System i

Sicurezza
EIM (Enterprise Identity Mapping)

Versione 6 Release 1

System i

Sicurezza
EIM (Enterprise Identity Mapping)

Versione 6 Release 1

Nota

Prima di utilizzare le informazioni di seguito riportate e il prodotto da esse supportato, leggere le informazioni in “Informazioni particolari”, a pagina 137.

La presente edizione si applica alla versione 6, release 1, livello di modifica 0 di IBM i5/OS (numero prodotto 5761–SS1) e a tutti i release e livelli di modifica successivi a meno che non venga indicato diversamente nelle nuove edizioni. Questa versione non viene eseguita su tutti i modelli RISC (reduced instruction set computer) né sui modelli CISC.

Indice

EIM (Enterprise Identity Mapping)

EIM (Enterprise Identity Mapping) per la piattaforma System i è l'implementazione i5/OS di un'infrastruttura IBM che consente agli amministratori e agli sviluppatori delle applicazioni di risolvere il problema di gestire più registri utenti nell'ambito della propria azienda.

Molte società in rete affrontano il problema di più registri utenti, tale problema richiede che ogni persona o entità all'interno della società disponga di un'identità utente in ogni registro. La necessità di più registri utenti si trasforma velocemente in un problema amministrativo ampio che influisce sugli utenti, sugli amministratori e sugli sviluppatori di applicazioni. EIM consente soluzioni economiche per una gestione più semplice di più registri utenti e identità utente nella propria società.

EIM consente di creare un sistema di corrispondenze di identità, denominate associazioni, tra le varie identità utente nei vari registri utenti per una persona nella propria azienda. EIM fornisce anche una serie comune di API che possono essere utilizzare tra le piattaforme per sviluppare le applicazioni che possono utilizzare le corrispondenze di identità create per ricercare le relazioni tra identità utente. Inoltre, è possibile utilizzare EIM insieme al servizio di autenticazione di rete, l'implementazione i5/OS di Kerberos, per fornire un ambiente con SSO.

È possibile configurare e gestire EIM tramite System i Navigator, la GUI di System i. La piattaforma System i utilizza EIM per abilitare le interfacce i5/OS ad autenticare gli utenti tramite il servizio di autenticazione di rete. Le applicazioni, come pure i5/OS, possono accettare i certificati Kerberos ed utilizzare EIM per trovare il profilo utente che rappresenta la stessa persona rappresentata dal certificato Kerberos.

Per ulteriori informazioni su come funzione EIM, sui concetti di EIM e su come è possibile utilizzare EIM nella propria azienda, consultare quanto segue:

Novità nella V6R1

Leggere le informazioni nuove o modificate in modo significativo relative alla raccolta di argomenti su EIM (Enterprise Identity Mapping).

Funzione nuova o migliorata per EIM

- Nei relese precedenti i5/OS EIM supportava solo la corrispondenza a un'identità utente locale per sistema. In i5/OS V6R1 EIM supporta la selezione da più corrispondenze identità utente locale per lo stesso sistema, utilizzando l'indirizzo IP del sistema di destinazione per selezionare la corrispondenza identità utente locale corretta su tale sistema.

Inoltre, è stato aggiornato l'argomento Single sign-on per fornire la documentazione sull'implementazione di EIM come parte di un ambiente con SSO per ridurre la gestione delle parole d'ordine. Questo argomento fornisce vari scenari dettagliati di situazioni con SSO con delle istruzioni di configurazione dettagliate per implementarle.

Come esaminare le novità o le modifiche

Per aiutare l'utente a identificare dove sono state apportate delle modifiche tecniche, queste informazioni utilizzano:

- L'immagine » per segnalare dove iniziano le informazioni nuove o modificate.
- L'immagine « per segnalare dove finiscono le informazioni nuove o modificate.

Per ulteriori informazioni sulle novità o le modifiche di questo release, consultare il Memorandum per gli utenti.

File PDF per EIM (Enterprise Identity Mapping)

È possibile visualizzare e stampare un file PDF che contiene le presenti informazioni.

Per visualizzare o scaricare la versione PDF di questo documento, selezionare Enterprise Identity Mapping (circa 1820 KB).

È possibile visualizzare o scaricare i PDF dei seguenti argomenti correlati:

- Network authentication services (circa 1398 KB) contiene informazioni su come configurare il servizio di autenticazione di rete insieme a EIM per creare un ambiente con SSO.
- IBM Tivoli Directory Server per i5/OS (LDAP) (circa 1700 KB) contiene delle informazioni su come configurare il server LDAP, che è possibile utilizzare come un'unità di controllo di dominio EIM insieme alle informazioni sulla configurazione LDAP avanzata.

Salvataggio di file PDF

Per salvare il formato PDF sulla propria stazione di lavoro per la visualizzazione o per la stampa:

1. Fare clic con il tasto destro del mouse sul collegamento PDF nel proprio browser.
2. Fare clic sull'opzione che consente il salvataggio del PDF in locale.
3. Portarsi all'indirizzario in cui si desidera salvare il PDF.
4. Fare clic su **Salva**.

Come scaricare Adobe Reader

Per visualizzare o stampare tali PDF, è necessario che sul sistema sia installato Adobe Reader. È possibile scaricare una copia gratuita dal sito Web Adobe (www.adobe.com/products/acrobat/readstep.html) .

Panoramica su EIM

EIM (Enterprise Identity Mapping) contribuisce a risolvere i problemi che insorgono quando l'utente cerca di gestire più di un registro utenti.

Gli ambienti di rete odierni sono composti da un gruppo complesso di sistemi e applicazioni, rendendo così necessaria la gestione di più registri utenti. La gestione di più registri utenti si trasforma velocemente in un problema amministrativo ampio che influisce sugli utenti, sugli amministratori e sugli sviluppatori di applicazioni. Di conseguenza, molte società sono continuamente alle prese con una gestione più sicura dell'autenticazione e dell'autorizzazione per i sistemi e le applicazioni. EIM consente agli amministratori ed agli sviluppatori delle applicazioni di risolvere questo problema in modo molto più semplice ed economico di quanto era possibile fare in precedenza.

Le informazioni riportate di seguito descrivono i problemi, tracciano gli approcci aziendali correnti e spiegano il motivo per cui l'approccio EIM si rivela migliore.

Problema di gestione di più registri utenti

Molti amministratori gestiscono reti che includono diversi sistemi e server, ognuno con una modalità univoca di gestione degli utenti attraverso i vari registri utenti. In queste reti complesse, gli amministratori sono responsabili della gestione delle identità di ogni utente e delle parole d'ordine su più sistemi. Inoltre, gli amministratori devono spesso sincronizzare queste identità e parole d'ordine e gli utenti hanno la responsabilità di ricordare più identità e parole d'ordine e di tenerle sincronizzate. Il costo utente e amministratore in questo ambiente è eccessivo. Di conseguenza, spesso gli amministratori

trascorrono molto tempo nella risoluzione di tentativi di collegamento non riusciti e nella reimpostazione delle parole d'ordine dimenticate invece di gestire la società.

Il problema della gestione di più registri utenti influisce anche sugli sviluppatori di applicazioni che desiderano fornire applicazioni eterogenee o multilivello. Questi sviluppatori sono a conoscenza del fatto che i dati aziendali importanti per i clienti sono diffusi attraverso molti sistemi differenti e che ogni sistema possiede i propri registri utenti. Di conseguenza, gli sviluppatori devono creare registri utenti proprietari e una semantica di sicurezza associata per le loro applicazioni. Sebbene ciò risolva il problema per lo sviluppatore dell'applicazione, aumenta il costo per gli utenti e gli amministratori.

Approcci correnti

Per la risoluzione del problema della gestione di più registri utenti, sono disponibili diversi approcci aziendali correnti, ma tutti forniscono soluzioni incomplete. Ad esempio, LDAP (Lightweight Directory Access Protocol) fornisce una soluzione di registro utenti distribuita. Tuttavia, l'utilizzo di LDAP (o altre soluzioni note come Microsoft Passport) indica che gli amministratori devono gestire ancora un altro registro utenti e la semantica della sicurezza oppure devono sostituire le applicazioni esistenti create per utilizzare tali registri.

Utilizzando questo tipo di soluzione, gli amministratori devono gestire più meccanismi di sicurezza per singole risorse, aumentando così il carico di lavoro amministrativo e aumentando potenzialmente la possibilità di esporsi a rischi per la sicurezza. Quando più meccanismi supportano una singola risorsa, le possibilità di modificare l'autorizzazione tramite uno dei meccanismi e di dimenticarsi di averla modificata per uno o più meccanismi sono molto più alte. Ad esempio, un'esposizione della sicurezza può verificarsi quando ad un utente viene giustamente negato l'accesso tramite un'interfaccia, ma gli viene consentite tramite altre interfacce.

Una volta completato questo lavoro, gli amministratori scoprono che non hanno completamente risolto il problema. Generalmente le società hanno investito troppo denaro nei registri utenti correnti e nella relativa semantica di sicurezza per utilizzare questo tipo di soluzione pratica. La creazione di un altro registro utenti e della semantica associata risolve il problema per il fornitore dell'applicazione ma non i problemi per gli utenti e gli amministratori.

Un'altra possibile soluzione consiste nell'utilizzare un approccio di tipo SSO. Sono disponibili diversi prodotti che consentono agli amministratori di gestire i file che contengono tutte le identità e le parole d'ordine dell'utente. Tuttavia, questo approccio presenta diversi punti deboli:

- Esso indirizza solo uno dei problemi rilevati dagli utenti. Sebbene consenta agli utenti di collegarsi su più sistemi fornendo un'identità e una parola d'ordine, non elimina la necessità degli utenti di disporre di parole d'ordine su altri sistemi o di gestire queste parole d'ordine.
- Introduce un nuovo problema creando un'esposizione di sicurezza in quanto in questi file viene memorizzato il testo in chiaro o codificato delle parole d'ordine. Le parole d'ordine non devono mai essere memorizzate in file con testo in chiaro oppure qualsiasi utente, inclusi gli amministratori, potrà facilmente accedervi.
- Non risolve i problemi degli sviluppatori di applicazioni di terzi che forniscono applicazioni eterogenee multilivello. Devono ancora fornire registri utenti proprietari per le loro applicazioni.

Malgrado questi punti deboli, alcune società hanno deciso di adottare questi approcci in quanto forniscono miglioramenti per più problemi di registro utenti.

Approccio EIM

EIM offre un nuovo approccio per creare in modo economico delle soluzioni per gestire in modo più semplice più registri utente e identità utente in un ambiente applicativo eterogeneo a più livelli. EIM è un'architettura che rappresenta, descrivendole, le relazioni tra individui o entità (come i server di file e di

stampa) nell'azienda e varie identità che le rappresentano all'interno di un'azienda. Inoltre, EIM fornisce una serie di API che consentono alle applicazioni di porre delle domande su queste applicazioni.

Ad esempio, data un'identità utente di una persona in un registro utenti, è possibile determinare quale identità presente in un altro registro rappresenta la stessa persona. Se l'utente viene autenticato con un'identità utente ed è possibile mettere in corrispondenza tale identità utente con l'identità appropriata in un altro registro utente, l'utente non deve necessariamente fornire nuovamente le credenziali per l'autenticazione. Si conosce l'identità dell'utente ed è necessario conoscere solo quale identità utente rappresenta quell'utente in un altro registro utente. Quindi, EIM fornisce una funzione di messa in corrispondenza dell'identità generalizzata per la società.

EIM consente corrispondenze uno-molti (in altri termini, un singolo utente con più identità in un singolo registro utenti). Tuttavia, l'amministratore non è necessario che abbia corrispondenze singole specifiche per tutti le identità utente in un registro utenti. EIM consente inoltre corrispondenze molti ad uno (in altre parole, più utenti in corrispondenza con una singola identità utente in un singolo registro utenti).

La capacità di mettere in corrispondenza le identità dell'utente in diversi registri utenti fornisce molti benefici. Innanzitutto, le applicazioni possono utilizzare un registro utente per l'autenticazione mentre utilizzano un registro utente completamente diverso per l'autorizzazione. Ad esempio, un amministratore può associare un'identità utente Windows identità utente in un registro Kerberos ad un profilo utente i5/OS in un altro registro utenti per accedere alle risorse i5/OS cui è autorizzato il profilo i5/OS.

EIM è un'architettura aperta che gli amministratori possono utilizzare per rappresentare le relazioni di corrispondenza identità per qualsiasi registro. Non richiede di copiare i dati esistenti su un nuovo contenitore e di tenere entrambe le copie sincronizzate. Solo i nuovi dati introdotti da EIM costituiscono le informazioni sulla relazione. EIM memorizza questi dati in un indirizzario LDAP, che fornisce la flessibilità di gestire i dati in un luogo e di avere repliche in qualsiasi luogo vengano utilizzate le informazioni. Infine, EIM fornisce alle società e agli sviluppatori di applicazioni la flessibilità di operare in modo semplice in un'ampia gamma di ambienti con costi inferiori di quelli eventualmente sostenibili senza questo supporto.

EIM, utilizzato insieme al servizio di autenticazione di rete, l'implementazione i5/OS di Kerberos, fornisce una soluzione con SSO. È possibile scrivere le applicazioni in modo che utilizzino le API GSS ed EIM per accettare i certificati Kerberos e metterli in corrispondenza con un'altra identità utente associata in un registro utenti differente. È possibile pervenire all'associazione tra identità utente fornita da questa messa in corrispondenza di identità creando delle associazioni di identificativo che associano indirettamente un'identità utente ad un'altra tramite un identificativo EIM oppure creando delle associazioni normative che associano direttamente un'identità utente in un gruppo ad una singola, specifica, identità utente.

L'uso della messa in corrispondenza dell'identità richiede che gli amministratori effettuino quanto segue:

1. Configurare un dominio EIM nella rete. È possibile utilizzare il wizard Configurazione EIM per creare un'unità di controllo del dominio per il dominio e configurare l'accesso al dominio. Quando si utilizza il wizard, è possibile scegliere di creare un nuovo dominio EIM e creare un'unità di controllo del dominio sul sistema locale oppure su un sistema remoto. In alternativa, se già esiste un dominio EIM, è possibile scegliere di parteciparvi.
2. Determinare a quali utenti definiti per il server indirizzario dove si trova l'unità di controllo del dominio EIM è consentito gestire, oppure accedere a, specifiche informazioni nel dominio EIM ed assegnare questi utenti ai gruppi di controllo dell'accesso EIM appropriati.
3. Creare delle definizioni di registro EIM per i registri utente che parteciperanno al dominio EIM. Sebbene sia possibile definire un qualsiasi registro utente su un dominio EIM, è necessario definire i registri utente per quelle applicazioni e sistemi operativi abilitati all'EIM.
4. In base alle esigenze della propria implementazione di EIM, determinare quali delle seguenti attività eseguire per completare la propria configurazione EIM:

- Creare identificativi EIM per ogni utente univoco nel dominio e creare associazioni di identificativo per essi.
- Creare associazioni normativa.
- Creare un combinazione di entrambe le opzioni.

Informazioni correlate

Panoramica su SSO (Single sign-on)

Concetti di EIM

Per comprendere completamente come poter utilizzare EIM nella propria società, è necessario conoscere concettualmente come opera EIM (Enterprise Identity Mapping). Sebbene la configurazione e l'implementazione delle API di EIM possano differire a seconda delle piattaforme server, i concetti su EIM sono comuni tra le piattaforme IBM eServer.

La Figura 1 fornisce un esempio di implementazione di EIM in una società. Tre server hanno la funzione di client EIM e contengono applicazioni abilitate EIM che richiedono i dati EIM tramite le operazioni di ricerca EIM 6. L'unità di controllo del dominio 1 memorizza le informazioni sul dominio EIM 2, che comprende un identificativo EIM 3, associazioni 4 tra tali identitificativi EIM e identità utente, e definizioni di registro EIM 5.

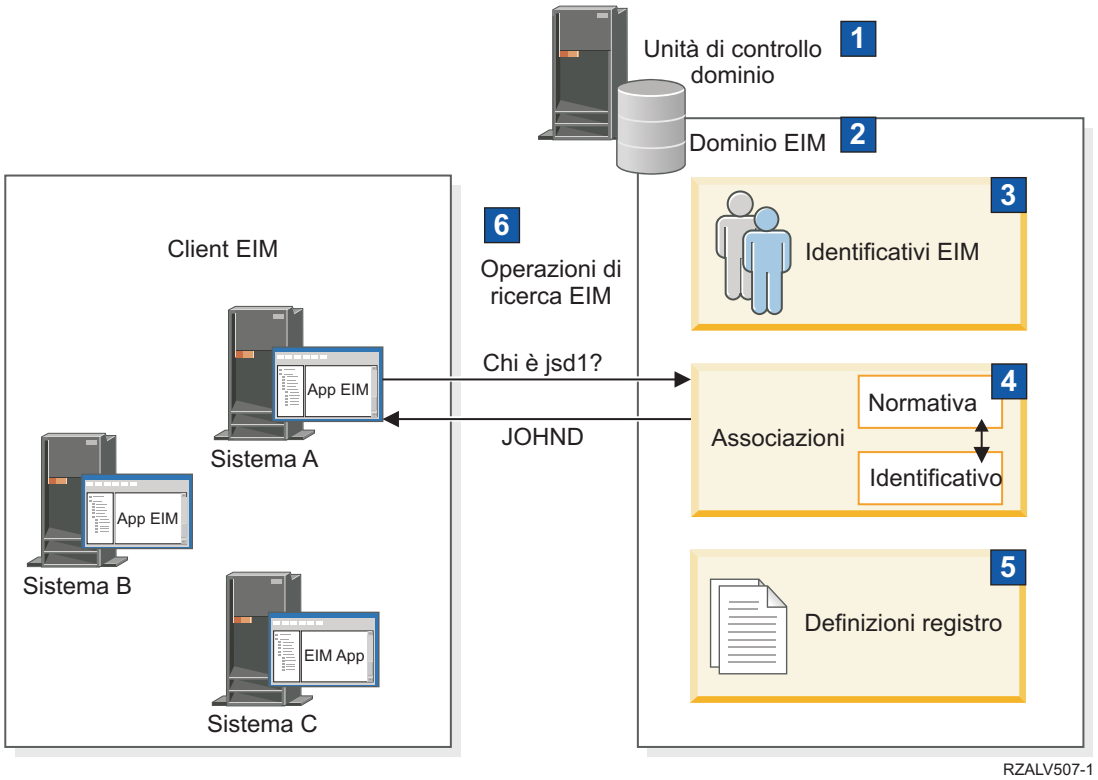


Figura 1. Un esempio di implementazione EIM

Consultare le informazioni di seguito riportate per meglio comprendere questi concetti EIM eServer:

Concetti correlati

"Concetti LDAP relativi a EIM" a pagina 48
EIM utilizza un server LDAP come unità di controllo del dominio per la memorizzazione dei dati EIM. Di conseguenza, è necessario comprendere alcuni concetti di LDAP correlati alla configurazione

ed all'utilizzo di EIM nella propria azienda. È ad esempio possibile utilizzare un DN LDAP come identità utente per configurare EIM ed eseguire l'autenticazione per l'unità di controllo del dominio EIM.

"Concetti di EIM per i5/OS" a pagina 50
È possibile implementare EIM (Enterprise Identity Mapping) su qualsiasi piattaforma IBM eServer. Tuttavia, quando si implementa EIM su un modello System i, bisogna essere consapevoli di alcune informazioni specifiche per l'implementazione di System i.

Unità di controllo del dominio EIM

Un'unità di controllo dominio EIM è un server LPDA (Lightweight Directory Access Protocol) configurato per gestire uno o più domini EIM Un dominio EIM è composto di tutti gli identificativi EIM, le associazioni EIM e i registri utenti definiti in tale dominio. I sistemi (client EIM) prendono parte al dominio EIM utilizzando i dati del dominio per le operazioni di ricerca EIM.

Attualmente, è possibile configurare IBM Tivoli Directory Server for i5/OS su alcune piattaforme IBM eServer in modo che funga da unità di controllo del dominio EIM. Ogni sistema che supporta le API EIM può partecipare nel dominio come client. Questi sistemi client utilizzano le API EIM per contattare un'unità di controllo del dominio EIM per essere eseguiti. L'ubicazione del client EIM determina se l'unità di controllo del dominio EIM è un sistema locale o remoto. L'unità di controllo del dominio è *locale* se il client EIM è in esecuzione sullo stesso sistema dell'unità di controllo del dominio. L'unità di controllo del dominio è *remota* se il client EIM è in esecuzione su un sistema separato dall'unità di controllo del dominio.

Nota: se si pianifica di configurare un server di indirizzario su un sistema remoto, il server di indirizzario deve fornire il supporto EIM. EIM richiede che l'unità di controllo dominio abbia come host un server indirizzario che supporta LPDA (Lightweight Directory Access Protocol) Versione 3. Inoltre, il prodotto server indirizzario deve essere configurato in modo da accettare lo schema EIM. IBM Tivoli Directory Server for i5/OS fornisce questo supporto.

Concetti correlati

"Operazioni di ricerca EIM" a pagina 28
Un'applicazione o un sistema operativo utilizza un'API EIM per eseguire un'operazione di ricerca in modo che l'applicazione o il sistema operativo possa eseguire la corrispondenza da un'identità utente in un registro ad un'altra identità utente in un altro registro. Un'operazione di ricerca EIM è un processo attraverso il quale un'applicazione o un sistema operativo rileva un'identità utente associata sconosciuta in uno specifico registro di destinazione, fornendo alcune informazioni note e affidabili.

"Schema LDAP ed altre considerazioni per EIM" a pagina 49
Utilizzare queste informazioni per comprendere gli elementi richiesti per il corretto funzionamento del server dell'indirizzario con EIM (Enterprise Identity Mapping).

Dominio EIM

Un dominio EIM (Enterprise Identity Mapping) è un indirizzario presente nel server LPDA (Lightweight Directory Access Protocol) che contiene i dati EIM di una società.

Un dominio EIM è la raccolta di tutti gli identificativi EIM, tutte le associazioni EIM e tutti i registri utenti definiti in tale dominio ed il controllo di accesso per i dati. I sistemi (client EIM) prendono parte al dominio utilizzando i dati di dominio per le operazioni di ricerca EIM.

Un dominio EIM è qualcosa di diverso rispetto a un registro utenti. Un registro utente definisce una serie di identità utente note e garantite da una particolare istanza di un sistema operativo o di un'applicazione. Un registro utente contiene anche le informazioni necessarie all'autenticazione dell'utente dell'identità. Inoltre, un registro utente contiene spesso altri attributi quali le preferenze utente, i privilegi di sistema o le informazioni personali per quella identità.

Al contrario, un dominio EIM *fa riferimento* alle identità utente che sono definite nei registri utenti. Un dominio EIM contiene informazioni sulla *relazione* tra le identità presenti nei vari registri utenti (nome utente, tipo registro e istanza registro) e le persone o le entità reali rappresentate da tali identità.

La Figura 2 mostra i dati memorizzati all'interno di un dominio EIM. Questi dati includono identificativi EIM, definizioni di registro EIM e associazioni EIM. I dati EIM definiscono la relazione tra le identità utente e gli individui o entità rappresentati da queste identità in un'azienda.

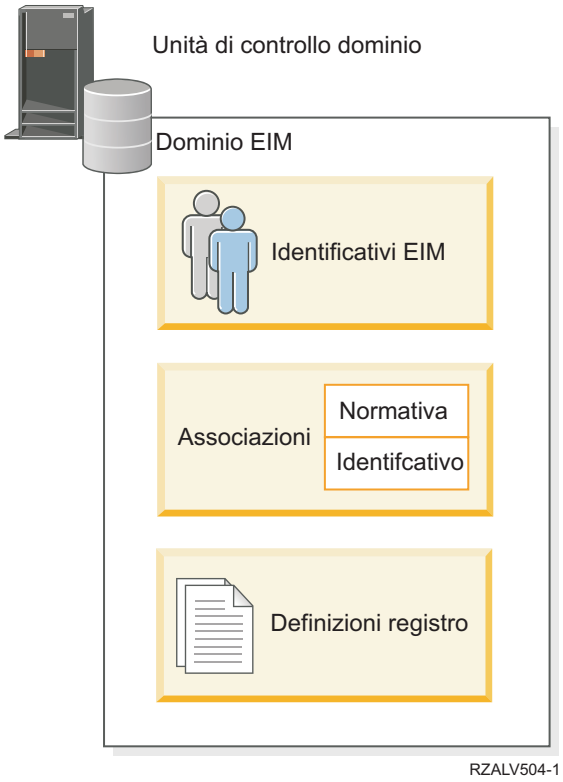


Figura 2. Dominio EIM e dati memorizzati nel dominio

I dati EIM includono:

Definizioni di registro EIM
Ogni definizione di registro EIM creata rappresenta un registro utenti effettivo (e le informazioni sull'identità utente in esso contenute) presente su un sistema nell'ambito dell'impresa. Una volta definito uno specifico registro utenti in EIM, tale registro può entrare a far parte del dominio EIM. È possibile creare due tipi di definizioni di registro; un tipo fa riferimento ai registri utenti di sistema e l'altro tipo fa riferimento ai registri utenti applicazione.

