusso di lavoro, di controllo, dell'archivio oggetti, di rapporto e l'archivio di persistenza delle attività I database del flusso di lavoro, di persistenza delle attività e di controllo hanno una frequenza di modifica più elevata e i backup devono essere pianificati di conseguenza.	Consultare la documentazione fornita con il software del database.

Componente	Descrizione	Metodo di backup
Policy Store di SiteMinder	Una directory utente LDAP o un database relazionale con oggetti per il Policy Server di SiteMinder, se si sta utilizzando SiteMinder	Consultare la documentazione fornita con il software del database o LDAP.
Directory di provisioning	Una directory utente LDAP che contiene i record per gli utenti di provisioning e gli oggetti di provisioning	Consultare la documentazione di CA Directory.
Archivi persistenti JMS del server applicazioni	Gli archivi utilizzati per conservare i messaggi di elaborazione di evento attività di CA Identity Manager	Consultare la documentazione del server applicazioni.
Database di reporting	Database snapshot Database di BusinessObjects	Consultare la documentazione fornita con il software del database.
Rapporti personalizzati	Rapporti personalizzati e file XML correlati	Consultare la documentazione relativa a BusinessObjects Enterprise, versione 2 e versione 2 SP 4 nel sito Web della documentazione SAP.

Nei piani di backup includere i seguenti componenti utilizzando un programma di backup del file system:

Componente	Descrizione
Componenti del server Web	Configurazione dei componenti del server Web distribuiti, come ad esempio i plug-in del server applicazioni e gli agenti Web di SiteMinder. Se si utilizza il bilanciamento del carico o se si sta utilizzando SiteMinder per proteggere l'accesso alla console utente, è obbligatorio utilizzare un front-end del server Web.
File di dati XML	Tutti i file degli ambienti e delle directory di CA Identity Manager utilizzati per creare, gestire ed archiviare gli oggetti dell'archivio oggetti di CA Identity Manager.
Componenti di personalizzazione di CA Identity Manager	I file trovati nelle seguenti cartelle iam_im.ear distribuite: ■ Config ■ User_console.war WEB-INF\web.xml
Script e programmi	Programmi, uscite di programma e script TEWS
Componenti di Connector Xpress	Connettori personalizzati File di progetto di Connector Xpress
Documentazione del ripristino di emergenza	Una volta creata la propria documentazione per il ripristino di emergenza, eseguirne regolarmente il backup se le istruzioni vengono modificate.

Sviluppo di procedure di ripristino

Le procedure di ripristino dipendono dal metodo di backup. Il processo di ripristino di un sistema con errori dipende dalle circostanze. Tuttavia, in molti casi, il metodo di ripristino consiste nella reinstallazione del software. Per informazioni, consultare il capitolo Provisioning a disponibilità elevata della *Guida all'installazione.*

Ripristino dell'archivio utenti di CA Identity Manager

Per ripristinare l'archivio utenti di CA Identity Manager, consultare la documentazione fornita con il software del database o LDAP. Verificare che l'archivio dati ripristinato dal backup sia intatto, compreso l'accesso a tutti gli archivi utenti.

Ripristino dei database di CA Identity Manager

Per ripristinare i database di CA Identity Manager, consultare la documentazione fornita con il database. Verificare che l'archivio dati ripristinato dal backup sia intatto, compreso l'accesso a tutti i database.

Ripristino del Policy Store di SiteMinder

Per ripristinare il Policy Store di SiteMinder, consultare la documentazione fornita con il software del database o LDAP. Verificare che l'archivio dati ripristinato dal backup sia intatto, compreso l'accesso a tutti gli archivi utenti.

Ripristino del server di CA Identity Manager

Se si perde un nodo cluster per un server di CA Identity Manager, eseguire le fasi seguenti:

1. Utilizzare la procedura standard documentata per aggiungere un nodo.

   Consultare il capitolo di *Guida all'installazione* sull'installazione dei cluster.

2. Aggiornare la connessione al server di provisioning.

   Consultare la sezione sul failover del provisioning nel capitolo Disponibilità elevata della *Guida all'installazione.*

Ripristino di una directory e di un server di provisioning

È possibile ripristinare un server di provisioning perso attraverso l'installazione di un server alternativo. Se tutti i sistemi presentano errori, ripristinare i dati persi durante l'emergenza.

Utilizzare le seguenti fasi:

1. Copiare eventuali file di schema personalizzati nella directory config\schema di CA Directory.
2. Installare la nuova directory di provisioning.

   Gli archivi dati saranno vuoti.
3. Ripristinare i dati dalla posizione di backup.
4. Utilizzare il programma di installazione del server di provisioning, fornendo i dettagli relativi alla directory di provisioning appena ripristinata.

   Le informazioni di dominio dovrebbero essere già presenti.
5. Ripristinare dal backup eventuali connettori personalizzati e file di configurazione.

Nota: per ulteriori informazioni, consultare la documentazione di CA Directory.

Ripristino di server di connessione

Se si perde un server di connessione, eseguire le seguenti fasi:

1. Utilizzare il programma di installazione del server di connessione per installare un nuovo server di connessione

   Registrarlo con il server di provisioning durante l'installazione.
2. Rimuovere la registrazione del server di connessione perso utilizzando csfconfig o Connector Xpress.