Identificativi EIM
Ogni identificativo EIM creato in modo univoco rappresenta una persona o un'entità (ad esempio un server di stampa o un server dei file) nell'ambito di un'azienda. È possibile creare un identificativo EIM quando si desidera avere delle corrispondenze uno-a-uno tra le identità utente che appartengono ad una persona o a un'entità cui corrisponde l'identificativo EIM.

Associazioni EIM
Le associazioni EIM create dall'utente rappresentano delle relazioni tra identità utente. È necessario definire delle associazioni per consentire ai client EIM di utilizzare le API EIM di eseguire operazioni di ricerca EIM con esito positivo. Queste operazioni di ricerca EIM ricercano le associazioni definite in un dominio EIM. È possibile creare due tipi di associazioni differenti:

Associazioni di identificativi
Le associazioni di identificativi consentono di definire una relazione uno-a-uno tra

identità utente tramite un identificativo EIM definito per una persona. Ciascuna associazione di identificativi EIM creata dall'utente rappresenta una singola, specifica relazione tra un identificativo EIM ed un'identità utente associata nell'ambito di un'azienda. Le associazioni di identificativi forniscono le informazioni che collegano un identificativo EIM ad una specifica identità utente in uno specifico registro utenti e consente di creare una corrispondenza di identità uno-a-uno per un utente. Le associazioni di identità sono utili soprattutto quando delle persone hanno delle identità utente con autorizzazioni speciali e con altri privilegi che si desidera controllare in modo specifico creando delle corrispondenze uno-a-uno tra le loro identità utente.

Associazioni normativa

Le associazioni normativa consentono di definire una relazione tra un gruppo di identità utente in uno o più registri utenti ed una singola identità utente in un altro registro utenti. Ciascuna associazione normativa EIM creata determina una corrispondenza uno-a-uno tra il gruppo di origine di identità utente in un registro utenti ed una singola identità utente di destinazione. Di norma, si creano delle associazioni normativa per mettere in corrispondenza un gruppo di utenti che richiedono tutti lo stesso livello di autorizzazione con una singola identità utente che dispone di tale livello di autorizzazione.

Concetti correlati

"Definizioni di registro EIM" a pagina 11
Una definizione registro EIM (Enterprise Identity Mapping) è una voce all'interno di EIM che si crea per rappresentare un registro utenti effettivo che esiste su un sistema all'interno della propria azienda. Un registro utenti funziona come un indirizzario e contiene un elenco di identità utente valide per un determinato sistema o applicazione.

"Identificativo EIM"
Un identificativo EIM (Enterprise Identity Mapping) rappresenta una persona o un'entità in una società. Una tipica rete è composta da diverse applicazioni e piattaforme hardware e dai registri utenti associati. La maggior parte delle piattaforme e molte delle applicazioni utilizzano registri utenti specifici della piattaforma o dell'applicazione. Questi registri contengono tutte le informazioni di identificazione utente per gli utenti che gestiscono quei server o applicazioni.

"Operazioni di ricerca EIM" a pagina 28
Un'applicazione o un sistema operativo utilizza un'API EIM per eseguire un'operazione di ricerca in modo che l'applicazione o il sistema operativo possa eseguire la corrispondenza da un'identità utente in un registro ad un'altra identità utente in un altro registro. Un'operazione di ricerca EIM è un processo attraverso il quale un'applicazione o un sistema operativo rileva un'identità utente associata sconosciuta in uno specifico registro di destinazione, fornendo alcune informazioni note e affidabili.

Identificativo EIM

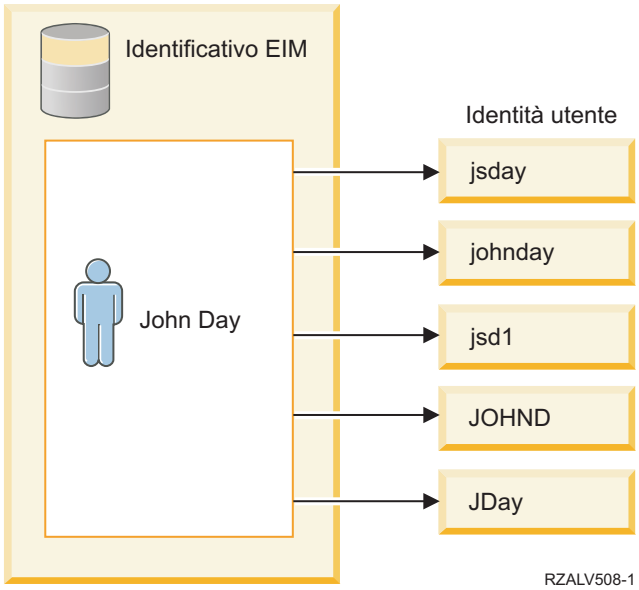
Un identificativo EIM (Enterprise Identity Mapping) rappresenta una persona o un'entità in una società. Una tipica rete è composta da diverse applicazioni e piattaforme hardware e dai registri utenti associati. La maggior parte delle piattaforme e molte delle applicazioni utilizzano registri utenti specifici della piattaforma o dell'applicazione. Questi registri contengono tutte le informazioni di identificazione utente per gli utenti che gestiscono quei server o applicazioni.

È possibile utilizzare EIM per creare degli identificativi EIM per le persone o le entità nella propria azienda. È possibile, poi, creare delle associazioni di identificativi, o delle corrispondenze di identità dirette (uno-a-uno), tra l'identificativo EIM e le diverse identità utente per la persona o entità rappresentata dall'identificativo EIM. Questo processo facilita la costruzione di applicazioni eterogenee a più livelli. In questo modo, si facilita anche la costruzione e l'utilizzo degli strumenti che semplificano l'amministrazione necessaria alla gestione dell'identità utente che un individuo o un'entità possiede all'interno dell'azienda.

Identificativo EIM che rappresenta una persona

La Figura 3 illustra un esempio di un identificativo EIM che rappresenta una persona che si chiama *John Day* e le sue diverse identità utente in una società. In questo esempio, la persona *John Day* dispone di cinque identificativi utente in quattro diversi registri utente: `johnday`, `jsd1`, `JOHND`, `jsday` e `JDay`.

Figura 3: la relazione tra l'identificativo EIM di *John Day* e le sue diverse identità utente

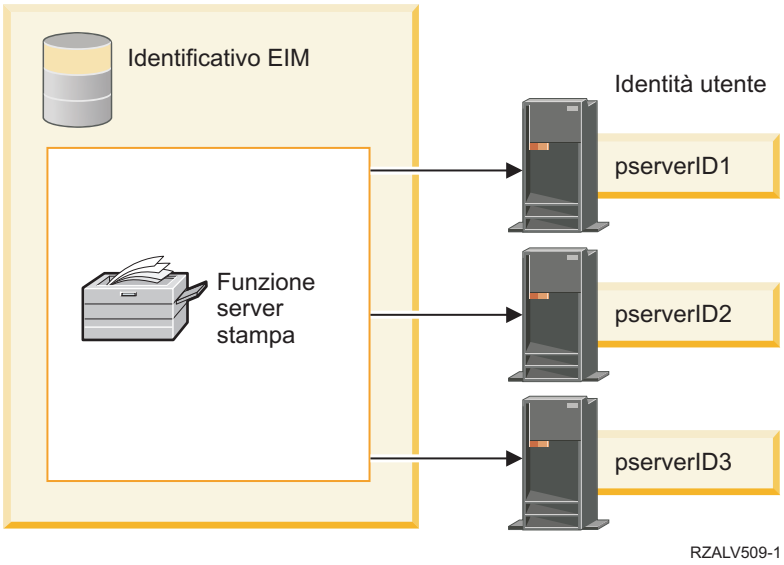


In EIM, è possibile creare associazioni che definiscono le relazioni tra l'identificativo `John Day` e ognuna delle diverse identità utente di *John Day*. Creando queste associazioni per definire queste relazioni, è possibile scrivere delle applicazioni che utilizzino le API relative ad EIM per ricercare un'identità utente necessaria, ma sconosciuta, in base ad un'identità utente nota.

Identificativo EIM che rappresenta un'entità

Oltre a rappresentare gli utenti, gli identificativi EIM possono rappresentare le entità all'interno della propria società come mostra la Figura 4. Ad esempio, spesso la funzione del server di stampa in una società viene eseguita su più sistemi. Nella Figura 4, la funzione del server di stampa nella società viene eseguita su tre diversi sistemi sotto tre diverse identità `pserverID1`, `pserverID2` e `pserverID3`.

Figura 4: la relazione tra l'identificativo EIM che rappresenta la funzione del server di stampa e le diverse identità utente relative a tale funzione



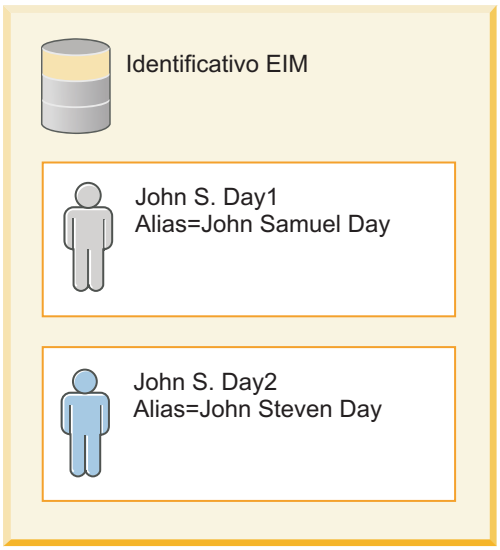
Con EIM, è possibile creare un singolo identificativo che rappresenta la funzione del server di stampa all'interno dell'intera società. Come illustrato dall'esempio, l'identificativo EIM `Funzione server di stampa` rappresenta l'effettiva entità della funzione del server di stampa nell'azienda. Le associazioni sono create per definire le relazioni tra l'identificativo EIM (`Funzione server di stampa`) e ognuna delle entità utente per questa funzione (`pserverID1`, `pserverID2` e `pserverID3`). Queste associazioni consentono agli sviluppatori di applicazioni di utilizzare le operazioni di ricerca EIM per trovare una specifica funzione del server di stampa. I fornitori dell'applicazione possono poi scrivere le applicazioni distribuite che gestiscono la funzione del server di stampa in modo più semplice nella società.

Alias e identificativi EIM

I nomi degli identificativi EIM devono essere univoci all'interno di un dominio EIM. Gli alias possono risolvere situazioni in cui l'utilizzo di nomi identificativi univoci può risultare difficoltoso. Risulta utile utilizzare gli alias di un identificativo EIM, ad esempio, in situazioni in cui il nome legale di un utente è diverso da quello con cui l'utente è noto. Ad esempio, diversi soggetti di un'azienda possono condividere lo stesso nome; ciò può creare confusione se si utilizzano i nomi propri come identificativi EIM.

La Figura 5 mostra un esempio in cui in una società sono presenti due utenti che si chiamano *John S. Day*. L'amministratore EIM crea due identificativi diversi per distinguere i due utenti: `John S. Day1` e `John S. Day2`. Tuttavia, quale *John S. Day* venga rappresentato da ognuno di questi due identificativi non è subito chiaro.

Figura 5: gli alias dei due identificativi EIM si basano sul nome proprio condiviso *John S. Day*



RZALV511-1

Utilizzando gli alias, invece, l'amministratore EIM è in grado di fornire informazioni aggiuntive sull'individuo per ciascun identificativo EIM. Ogni identificativo EIM può avere associati diversi alias per identificare il *John S. Day* rappresentato dall'identificativo EIM. Ad esempio, gli alias aggiuntivi possono contenere il numero impiegato, il numero del reparto, le mansioni di ciascun utente o un qualsiasi altro attributo distintivo. In quest'esempio, un alias per `John S. Day1` potrebbe essere `John Samuel Day` e un alias per `John S. Day2` potrebbe essere `John Steven Day`.

È possibile utilizzare le informazioni di alias come ausilio nell'individuazione di uno specifico identificativo EIM. Ad esempio, un'applicazione che utilizza EIM può specificare un alias che questo usa per trovare l'identificativo EIM appropriato per l'applicazione. Un amministratore può aggiungere questo alias ad un identificativo EIM in modo che l'applicazione possa utilizzare l'alias piuttosto che il nome identificativo univoco per operazioni EIM. Un'applicazione può specificare queste informazioni quando utilizza la API per ottenere le identità di destinazione EIM dall'identificativo (`eimGetTargetFromIdentifier()`) per eseguire un'operazione di ricerca EIM per trovare l'appropriata identità utente di cui ha bisogno.

Concetti correlati

"Dominio EIM" a pagina 6
Un dominio EIM (Enterprise Identity Mapping) è un indirizzario presente nel server LPDA (Lightweight Directory Access Protocol) che contiene i dati EIM di una società.

Definizioni di registro EIM

Una definizione registro EIM (Enterprise Identity Mapping) è una voce all'interno di EIM che si crea per rappresentare un registro utenti effettivo che esiste su un sistema all'interno della propria azienda. Un registro utenti funziona come un indirizzario e contiene un elenco di identità utente valide per un determinato sistema o applicazione.

Un registro utente di base contiene le identità utente e le relative parole d'ordine. Un esempio di un registro utenti è il registro di z/OS Security Server Resource Access Control Facility (RACF). I registri utenti possono contenere anche altre informazioni. Ad esempio, un indirizzario LDAP (Lightweight Directory Access Protocol) contiene DN (distinguished name) collegati, parole d'ordine e controlli di accesso ai dati memorizzati in LDAP. Altri esempi di registri utenti comuni soni i principal nell'ambito Kerberos oppure le identità utente in un dominio Windows Active Directory ed il registro dei profili utente di i5/OS.

È inoltre possibile definire i registri utenti che sono presenti all'interno di altri registri utenti. Alcune applicazioni utilizzano una sottoserie di identità utente all'interno di una singola istanza di un registro utenti. Ad esempio, il registro z/OS Security Server (RACF) può contenere dei registri utenti specifici che sono una sottoserie degli utenti all'interno dell'intero registro utente RACF.

Le definizioni di registro EIM forniscono informazioni relative a tali registri utenti in una società. L'amministratore definisce questi registri su EIM fornendo le seguenti informazioni:

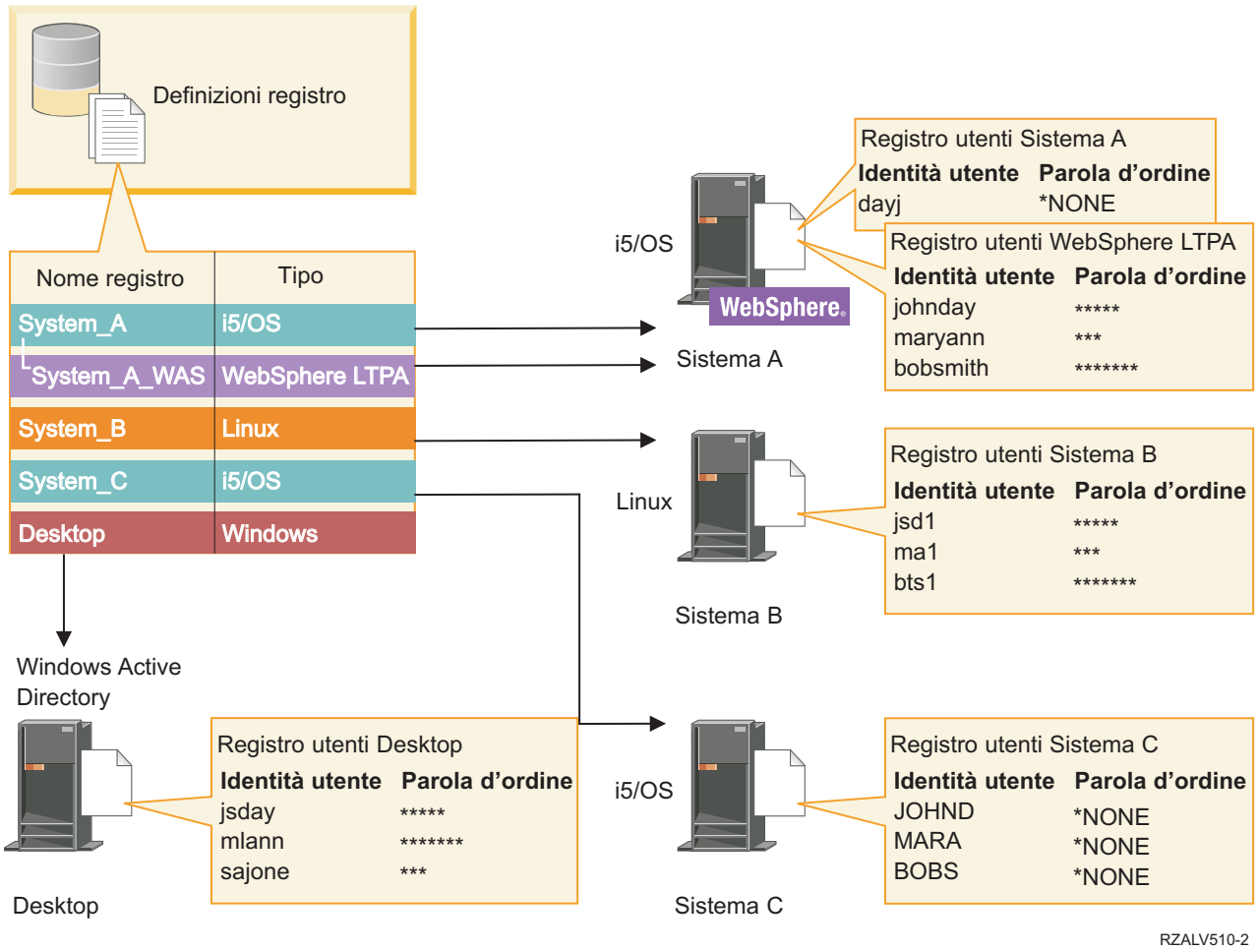
- Un nome registro EIM univoco e arbitrario. Ciascuna definizione di registro rappresenta una specifica istanza di un registro utenti. Di conseguenza, è necessario scegliere un nome definizione di registro EIM che sia di aiuto nell'identificare una particolare istanza del registro utenti. Ad esempio, è possibile scegliere il nome host TCP/IP per un registro utente del sistema oppure il nome host combinato con il nome dell'applicazione per un registro utente dell'applicazione. È possibile utilizzare una qualsiasi combinazione di caratteri alfanumerici, di caratteri in maiuscolo e minuscolo e di spazi per creare dei nomi di definizioni di registro EIM univoci.
- Il tipo di registro utente. EIM fornisce un certo numero di tipi di registro utenti predefiniti che abbraccia la maggior parte dei registri utenti dei sistemi operativi. Questi includono:
  - AIX
  - Domino - nome lungo
  - Domino - nome breve
  - Kerberos
  - Kerberos - sensibile al maiuscolo e al minuscolo
  - LDAP
  - - LDAP - nome breve
  - Linux
  - Novell Directory Server
  - - Altro
  - - Altro - sensibile al maiuscolo e al minuscolo
  - i5/OS (o OS/400)
  - Tivoli Access Manager
  - RACF
  - Windows - locale
  - Dominio Windows (Kerberos) (Questo tipo è sensibile al maiuscolo/minuscolo).
  - X.509

  anche se i tipi di definizione di registro predefiniti abbracciano la maggior parte dei registri utenti di sistema operativo, è possibile che occorra creare una definizione di registro per cui EIM non include un tipo di registro predefinito. In questo caso esistono due opzioni. È possibile utilizzare una definizione di registro esistente che corrisponde alle caratteristiche del proprio registro utenti oppure è possibile definire un tipo di registro utenti privato. Ad esempio, nella Figura 6, l'amministratore si è attenuto al processo richiesto e ha definito il tipo di registro come `WebSphere LTPA` per la definizione di registro applicazione `System_A_WAS`.

Nella Figura 6, l'amministratore ha creato le definizioni di registro di sistema EIM per i registri utenti che rappresentano il Sistema A, il Sistema B, il Sistema C ed una Windows Active Directory che contiene i principal Kerberos degli utenti con cui questi si collegano alle stazioni di lavoro dei propri desktop. Inoltre, l'amministratore ha creato una definizione di registro applicazione per WebSphere (R) Lightweight Third-Party Authentication (LTPA), che viene eseguito su un Sistema A. Il nome di definizione di registro utilizzato dall'amministratore aiuta ad identificare la specifica ricorrenza del tipo di registro utenti. Ad esempio, spesso un indirizzo IP o un nome host è sufficiente per molti tipi di registri utenti. In quest'esempio, l'amministratore utilizza `System_A_WAS` come nome di definizione di

registro applicazione per identificare questa specifica istanza dell'applicazione WebSphere LTPA. Egli specifica inoltre che il registro di sistema principale per la definizione di registro applicazione è il registro `System_A`.

Figura 6: definizioni di registro EIM per cinque registri utenti in un'azienda



Nota: per ridurre ulteriormente il bisogno di gestire le parole d'ordine degli utenti, l'amministratore nella Figura 6 imposta le parole d'ordine dei profili utente i5/OS su un Sistema A e su un sistema C su *NONE. L'amministratore, in questo caso, sta configurando un ambiente con SSO e la sola applicazione con la quale possono lavorare i suoi utenti sono le applicazioni abilitate a EIM, come System i Navigator. Di conseguenza, l'amministratore vuole eliminare le parole d'ordine dai loro profilo utente i5/OS in modo tale che sia gli utenti che l'amministratore stesso abbiano un numero minore di parole d'ordine da gestire.

Concetti correlati

"Dominio EIM" a pagina 6
Un dominio EIM (Enterprise Identity Mapping) è un indirizzario presente nel server LPDA (Lightweight Directory Access Protocol) che contiene i dati EIM di una società.

"Definizione di un tipo di registro utente privato in EIM" a pagina 100
Quando si crea una definizione di registro EIM (Enterprise Identity Mapping) è possibile specificare uno dei vari tipi di registro utenti predefiniti per rappresentare un effettivo registro utenti che esiste su un sistema all'interno della propria azienda.

Definizioni registro utenti

Una definizione di registro di sistema è una voce che si crea in EIM per rappresentare e descrivere un registro utenti distinto in una rete o in un server.

È possibile creare una definizione di registro di sistema EIM per un registro utente quando il registro nell'azienda ha una delle seguenti caratteristiche:

- Il registro è fornito da un sistema operativo, come AIX, i5/OS oppure da un prodotto per la gestione della sicurezza, come z/OS Security Server Resource Access Control Facility (RACF).
- Il registro contiene identità utente univoche per una specifica applicazione, come Lotus Notes.
- Il registro contiene identità utente distribuite, come ad esempio i principal Kerberos o i DN LDAP (Lightweight Directory Access Protocol).

Le operazioni di ricerca EIM vengono eseguite correttamente indipendentemente dal fatto che un amministratore EIM definisca un registro come sistema o applicazione. Tuttavia, le definizioni separate del registro consentono la gestione dei dati di corrispondenza sulla base dell'applicazione. La responsabilità della gestione delle corrispondenze specifiche dell'applicazione possono essere assegnate ad un amministratore per uno specifico registro.

Attività correlate

"Aggiunta di una definizione del registro dell'applicazione" a pagina 98
Per creare una definizione registro applicazione, è necessario essere connessi al dominio EIM (Enterprise Identity Mapping) in cui si desidera lavorare e disporre del controllo di accesso dell'amministratore EIM.

Definizioni registro applicazioni

Una definizione del registro applicazioni è una voce all'interno di EIM che l'utente può creare per descrivere e rappresentare una sottoserie di identità utente definite in un registro di sistema. Queste identità utente condividono una serie comune di attributi o caratteristiche che consente loro di utilizzare un'applicazione particolare o una serie di applicazioni.

Le definizioni del registro delle applicazioni rappresentano i registri utente esistenti all'interno di altri registri utente. Ad esempio, il registro z/OS Security Server (RACF) può contenere dei registri utenti specifici che sono una sottoserie degli utenti all'interno dell'intero registro utente RACF. A causa di questa relazione, è necessario specificare il nome del registro di sistema principale per le eventuali definizioni di registro applicazione che si creano.

È possibile creare una definizione di registro applicazione EIM per un registro utenti quando le identità utente nel registro hanno le seguenti caratteristiche:

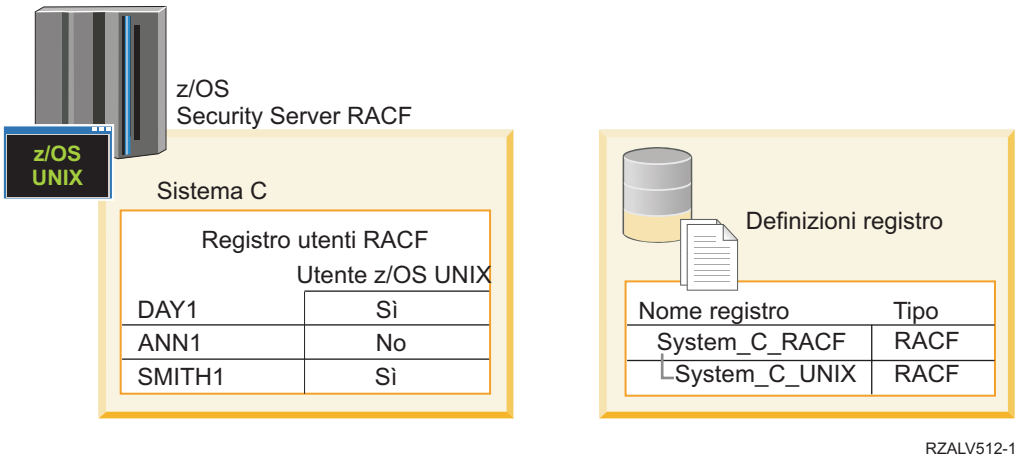
- Le identità utente per un'applicazione non sono memorizzate in un registro utenti specifico per l'applicazione.
- Le identità utente per un'applicazione sono memorizzate in un registro di sistema che contiene le identità utente per le altre applicazioni.

Le operazioni di ricerca EIM vengono eseguite correttamente indipendentemente dal fatto che un amministratore EIM crei una definizione di registro di sistema o di applicazione per un registro utenti. Tuttavia, le definizioni separate del registro consentono la gestione dei dati di corrispondenza sulla base dell'applicazione. La responsabilità della gestione delle corrispondenze specifiche dell'applicazione possono essere assegnate ad un amministratore per uno specifico registro.

Ad esempio, la Figura 7 mostra come un amministratore EIM ha creato una definizione di registro di sistema per rappresentare un registro z/OS Security Server RACF. L'amministratore ha inoltre creato una definizione di registro applicazione per rappresentare le identità utente all'interno del registro RACF che utilizza z/OS(TM) UNIX System Services (z/OS UNIX). Il Sistema C contiene un registro utenti RACF che contiene le informazioni relative a tre identità utente, `DAY1`, `ANN1` e `SMITH1`. Due di queste identità utente (`DAY1` e `SMITH1`) accedono a z/OS UNIX sul Sistema C. Queste identità utente sono effettivamente degli

utenti RACF con degli attributi univoci che li identificano come utenti z/OS UNIX. All'interno delle definizioni di registro EIM, l'amministratore EIM ha definito `System_C_RACF` per rappresentare il registro utenti RACF generale. L'amministratore ha inoltre definito `System_C_UNIX` per rappresentare le identità utente che hanno attributi z/OS UNIX.

Figura 7: definizioni di registro EIM per il registro utenti RACF e per gli utenti di z/OS UNIX



Definizioni del registro di gruppo

Il raggruppamento logico delle definizioni di registro consente di ridurre la quantità di lavoro che è necessario eseguire per configurare la corrispondenza EIM. È possibile gestire una definizione del registro di gruppo come se fosse una singola definizione del registro.

Tutti i membri della definizione del registro di gruppo generalmente contengono almeno un'identità utente comune su cui si desidera creare un'associazione di origine o di destinazione. Il raggruppamento dei membri consente di creare una singola associazione, anziché più associazioni, alla definizione del registro di gruppo e all'identità utente.

Ad esempio, John Day si collega al proprio sistema principale con identità utente `jday` e utilizza la stessa identità utente, `JOHND`, su più sistemi. Quindi, il registro utente per ogni sistema contiene l'identità utente `JOHND`. Generalmente, John Day crea un'associazione di destinazione separata dall'identificativo EIM John Day a ogni singolo registro utente che contiene l'identità utente `JOHND`. Per ridurre la quantità di lavoro che tale utente deve eseguire per configurare la corrispondenza EIM, può creare una definizione del registro di gruppo con tutti i registri utente che contengono l'identità utente `JOHND` come membri del gruppo. Egli può quindi creare una singola associazione di destinazione dall'identificativo EIM `John Day` alla definizione del registro di gruppo anziché più associazioni di destinazione dall'identificativo EIM John Day a ciascuna delle singole definizioni del registro. Questa singola associazione di destinazione alla definizione del registro di gruppo consente all'identità utente di John Day, `jday`, di stabilire una corrispondenza con l'identità `JOHND`.

Consultare le seguenti informazioni relative alle definizioni del registro di gruppo:

- Tutti i membri (singole definizioni del registro) della definizione del registro di gruppo devono avere la stessa sensibilità al maiuscolo/minuscolo.
- Tutti i membri (singole definizioni del registro) della definizione del registro di gruppo devono essere definiti nel dominio EIM prima di potere essere aggiunti a una definizione del registro di gruppo.
- Una definizione del registro può essere membro di più gruppi, ma si consiglia di evitare di specificare un singolo registro utente come membro di più definizioni del registro di gruppo poiché l'operazione di ricerca potrebbe restituire risultati ambigui. La definizione del registro di gruppo non può essere membro di un'altra definizione del registro di gruppo.

Concetti correlati

"Esempi di operazioni di ricerca: Esempio 5" a pagina 36
Utilizzare questo esempio per comprendere le operazioni di ricerca che restituiscono risultati ambigui che coinvolgono le definizioni del registro di gruppo.

Associazioni EIM

Un'associazione EIM (Enterprise Identity Mapping) è una voce che l'utente crea in un dominio EIM per definire una relazione tra le identità utente in registri utenti differenti. Il tipo di associazione creato determina se la relazione definita è diretta o indiretta.

È possibile creare due tipi di associazioni in EIM: le associazioni di identificativi, per definire delle associazioni uno-a-uno, e le associazioni normativa. È possibile utilizzare le associazioni normativa invece di, oppure insieme ad, associazioni di identificativi. Il modo in cui si utilizzano le associazioni dipende dal proprio piano generale di implementazione di EIM.

Per ulteriori informazioni sull'utilizzo delle associazioni, consultare le seguenti informazioni:

Ricerca delle informazioni

Con EIM (Enterprise Identity Mapping) è possibile fornire dati facoltativi detti informazioni di ricerca per identificare ulteriormente un'identità utente. Questa identità utente di destinazione può essere specificata in un'associazione identificativi o in un'associazione di normative.

Le informazioni di ricerca sono una stringa di caratteri univoca che l'API EIM `eimGetTargetFromSource` o l'API EIM `eimGetTargetFromIdentifier` possono utilizzare durante un'operazione di ricerca corrispondenze per definire ulteriormente la ricerca dell'identità utente di destinazione che è l'oggetto dell'operazione. I dati specificati per le informazioni di ricerca corrispondono al parametro informazioni aggiuntive utenti registro per queste API EIM.

Le informazioni di ricerca sono necessarie solo quando un'operazione di ricerca corrispondenze può restituire più di un'identità utente di destinazione. Un'operazione di ricerca corrispondenze può restituire più identità utente destinazione quando si verificano una o più delle seguenti situazioni:

- Un identificativo EIM ha più associazioni di destinazione singole per lo stesso registro destinazione.
- Più di un identificativo EIM ha la stessa identità utente specificata in un'associazione di origine e ciascuno di questi identificativi EIM ha un'associazione di destinazione allo stesso registro di destinazione, anche se l'identità utente specificata per ciascuna associazione di destinazione potrebbe essere differente.
- Più di un'associazione normativa di dominio predefinita ha lo stesso registro di destinazione.
- Più di un'associazione normativa di registro predefinita specifica lo stesso registro di origine e lo stesso registro di destinazione.
- Più di un'associazione normativa filtro certificato specifica lo stesso registro X.509 di origine, lo stesso filtro di certificati e lo stesso registro di destinazione.

Nota: un'operazione di ricerca corrispondenze che restituisce più di una identità utente di destinazione può creare problemi per applicazioni abilitate EIM, inclusi applicazioni e prodotti i5/OS, non progettati per gestire questi risultati ambigui. Tuttavia, le applicazioni base i5/OS come System i Access per Windows non possono utilizzare le informazioni di ricerca per distinguere tra più identità utenti di destinazione restituite da un'operazione di ricerca. Di conseguenza, è possibile prendere in considerazione il ridefinire le associazioni per il dominio per assicurare che un'operazione di ricerca di corrispondenze possa restituire una singola identità utente di destinazione per assicurare che le applicazioni i5/OS di base possano eseguire correttamente le operazioni di ricerca e eseguire messe in corrispondenza di identità.

È possibile utilizzare le informazioni di ricerca per evitare situazioni in cui sia possibile che operazioni di ricerca corrispondenze restituiscano più di un'identità utente di destinazione. Per evitare che operazioni di ricerca corrispondenze restituiscano più identità utente di destinazione, è necessario definire

informazioni di ricerca univoche per ogni identità utente di destinazione in ogni associazione. Queste informazioni di ricerca devono essere fornite nell'operazione di ricerca corrispondenze per garantire che l'operazione possa restituire un'identità utente destinazione univoca. Altrimenti, applicazioni che si basano su EIM potrebbero non essere in grado di stabilire l'esatta identità di destinazione da utilizzare.

Si ha, ad esempio, un identificativo EIM denominato `John Day` che ha due profili utente sul Sistema A. Uno di questi profili utente è `JDUSER` sul Sistema A e un altro è `JDSECADM`, che ha l'autorizzazione speciale di amministratore della sicurezza. Ci sono due associazioni di destinazione per l'identificativo John Day. Una di questa associazioni di destinazione è per l'identità utente `JDUSER` nel registro di destinazione di `Sistema_A` ed ha le informazioni di ricerca di `autorizzazione utente` specificate per `JDUSER`. L'altra associazione di destinazione è per l'identità utente `JDSECADM` nel registro di destinazione di `Sistema_A` ed ha le informazioni di ricerca di `addetto alla sicurezza` specificate per `JDSECADM`.

Se un'operazione di ricerca di corrispondenze non specifica informazioni di ricerca, l'operazione di ricerca restituisce entrambe le identità utente, `JDUSER` e `JDSECADM`. Se un'operazione di ricerca di corrispondenze specifica le informazioni di ricerca `autorizzazione utente`, l'operazione di ricerca restituisce solo l'identità utente `JDUSER`. Se un'operazione di ricerca di corrispondenze specifica le informazioni di ricerca `addetto alla sicurezza`, l'operazione di ricerca restituisce solo l'identità utente `JDSECADM`.

Nota: se si cancella l'ultima associazione di destinazione per un'identità utente (sia che si tratti di un'associazione di identificativi che di un'associazione normativa), anche l'identità utente di destinazione e tutte le informazioni di ricerca vengono cancellate dal dominio.

Poiché è possibile utilizzare le associazioni normativa certificato ed altre associazioni in diversi modi che si sovrappongono, sarebbe necessaria una conoscenza approfondita sia del supporto normativa corrispondenze EIM che del modo in cui funzionano le operazioni di ricerca prima di creare ed utilizzare delle associazioni normativa certificato.

Concetti correlati

"Abilitazione e supporto normativa corrispondenze EIM" a pagina 38
Il supporto normativa corrispondenze EIM (Enterprise Identity Mapping) consente di utilizzare le associazioni normativa ed anche delle specifiche associazioni di identificativi in un dominio EIM. È possibile utilizzare le associazioni normativa invece di, oppure insieme ad, associazioni di identificativi.

"Operazioni di ricerca EIM" a pagina 28
Un'applicazione o un sistema operativo utilizza un'API EIM per eseguire un'operazione di ricerca in modo che l'applicazione o il sistema operativo possa eseguire la corrispondenza da un'identità utente in un registro ad un'altra identità utente in un altro registro. Un'operazione di ricerca EIM è un processo attraverso il quale un'applicazione o un sistema operativo rileva un'identità utente associata sconosciuta in uno specifico registro di destinazione, fornendo alcune informazioni note e affidabili.

"Associazioni normative dominio predefinito" a pagina 21
Un'associazione normativa di dominio predefinita è un tipo di associazione normativa che è possibile utilizzare per creare corrispondenze molti-ad-uno tra identità utente.

"Associazioni normative registro predefinito" a pagina 23
Un'associazione normativa di registro predefinita è un tipo di associazione normativa che è possibile utilizzare per creare corrispondenze molti-ad-uno tra identità utente.

Associazioni identificativo

Un identificativo EIM rappresenta una specifica persona o entità in una società. Un'associazione di identificativi EIM descrive una relazione tra un identificativo EIM ed una singola identità utente in un registro utente che rappresenta anche detta persona. Quando si creano le associazioni tra un identificativo EIM e tutte le identità utente di un'entità o di una persona, si forniscono informazioni complete e uniche su come tale persona o entità utilizza le risorse all'interno di un'azienda.

Le identità utente possono essere utilizzare per l'autenticazione, per l'autorizzazione o per entrambe le funzioni. *L'autenticazione* è il processo di verifica che viene effettuato su un'entità o una persona, che

fornisce un'identità utente, per controllare se dispone del diritto di assumere tale identità. Tale operazione viene spesso effettuata obbligando la persona che inoltra l'identità a fornire informazioni private o riservate associate all'identità utente, come ad esempio una parola d'ordine. *L'autorizzazione* è il processo tramite cui ci si assicura che un'identità utente autenticata in modo appropriato possa eseguire solo funzioni o accedere a risorse per le quali dispone di privilegi. In precedenza, quasi tutte le applicazioni venivano forzate ad utilizzare le identità presenti in un singolo registro utenti sia per l'autenticazione che per l'autorizzazione. Utilizzando le operazioni di ricerca EIM, le applicazioni ora possono utilizzare le identità in un registro utenti ed utilizzare le identità utente associate in un differente registro utenti per l'autorizzazione.

L'identificativo EIM fornisce un'associazione indiretta tra quelle identità utente, che consente alle applicazioni di reperire un'identità utente differente per un identificativo EIM in base ad un'identità utente conosciuta. EIM fornisce le API che consentono alle applicazioni di rilevare un'identità utente sconosciuta in un registro utente (destinazione) specifico fornendo un'identità utente nota in qualche altro registro utente (origine). Questo processo è detto corrispondenza identità.

In EIM, un amministratore è in grado di definire tre diversi tipi di associazioni per descrivere la relazione tra un identificativo EIM e un'identità utente. Le associazioni di identificativi possono essere di uno dei seguenti tipi: di origine, di destinazione o amministrative. Il tipo di associazione creato è basato su come viene utilizzata l'identità utente. È ad esempio possibile creare delle associazioni di origine e di destinazione per quelle identità utente che si desidera partecipino alle operazioni di ricerca di corrispondenze. Di norma, se un'identità utente viene utilizzata per l'autenticazione, si crea per essa un'associazione di origine. Si creano quindi delle associazioni di destinazione per quelle identità utente utilizzate per l'autorizzazione.

Prima di poter creare un'associazione identificativo, è necessario innanzitutto creare l'identificativo EIM appropriato e l'appropriata definizione registro EIM per il registro utenti che contiene l'identità utente associata. Un'associazione definisce una relazione tra un identificativo EIM e un'identità utente utilizzando le seguenti informazioni:

- Nome identificativo EIM
- Nome identità utente
- Nome definizione registro EIM
- Tipo di associazione
- Facoltativo: informazioni di ricerca per identificare ulteriormente l'identità utente di destinazione in un'associazione di destinazione.

Associazione origine

Un'associazione origine consente di utilizzare l'identità utente come origine in un'operazione di ricerca EIM per rilevare un'identità utente diversa associata allo stesso identificativo EIM.

Quando un'identità utente viene utilizzata per l'*autenticazione*, tale identità deve disporre di un'associazione origine ad un identificativo EIM. Ad esempio, si potrebbe creare un'associazioni origine per un principal Kerberos poiché questa forma di identità utente viene utilizzata per l'autenticazione. Per assicurare l'esito positivo delle operazioni di ricerca di corrispondenze per gli identificativi EIM, è necessario utilizzare associazioni di origine e di destinazione insieme per un singolo identificativo EIM.

Associazione di destinazione

Un'associazione di destinazione consente la restituzione dell'identità utente come risultato di un'operazione di ricerca EIM. Le identità utente che rappresentano gli utenti finali solitamente necessitano della sola associazione di destinazione.

Quando un'identità utente viene utilizzata per l'*autorizzazione* invece che per l'autenticazione, tale identità deve disporre di un'associazione di destinazione ad un identificativo EIM. Ad esempio, si potrebbe creare

un'associazione di destinazione per un profilo utente i5/OS poiché questa forma di identità utente determina di quali risorse e privilegi dispone l'utente su una piattaforma specifica System i. Per assicurare l'esito positivo delle operazioni di ricerca di corrispondenze per gli identificativi EIM, è necessario utilizzare associazioni di origine e di destinazione insieme per un singolo identificativo EIM.

Relazione tra associazioni di origine e di destinazione

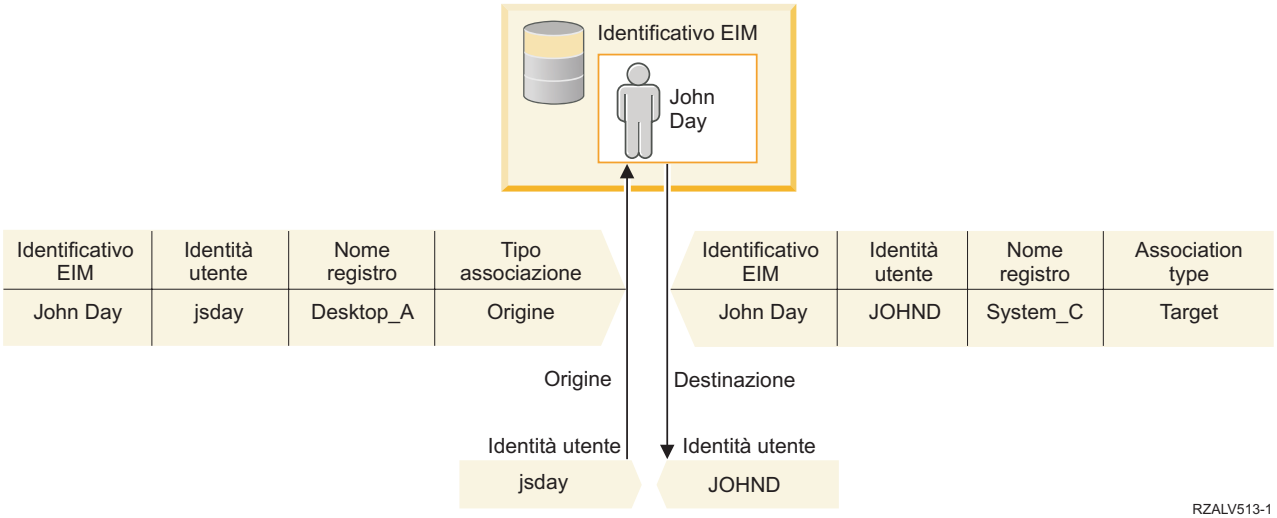
Per assicurare la corretta esecuzione delle operazioni di ricerca di corrispondenze, bisogna creare almeno un'associazione di origine ed una o più associazioni di destinazione per un singolo identificativo EIM. Di norma, si crea un'associazione di destinazione per ciascuna identità utente in un registro utenti che la persona può utilizzare per l'autorizzazione al sistema o all'applicazione cui corrisponde il registro utenti.

Ad esempio, gli utenti nella propria impresa normalmente si collegano ed eseguono l'autenticazione sui desktop Windows e accedono a una piattaforma System i per eseguire numerose attività. Gli utenti accedono ai loro desktop utilizzando un principal Kerberos ed accedono alla piattaforma System i utilizzando un profilo utente i5/OS. Si desidera creare un ambiente SSO (single sign-on) in cui gli utenti effettuano l'autenticazione per i propri desktop utilizzando il relativo principal Kerberos e non devono più effettuare l'autenticazione manuale per la piattaforma System i.

Per eseguire quest'operazione, si crea un'associazione di origine per il principal Kerberos per ogni utente e per l'identificativo EIM di detto utente. Si crea quindi un'associazione di destinazione per il profilo utente i5/OS per ciascun utente e per l'identificativo EIM di detto utente. Questa configurazione garantisce che i5/OS possa eseguire un'operazione di ricerca corrispondenze per stabilire il profilo utente corretto necessario per un utente che accede alla piattaforma System i dopo aver effettuato l'autenticazione per il proprio desktop. i5/OS quindi consente l'accesso dell'utente alle risorse sul server in base al profilo utente appropriato senza richiedere all'utente l'autenticazione manuale per il server.

La Figura 6 illustra un altro esempio in cui un amministratore EIM crea due associazioni, un'associazione di origine ed un'associazione di destinazione, per l'identificativo EIM `John Day` per definire la relazione tra quest'identificativo e due identità utente associate. L'amministratore crea un'associazione di origine per `jsday`, un principal Kerberos nel registro utenti `Desktop`. L'amministratore crea inoltre un'associazione di destinazione per `JOHND`, il profilo utente i5/OS nel registro utenti `System_C`. Queste associazioni forniscono il mezzo attraverso il quale le applicazioni ottengono un'identità utente sconosciuta (destinazione, `JOHND`) in base a un'identità utente nota (origine, `jsday`) come parte di un'operazione di ricerca EIM.

Figura 6: le associazioni di origine e di destinazione EIM per l'identificativo EIM `John Day`



Per estendere l'esempio, si supponga che l'amministratore EIM realizza che John Day utilizza lo stesso profilo utente i5/OS, jsd1, su cinque sistemi differenti. In questa situazione, è necessario che l'amministratore crei sei associazioni per l'identificativo EIM John Day per definire la relazione tra questo identificativo e un'identità utente associata in cinque registri utente: un'associazione di origine per johnday, un principal Kerberos nel registro utente Desktop_A e cinque associazioni di destinazione per jsd1, il profilo utente i5/OS nei cinque registri utente: System_B, System_C, System_D, System_E e System_F. Per ridurre la quantità di lavoro da eseguire per la configurazione dell'associazione EIM, l'amministratore EIM crea una definizione del registro di gruppo. I membri della definizione del registro di gruppo includono i nomi di definizione del registro di System_B, System_C, System_D, System_E e System_F. Il raggruppamento dei membri consente all'amministratore di creare una singola associazione di destinazione alla definizione del registro di gruppo e all'identità dell'utente, anziché più associazioni a singoli nomi di definizione del registro. Le associazioni di origine e di destinazione forniscono il mezzo attraverso il quale le applicazioni ottengono un'identità utente sconosciuta (destinazione, jsd1) nei cinque registri utente rappresentati come membri della definizione del registro di gruppo in base a un'identità utente nota (origine, johnday) come parte di un'operazione di ricerca EIM.

Per alcuni utenti, potrebbe essere necessario creare un'associazione sia di origine che di destinazione per la stessa identità utente. Questa operazione è necessaria quando un individuo utilizza un singolo sistema sia come client che come server o per gli individui che svolgono le funzioni degli amministratori.

Nota: le identità utente che rappresentano gli utenti tipici generalmente necessitano solo di un'associazione di destinazione.

Per alcuni utenti, potrebbe essere necessario creare un'associazione sia di origine che di destinazione per la stessa identità utente. Questa operazione è necessaria quando un individuo utilizza un singolo sistema sia come client che come server o per gli individui che svolgono le funzioni degli amministratori.