Ripristino di un server di rapporto

Se si perde il server di rapporto, consultare la documentazione di BusinessObjects per le procedure applicabili. Sul sito Web della documentazione SAP, cercare la documentazione relativa a Business Objects Enterprise, versione 2 e versione 2 SP 4.

Ripristino delle attività di amministrazione

Se un'attività di amministrazione era in esecuzione al momento dell'emergenza, può essere ripristinata alle seguenti condizioni.

- Tutte le attività di amministrazione con stato In sospeso in attesa di approvazioni continuano a essere disponibili se vengono preservati gli archivi utilizzati per gestire quelle informazioni di stato. Gli archivi includono il database di persistenza delle attività, l'archivio JMS che contiene i messaggi JMS di attività ed evento e il database del flusso di lavoro.
- Le attività con stato In corso (o in qualsiasi stato diverso da In sospeso) sono soggette a condizioni aggiuntive.

  Un'attività in questo stato richiede la registrazione di un nuovo messaggio JMS nella coda di messaggi di evento di CA Identity Manager per continuare ad essere elaborata. Le interruzioni che si verificano prima della registrazione di tale evento nella coda impediscono all'attività di continuare al ripristino.

  In questa situazione, sono disponibili due opzioni per il ripristino dell'attività:

  - Se l'attività è presente nell'attività Visualizza attività inoltrate con stato Non riuscito, accedere alla pagina dei dettagli dell'attività e utilizzare l'opzione Resubmit Task (Inoltra nuovamente attività).
  - Inoltrare una nuova attività con le stesse modifiche.

Documentazione del piano di ripristino

Sulla base delle linee guida in questo capitolo, si consiglia di sviluppare una documentazione di ripristino di emergenza specifica per l'organizzazione.

Considerare il seguente approccio:

1. Identificare i nomi e le posizioni dei sistemi nell'architettura e alternare i componenti per ciascun sistema.

   Per ciascun sistema, elencare il software installato, come ad esempio il JDK specifico installato, la versione di correzione di un server applicazioni e la quantità di memoria installata. Questo dettaglio è necessario per qualsiasi sistema si ritiene necessario rigenerare completamente.
2. Scrivere le procedure per ripristinare ciascun componente o per rigenerare un sistema completo, se necessario.
3. Identificare un metodo di individuazione o di ripristino di nomi utenti e password nei sistemi e nelle interfacce utenti di CA Identity Manager qualora siano noti solamente a una o due persone.
4. Proteggere la documentazione di ripristino di emergenza da eventuali perdite creando una copia di backup da archiviare in una posizione remota ben nota.

Verifica del piano di ripristino

Per garantire un corretto ripristino da un'emergenza, è possibile pianificare un'emergenza simulata, in cui certi sistemi diventano non disponibili. Considerare le verifiche descritte nelle sezioni seguenti.

1. Verifica del processo di failover.
2. Verifica del ripristino dei sistemi.

Verifica del processo di failover

Tutti i server o tutte le directory dovrebbero disporre di un server o di una directory alternativi in un sito remoto che comprenda i seguenti componenti:

- Server di CA Identity Manager
- Server di provisioning
- Directory di provisioning
- Server di connessione Java e C++
- Server di rapporto
- Server dei criteri

Arrestare manualmente tutti i componenti e verificare che tutte le operazioni continuino a funzionare, utilizzando il componente alternativo. Ad esempio, si potrebbe eseguire la seguente verifica del server di provisioning:

1. In un sistema con il server di provisioning primario, arrestare il servizi del servizio di provisioning dalla finestra di dialogo dei servizi Windows.

   Il server di provisioning primario viene arrestato.
2. Nella console utente eseguire le seguenti azioni:
   a. Assegnare un ruolo di provisioning a un utente.
   b. Verificare che gli account dell'endpoint vengano creati per quell'utente.

      Gli account creati dipendono dal server di provisioning alternativo che gestisce la comunicazione con il server di CA Identity Manager.

Questa procedura è un esempio di una verifica. Per ciascun componente arrestato, sviluppare simili verifiche per controllare che il componente alternativo sia in uso.

Verifica delle procedure di ripristino

In base alla documentazione di ripristino di emergenza, eseguire una verifica per ciascun componente fondamentale per confermare che è possibile ripristinare il sistema perso.

Formazione sul piano di ripristino

Una volta ritenute affidabili le procedure di ripristino, occorre far sì che le persone che devono implementare il ripristino siano in grado di farlo. L'organizzazione può richiedere operazioni aggiuntive, tuttavia, di seguito si riportano alcune linee guida generali:

1. Rendere pubblica la posizione della documentazione di ripristino.
2. Eseguire una simulazione della formazione.
3. Includere il feedback ricevuto durante la formazione in modo da garantire che le procedure finali di ripristino di emergenza siano sufficienti.

Nota: si può anche scegliere di utilizzare la formazione come opportunità per assegnare l'incarico di coordinatori del ripristino, comprese una persona come coordinatore di ripristino e una seconda persona come coordinatore alternativo. Queste persone dovrebbero incontrarsi in una determinata posizione per iniziare a redigere il piano di ripristino di emergenza.