Ad esempio, un amministratore utilizza la funzione Management Central in System i Navigator per gestire un sistema centrale e vari sistemi endpoint. L'amministratore esegue varie funzioni e queste funzioni possono avere origine sul sistema centrale o su un sistema endpoint. In questa situazione, creare sia un'associazione di origine che un'associazione di destinazione per ciascuna delle identità utente dell'amministrazione su ciascuno dei sistemi. Questo assicura che, indipendentemente dal sistema utilizzato dall'amministratore per originare l'accesso ad uno degli altri sistemi, l'identità utente utilizzata per originare l'accesso all'altro sistema può essere messa in corrispondenza con l'appropriata identità utente per il successivo sistema cui accede l'amministratore.

Associazione amministrativa

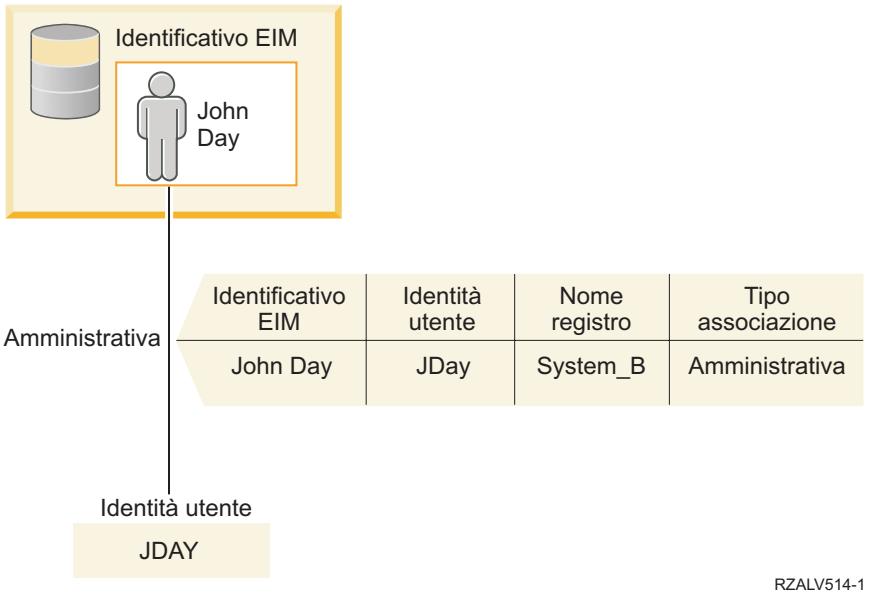
Un'associazione amministrativa per un identificativo EIM viene solitamente utilizzata per spiegare che la persona o l'entità rappresentata dall'identificativo EIM possiede un'identità utente che necessita di considerazioni speciali per un sistema specifico. È possibile utilizzare questo tipo di associazione, ad esempio, con registri utenti altamente sensibili.

A causa della particolarità delle associazioni amministrative, questo tipo di associazione non può prendere parte alle operazioni di ricerca delle corrispondenze EIM. Di conseguenza, l'operazione di ricerca EIM che fornisce un'identità utente origine con un'associazione amministrativa non restituisce alcun risultato. In modo simile, un'identità utente con un'associazione amministrativa non viene mai restituita come risultato di un'operazione di ricerca EIM.

La Figura 7 illustra un esempio di associazione amministrativa. In questo esempio, un impiegato che si chiama John Day ha un'identità utente di John_Day sul Sistema A ed un'identità utente di JDay sul Sistema B, che è un sistema altamente sicuro. Il responsabile di sistema vuole garantire che gli utenti vengano autenticati nel Sistema B utilizzando solo il registro utente locale di questo sistema. L'amministratore non desidera consentire che un'applicazione autentichi John Day per il sistema utilizzando qualche altro meccanismo di autenticazione. Utilizzando un'associazione amministrativa per l'identità utente JDay nel Sistema B, l'amministratore EIM può vedere che John Day possiede un account

sul Sistema B, ma EIM non restituisce informazioni sull'identità JDay nelle operazioni di ricerca EIM. Anche se le applicazioni sono presenti su questo sistema che utilizza le operazioni di ricerca EIM, tali applicazioni non sono in grado di rilevare le identità utente che dispongono di associazioni amministrative.

Figura 7: associazione amministrativa EIM per l'identificativo EIM John Day



Associazioni normativa

La normativa di corrispondenze di EIM (Enterprise Identity Mapping) consente ad un amministratore EIM di creare ed utilizzare delle associazioni normativa per definire una relazione tra più identità utente in uno o più registri utenti ed una singola identità utente in un altro registro utenti.

Le associazioni normativa utilizzano il supporto normativa corrispondenze EIM per creare corrispondenze molti-ad-uno tra identità utente senza coinvolgere un identificativo EIM. È possibile utilizzare associazioni normativa invece di, oppure insieme ad, associazioni di identificativi che forniscono corrispondenze uno-a-uno tra un identificativo EIM ed una singola identità utente.

Un'associazione normativa influenza solo quelle identità utente per cui non esistono singole associazioni EIM specifiche. Quando esistono associazioni di identificativi specifiche tra un identificativo EIM e delle identità utente, l'identità utente di destinazione dall'associazione identificativo viene restituita all'applicazione che esegue l'operazione di ricerca, anche quando esiste un'associazione normativa ed è abilitato l'uso delle associazioni normativa.

È possibile creare tre tipi differenti di associazioni normativa:

Concetti correlati

"Operazioni di ricerca EIM" a pagina 28
Un'applicazione o un sistema operativo utilizza un'API EIM per eseguire un'operazione di ricerca in modo che l'applicazione o il sistema operativo possa eseguire la corrispondenza da un'identità utente in un registro ad un'altra identità utente in un altro registro. Un'operazione di ricerca EIM è un processo attraverso il quale un'applicazione o un sistema operativo rileva un'identità utente associata sconosciuta in uno specifico registro di destinazione, fornendo alcune informazioni note e affidabili.

Associazioni normative dominio predefinito:

Un'associazione normativa di dominio predefinita è un tipo di associazione normativa che è possibile utilizzare per creare corrispondenze molti-ad-uno tra identità utente.

È possibile utilizzare un'associazione normativa del dominio predefinito per mettere in corrispondenza una serie origine di più identità utente (in questo caso, tutti gli utenti nel dominio) con una singola identità utente di destinazione in un registro utente di destinazione specificato. In un'associazione normativa del dominio predefinito, tutti gli utenti nel dominio corrispondono all'origine dell'associazione normativa e vengono messi in corrispondenza con un singolo registro di destinazione e un'identità utente di destinazione.

Per utilizzare un'associazione normativa di dominio predefinita, è necessario abilitare ricerche di corrispondenze tramite associazioni normativa per il dominio. È necessario anche abilitare le ricerche di corrispondenze per il registro utente di destinazione dell'associazione normativa. Quando si configura quest'abilitazione, i registri utenti nell'associazione normativa possono partecipare alle operazioni di ricerca corrispondenze.

L'associazione normativa di dominio predefinita ha effetto quando un'operazione di ricerca di corrispondenze non viene soddisfatta da associazioni di identificativi, associazioni normativa filtro certificato o associazioni normativa di registro predefinite per il registro di destinazione. Il risultato è che tutte le identità utente nel dominio vengono messe in corrispondenza con la singola identità utente di destinazione, come specificato dall'associazione normativa di dominio predefinita.

Ad esempio, si crea un'associazione normativa dominio predefinita con un'identità utente di destinazione `John_Day` nel registro destinazione `Registry_xyz` e non si sono create delle associazioni di identificativi o altre associazioni normativa che corrispondono a questa identità utente. Pertanto, quando si specifica `Registry_xyz` come registro di destinazione nelle operazioni di ricerca, la normativa dominio predefinita assicura che l'identità utente di destinazione `John_Day` sia restituita per tutte le identità utente nel dominio per cui non è stata definita alcuna altra associazione.

Per definire un'associazione normativa del dominio predefinito, è necessario specificare queste due informazioni:

- **Registro di destinazione**. Il registro di destinazione che si specifica è il nome della definizione di registro EIM (Enterprise Identity Mapping) che contiene l'identità utente con cui tutte le identità utente nel dominio vanno messe in corrispondenza.
- **Utente di destinazione**. L'utente di destinazione è il nome dell'identità utente restituita come la destinazione di un'operazione di ricerca di corrispondenze EIM basata su quest'associazione normativa.

È possibile definire un'associazione normativa del dominio predefinito per ciascun registro nel dominio. Se due o più associazioni normativa dominio fanno riferimento allo stesso registro di destinazione, è necessario definire informazioni di ricerca univoche per ognuna di queste associazioni normativa per garantire che le operazioni di ricerca corrispondenze possano distinguere tra esse. In caso contrario, le operazioni di ricerca delle corrispondenze possono restituire più identità utente di destinazione. Come risultato di queste operazioni ambigue, le applicazioni che si basano su EIM potrebbero non essere in grado di stabilire l'esatta identità utente di destinazione da utilizzare.

Poiché è possibile utilizzare le associazioni normativa in diversi modi che si sovrappongono, è necessario avere una conoscenza approfondita del supporto normativa corrispondenza EIM e del modo in cui funzionano le operazioni di ricerca prima di creare ed utilizzare delle associazioni normativa.

Nota: è possibile creare un'associazione di normativa dominio predefinita, con un'identità utente di destinazione che esiste all'interno di una definizione del registro di gruppo. Tutti gli utenti nel dominio rappresentano l'origine dell'associazione normativa e vengono messi in corrispondenza con un'identità utente di destinazione in una definizione del registro di gruppo di destinazione. L'identità dell'utente definita nell'associazione della normativa di dominio predefinita esiste all'interno dei membri della definizione del registro di gruppo.

Ad esempio, John Day usa lo stesso profilo utente i5/OS, John_Day, su cinque sistemi differenti: Sistema B, Sistema C, Sistema D, Sistema E e Sistema F. Per ridurre la quantità di lavoro che tale utente deve eseguire per configurare la corrispondenza EIM, l'amministratore EIM crea una definizione del registro di gruppo denominata Group_1. I membri di tale definizione includono i nomi definizione del registro di System_B, System_C, System_D, System_E e System_F. Il raggruppamento dei membri consente all'amministratore di creare una singola associazione di destinazione all'identità utente e alla definizione del registro di gruppo, anziché più associazioni alle singole definizioni del registro.

L'amministratore EIM crea un'associazione normativa dominio predefinita con un'identità utente di destinazione John_Day nel registro destinazione Group_1. In questo caso, non si applica nessun'altra associazione di identificativi o normativa. Pertanto, quando si specifica Group_1 come registro di destinazione nelle operazioni di ricerca, la normativa dominio predefinita assicura che l'identità utente di destinazione John_Day sia restituita per tutte le identità utente nel dominio per cui non è stata definita alcuna associazione.

Concetti correlati

"Ricerca delle informazioni" a pagina 16
Con EIM (Enterprise Identity Mapping) è possibile fornire dati facoltativi detti informazioni di ricerca per identificare ulteriormente un'identità utente. Questa identità utente di destinazione può essere specificata in un'associazione identificativi o in un'associazione di normative.

"Abilitazione e supporto normativa corrispondenze EIM" a pagina 38
Il supporto normativa corrispondenze EIM (Enterprise Identity Mapping) consente di utilizzare le associazioni normativa ed anche delle specifiche associazioni di identificativi in un dominio EIM. È possibile utilizzare le associazioni normativa invece di, oppure insieme ad, associazioni di identificativi.

Associazioni normative registro predefinito:

Un'associazione normativa di registro predefinita è un tipo di associazione normativa che è possibile utilizzare per creare corrispondenze molti-ad-uno tra identità utente.

È possibile utilizzare un'associazione normativa del registro predefinito per mettere in corrispondenza una serie di origine di più identità utente (in questo caso quelle presenti in un singolo registro) con una singola identità utente di destinazione all'interno di un registro utente di destinazione specificato. All'interno di un'associazione normativa del registro predefinito, tutti gli utenti in un singolo registro sono l'origine dell'associazione normativa e vengono messi in corrispondenza con un singolo registro di destinazione e un utente di destinazione.

Per utilizzare associazioni normativa di registro predefinite, è necessario abilitare le ricerche di corrispondenze tramite le associazioni normativa per il dominio. È necessario anche abilitare ricerche di corrispondenze per il registro origine e abilitare ricerche di corrispondenze e l'uso di associazioni normativa per il registro utenti di destinazione dell'associazione normativa. Quando si configura quest'abilitazione, i registri utenti nell'associazione normativa possono partecipare alle operazioni di ricerca corrispondenze.

L'associazione normativa di registro predefinita ha effetto quando un'operazione di ricerca di corrispondenze non viene soddisfatta da associazioni di identificativi, associazioni normativa filtro certificato o altre associazioni normativa di registro predefinite per il registro di destinazione. Il risultato è che tutte le identità utente nel registro di origine vengono messe in corrispondenza con la singola identità utente di destinazione, come specificato dall'associazione normativa di registro predefinita.

Ad esempio, si crea un'associazione normativa registro predefinita con un registro origine my_realm.com, che sono principal in uno specifico dominio Kerberos. Per questa associazione normativa, si specifica anche un'identità utente di destinazione general_user1 nel registro di destinazione i5/OS_system_reg, che è un profilo utente specifico in un registro utenti i5/OS. In questo caso, non si sono create associazioni

identificativo o associazioni normativa valide per le identità utente nel registro origine. Perciò, quando viene specificato i5/OS_system_reg come registro di destinazione e my_realm.com viene specificato come registro di origine in operazioni di ricerca, l'associazione normativa di registro predefinita assicura che l'identità utente di destinazione general_user1 venga restituita per tutte le identità utente in my_realm.com per cui non è stata definita alcuna associazione di identificativi specifica o associazione normativa filtro certificato.

Per definire un'associazione normativa del registro predefinito, è necessario specificare queste tre informazioni:

- **Registro di origine**. Questa è la definizione di registro che si desidera venga utilizzata dall'associazione normativa come origine della messa in corrispondenza. Tutte le identità utente nel registro utenti di origine devono essere messe in corrispondenza con l'utente di destinazione specificato dell'associazione normativa.
- **Registro di destinazione**. Il registro di destinazione che si specifica è il nome di una definizione di registro EIM (Enterprise Identity Mapping) Il registro di destinazione deve contenere l'identità utente di destinazione con cui devono essere messe in corrispondenza tutte le identità utente nel registro di origine.
- **Utente di destinazione**. L'utente di destinazione è il nome dell'identità utente restituita come la destinazione di un'operazione di ricerca di corrispondenze EIM basata su quest'associazione normativa.

È possibile definire più di un'associazione normativa del registro predefinito. Se due o più associazioni normativa con lo stesso registro origine fanno riferimento allo stesso registro di destinazione, è necessario definire informazioni di ricerca univoche per ognuna di queste associazioni normativa per garantire che le operazioni di ricerca corrispondenze possano distinguere tra esse. In caso contrario, le operazioni di ricerca delle corrispondenze possono restituire più identità utente di destinazione. Come conseguenza di questi risultati ambigui, le applicazioni che si basano su EIM potrebbero non essere in grado di stabilire l'esatta identità di destinazione da utilizzare.

Poiché è possibile utilizzare le associazioni normativa in diversi modi che si sovrappongono, è necessario avere una conoscenza approfondita del supporto normativa corrispondenza EIM e del modo in cui funzionano le operazioni di ricerca prima di creare ed utilizzare delle associazioni normativa.

Nota: è possibile creare un'associazione di normativa registro predefinita, con un'identità utente di destinazione che esiste all'interno di una definizione del registro di gruppo. Tutti gli utenti nel registro utente di origine rappresentano l'origine dell'associazione normativa e vengono messi in corrispondenza con un'identità utente di destinazione in una definizione del registro di gruppo di destinazione. L'identità dell'utente definita nell'associazione della normativa di registro predefinita esiste all'interno dei membri della definizione del registro di gruppo.

Ad esempio, John Day usa lo stesso profilo utente i5/OS, John_Day, su cinque sistemi differenti: System_B, System_C, System_D, System_E e System_F. Per ridurre la quantità di lavoro che tale utente deve eseguire per configurare la corrispondenza EIM, l'amministratore EIM crea una definizione del registro di gruppo denominata Group_1. I membri della definizione del registro di gruppo includono i nomi di definizione del registro di System_B, System_C, System_D, System_E e System_F. Il raggruppamento dei membri consente all'amministratore di creare una singola associazione di destinazione alla definizione del registro di gruppo e all'identità dell'utente, anziché più associazioni alle singole definizioni del registro.

L'amministratore EIM crea un'associazione normativa registro predefinita con un registro origine my_realm.com, che sono principal in uno specifico dominio Kerberos. Per questa associazione normativa, egli specifica un'identità utente di destinazione, John_Day, nel registro di destinazione Group_1. In questo caso, non viene applicata nessun'altra associazione di identificativo né di normativa. Perciò, quando viene specificato Group_1 come registro di destinazione e my_realm.com come registro di origine in operazioni di ricerca, l'associazione normativa di registro predefinita

assicura che l'identità utente di destinazione `John_Day` venga restituita per tutte le identità utente in `my_realm.com` per cui non è stata definita alcuna associazione di identificativi specifica.

Concetti correlati

"Ricerca delle informazioni" a pagina 16
Con EIM (Enterprise Identity Mapping) è possibile fornire dati facoltativi detti informazioni di ricerca per identificare ulteriormente un'identità utente. Questa identità utente di destinazione può essere specificata in un'associazione identificativi o in un'associazione di normative.

"Abilitazione e supporto normativa corrispondenze EIM" a pagina 38
Il supporto normativa corrispondenze EIM (Enterprise Identity Mapping) consente di utilizzare le associazioni normativa ed anche delle specifiche associazioni di identificativi in un dominio EIM. È possibile utilizzare le associazioni normativa invece di, oppure insieme ad, associazioni di identificativi.

Associazioni normativa filtro certificato:

Un'associazione normativa filtro certificato è un tipo di associazione normativa che è possibile utilizzare per creare corrispondenze molti-ad-uno tra identità utente. È possibile utilizzare un'associazione normativa filtro certificato per mettere in corrispondenza una serie di certificati origine con una singola identità utente di destinazione nel registro utenti di destinazione specificato.

In un'associazione normativa filtro certificato, è necessario specificare una serie di certificati in un singolo registro X.509 come origine dell'associazione normativa. Questi certificati vengono messi in corrispondenza con un singolo registro di destinazione e con un utente di destinazione specificati. A differenza di un'associazione normativa registro predefinita in cui tutti gli utenti in un singolo registro rappresentano l'origine dell'associazione normativa, l'ambito di un'associazione normativa filtro certificato è più flessibile. È possibile specificare una sottoserie di certificati nel registro come origine. Il filtro certificato che si specifica per l'associazione normativa è quello che determina il relativo ambito.

Nota: creare e utilizzare un'associazione normativa del registro predefinito quando si desidera mettere in corrispondenza tutti i certificati contenuti in un registro utenti X.509 con una singola identità utente di destinazione.

Per utilizzare associazioni normativa filtro certificato, è necessario abilitare ricerche di corrispondenze tramite associazioni normativa per il dominio. È necessario anche abilitare ricerche di corrispondenze per il registro di origine e abilitare ricerche di corrispondenze e l'uso di associazioni normativa per il registro utenti di destinazione dell'associazione normativa. Quando si configura quest'abilitazione, i registri utenti nell'associazione normativa possono partecipare alle operazioni di ricerca corrispondenze.

Quando un certificato digitale è l'identità utente di origine in un'operazione di ricerca corrispondenze EIM (dopo che l'applicazione richiedente utilizza la API EIM `eimFormatUserIdentity()` per formattare il nome dell'identità utente), EIM controlla innanzitutto se esiste un'associazione identificativo tra un identificativo EIM e l'identità utente specificata. Se non esiste, EIM confronta le informazioni sul DN nel certificato con quelle sul DN, intero o parziale, specificate nel filtro per l'associazione normativa. Se le informazioni sul DN nel certificato soddisfano i criteri del filtro, EIM restituisce l'identità dell'utente di destinazione specificata dall'associazione normativa. Il risultato è che i certificati nel registro X.509 di origine che soddisfano i criteri di filtro certificato vengono associati alla singola identità utente di destinazione, come specificato dall'associazione normativa filtro certificato.

Si crea, ad esempio, un'associazione normativa filtro certificato che ha un registro di origine di `certificates.x509`. Questo registro contiene i certificati per tutti gli impiegati della società, compresi quelli che tutti i responsabili nel reparto di gestione del personale utilizzano per accedere a determinate pagine Web interne private e ad altre risorse cui accedono tramite un modello System i. Per quest'associazione normativa, si specifica anche un'identità utente di destinazione di `hr_managers` (responsabili della gestione del personale) nel registro di destinazione `system_abc` che è un profilo utente specifico in un registro utenti i5/OS. Per assicurare che solo i certificati che appartengono ai responsabili

della gestione del personale vengano coperti da quest'associazione normativa, specificare un filtro certificato con un SDN (subject distinguished name - DN soggetto) di `ou=hrmgr,o=myco.com,c=us`.

In questo caso, non si sono create associazioni di identificativi o altre associazioni normativa filtro certificato valide per le identità utente nel registro di origine. Pertanto, quando viene specificato `system_abc` come registro di destinazione e viene specificato `certificates.x509` come registro di origine nelle operazioni di ricerca, l'associazione normativa filtro certificato assicura che l'identità utente di destinazione `hr_managers` sia restituita per tutti i certificati nel registro `certificates.x509` che corrispondono al filtro certificato specificato e per cui non sono state definite delle specifiche associazioni di identificativi.

Specificare le seguenti informazioni per definire un'associazione normativa filtro certificato:

- **Registro di origine**. La definizione di registro di origine che si specifica deve essere un registro utenti di tipo X.509. La normativa filtro certificato crea un'associazione tra le identità utente in questo registro utente X.509 e una singola identità utente di destinazione specifica. L'associazione si applica solo alle identità utente nel registro che corrispondono ai criteri di filtro del certificato specificati per questa normativa.
- **Filtro certificato**. Un filtro del certificato definisce una serie di attributi del certificato utente simili. L'associazione normativa filtro certificato mette in corrispondenza i certificati con questi attributi definiti nel registro utente X.509 con un'identità utente di destinazione specifica. Il filtro viene specificato in base a una combinazione di SDN (subject distinguished name - DN soggetto) e IDN (issuer distinguished name - DN emittente) che corrisponde ai certificati che si desidera utilizzare come origine della corrispondenza. Il filtro certificato specificato per la normativa deve già esistere nel dominio EIM.
- **Registro di destinazione**. La definizione del registro di destinazione che si specifica è il registro utenti che contiene l'identità utente alla quale si desidera mettere in corrispondenza i certificati che corrispondono al filtro del certificato.
- **Utente di destinazione**r. L'utente di destinazione corrisponde al nome dell'identità utente restituita come destinazione di un'operazione di ricerca delle corrispondenze EIM in base a questa associazione normativa

Poiché è possibile utilizzare le associazioni normativa certificato ed altre associazioni in diversi modi che si sovrappongono, sarebbe necessaria una conoscenza approfondita sia del supporto normativa corrispondenze EIM che del modo in cui funzionano le operazioni di ricerca prima di creare ed utilizzare delle associazioni normativa certificato.

Nota: è possibile creare un'associazione di normativa filtro del certificato, con un'identità utente di destinazione che esiste all'interno di una definizione del registro di gruppo. Gli utenti nel registro di origine che corrispondono ai criteri specificati dal filtro certificato rappresentano l'origine dell'associazione normativa e vengono messi in corrispondenza con un'identità utente di destinazione in una definizione del registro di gruppo di destinazione. L'identità dell'utente definita nell'associazione della normativa filtro del certificato esiste all'interno dei membri della definizione del registro di gruppo.

Ad esempio, John Day usa lo stesso profilo utente i5/OS, `John_Day`, su cinque sistemi differenti: Sistema B, Sistema C, Sistema D, Sistema E e Sistema F. Per ridurre la quantità di lavoro che tale utente deve eseguire per configurare la corrispondenza EIM, l'amministratore EIM crea una definizione del registro di gruppo. I membri di tale definizione includono i nomi definizione del registro di `System_B`, `System_C`, `System_D`, `System_E` e `System_F`. Il raggruppamento dei membri consente all'amministratore di creare una singola associazione di destinazione all'identità utente e alla definizione del registro di gruppo, anziché più associazioni alle singole definizioni del registro.

L'amministratore EIM crea un'associazione normativa filtro del certificato in cui definisce una sottoserie di certificati all'interno di un singolo registro X.509 come origine dell'associazione normativa. Egli specifica un'identità utente di destinazione, `John_Day`, nel registro di destinazione

`Group_1`. In questo caso, non viene applicata nessun'altra associazione specifica di identificativo né di normativa filtro del certificato. Il risultato è che, quando si specifica `Group_1` come registro di destinazione nelle operazioni di ricerca, tutti i certificati nel registro X.509 di origine che corrispondono ai criteri di filtro certificato vengono associati all'identità utente di destinazione specificata.

Filtri certificato:

Un filtro del certificato definisce una serie di attributi del certificato DN (distinguished name) simili per un gruppo di certificati utente in un registro utenti X.509 di origine. È possibile utilizzare il filtro certificato come base per un'associazione normativa filtro certificato.

Il filtro certificato in un'associazione normativa determina i certificati nel registro X.509 origine specificato da corrispondere all'utente di destinazione specificato. I certificati per cui le informazioni sul DN soggetto e sul DN emittente che soddisfano i criteri del filtro vengono messi in corrispondenza con l'utente di destinazione specificato durante le operazioni di ricerca della corrispondenza EIM.

Creare, ad esempio, un filtro certificato con un SDN (Subject Distinguished Name - DN soggetto) di `o=ibm,c=us`. Tutti i certificati con questi DN come parte delle loro informazioni SDN soddisfano i criteri del filtro, come ad esempio un certificato con un SDN di `cn=JohnDay,ou=LegalDept,o=ibm,c=us`. Se il certificato soddisfa i criteri di più di un filtro certificato, ha la precedenza il valore del filtro certificato più specifico cui corrisponde un certificato. Si ha ad esempio un filtro certificato con un SDN di `o=ibm,c=us` e si ha un altro filtro certificato con un SDN di `ou=LegalDept,o=ibm,c=us`. Se si ha un certificato nel registro X.509 di origine con un SDN di `cn=JohnDay,ou=LegalDept,o=ibm,c=us` viene quindi utilizzato il secondo, o più specifico, filtro certificato. Se si ha un certificato nel registro X.509 di origine con un SDN di `cn=SharonJones,o=ibm,c=us` viene quindi utilizzato il filtro certificato meno specifico perché il certificato corrisponde maggiormente ai suoi criteri.

È possibile specificare uno o entrambi i seguenti elementi per definire un filtro certificato:

- SDN (subject distinguished name - DN soggetto). Il DN completo o parziale che si specifica per il filtro deve corrispondere alla parte relativa all'SDN (DN soggetto) del certificato digitale, che definisce il proprietario del certificato. È possibile fornire la stringa SDN (DN soggetto) completa oppure fornire uno o più DN parziali che potrebbero costituire l'SDN completo.
- IDN (issuer distinguished name - DN emittente). Il DN completo o parziale che si specifica per il filtro deve corrispondere alla parte relativa all'IDN (DN emittente) del certificato digitale, che definisce l'autorità di certificazione che ha rilasciato il certificato. È possibile fornire la stringa IDN (DN emittente) completa oppure è possibile fornire uno o più DN parziali che potrebbero costituire l'IDN completo.

Ci sono vari metodi che è possibile utilizzare per creare un filtro certificato, compreso l'utilizzo della API di formattazione del filtro di normativa EIM (eimFormatPolicyFilter) per generare dei filtri certificato utilizzando un certificato come un modello per creare i DN necessari nell'ordine e nel formato corretti per l'SDN e l'IDN.

Concetti correlati

"DN (distinguished name)" a pagina 48
Un DN (distinguished name) è una voce LDAP che identifica in modo univoco e descrive una voce in un server (LDAP) di indirizzario. È possibile utilizzare il wizard di configurazione di EIM per configurare il server di indirizzario per memorizzare le informazioni sul dominio EIM. Poiché EIM utilizza il server di indirizzario per memorizzare i dati EIM, è possibile utilizzare i DN come mezzo di autenticazione nell'unità di controllo del dominio EIM.

Informazioni correlate

API di formattazione del filtro di normativa EIM (eimFormatPolicyFilter)

Operazioni di ricerca EIM

Un'applicazione o un sistema operativo utilizza un'API EIM per eseguire un'operazione di ricerca in modo che l'applicazione o il sistema operativo possa eseguire la corrispondenza da un'identità utente in un registro ad un'altra identità utente in un altro registro. Un'operazione di ricerca EIM è un processo attraverso il quale un'applicazione o un sistema operativo rileva un'identità utente associata sconosciuta in uno specifico registro di destinazione, fornendo alcune informazioni note e affidabili.

Le applicazioni che utilizzano le API EIM possono eseguire queste operazioni di ricerca EIM sulle informazioni, solo se quelle vengono memorizzate nel dominio EIM. Un'applicazione può eseguire uno di due tipi di operazioni di ricerca EIM in base al tipo di informazioni fornito dall'applicazione come origine dell'operazione di ricerca EIM: un'identità utente o un identificativo EIM.

Quando le applicazioni o i sistemi operativi utilizzano la API `eimGetTargetFromSource()` per ottenere un'identità utente di destinazione per uno specifico registro di destinazione, essi devono fornire un'*identità utente come origine* dell'operazione di ricerca. Perché venga utilizzata come origine in un'operazione di ricerca EIM, un'identità utente deve avere un'associazione origine identificativi definita per essa o deve essere coperta da un'associazione normativa. Quando un'applicazione o un sistema operativo utilizza questa API, l'applicazione o il sistema operativo deve fornire tre elementi informativi:

- Un'identità utente come origine oppure un punto di inizio dell'operazione.
- Il nome della definizione del registro EIM per l'identità utente origine.
- Il nome della definizione del registro EIM che è la destinazione dell'operazione di ricerca EIM. Questa definizione del registro descrive il registro utente contenente l'identità utente ricercata dall'applicazione.

Quando le applicazioni o i sistemi operativi utilizzano la API `eimGetTargetFromIdentifier()` per ottenere un'identità utente per un determinato registro di destinazione, essi devono fornire un *identificativo EIM come origine* dell'operazione di ricerca EIM. Quando un'applicazione utilizza questa API, l'applicazione deve fornire due informazioni:

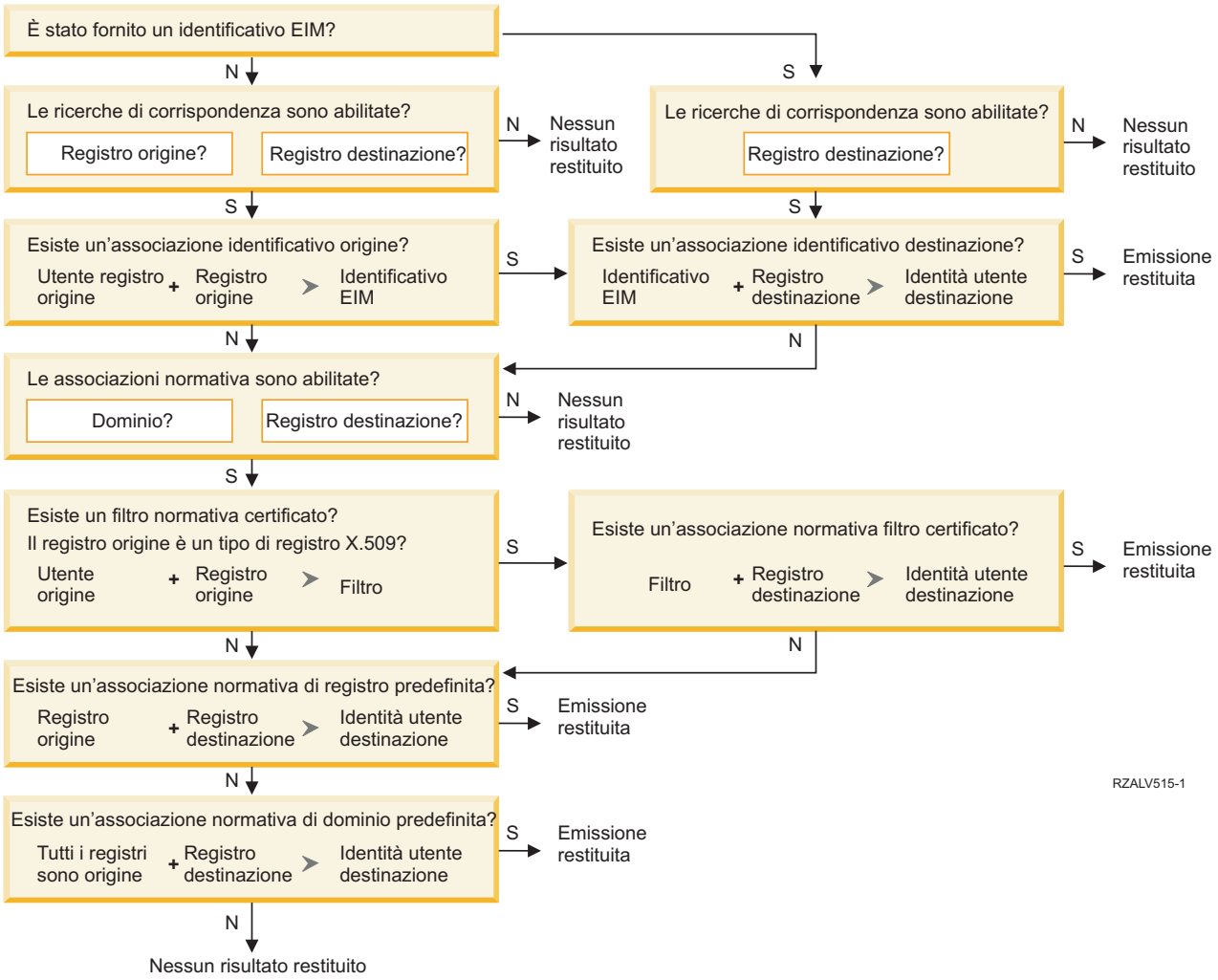
- Un identificativo EIM come origine oppure un punto di inizio dell'operazione.
- Il nome della definizione del registro EIM che è la destinazione dell'operazione di ricerca EIM. Questa definizione del registro descrive il registro utente contenente l'identità utente ricercata dall'applicazione.

Affinché un'identità utente venga restituita come destinazione di ciascun tipo di operazione di ricerca EIM, l'identità utente deve disporre di un'associazione di destinazione definita. Questa associazione di destinazione può avere il formato di un'associazione identificativo o di una associazione normativa.

Le informazioni fornite vengono passate a EIM e l'operazione di ricerca EIM ricerca e restituisce le eventuali identità utente di destinazione, ricercando i dati EIM nel seguente ordine, come illustra la Figura 10:

1. L'associazione di destinazione identificativi per un identificativo EIM. L'identificativo EIM viene identificato in uno di questi due modi: Esso viene fornito dall'API `eimGetTargetFromIdentifier()`. Oppure, l'identificativo EIM è determinato dalle informazioni fornite dall'API `eimGetTargetFromSource()`.
2. Associazione normativa filtro certificato.
3. Associazione normativa registro predefinita.
4. Associazione normativa dominio predefinita.

Figura 10: diagramma di flusso dell'elaborazione generale delle operazioni di ricerca EIM



Nota: nel seguente diagramma di flusso, le operazioni di ricerca esaminano la singola definizione di registro, al esempio il registro di origine o di destinazione specificato. Se le operazioni di ricerca non trovano una corrispondenza utilizzando la singola definizione di registro, viene determinato se la singola definizione di registro è un membro di una definizione di registro del gruppo. Se è membro di una definizione di registro del gruppo, l'operazione di controllo esamina tale definizione per soddisfare la richiesta di ricerca corrispondenza.

L'operazione di ricerca si svolge in questo modo:

1. L'operazione di ricerca controlla se sono abilitate le ricerche di corrispondenze. L'operazione di ricerca determina se le ricerche di corrispondenze sono abilitate per il registro origine specificato, per il registro di destinazione specificato oppure per entrambi i registri specificati. Se le ricerche di corrispondenze non sono abilitate per uno o entrambi i registri, l'operazione di ricerca termina senza restituire un'identità utente di destinazione.
2. L'operazione di ricerca controlla se vi sono associazioni di identificativi che corrispondono ai criteri di ricerca. Se era stato fornito un identificativo EIM, l'operazione di ricerca utilizza il nome di identificativo EIM specificato. Altrimenti, l'operazione di ricerca controlla se vi è una specifica associazione origine identificativi specifica che corrisponda all'identità utente origine e al registro origine forniti. Se esiste, l'operazione di ricerca la utilizza per determinare il nome identificativo EIM appropriato. L'operazione di ricerca utilizza quindi il nome identificativo EIM per ricercare un'associazione di destinazione identificativo per l'identificativo EIM che corrisponda al nome di

definizione di registro EIM di destinazione specificato. Se vi è un'associazione di destinazione identificativi che corrisponde, l'operazione di ricerca restituisce l'identità utente di destinazione definita nell'associazione di destinazione.

3. L'operazione di ricerca controlla se l'uso delle associazioni normativa è abilitato. L'operazione di ricerca controlla se il dominio è abilitato a consentire le ricerche di corrispondenze utilizzando le associazioni normativa. L'operazione di ricerca controlla inoltre se il registro di destinazione è abilitato ad utilizzare associazioni normativa. Se il dominio non è abilitato per le associazioni normativa o se il registro non è abilitato per le associazioni normativa, l'operazione di ricerca termina senza restituire un'identità utente di destinazione.
4. L'operazione di ricerca controlla se sono presenti associazioni normativa filtro certificato. L'operazione di ricerca controlla se il registro origine è un tipo di registro X.509. Se è un tipo di registro X.509, l'operazione di ricerca controlla se vi è un'associazione normativa filtro certificato che corrisponde ai nomi definizione registro di origine e di destinazione. L'operazione di ricerca controlla se ci sono certificati nel registro X.509 origine che soddisfano i criteri specificati nell'associazione normativa filtro certificato. Se c'è un'associazione normativa corrispondente e ci sono dei certificati che soddisfano i criteri di filtro certificato, l'operazione di ricerca restituisce l'identità utente di destinazione appropriata per detta associazione normativa.
5. L'operazione di ricerca controlla se vi sono associazioni normativa di registro predefinite.L'operazione di ricerca controlla se c'è un'associazione normativa di registro predefinita che corrisponde ai nomi di definizione di registro origine e di destinazione. Se c'è un'associazione normativa corrispondente, l'operazione di ricerca restituisce l'identità utente di destinazione appropriata per detta associazione normativa.
6. L'operazione di ricerca controlla le associazioni normativa di dominio predefinite.L'operazione di ricerca controlla se c'è un'associazione normativa di dominio predefinita definita per la definizione di registro di destinazione. Se vi è un'associazione normativa corrispondente, l'operazione di ricerca restituisce l'identità utente di destinazione associata per detta associazione normativa.
7. L'operazione di ricerca non è in grado di restituire alcun risultato.

Per ulteriori informazioni sulle operazioni di ricerca EIM, esaminare i seguenti esempi:

Concetti correlati

"Dominio EIM" a pagina 6
Un dominio EIM (Enterprise Identity Mapping) è un indirizzario presente nel server LPDA (Lightweight Directory Access Protocol) che contiene i dati EIM di una società.

"Associazioni normativa" a pagina 21
La normativa di corrispondenze di EIM (Enterprise Identity Mapping) consente ad un amministratore EIM di creare ed utilizzare delle associazioni normativa per definire una relazione tra più identità utente in uno o più registri utenti ed una singola identità utente in un altro registro utenti.

"Unità di controllo del dominio EIM" a pagina 6
Un'unità di controllo dominio EIM è un server LPDA (Lightweight Directory Access Protocol) configurato per gestire uno o più domini EIM Un dominio EIM è composto di tutti gli identificativi EIM, le associazioni EIM e i registri utenti definiti in tale dominio. I sistemi (client EIM) prendono parte al dominio EIM utilizzando i dati del dominio per le operazioni di ricerca EIM.

"Ricerca delle informazioni" a pagina 16
Con EIM (Enterprise Identity Mapping) è possibile fornire dati facoltativi detti informazioni di ricerca per identificare ulteriormente un'identità utente. Questa identità utente di destinazione può essere specificata in un'associazione identificativi o in un'associazione di normative.

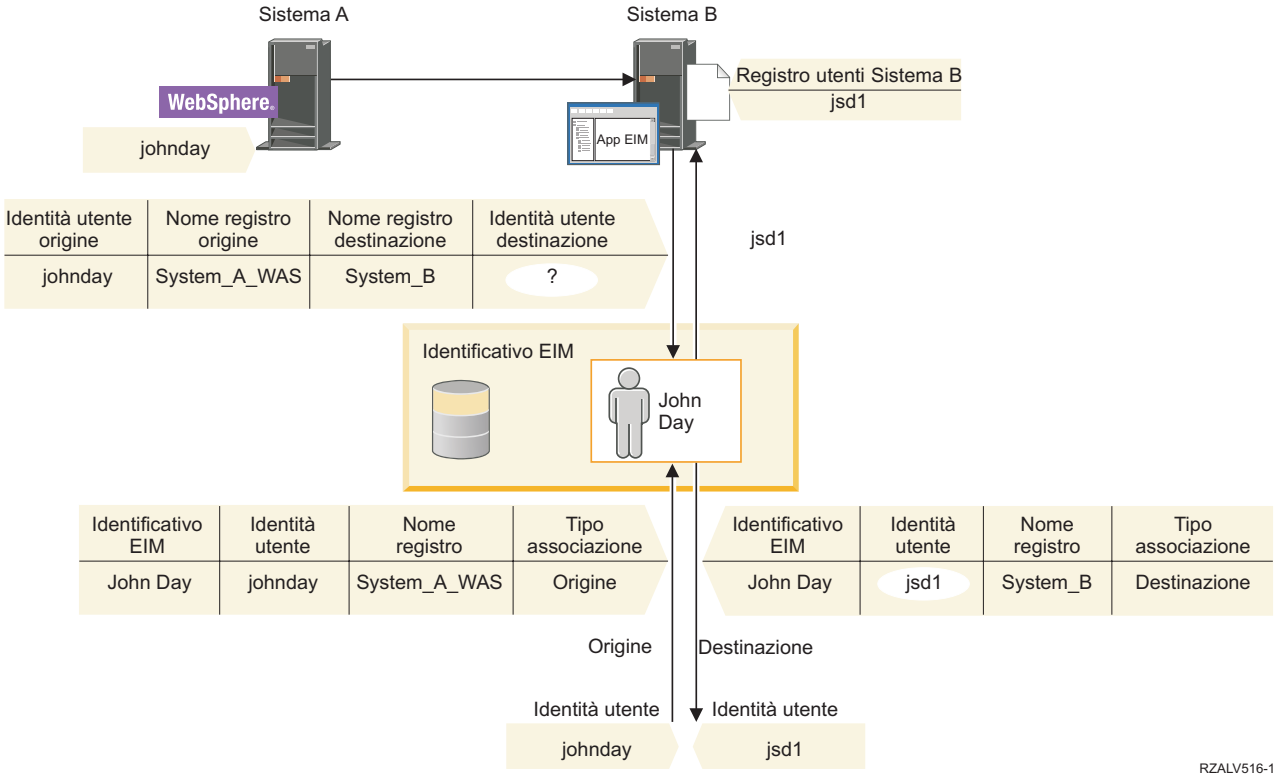
Esempi di operazioni di ricerca: Esempio 1

Utilizzare questo esempio per apprendere le modalità di funzionamento del flusso di lavoro per un'operazione di ricerca che restituisce un'identità utente di destinazione da associazioni identificativo specifiche basate sull'identità utente nota.

Nella Figura 11, l'identità utente `johnday` viene autenticata su WebSphere Application Server tramite LPTA (Lightweight Third-Party Authentication) sul Sistema A. WebSphere Application Server sul Sistema

A richiama un programma integrato sul Sistema B per accedere ai dati sul Sistema B. Il programma integrato utilizza un'API EIM per eseguire un'operazione di ricerca EIM basata sull'identità utente sul Sistema A come origine dell'operazione. L'applicazione fornisce le seguenti informazioni per eseguire l'operazione: `johnday` come identità utente di origine, `System_A_WAS` come nome della definizione del registro EIM di origine e `System_B` come nome della definizione del registro EIM di destinazione. Queste informazioni di origine vengono inoltrate a EIM e l'operazione di ricerca EIM trova un'associazione origine identificativi che corrisponde alle informazioni. Utilizzando il nome identificativo EIM `John Day`, l'operazione di ricerca EIM ricerca un'associazione di destinazione identificativi per quest'identificativo che corrisponda al nome di definizione di registro EIM per `System_B`. Una volta rilevata l'associazione di destinazione corrispondente, l'operazione di ricerca EIM restituisce l'identità utente `jsd1` all'applicazione.

Figura 11: l'operazione di ricerca EIM restituisce un'identità utente di destinazione da associazioni di identificativi specifiche sulla base dell'identità utente conosciuta `johnday`



Esempi di operazioni di ricerca: Esempio 2

Utilizzare questo esempio per apprendere le modalità di funzionamento del flusso di lavoro per un'operazione di ricerca che restituisce un'identità utente di destinazione da associazioni identificativo specifiche basate sul principal Kerberos noto.

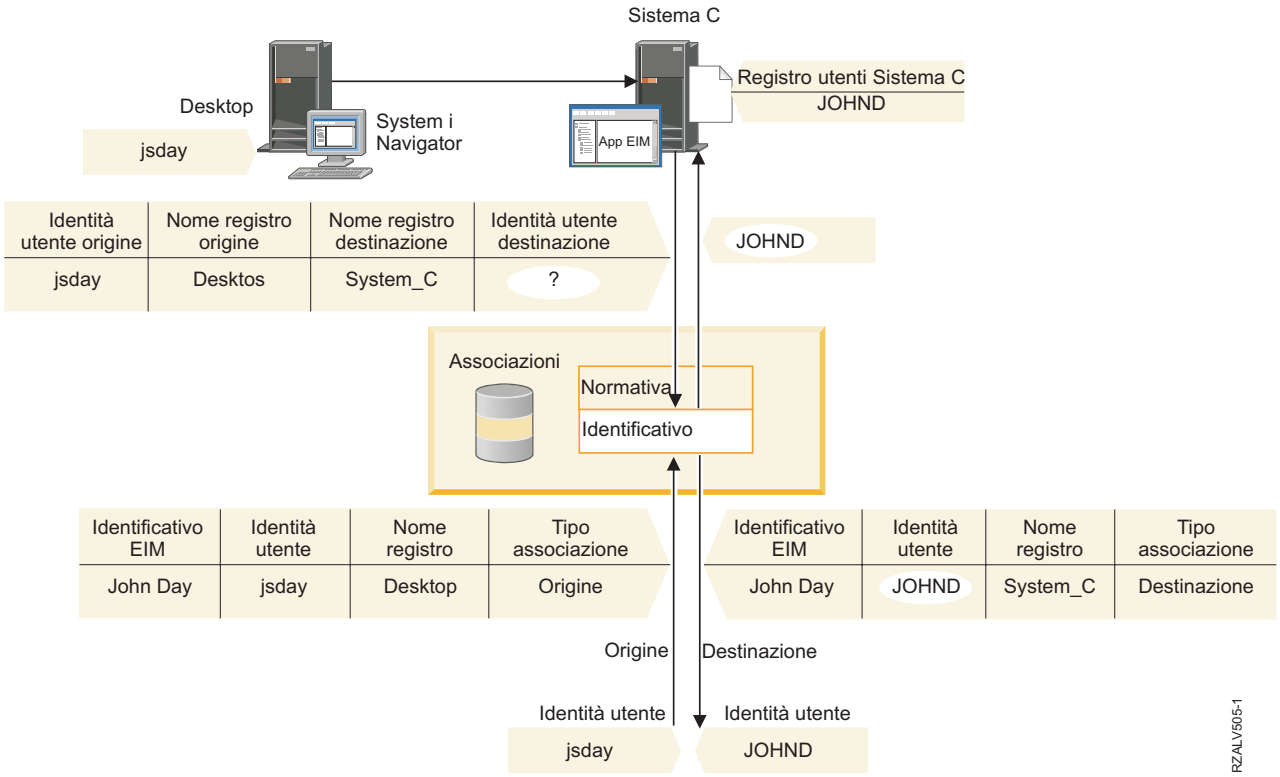
Nella Figura 12, un amministratore desidera mettere in corrispondenza un utente Windows in un registro Windows Active Directory con un profilo utente i5/OS. Kerberos è il metodo di autenticazione utilizzato da Windows ed il nome del registro Windows Active Directory come definito dall'amministratore in EIM è `Desktop`. L'identità utente che l'amministratore da cui l'amministratore desidera eseguire la messa in corrispondenza è un principal Kerberos denominato `jsday`. Il nome del registro i5/OS come definito dall'amministratore in EIM è `System_C` e l'identità utente con cui l'amministratore desidera eseguire la corrispondenza è il profilo utente denominato `JOHND`.

L'amministratore crea un identificativo EIM denominato `John Day`. Quindi aggiunge due associazioni a questo identificativo EIM:

- Un'associazione origine per il principal Kerberos denominato `jsday` nel registro `Desktop`.

- Un'associazione di destinazione per il profilo utente i5/OS denominato JOHND nel registro System_C.

Figura 12: l'operazione di ricerca EIM restituisce un'identità utente di destinazione da associazioni di identificativi specifiche sulla base del principal Kerberos noto jsday



Questa configurazione consente ad un'operazione di ricerca di corrispondenze di eseguire la messa in corrispondenza dal principal Kerberos al profilo utente i5/OS nel seguente modo:

Identità utente e registro origine	**--->**	**Identificativo EIM**	**--->**	**Identità utente di destinazione**
jsday nel registro Desktop	--->	John Day	--->	JOHND (nel registro System_C)

L'operazione di ricerca si svolge in questo modo:

1. L'utente jsday accede a, ed esegue l'autenticazione su, Windows tramite il suo principal Kerberos nel registro Windows Active Directory Desktop.
2. L'utente apre System i Navigator per accedere ai dati su System_C.
3. i5/OS utilizza una API EIM per eseguire un'operazione di ricerca EIM con un'identità utente origine di jsday, un registro origine Desktop ed un registro di destinazione di System_C.
4. L'operazione di ricerca EIM controlla se le ricerche di corrispondenze sono abilitate per il registro origine Desktop ed il registro di destinazione System_C. Lo sono.
5. L'operazione di ricerca controlla la presenza di una specifica associazione origine identificativi corrispondente all'identità utente origine fornita jsday in un registro origine Desktop.
6. L'operazione di ricerca utilizza l'associazione origine identificativi corrispondente per determinare il nome identificativo EIM appropriato, che è John Day.

7. L'operazione di ricerca utilizza questo nome identificativo EIM per ricercare un'associazione di destinazione identificativi per l'identificativo EIM che corrisponde al nome di definizione di registro EIM di destinazione System_C.
8. Esiste tale associazione di destinazione identificativi e l'operazione di ricerca restituisce l'identità utente di destinazione JOHND, come definita nell'associazione di destinazione.
9. Dopo che è stata completata l'operazione di ricerca di corrispondenze, System i Navigator inizia l'esecuzione sotto il profilo utente JOHND. L'autorizzazione dell'utente ad accedere alle risorse ed eseguire le azioni in System i Navigator è determinata dall'autorizzazione definita per il profilo utente JOHND piuttosto che da quella definita per l'identità utente jsday.

Esempi di operazioni di ricerca: Esempio 3

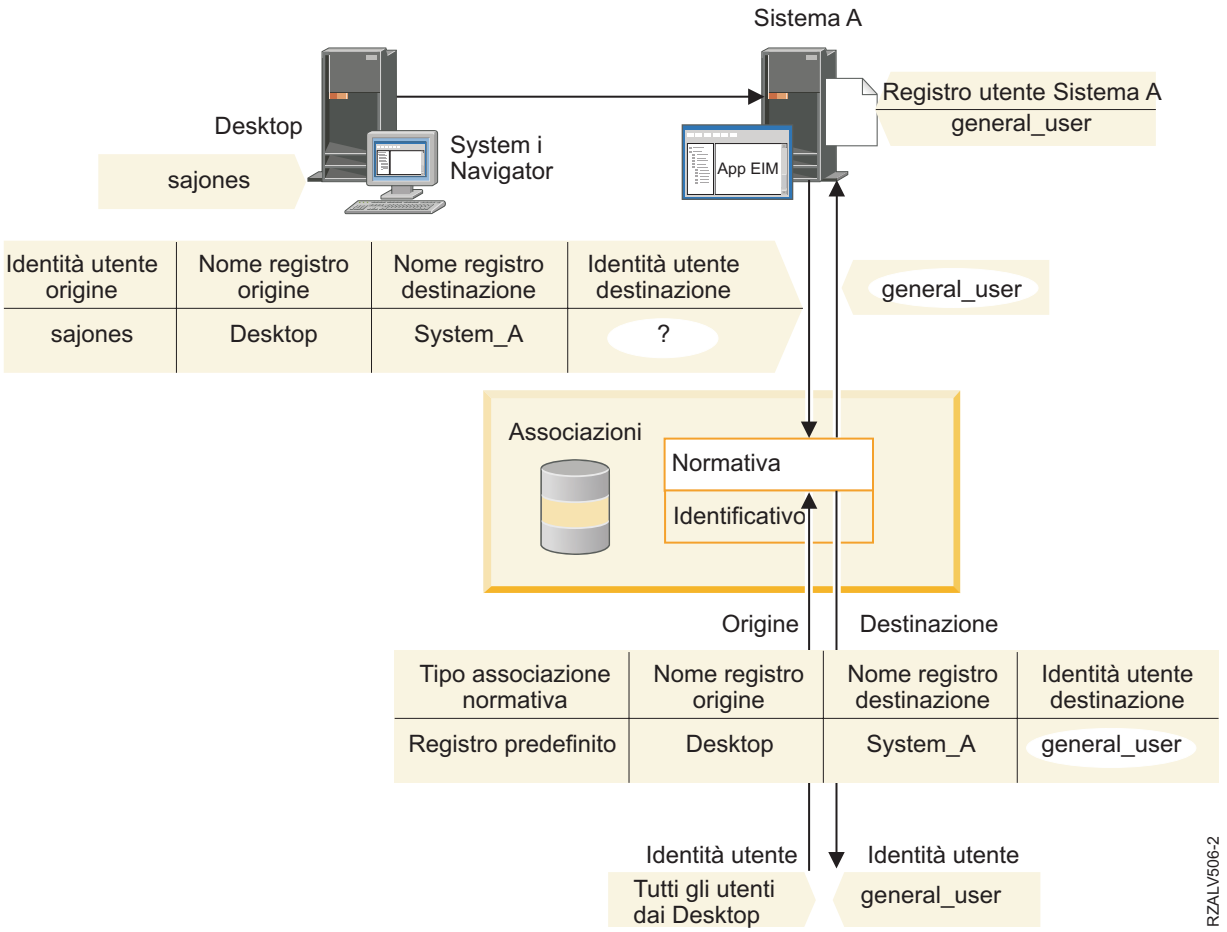
Utilizzare questo esempio per apprendere le modalità di funzionamento del flusso di lavoro per un'operazione di ricerca che restituisce un'identità utente di destinazione da un'associazione normativa di registro predefinita.

Nella Figura 13, un amministratore desidera mettere in corrispondenza tutti gli utenti di stazione di lavoro desktop nel registro Windows Active Directory ad un singolo profilo utente i5/OS denominato general_user in un registro i5/OS denominato System_A in EIM. Kerberos è il metodo di autenticazione utilizzato da Windows ed il nome del registro Windows Active Directory come definito dall'amministratore in EIM è Desktop. Una delle identità utente da cui l'amministratore desidera eseguire la messa in corrispondenza è un principal Kerberos denominato sajones.

L'amministratore crea un'associazione normativa registro predefinita con le seguenti informazioni:

- Un registro origine Desktop.
- Un registro di destinazione System_A.
- Un'identità utente destinazione general_user.

Figura 13: un'operazione di ricerca restituisce un'identità utente di destinazione da un'associazione normativa di registro predefinita.



Questa configurazione consente ad un'operazione di ricerca di corrispondenze di mettere in corrispondenza tutti i principal Kerberos nel registro `Desktop`, compreso il principal `sajones`, al profilo utente i5/OS denominato `general_user` nel seguente modo:

Identità utente e registro origine	**--->**	**Associazione normativa registro predefinita**	**--->**	**Identità utente di destinazione**
`sajones` nel registro `Desktop`	--->	Associazione normativa registro predefinita	--->	`general_user` (nel registro `System_A`)

L'operazione di ricerca si svolge in questo modo:

1. L'utente `sajones` si collega ed esegue l'autenticazione sul desktop Windows tramite il suo principal Kerberos nel registro `Desktop`.
2. L'utente apre System i Navigator per accedere ai dati su System A.
3. i5/OS utilizza una API EIM per eseguire un'operazione di ricerca EIM con un'identità utente origine di `sajones`, un registro origine di `Desktop` ed un registro di destinazione di `System_A`.
4. L'operazione di ricerca EIM controlla se le ricerche di corrispondenze sono abilitate per il registro origine `Desktop` ed il registro di destinazione `System_A`. Lo sono.
5. L'operazione di ricerca controlla la presenza di una specifica associazione origine identificativi corrispondente all'identità utente origine fornita `sajones` in un registro origine `Desktop`. Non trova un'associazione identificativo corrispondente.

6. L'operazione di ricerca controlla inoltre se il dominio è abilitato ad utilizzare associazioni normativa. Lo è.
7. L'operazione di ricerca controlla se il registro di destinazione (System_A) è abilitato ad utilizzare associazioni normativa. Lo è.
8. L'operazione di ricerca controlla se il registro origine (Desktop) è un registro X.509. Non lo è.
9. L'operazione di ricerca controlla se vi è un'associazione normativa di registro predefinita che corrisponda al nome di definizione di registro origine (Desktop) e al nome di definizione di registro di destinazione (System_A).
10. L'operazione di ricerca determina che ne esiste una e restituisce general_user come identità utente destinazione.

A volte un'operazione di ricerca EIM restituisce dei risultati ambigui. Questo può succedere, ad esempio, quando più di un'identità utente di destinazione corrisponde ai criteri dell'operazione di ricerca specificati. Alcune applicazioni abilitate a EIM, comprese le applicazioni ed i prodotti i5/OS non sono progettati per gestire questi risultati ambigui e potrebbero avere esito negativo o dare risultati imprevisti. L'utente potrebbe dover intraprendere un'azione per risolvere questa situazione. Ad esempio, potrebbe essere necessario modificare la configurazione EIM o definire informazioni di ricerca per ogni identità utente di destinazione per impedire la corrispondenza di più identità utente di destinazione. È inoltre possibile verificare una corrispondenza per stabilire se le modifiche apportate funzionano come previsto.

Esempi di operazioni di ricerca: Esempio 4

Utilizzare questo esempio per apprendere le modalità di funzionamento del flusso di lavoro per un'operazione di ricerca che restituisce un'identità utente di destinazione in un registro utente che è un membro di una definizione del registro di gruppo.

Un amministratore desidera mettere in corrispondenza un utente Windows con un profilo utente i5/OS. Kerberos è il metodo di autenticazione utilizzato da Windows e il nome del registro Kerberos come è stato definito dall'amministratore in EIM è Desktop_A. L'identità utente con cui l'amministratore desidera eseguire la corrispondenza è un principale Kerberos denominato jday. Il nome della definizione di registro i5/OS come definito dall'amministratore in EIM è Group_1 e l'identità utente con cui l'amministratore desidera eseguire la corrispondenza è il profilo utente denominato JOHND presente in tre singoli registri: System_B, System_C e System_D. Ogni singolo registro è membro della definizione del registro di gruppo Group_1.

L'amministratore crea un identificativo EIM denominato John Day. Quindi aggiunge due associazioni a questo identificativo EIM:

- Un'associazione origine per il principal Kerberos denominata jday nel registro Desktop_A.
- Un'associazione di destinazione per il profilo utente i5/OS denominato JOHND nel registro Group_1 .

Questa configurazione consente ad un'operazione di ricerca di corrispondenze di eseguire la messa in corrispondenza dal principal Kerberos al profilo utente i5/OS nel seguente modo:

Identità utente e registro origine	**--->**	**Identificativo EIM**	**--->**	**Identità utente di destinazione**
jday nel registro Desktop_A	--->	John Day	--->	JOHND (nella definizione del registro di gruppo Group_1)

L'operazione di ricerca si svolge in questo modo:

1. L'utente (jday) si collega ed esegue l'autenticazione su Windows in Desktop_A.
2. L'utente apre System i Navigator per accedere ai dati su System_B.

3. i5/OS utilizza una API EIM per eseguire un'operazione di ricerca EIM con un'identità utente origine di `jday`, un registro origine di `Desktop` ed un registro di destinazione Desktop_A di System_B.
4. L'operazione di ricerca EIM controlla se le ricerche di corrispondenze sono abilitate per il registro origine (`Desktop_A`) e per il registro di destinazione (`System_B`).
5. L'operazione di ricerca verifica la presenza di una specifica associazione origine corrispondente all'identità utente di origine fornita `jday` in un registro origine `Desktop_A`.
6. L'operazione di ricerca utilizza l'associazione origine corrispondente per determinare il nome identificativo EIM appropriato, che è `John Day`.
7. L'operazione di ricerca utilizza questo nome identificativo EIM per ricercare una singola associazione di destinazione per l'identificativo EIM che corrisponde al nome di definizione registro EIM di destinazione specificato, `System_B` (Non ne è presente alcuna).
8. L'operazione di ricerca verifica se il registro di origine (`Desktop_A`) è un membro delle definizioni del registro di gruppo. (Non lo è).
9. L'operazione di ricerca verifica se il registro di destinazione (`System_B`) è un membro delle definizioni del registro di gruppo. È membro della definizione del registro di gruppo `Group_1`.
10. L'operazione di ricerca utilizza il nome identificativo EIM per ricercare una singola associazione di destinazione per l'identificativo EIM che corrisponde al nome di definizione di registro EIM di destinazione specificato, `Group_1`.
11. Esiste tale associazione di destinazione e l'operazione di ricerca restituisce l'identità utente di destinazione `JOHND`, come definita nell'associazione di destinazione.

Nota: in alcuni casi, l'operazione di ricerca EIM restituisce risultati ambigui quando più di un'identità utente di destinazione corrisponde ai criteri dell'operazione di ricerca specificati. Poiché EIM non può restituire una singola identità utente di destinazione, le applicazioni abilitate EIM, inclusi applicazioni e prodotti i5/OS, che non sono progettate per gestire questi risultati ambigui possono avere esito negativo o dare risultati imprevisti. L'utente potrebbe dover intraprendere un'azione per risolvere questa situazione. Ad esempio, potrebbe essere necessario modificare la configurazione EIM o definire informazioni di ricerca per ogni identità utente di destinazione per impedire la corrispondenza di più identità utente di destinazione. È possibile verificare una corrispondenza per stabilire se le modifiche apportate funzionano come previsto.

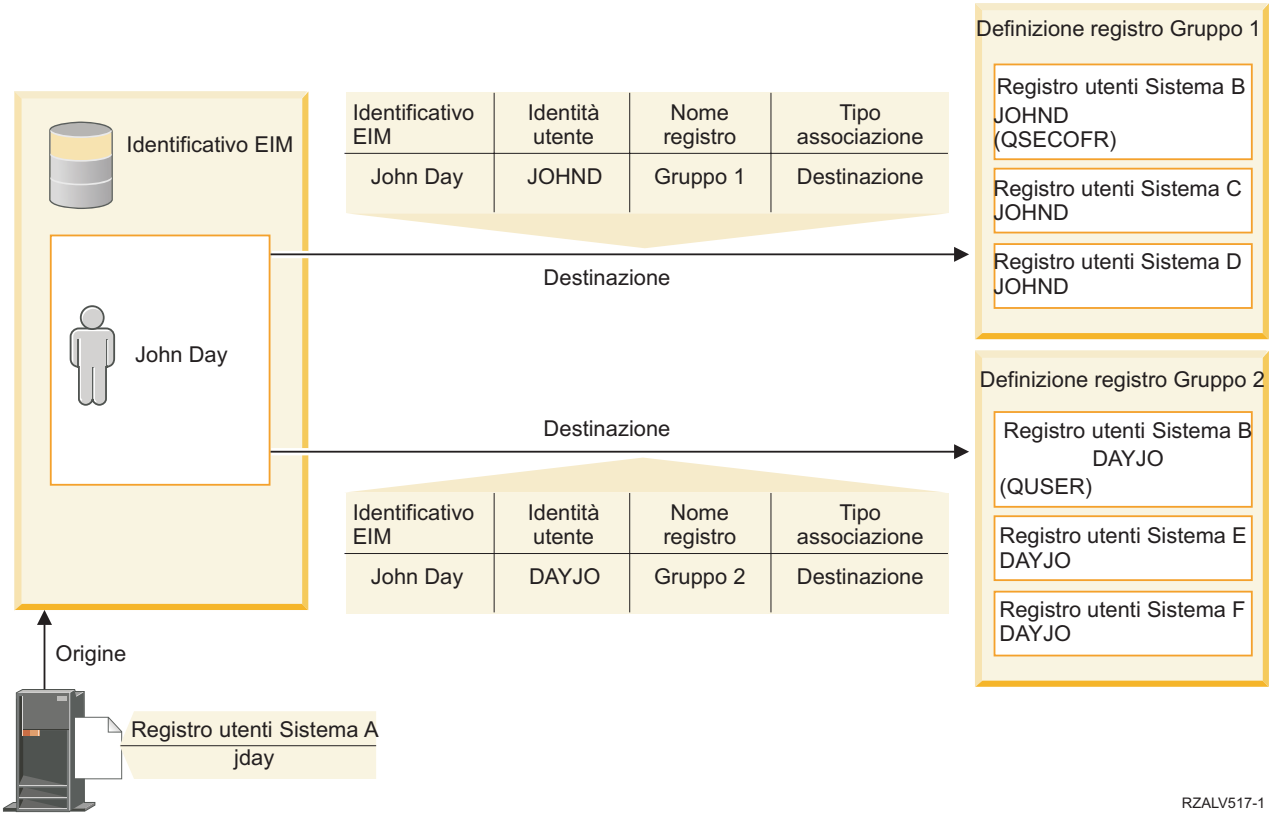
Esempi di operazioni di ricerca: Esempio 5

Utilizzare questo esempio per comprendere le operazioni di ricerca che restituiscono risultati ambigui che coinvolgono le definizioni del registro di gruppo.

In alcuni casi, l'operazione di ricerca corrispondenza restituisce risultati ambigui quando più di un'identità utente di destinazione corrisponde ai criteri di ricerca specificati. Dal momento che un'operazione con risultati ambigui può causare l'esito negativo delle applicazioni o dei risultati imprevisti, è necessario agire al fine di impedire o risolvere la situazione.

In particolare, tenere presente che le operazioni di ricerca possono restituire risultati ambigui quando si specifica una singola definizione del registro utente come membro di più definizioni del registro di gruppo. Se una singola definizione del registro utente è membro di più definizioni del registro di gruppo e si creano singole associazioni di normativa o di identificativo EIM che utilizzano una definizione del registro di gruppo come registro di origine o di destinazione, è possibile che le operazioni di ricerca restituiscano risultati ambigui. Ad esempio, è possibile utilizzare due identità utente differenti per eseguire due tipi diversi di attività di sistema: le attività che richiedono l'identità utente con autorizzazione QSECOFR possono essere eseguite come responsabile della sicurezza, mentre le attività che richiedono l'identità utente con autorizzazione QUSER possono essere eseguite come utente normale. Se entrambe le identità utente si trovano all'interno del singolo registro utente che è membro di due differenti definizioni del registro di gruppo e si creano associazioni identificativo di destinazione a entrambe le identità utente di destinazione, le operazioni di ricerca rilevano entrambe le identità utente di destinazione e, di conseguenza, restituiscono risultati ambigui.

Il seguente esempio descrive come potrebbe verificarsi questo problema quando si specifica un singolo registro utente come membro di due definizioni del registro di gruppo e si specifica una delle definizioni del registro di gruppo come registro di destinazione in due associazioni dell'identificativo EIM.



Esempio:

John Day presenta le seguenti identità utente all'interno di una definizione di registro del sistema denominata registro utente `System_B`:

- JOHND
- DAYJO

Il registro utente `System_B` è un membro delle seguenti definizioni del registro di gruppo:

- `Gruppo 1`
- `Gruppo 2`

L'identificativo EIM John Day presenta due associazioni di destinazione con le seguenti specifiche:

- Associazione di destinazione: il registro di destinazione è `Gruppo 1` che contiene l'identità utente `JOHND` nel registro utente `Sistema B`.
- Associazione di destinazione: il registro di destinazione è `Gruppo 2` che contiene l'identità utente `DAYJO` nel registro utente `Sistema B`.

In questa situazione, l'operazione di ricerca corrispondenza restituisce risultati ambigui perché più di un'identità utente di destinazione corrisponde ai criteri di ricerca specificati; entrambe le identità utente (`JOHND` e `DAYOJO`) corrispondono ai criteri di ricerca specificati.

In modo simile, è possibile che le operazioni di ricerca corrispondenza restituiscano risultati ambigui se si creano due associazioni normativa (anziché singole associazioni identificativo EIM) che utilizzano le definizioni del registro di gruppo come registri di destinazione.

Per impedire che le operazioni di ricerca restituiscano risultati ambigui che coinvolgono le definizioni del registro di gruppo, considerare le seguenti linee guida:

- Specificare un singolo registro utente come membro di un'unica definizione del registro di gruppo.
- Prestare attenzione nella creazione di singole associazioni identificativo EIM o le associazioni normativa che utilizzano le definizioni del registro di gruppo come registro di origine o di destinazione. Verificare che la definizione del registro di gruppo sia membro di un'unica definizione del registro di gruppo. Tenere presente che, se un membro della definizione del registro del gruppo di destinazione è anche membro di un'altra definizione del registro di gruppo, è possibile che le operazioni di ricerca restituisca risultati ambigui.
- In una situazione con risultati ambigui in cui si specifica una singola definizione di registro come membro di più definizioni del registro di gruppo e si crea una singola associazione di identificativo o di normativa che utilizza una di tali definizioni come registro di origine o di destinazione, è possibile definire informazioni univoche per ogni identità utente di destinazione in ogni associazione per rendere più approfondita la ricerca.

È possibile definire le seguenti informazioni di ricerca per ogni identità utente di destinazione nell'esempio relativo a John Day:

- Per `JOHND`: definire `Amministratore` come informazioni di ricerca
- Per `DAYJO`: definire `Utente` come informazioni di ricerca

Tuttavia, le applicazioni base i5/OS come System i Access per Windows non possono utilizzare le informazioni di ricerca per distinguere tra più identità utenti di destinazione restituite da un'operazione di ricerca. Di conseguenza, è possibile prendere in considerazione il ridefinire le associazioni per il dominio per assicurare che un'operazione di ricerca di corrispondenze possa restituire una singola identità utente di destinazione per assicurare che le applicazioni i5/OS di base possano eseguire correttamente le operazioni di ricerca e eseguire messe in corrispondenza di identità.

Concetti correlati

"Definizioni del registro di gruppo" a pagina 15
Il raggruppamento logico delle definizioni di registro consente di ridurre la quantità di lavoro che è necessario eseguire per configurare la corrispondenza EIM. È possibile gestire una definizione del registro di gruppo come se fosse una singola definizione del registro.

Abilitazione e supporto normativa corrispondenze EIM

Il supporto normativa corrispondenze EIM (Enterprise Identity Mapping) consente di utilizzare le associazioni normativa ed anche delle specifiche associazioni di identificativi in un dominio EIM. È possibile utilizzare le associazioni normativa invece di, oppure insieme ad, associazioni di identificativi.

Il supporto normativa corrispondenze EIM fornisce un mezzo per abilitare e disabilitare l'utilizzo delle associazioni normativa per l'intero dominio ed anche per ogni specifico registro utenti di destinazione. EIM inoltre consente di impostare la possibilità che un registro specifico participi alle operazioni di ricerca corrispondenze in generale. Di conseguenza, è possibile utilizzare il supporto normativa corrispondenze per controllare con maggior precisione la modalità di restituzione dei risultati da parte delle operazioni di ricerca.

L'impostazione predefinita per un dominio EIM è la disabilitazione per il dominio delle ricerche delle corrispondenze che utilizzano associazioni normativa. Quando l'utilizzo delle associazioni normativa è disabilitato per il dominio, tutte le operazioni di ricerca corrispondenze per il dominio restituiscono risultati solo utilizzando associazioni di identificativi specifiche tra identità utente ed identificativi EIM.

Le impostazioni predefinite per ogni singolo registro sono l'abilitazione della partecipazione alla ricerca corrispondenze e la disabilitazione dell'uso di associazioni normativa. Quando si abilita l'uso delle associazioni normativa per un singolo registro di destinazione, è necessario anche assicurare che questa impostazione sia abilitata per il dominio.

È possibile configurare la partecipazione alla ricerca corrispondenze e l'uso delle associazioni normativa per ogni registro in uno di questi tre modi:

- Le operazioni di ricerca delle corrispondenze non possono essere assolutamente utilizzate per il registro specificato. In altre parole, un'applicazione che esegue un'operazione di ricerca corrispondenza che coinvolge tale registro non riuscirà a restituire risultati.
- Operazioni di ricerca corrispondenze possono utilizzare associazioni di identificativi specifiche solo tra identità utente ed identificativi EIM. Le ricerche delle corrispondenze sono abilitate per il registro, ma l'uso delle associazioni normativa è disabilitato per lo stesso registro.
- Operazioni di ricerca corrispondenze possono utilizzare associazioni di identificativi specifiche quando esistono e associazioni normativa quando non esistono associazioni di identificativi specifiche (tutte le impostazioni sono abilitate).

Concetti correlati

"Ricerca delle informazioni" a pagina 16
Con EIM (Enterprise Identity Mapping) è possibile fornire dati facoltativi detti informazioni di ricerca per identificare ulteriormente un'identità utente. Questa identità utente di destinazione può essere specificata in un'associazione identificativi o in un'associazione di normative.

"Associazioni normative dominio predefinito" a pagina 21
Un'associazione normativa di dominio predefinita è un tipo di associazione normativa che è possibile utilizzare per creare corrispondenze molti-ad-uno tra identità utente.

"Associazioni normative registro predefinito" a pagina 23
Un'associazione normativa di registro predefinita è un tipo di associazione normativa che è possibile utilizzare per creare corrispondenze molti-ad-uno tra identità utente.

"Creazione di un'associazione normativa" a pagina 110
Un'associazione normativa fornisce un metodo per definire direttamente una relazione tra più identità utente in uno o più registri ed una singola identità utente di destinazione in un altro registro.

Attività correlate

"Abilitare le associazioni normativa per un dominio" a pagina 93
Un'associazione normativa consente di creare corrispondenze molte a una in situazioni in cui non esistono associazioni tra identità utente e un identificativo EIM.

"Abilitazione del supporto di ricerca corrispondenze e dell'uso di associazioni normativa per un registro destinazione" a pagina 102
Il supporto normativa di corrispondenza EIM (Enterprise Identity Mapping) permette di utilizzare le associazioni normativa come un mezzo per la creazione di corrispondenze di tipo 'molti a uno' in situazioni in cui non esistono associazioni tra delle identità utente e un identificativo EIM. È possibile utilizzare un'associazione normativa per mettere in corrispondenza una serie origine di più identità utente (piuttosto che una singola identità utente) con una singola identità utente di destinazione in un registro utenti di destinazione specificato.

Controllo di accesso EIM

Un utente EIM è un utente che possiede il controllo di accesso EIM in base all'appartenenza ad un gruppo utenti LDAP (Lightweight Directory Access Protocol) predefinito per uno specifico dominio.

La specifica del controllo accesso EIM per un utente aggiunge quell'utente ad uno specifico gruppo utenti LDAP per un particolare dominio. Ogni gruppo LDAP ha l'autorizzazione ad eseguire specifiche attività amministrative EIM per tale dominio. Le attività amministrative e il tipo, comprese le operazioni di ricerca, che un utente EIM può eseguire variano in base al gruppo di controllo di accesso a cui appartiene l'utente EIM.

Nota: per configurare EIM, è necessario provare di essere ritenuto attendibile nel contesto della rete, non da uno specifico sistema. L'autorizzazione a configurare EIM non è basata sull'autorizzazione di profilo utente i5/OS di cui si dispone, ma piuttosto sull'autorizzazione di controllo di accesso EIM di cui si dispone. EIM è una risorsa di rete, non una risorsa per un particolare sistema; di conseguenza, EIM non riconosce delle autorizzazioni speciali specifiche per i5/OS come *ALLOBJ

e *SECADM per la configurazione. Dopo che EIM è stato configurato, tuttavia, l'autorizzazione ad eseguire delle attività può essere basata su vari tipi di utente differenti, compresi i profili utente i5/OS. Ad esempio, IBM Tivoli Directory Server for i5/OS tratta i profili i5/OS con l'autorizzazione speciale *ALLOBJ e *IOSYSCFG come amministratori di indirizzario.

Solo utenti con il controllo accesso amministratore EIM possono aggiungere altri utenti ad un gruppo controllo accesso EIM o modificare le impostazioni del controllo accesso di altri utenti. Prima che un utente possa divenire membro di un gruppo di controllo di accesso EIM, è necessario che tale utente disponga di una voce del server dell'indirizzario che agisca come unità di controllo del dominio EIM. Inoltre, solo determinati tipi di utenti possono divenire membri di un gruppo di controllo di accesso EIM. L'identità utente può avere il formato di un principal Kerberos, un DN (distinguished name) LDAP o un profilo utente i5/OS fintanto che l'identità utente è definita nel server indirizzario.

Nota: perché sia disponibile il tipo utente principal Kerberos in EIM, è necessario che sia configurato sul sistema il servizio di autenticazione di rete. Perché sia disponibile il tipo profilo utente i5/OS in EIM, è necessario che sia configurato un suffisso oggetto sistema sul server indirizzario. Questo consente al server indirizzario di fare riferimento agli oggetti sistema i5/OS, come ad esempio i profili utente i5/OS.

Seguono brevi descrizioni delle funzioni che possono essere eseguite da ogni gruppo di autorizzazione EIM:

Amministratore LDAP (Lightweight Directory Access Protocol)

L'amministratore LDAP è un DN speciale nell'indirizzario che è un amministratore per l'intero indirizzario. Pertanto, l'amministratore LDAP ha accesso a tutte le funzioni amministrative di EIM e ha accesso all'intero indirizzario. Un utente con tale controllo accesso può svolgere le seguenti funzioni:

- Creare un dominio.
- Cancellare un dominio.
- Creare ed eliminare gli identificativi EIM.
- Creare ed eliminare le definizioni del registro EIM.
- Creare ed eliminare le associazioni di origine, di destinazione e amministrative.
- Creare ed eliminare le associazioni normativa.
- Creare ed eliminare i filtri certificato.
- Abilitare e disabilitare l'utilizzo delle associazioni normativa per un dominio.
- Abilitare e disabilitare le ricerche di corrispondenza per un registro.
- Abilitare e disabilitare l'utilizzo delle associazioni normativa per un registro.
- Eseguire le operazioni di ricerca EIM.
- Richiamare associazioni di identificativi, associazioni normativa, filtri certificato, identificativi EIM e definizioni registro EIM.
- Aggiungere, eliminare ed elencare le informazioni sul controllo di accesso EIM.
- Modificare e rimuovere le informazioni sulle credenziali per un utente del registro.

Amministrat. EIM

L'appartenenza a questo gruppo di controllo di accesso consente all'utente di gestire tutti i dati EIM all'interno di questo dominio EIM. Un utente con tale controllo accesso può svolgere le seguenti funzioni:

- Cancellare un dominio.
- Creare ed eliminare gli identificativi EIM.
- Creare ed eliminare le definizioni del registro EIM.
- Creare ed eliminare le associazioni di origine, di destinazione e amministrative.
- Creare ed eliminare le associazioni normativa.

- Creare ed eliminare i filtri certificato.
- Abilitare e disabilitare l'utilizzo delle associazioni normativa per un dominio.
- Abilitare e disabilitare le ricerche di corrispondenza per un registro.
- Abilitare e disabilitare l'utilizzo delle associazioni normativa per un registro.
- Eseguire le operazioni di ricerca EIM.
- Richiamare associazioni di identificativi, associazioni normativa, filtri certificato, identificativi EIM e definizioni registro EIM.
- Aggiungere, eliminare ed elencare le informazioni sul controllo di accesso EIM.
- Modificare e rimuovere le informazioni sulle credenziali per un utente del registro.

Amministratore identificativo

L'appartenenza a questo gruppo di controllo dell'accesso consente all'utente di aggiungere e modificare gli identificativi EIM e di gestire associazioni amministrative, di origine e di destinazione. Un utente che dispone di questo controllo di accesso può effettuare le seguenti funzioni:

- Creare gli identificativi EIM.
- Aggiungere ed eliminare le associazioni di origine.
- Aggiungere ed eliminare le associazioni amministrative.
- Eseguire le operazioni di ricerca EIM.
- Richiamare associazioni di identificativi, associazioni normativa, filtri certificato, identificativi EIM e definizioni registro EIM.

Operazioni di corrispondenza EIM

L'appartenenza a questo gruppo di controllo di accesso consente all'utente di eseguire delle operazioni di ricerca corrispondenze EIM. Un utente che dispone di questo controllo di accesso può effettuare le seguenti funzioni:

- Eseguire le operazioni di ricerca EIM.
- Richiamare associazioni di identificativi, associazioni normativa, filtri certificato, identificativi EIM e definizioni registro EIM.

Amministratore registro

L'appartenenza a questo gruppo di controllo dell'accesso consente all'utente di gestire tutte le definizioni di registro EIM. Un utente che dispone di questo controllo di accesso può effettuare le seguenti funzioni:

- Aggiungere ed eliminare le associazioni di destinazione.
- Creare ed eliminare le associazioni normativa.
- Creare ed eliminare i filtri certificato.
- Abilitare e disabilitare le ricerche di corrispondenza per un registro.
- Abilitare e disabilitare l'utilizzo delle associazioni normativa per un registro.
- Eseguire le operazioni di ricerca EIM.
- Richiamare associazioni di identificativi, associazioni normativa, filtri certificato, identificativi EIM e definizioni registro EIM.

Amministratore per i registri selezionati

L'appartenenza a questo gruppo di controllo di accesso consente all'utente di gestire informazioni EIM solo per una definizione registro utenti specificata (come ad esempio `Registry_X`). L'appartenenza a questo gruppo di controllo di accesso consente inoltre all'utente di aggiungere ed eliminare associazioni di destinazione per una specifica definizione di registro utenti. Per avvantaggiarsi appieno delle operazioni di ricerca di corrispondenze e delle associazioni normativa, un utente con tale controllo

accesso dovrebbe avere anche il controllo accesso **Operazioni corrispondenza EIM** . Questo controllo di accesso consente ad un utente di eseguire le seguenti funzioni per delle specifiche definizioni di registro autorizzate:

- Creare, eliminare ed elencare associazioni di destinazione solo per le definizioni registro EIM specificate.
- Aggiungere ed eliminare delle associazioni normativa di dominio predefinite.
- Aggiungere ed eliminare associazioni normativa solo per le definizioni di registro specificate.
- Aggiungere i filtri certificato solo per le definizioni dei registri specificate.
- Abilitare e disabilitare le ricerche di corrispondenza solo per le definizioni dei registri specificate.
- Abilitare e disabilitare l'utilizzo delle associazioni normativa solo per le definizioni registro specificate.
- Richiamare gli identificativi EIM.
- Richiamare associazioni di identificativi e filtri certificato solo per le definizioni registro specificate.
- Richiamare le informazioni della definizione dei registri EIM solo per le definizioni di registro specificate.

Nota: se la definizione di registro specificata è una definizione di gruppo, un utente con Amministratore per il controllo accesso ai registri selezionati dispone dell'accesso di amministratore soltanto al gruppo, non ai membri del gruppo.

Un utente che dispone sia del controllo di accesso **Amministratore per registri selezionati** che del controllo di accesso **Operazioni di ricerca della corrispondenza EIM** ha la possibilità di effettuare le seguenti funzioni:

- Aggiungere ed eliminare associazioni normativa solo per i registri specificati.
- Eseguire le operazioni di ricerca EIM.
- Richiamare tutte le associazioni di identificativi, le associazioni normativa, i filtri certificato, gli identificativi EIM e le definizioni registro EIM.

Ricerca credenziali

Questo gruppo di controllo dell'accesso consente all'utente di richiamare le informazioni sulle credenziali, come ad esempio le parole d'ordine.

Se un utente con questo controllo accesso desidera eseguire un'ulteriore operazione EIM, è necessario che sia membro del gruppo di controllo dell'accesso che fornisce l'autorizzazione per l'operazione EIM desiderata. Ad esempio, se un utente con questo controllo accesso desidera richiamare l'associazione di destinazione da un'associazione di origine, è necessario che sia membro di uno dei seguenti gruppi di controllo dell'accesso:

- Amministrat. EIM
- Amministratore identificativo
- Operazioni di ricerca delle corrispondenze EIM
- Amministratore registro

Concetti correlati

"Considerazioni sul profilo utente i5/OS per EIM" a pagina 51
Il fatto di potere eseguire delle attività in EIM (Enterprise Identity Mapping) non è basato sull'autorizzazione di profilo utente i5/OS, ma piuttosto sull'autorizzazione di controllo di accesso EIM di cui si dispone.

"Identificazione delle competenze e dei ruoli necessari" a pagina 55
EIM è progettato per consentire facilmente ad una sola persona di essere il responsabile per la configurazione e l'amministrazione in una piccola organizzazione. In un'organizzazione di dimensioni maggiori, tuttavia, si potrebbe preferire ripartire queste responsabilità tra più persone.

Attività correlate

"Gestione del controllo di accesso utente EIM" a pagina 124
Un utente EIM (Enterprise Identity Mapping) è un utente che possiede il controllo di accesso EIM in base all'appartenenza a gruppi utenti LDAP (Lightweight Directory Access Protocol) predefiniti. Specificando il controllo di accesso EIM per un utente, tale utente viene aggiunto a un gruppo di utenti LDAP specifico.

Gruppo di controllo accesso EIM: autorizzazione API

Queste informazioni visualizzano tabelle organizzate dall'operazione EIM (Enterprise Identity Mapping) eseguita dall'API.

Ciascuna tabella visualizza ciascuna API EIM, i diversi gruppi di controllo di accesso EIM e se il gruppo di controllo di accesso dispone dell'autorizzazione peer eseguire una specifica funzione EIM.

Tabella 1. Gestione dei domini

API EIM	Amministrat. LDAP	Amministrat. EIM	Amministrat. identificativi	Ricerca di corrispond. EIM	Amministrat. registro	Amministrat. per il registro selezionato
eimChangeDomain	X	X	-	-	-	-
eimCreateDomain	X	-	-	-	-	-
eimDeleteDomain	X	X	-	-	-	-
eimListDomains	X	X	-	-	-	-

Tabella 2. Gestione degli identificativi

API EIM	Amministrat. LDAP	Amministrat. EIM	Amministrat. identificativi EIM	Ricerca di corrispond. EIM	Amministrat. registri EIM	Amministrat. registro X EIM
eimAddIdentifier	X	X	X	-	-	-
eimChangeIdentifier	X	X	X	-	-	-
eimListIdentifiers	X	X	X	X	X	X
eimRemoveIdentifier	X	X	-	-	-	-
eimGetAssociated Identificativi	X	X	X	X	X	X

Tabella 3. Gestione dei registri

API EIM	Amministrat. LDAP	Amministrat. EIM	Amministrat. identificativi EIM	Ricerca di corrispond. EIM	Amministrat. registri EIM	Amministrat. registro X EIM
eimAddApplication Registro	X	X	-	-	-	-
eimAddSystemRegistry	X	X	-	-	-	-
eimChangeRegistry	X	X	-	-	X	X
eimChange RegistryUser	X	X	-	-	X	X
eimChangeRegistryAlias	X	X	-	-	X	X
eimGetRegistry NameFromAlias	X	X	X	X	X	X
eimListRegistries	X	X	X	X	X	X
eimListRegistry Associazioni	X	X	X	X	X	X
eimListRegistryAliases	X	X	X	X	X	X
eimListRegistry Utenti	X	X	X	X	X	X
eimRemoveRegistry	X	X	-	-	-	-

Tabella 4. Gestione delle associazioni di identificativo. Per le API `eimAddAssociation()` e `eimRemoveAssociation()` ci sono quattro parametri che determinano il tipo di associazione che si sta aggiungendo o eliminando. L'autorizzazione a queste API differisce in base al tipo di associazione specificato in questi argomenti. Nella tabella riportata di seguito, per ognuna di queste API viene incluso il tipo di associazione.

API EIM	Amministrat. LDAP	Amministrat. EIM	Amministrat. identificativi EIM	Ricerca di corrispond. EIM	Amministrat. registri EIM	Amministrat. registro X EIM
eimAddAssociation (amministrativa)	X	X	X	-	-	-
eimAddAssociation (origine)	X	X	X	-	-	-
eimAddAssociation (origine e destinazione)	X	X	X	-	X	X
eimAddAssociation (destinazione)	X	X	-	-	X	X
eimListAssociations	X	X	X	X	X	X
eimRemoveAssociation (amministrativa)	X	X	X	-	-	-
eimRemoveAssociation (origine)	X	X	X	-	-	-
eimRemoveAssociation (origine e destinazione)	X	X	X	-	X	X
eimRemoveAssociation (destinazione)	X	X	-	-	X	X

Tabella 5. Gestione delle associazioni di criterio

API EIM	Amministrat. LDAP	Amministrat. EIM	Amministrat. identificativi EIM	Ricerca di corrispond. EIM	Amministrat. registri EIM	Amministrat. registro X EIM
eimAddPolicyAssociation	X	X	-	-	X	X
eimAddPolicyFilter	X	X	-	-	X	X
eimListPolicyFilters	X	X	X	X	X	X
eimRemove PolicyAssociation	X	X			X	X
eimRemovePolicyFilter	-	-	-	-	-	

Tabella 6. Gestione delle associazioni

API EIM	Amministrat. LDAP	Amministrat. EIM	Amministrat. identificativi EIM	Ricerca di corrispond. EIM	Amministrat. registri EIM	Amministrat. registro X EIM
eimGetAssociatedIdentifier	X	X	X	X	X	X
eimGetTargetFromIdentifier	X	X	X	X	X	X
eimGetTargetFromSource	X	X	X	X	X	X

Tabella 7. Gestione dell'accesso

API EIM	Amministrat. LDAP	Amministrat. EIM	Amministrat. identificativi EIM	Ricerca di corrispond. EIM	Amministrat. registri EIM	Amministrat. registro X EIM
eimAddAccess	X	X	-	-	-	-
eimListAccess	X	X	-	-	-	-
eimListUserAccess	X	X	-	-	-	-
eimQueryAccess	X	X	-	-	-	-
eimRemoveAccess	X	X	-	-	-	-

Gruppo di controllo di accesso EIM; autorizzazione attività EIM

Queste informazioni visualizzano una tabella che spiega le relazioni tra i diversi gruppi di controllo dell'accesso EIM (Enterprise Identity Mapping) e le attività EIM che possono eseguire.

Sebbene amministratore LDAP non è elencato nella tabella, questo livello del controllo di accesso si rende necessario per creare un nuovo dominio EIM. Inoltre, l'amministratore LDAP dispone dello stesso controllo di accesso dell'amministratore EIM, ma quest'ultimo non dispone automaticamente del controllo di accesso dell'amministratore LDAP.

Tabella 8. Tabella 1: gruppi di controllo di accesso EIM

Attività EIM	**Amministratore EIM**	**Amministratore identificativi**	**Operazioni di ricerca corrispondenza EIM**	**Amministratore registro**	**Amministratore per il registro selezionato**	**Ricerca credenziali**
Creare dominio	-	-	-	-	-	
Cancellare dominio	X	-	-	-	-	
Modificare dominio	X	-	-	-	-	
Abilitare - Disabilitare associazioni normativa per dominio	X	-	-	-	-	
Ricercare domini	X	-	-	-	-	
Aggiungere registro di sistema	X	-	-	-	-	
Aggiungere registro applicazione	X	-	-	-	-	
Eliminare registro	X	-	-	-	-	
Modificare registro	X	-	-	X	X	
Abilitare - Disabilitare ricerche di corrispondenza per registro	X	-	-	X	X	
Abilitare - Disabilitare associazioni normativa per registro	X	-	-	X	X	
Ricercare i registri	X	X	X	X	X	

Tabella 8. Tabella 1: gruppi di controllo di accesso EIM (Continua)

Attività EIM	Amministratore EIM	Amministratore identificativi	Operazioni di ricerca corrispondenza EIM	Amministratore registro	Amministratore per il registro selezionato	Ricerca credenziali
Aggiungere identificativo	X	X	-	-	-	
Eliminare identificativo	X	-	-	-	-	
Modificare identificativo	X	X	-	-	-	
Ricercare gli identificativi	X	X	X	X	X	
Richiamare gli identificativi associati	X	X	X	X	X	
Aggiungere - eliminare associazione amministrativa	X	X	-	-	-	
Aggiungere - eliminare associazione di origine	X	X	-	-	-	
Aggiungere - eliminare associazione di destinazione	X	-	-	X	X	
Aggiungere - eliminare associazione normativa	X	-	-	X	X	
Aggiungere - eliminare filtro certificato	X	-	-	X	X	
Ricercare filtro certificato	X	X	X	X	X	
Ricercare associazioni	X	X	X	X	X	
Ricercare associazioni normativa	X	X	X	X	X	
Richiamare associazione di destinazione da associazione di origine	X	X	X	X	-	

Tabella 8. Tabella 1: gruppi di controllo di accesso EIM (Continua)

Attività EIM	Amministratore EIM	Amministratore identificativi	Operazioni di ricerca corrispondenza EIM	Amministratore registro	Amministratore per il registro selezionato	Ricerca credenziali
Richiamare associazione di destinazione da identificativo	X	X	X	X	X	
Modificare utenti registro	X	-	-	X	X	
Ricercare utenti registro	X	X	X	X	X	
Modificare alias di registro	X	-	-	X	X	
Ricercare alias di registro	X	X	X	X	X	
Richiamare registro da alias	X	X	X	X	X	
Aggiungere - Eliminare controllo accesso EIM	X	-	-	-	-	
Visualizzare membri gruppo controllo accesso	X	-	-	-	-	
Visualizzare controllo accesso EIM per un utente specificato	X	-	-	-	-	
Eseguire query del controllo accesso EIM	X	-	-	-	-	
Modificare credenziale	X	-	-	-	-	-
Richiamare credenziali	X	-	-	-	-	X
1 - Se la definizione di registro specificata è una definizione di gruppo, un utente con Amministratore per il controllo accesso ai registri selezionati dispone dell'accesso di amministratore soltanto al gruppo, non ai membri del gruppo.						

Concetti LDAP relativi a EIM

EIM utilizza un server LDAP come unità di controllo del dominio per la memorizzazione dei dati EIM. Di conseguenza, è necessario comprendere alcuni concetti di LDAP correlati alla configurazione ed all'utilizzo di EIM nella propria azienda. È ad esempio possibile utilizzare un DN LDAP come identità utente per configurare EIM ed eseguire l'autenticazione per l'unità di controllo del dominio EIM.

Per comprendere meglio la configurazione e l'utilizzo di EIM, è necessario comprendere i seguenti concetti LDAP:

Concetti correlati

"Concetti di EIM" a pagina 5
Per comprendere completamente come poter utilizzare EIM nella propria società, è necessario conoscere concettualmente come opera EIM (Enterprise Identity Mapping). Sebbene la configurazione e l'implementazione delle API di EIM possano differire a seconda delle piattaforme server, i concetti su EIM sono comuni tra le piattaforme IBM eServer.

DN (distinguished name)

Un DN (distinguished name) è una voce LDAP che identifica in modo univoco e descrive una voce in un server (LDAP) di indirizzario. È possibile utilizzare il wizard di configurazione di EIM per configurare il server di indirizzario per memorizzare le informazioni sul dominio EIM. Poiché EIM utilizza il server di indirizzario per memorizzare i dati EIM, è possibile utilizzare i DN come mezzo di autenticazione nell'unità di controllo del dominio EIM.

I DN sono composti dal nome della voce stessa e dai nomi, ordinati dal basso verso l'alto, degli oggetti precedenti nell'indirizzario LDAP. Un esempio di un DN completo può essere `cn=Tim Jones, o=IBM, c=US`. Ogni voce dispone di almeno un attributo che viene utilizzato per dare un nome alla voce. Questo attributo di denominazione viene definito RDN relative distinguished name) della voce. La voce precedente a uno specifico RDN è il suo DN principale. In questo esempio, `cn=Tim Jones` dà il nome alla voce, in modo che sia l'RDN. `o=IBM, c=US` è il DN principale per `cn=Tim Jones`.

Poiché EIM utilizza il server di indirizzario per memorizzare i dati EIM, è possibile utilizzare un DN per l'identità utente che esegue l'autenticazione nell'unità di controllo del dominio. È inoltre possibile utilizzare un DN per l'identità utente che configura EIM per la propria piattaforma System i. È ad esempio possibile utilizzare un DN quando si eseguono le seguenti operazioni:

- Configurare il server di indirizzario in modo che funga da unità di controllo del dominio EIM. Ciò viene effettuato creando ed utilizzando il DN che identifica l'amministratore di LDAP per il server di indirizzario. Se il server di indirizzario non è stato precedentemente configurato, è possibile configurarlo quando si utilizza il wizard di configurazione di EIM per creare e collegare un nuovo dominio.
- Si utilizza il wizard di configurazione di EIM per selezionare il tipo di identità utente che il wizard deve utilizzare per collegarsi all'unità di controllo del dominio EIM. Il DN è uno dei tipi di utente selezionabili. Il DN deve rappresentare un utente autorizzato a creare oggetti nello spazio del nome locale del server di indirizzario.
- Si utilizza il wizard di configurazione di EIM per selezionare il tipo di utente per eseguire le operazioni EIM al posto delle funzioni del sistema operativo. Queste operazioni includono le ricerche delle corrispondenze e la cancellazione delle associazioni quando si cancella un profilo utente i5/OS locale. Il DN è uno dei tipi di utente selezionabili.
- Ci si collega all'unità di controllo del dominio per un'amministrazione EIM, ad esempio, per gestire i registri e gli identificativi e per eseguire le operazioni di ricerca delle corrispondenze.
- Creare dei filtri certificato per determinare l'ambito di un'associazione normativa filtro certificato. Quando si crea un filtro certificato, è necessario fornire le informazioni sul DN per l'SDN (subject distinguished name - DN soggetto) o per l'IDN (issuer distinguished name - DN emittente) oppure il certificato per specificare i criteri utilizzati dal filtro per determinare quali certificati sono interessati dall'associazione normativa.

Concetti correlati

"DN (distinguished name) principale"
Un DN (distinguished name) principale è uno spazio nome del server indirizzario LDAP (Lightweight Directory Access Protocol). Le voci del server LDAP sono ordinate in una struttura gerarchica che può riflettere limiti politici, geografici, organizzativi o di dominio. Un DN viene considerato principale quando è la voce di indirizzario immediatamente superiore ad uno specifico DN.

"Filtri certificato" a pagina 27
Un filtro del certificato definisce una serie di attributi del certificato DN (distinguished name) simili per un gruppo di certificati utente in un registro utenti X.509 di origine. È possibile utilizzare il filtro certificato come base per un'associazione normativa filtro certificato.

Informazioni correlate

Concetti del server indirizzario

DN (distinguished name) principale

Un DN (distinguished name) principale è uno spazio nome del server indirizzario LDAP (Lightweight Directory Access Protocol). Le voci del server LDAP sono ordinate in una struttura gerarchica che può riflettere limiti politici, geografici, organizzativi o di dominio. Un DN viene considerato principale quando è la voce di indirizzario immediatamente superiore ad uno specifico DN.

Un esempio di un DN completo può essere `cn=Tim Jones, o=IBM, c=US`. Ogni voce dispone di almeno un attributo che viene utilizzato per dare un nome alla voce. Questo attributo di denominazione viene definito RDN relative distinguished name) della voce. La voce precedente un determinato RDN viene definita come DN principale. In questo esempio, `cn=Tim Jones` dà il nome alla voce, in modo che sia l'RDN. `o=IBM, c=US` è il DN principale per `cn=Tim Jones`.

EIM (Enterprise Identity Mapping) utilizza un server indirizzario come un'unità di controllo del dominio per la memorizzazione dei dati del dominio EIM. Il DN principale combinato con il nome del dominio EIM determina la posizione dei dati del dominio EIM nello spazio di nomi del server dell'indirizzario. Quando si utilizza il wizard di configurazione EIM per creare e partecipare a un nuovo dominio, è possibile scegliere di specificare un DN principale per il dominio che si sta creando. Utilizzando un DN principale, è possibile specificare il luogo dello spazio nome LDAP in cui devono trovarsi i dati EIM per il dominio. Se non si specifica un DN principale, i dati EIM risiederanno nel relativo suffisso nello spazio nome dell'ubicazione predefinita dei dati del dominio EIM sarà `ibm-eimDomainName=EIM`.

Concetti correlati

"DN (distinguished name)" a pagina 48
Un DN (distinguished name) è una voce LDAP che identifica in modo univoco e descrive una voce in un server (LDAP) di indirizzario. È possibile utilizzare il wizard di configurazione di EIM per configurare il server di indirizzario per memorizzare le informazioni sul dominio EIM. Poiché EIM utilizza il server di indirizzario per memorizzare i dati EIM, è possibile utilizzare i DN come mezzo di autenticazione nell'unità di controllo del dominio EIM.

Informazioni correlate

Concetti del server indirizzario

Schema LDAP ed altre considerazioni per EIM

Utilizzare queste informazioni per comprendere gli elementi richiesti per il corretto funzionamento del server dell'indirizzario con EIM (Enterprise Identity Mapping).

EIM richiede che l'unità di controllo del dominio si trovi in un server indirizzario che supporta LDAP (Lightweight Directory Access Protocol) Versione 3. Inoltre, il prodotto server indirizzario deve essere in grado di accettare lo schema EIM e comprendere i seguenti attributi e le seguenti classi di oggetto:

- L'attributo ibm-entryUUID.
- I tipi di attributo ibm:
  - acIEntry
  - acIPropagate

  - acISource
  - entryOwner
  - ownerPropagate
  - ownerSource
- Gli attributi EIM, compresi i tre nuovi attributi per il supporto dell'associazione normativa:
  - ibm-eimAdditionalInformation
  - ibm-eimAdminUserAssoc
  - ibm-eimDomainName, ibm-eimDomainVersion,
  - ibm-eimRegistryAliases
  - ibm-eimRegistryEntryName
  - ibm-eimRegistryName
  - ibm-eimRegistryType
  - ibm-eimSourceUserAssoc
  - ibm-eimTargetIdAssoc
  - ibm-eimTargetUserName
  - ibm-eimUserAssoc
  - ibm-eimFilterType
  - ibm-eimFilterValue
  - ibm-eimPolicyStatus
- Le classi di oggetto EIM, comprese le tre nuove classi per il supporto dell'associazione normativa:
  - ibm-eimApplicationRegistry
  - ibm-eimDomain
  - ibm-eimIdentifier
  - ibm-eimRegistry
  - ibm-eimRegistryUser
  - ibm-eimSourceRelationship
  - ibm-eimSystemRegsitry
  - ibm-eimTargetRelationship
  - ibm-eimFilterPolicy
  - ibm-eimDefaultPolicy
  - ibm-eimPolicyListAux

Concetti correlati

"Unità di controllo del dominio EIM" a pagina 6
Un'unità di controllo dominio EIM è un server LPDA (Lightweight Directory Access Protocol) configurato per gestire uno o più domini EIM Un dominio EIM è composto di tutti gli identificativi EIM, le associazioni EIM e i registri utenti definiti in tale dominio. I sistemi (client EIM) prendono parte al dominio EIM utilizzando i dati del dominio per le operazioni di ricerca EIM.

Concetti di EIM per i5/OS

| È possibile implementare EIM (Enterprise Identity Mapping) su qualsiasi piattaforma IBM eServer.
| Tuttavia, quando si implementa EIM su un modello System i, bisogna essere consapevoli di alcune
| informazioni specifiche per l'implementazione di System i.

Sono di seguito riportate delle informazioni utili relative alle applicazioni i5/OS abilitate per EIM, alle considerazioni sui profili utente e ad altri argomenti che possono aiutare ad utilizzare EIM su una piattaforma System i in modo efficace:

Concetti correlati

"Concetti di EIM" a pagina 5
Per comprendere completamente come poter utilizzare EIM nella propria società, è necessario conoscere concettualmente come opera EIM (Enterprise Identity Mapping). Sebbene la configurazione e l'implementazione delle API di EIM possano differire a seconda delle piattaforme server, i concetti su EIM sono comuni tra le piattaforme IBM eServer.

Considerazioni sul profilo utente i5/OS per EIM

Il fatto di potere eseguire delle attività in EIM (Enterprise Identity Mapping) non è basato sull'autorizzazione di profilo utente i5/OS, ma piuttosto sull'autorizzazione di controllo di accesso EIM di cui si dispone.

Ci sono delle attività aggiuntive che l'utente deve eseguire per impostare i5/OS per l'utilizzo di EIM. Queste attività aggiuntive richiedono che l'utente disponga di un profili utente i5/OS con le appropriate autorizzazioni speciali.

Per impostare i5/OS per l'utilizzo di EIM con System i Navigator, il profilo utente di cui si dispone deve avere le seguenti autorizzazioni speciali:

- Responsabile della sicurezza (*SECADM).
- Tutti gli oggetti (*ALLOBJ).
- Configurazione di sistema (*IOSYSCFG).

Miglioramento al comando per i profili utente i5/OS per gli identificativi EIM

Dopo avere configurato EIM per il proprio sistema, è possibile servirsi di un nuovo parametro sia per il comando CRTUSRPRF (Creazione profilo utente) che per il comando CHGUSRPRF (Modifica profilo utente); questo parametro è denominato EIMASSOC. È possibile utilizzare questo parametro per definire le associazioni di identificativi per il profilo utente specificato per il registro locale.

Quando si utilizza questo parametro, è possibile specificare le seguenti informazioni:

- Il nome di identificativo EIM, che può essere un nome nuove oppure un nome di identificativo esistente.
- Un'opzione di azione per l'associazione, che può essere di aggiungere (*ADD), sostituire (REPLACE) oppure eliminare (*REMOVE), l'associazione specificata.

  Nota: utilizzare l'opzione *ADD per impostare delle nuove associazioni. Utilizzare l'opzione *REPLACE, ad esempio, se si sono in precedenza definite delle associazioni per l'identificativo errato. L'opzione *REPLACE rimuove le eventuali associazioni esistenti del tipo specificato per il registro locale a qualsiasi altro identificativo ed aggiunge quindi quello specificato per il parametro. Utilizzare l'opzione *REMOVE per rimuovere le associazioni specificate dall'identificativo specificato.
- Il tipo di associazione di identificativi, che può essere di destinazione, origine, sia di destinazione che origine oppure un'associazione amministrativa.
- Creare o meno l'identificativo EIM specificato se non esiste già.

Di norma, si crea un'associazione di destinazione per un profilo i5/OS, soprattutto in un ambiente a collegamento singolo (SSO). Dopo avere utilizzato il comando per creare l'associazione di destinazione necessaria per il profilo utente (e l'identificativo EIM, se necessario), è possibile che occorra creare un'associazione di origine corrispondente. È possibile utilizzare System i Navigator per creare un'associazione di origine per un'altra identità utente, come ad esempio un Kerberos principal con il quale l'utente si collega alla rete.

Quando si è configurato EIM per il sistema, si sono specificate un'identità utente ed una parola d'ordine utilizzata dal sistema per eseguire le operazioni EIM per conto del sistema operativo. Quest'identità

utente deve avere autorizzazione di controllo di accesso EIM sufficiente per creare identificativi ed aggiungere associazioni.

Parole d'ordine di profili utente i5/OS e EIM

Come amministratore, il primo scopo per la configurazione di EIM come parte di un ambiente a collegamento singolo (SSO) è quello di ridurre la gestione delle parole d'ordine degli utenti che bisogna eseguire per i tipici utenti finali nella propria azienda. Utilizzando la corrispondenza di identità fornita da EIM insieme all'autenticazione Kerberos, si sa che i propri utenti dovranno eseguire un numero minore di collegamenti e ricordare e gestire un numero minore di parole d'ordine. Questo comporta dei vantaggi perché si ricevono meno chiamate per gestire problemi relativi alle identità utente messe in corrispondenza, come ad esempio le chiamate per reimpostare queste parole d'ordine quando gli utenti le dimenticano. Tuttavia, le proprie regole relative alle parole d'ordine delle normative di sicurezza sono ancora attive e bisogna ancora gestire questi profili utente per gli utenti quando le parole d'ordine scadono.

Per trarre ulteriore vantaggio dal proprio ambiente a collegamento singolo (SSO), prendere in considerazione la possibilità di modificare l'impostazione della parola d'ordine per quei profili utente che sono la destinazione di corrispondenze di identità. Come destinazione di una corrispondenza di identità, l'utente non deve più fornire la parola d'ordine per il profilo utente quando accede ad una piattaforma System i o a una risorsa i5/OS abilitata a EIM. Per i tipici utenti, è possibile modificare l'impostazione della parola d'ordine su *NONE in modo tale che non possa essere utilizzata alcuna parola d'ordine con il profilo utente. Il proprietario del profilo utente non ha più bisogno di una parola d'ordine a causa della corrispondenza di identità e dell'SSO. Impostando la parola d'ordine su *NONE, si ha un ulteriore vantaggio perché non si devono più gestire le scadenze delle parole d'ordine, né lo devono fare i propri utenti; inoltre, nessuno può utilizzare il profilo per collegarsi direttamente ad una piattaforma System i oppure per accedere a risorse i5/OS abilitate a EIM. Tuttavia, si potrebbe preferire che gli amministratori continuino ad avere un valore di parola d'ordine per i loro profili utente nel caso in cui debbano collegarsi direttamente ad una piattaforma System i. Se ad esempio la propria unità di controllo del dominio EIM non è attiva e non può verificarsi la corrispondenza di identità, un amministratore potrebbe avere bisogno di collegarsi direttamente ad una piattaforma System i fino a quando non viene risolto il problema con l'unità di controllo di dominio.

Concetti correlati

"Controllo di accesso EIM" a pagina 39
Un utente EIM è un utente che possiede il controllo di accesso EIM in base all'appartenenza ad un gruppo utenti LDAP (Lightweight Directory Access Protocol) predefinito per uno specifico dominio.

Informazioni correlate

Comando CRTUSRPRF (Creazione profilo utente)

Controllo i5/OS per EIM

Il tipo di controllo eseguito è una considerazione importante per il proprio piano di sicurezza generale.

Quando si configura e si utilizza EIM (Enterprise Identity Mapping), configurare il supporto di controllo per il server di indirizzario per assicurare di fornire l'appropriato livello di responsabilità richiesto dalla propria normativa di sicurezza. Il supporto di controllo può essere ad esempio utile nel determinare quali degli utenti messi in corrispondenza da un'associazione normativa hanno eseguito un'azione sul proprio sistema oppure modificato un oggetto.

Informazioni correlate

Controllo server indirizzario

Applicazioni abilitate per i5/OS

EIM può utilizzare una varietà di applicazioni i5/OS.

Le seguenti applicazioni i5/OS possono essere configurate per utilizzare EIM (Enterprise Identity Mapping):

- I server host i5/OS (attualmente utilizzati da System i Access per Windows
- e System i Navigator)
- Telnet Server (attualmente utilizzato da PC5250 e IBM WebSphere Host On-Demand)
- QFileSrv.400 ODBC (consente l'utilizzo dell'SSO tramite SQL)
- JDBC (consente l'utilizzo di EIM tramite SQL)
- Distributed Relational Database Architecture (DRDA) (consente l'utilizzo di EIM tramite SQL)
- IBM WebSphere Host On-Demand Versione 8, (funzione WEL (Web Express Logon - Collegamento rapido Web)
- i5/OS NetServer
- QFileSvr.400

Scenari: EIM (Enterprise Identity Mapping)

Utilizzare queste informazioni per comprendere le modalità di gestione di identità utente su differenti sistemi all'interno di un ambiente SSO.

EIM (Enterprise Identity Mapping) è una tecnologia di infrastruttura IBM che consente di tenere traccia delle identità utente nell'ambito di un'azienda e di gestirle. EIM viene di norma utilizzato con una tecnologia di autenticazione, come ad esempio il servizio di autenticazione di rete, per implementare un ambiente a collegamento singolo (SSO).

Informazioni correlate

Scenari di SSO

Pianificazione di EIM (Enterprise Identity Mapping)

prima di impostare EIM è necessario sviluppare un piano di implementazione di EIM (Enterprise Identity Mapping) per assicurarsi di configurare correttamente EIM in un ambiente System i o in un ambiente a piattaforma mista.

Un piano di implementazione è essenziale per configurare ed utilizzare correttamente EIM (Enterprise Identity Mapping) nella propria azienda. Per sviluppare il proprio piano, occorre raccogliere dei dati relativi ai sistemi, alle applicazioni ed agli utenti che utilizzeranno EIM. Si utilizzeranno le informazioni raccolte per decidere come configurare EIM in modo ottimale per la propria azienda.

Poiché EIM è una tecnologia di infrastruttura IBM eServer disponibile per tutte le piattaforme IBM, il modo in cui si pianifica la propria implementazione dipende da quali piattaforme ci sono nella propria azienda. Anche se ci sono varie attività di pianificazione specifiche per ciascuna piattaforma, molte attività di pianificazione EIM sono valide per tutte le piattaforme IBM. Consultare le attività di pianificazione EIM comuni per creare il proprio piano di implementazione generale. Per ulteriori informazioni su come pianificare la propria implementazione EIM, consultare le seguenti pagine:

Pianificazione di EIM per eServer

Un piano di implementazione è essenziale per configurare ed utilizzare correttamente EIM (Enterprise Identity Mapping) in un'azienda a piattaforma mista. Per sviluppare il proprio piano di implementazione, occorre raccogliere dei dati relativi ai sistemi, alle applicazioni ed agli utenti che utilizzeranno EIM. Si utilizzeranno le informazioni raccolte per decidere come configurare EIM in modo ottimale per un ambiente a piattaforma mista.

Il seguente elenco fornisce delle informazioni guida sulle attività di pianificazione da completare prima di configurare ed utilizzare EIM in un ambiente a piattaforma mista. Leggere attentamente le informazioni contenute in queste pagine per apprendere come pianificare correttamente le proprie esigenze di configurazione di EIM, compreso le competenze di cui deve essere dotato il proprio team di implementazione, quali informazioni bisogna raccogliere e quali decisioni relative alla configurazione

bisogna prendere. Potrebbe risultare utile stampare i fogli di lavoro per la pianificazione di EIM (numero 8 nel seguente elenco) in modo da poterli completare durante l'esecuzione del processo di pianificazione.

Requisiti di installazione di EIM (Enterprise Identity Mapping) per eServer

Per implementare correttamente EIM (Enterprise Identity Mapping), è necessario soddisfare tre requisiti: dell'applicazione, del sistema e a livello di rete o dell'azienda.

Requisiti a livello di rete o azienda

È necessario configurare un sistema nella propria azienda o nella propria rete che funga da unità di controllo del dominio EIM, che è un server LDAP (Lightweight Directory Access Protocol) configurato in maniera speciale che memorizza e fornisce dati di dominio EIM. Ci sono varie considerazioni da fare in merito alla scelta del prodotto di servizi indirizzario da utilizzare come un'unità di controllo del dominio, compreso il fatto che non tutti i prodotti server LDAP forniscono il supporto per l'unità di controllo del dominio EIM.

Un'altra considerazione riguarda la disponibilità di strumenti di amministrazione. Un'opzione consiste nel potere utilizzare le API EIM nelle proprie applicazioni per eseguire le funzioni amministrative. Se si pianifica l'utilizzo di IBM Tivoli Directory Server per i5/OS come unità di controllo del dominio EIM, è possibile utilizzare System i Navigator per gestire EIM. Se si pianifica l'utilizzo del prodotto IBM Directory, è possibile utilizzare il programma di utilità eimadmin che fa parte di SPE LDAP V1R4.

Sono di seguito riportate le informazioni di base sulle piattaforme IBM che forniscono un prodotto di server indirizzario che supporta EIM. Informazioni dettagliate sulla scelta di un server indirizzario per fornire il supporto per l'unità di controllo del dominio EIM sono disponibili nella sezione relativa alla pianificazione di un'unità di controllo del dominio EIM.

Requisiti del sistema e delle applicazioni

Ciascun sistema che partecipa ad un dominio EIM deve soddisfare i seguenti requisiti:

- Su di esso deve essere installato il software client LDAP.
- Deve disporre di un'implementazione delle API EIM.

Ciascuna applicazione che parteciperà ad un dominio EIM deve essere in grado di utilizzare le API EIM per eseguire le ricerche associazione ed altre operazioni.

Nota: nel caso di un'applicazione distribuita, potrebbe non essere necessario che sia il lato client che il lato server siano in grado di utilizzare le API EIM. Di norma, solo il lato server dell'applicazione potrebbe avere bisogno di utilizzare le API EIM.

La seguente tabella fornisce le informazioni sul supporto EIM fornito dalle piattaforme eServer. Le informazioni sono organizzate per piattaforma e le colonne indicano quanto segue:

- Il client EIM richiesto affinché la piattaforma supporti le API EIM.
- Il tipo di strumenti di amministrazione e di configurazione di EIM disponibili per la piattaforma.
- Il prodotto di server indirizzario che può essere installato per consentire alla piattaforma di fungere da unità di controllo del dominio EIM.

Non è necessario che una piattaforma sia in grado di fungere da unità di controllo del dominio EIM per partecipare ad un dominio EIM.

Tabella 9. Supporto EIM eServer

Piattaforma	Client EIM (supporto API)	Unità di controllo dominio	Strumenti di amministrazione EIM
AIX su System p	AIX R5.2	IBM Directory V5.1	Non disponibile

Tabella 9. Supporto EIM eServer (Continua)

Piattaforma	Client EIM (supporto API)	Unità di controllo dominio	Strumenti di amministrazione EIM
Linux • SLES8 su PPC64 • Red Hat 7.3 su i386 • SLES7 su System z	Scaricare uno dei seguenti: • Client IBM Directory V4.1 • Client IBM Directory V5.1 • Client Open LDAP v2.0.23	IBM Directory V5.1	Non disponibile
i5/OS su System i	i5/OS V5R3 o successivi	IBM Tivoli Directory Server for i5/OS	System i Navigator
Windows 2000 su System x	Scaricare uno dei seguenti: • Client IBM Directory V4.1 • Client IBM Directory V5.1	Client IBM Directory V5.1	Non disponibile
z/OS su System z	z/OS V1R4 LDAP SPE OW57137	z/OS V1R4 LDAP	V1R4 LDAP SPE OW57137

Un sistema può partecipare ad un dominio EIM a condizione che una piattaforma fornisca il supporto (API) client EIM. Non è necessario che una piattaforma fornisca il supporto per l'unità di controllo del dominio EIM tranne nel caso in cui si desideri utilizzare detta specifica piattaforma come unità di controllo del dominio EIM per la propria azienda.

Informazioni correlate

IBM Tivoli Directory Server

Identificazione delle competenze e dei ruoli necessari

EIM è progettato per consentire facilmente ad una sola persona di essere il responsabile per la configurazione e l'amministrazione in una piccola organizzazione. In un'organizzazione di dimensioni maggiori, tuttavia, si potrebbe preferire ripartire queste responsabilità tra più persone.

Il numero di persone di cui si ha bisogno nel team dipende dal numero di competenze richieste che ciascun suo membro ha, dai tipi di piattaforme che fanno parte dell'implementazione di EIM e dal modo in cui l'organizzazione preferisce dividere le sue regole di sicurezza e le sue responsabilità.

Una corretta implementazione di EIM richiede la configurazione e l'interazione di un certo numero di prodotti software. Poiché ciascuno di questi prodotti richiede delle competenze e dei ruoli specifici, si potrebbe scegliere di creare un team di implementazione di EIM composto da persone da vari, differenti, ambiti disciplinari, soprattutto se si lavora in un'organizzazione di notevoli dimensioni.

Le seguenti informazioni descrivono le competenze e le autorizzazioni di di controllo di accesso EIM richieste per implementare correttamente EIM. Queste competenze sono presentate in termini di posizioni lavorative per le persone in esse specializzate. Si fa ad esempio riferimento ad un'attività che richiede competenze di LDAP (Lightweight Directory Access Protocol) come un'attività per un amministratore per il server di indirizzario.

Membri del team e loro ruoli

Le seguenti informazioni descrivono le responsabilità e le autorizzazioni richieste dei ruoli necessari per gestire EIM. È possibile utilizzare quest'elenco di ruoli per determinare i membri del team necessari per installare e configurare i prodotti prerequisiti e per configurare EIM e uno o più domini EIM.

Una delle prime serie di ruoli che bisogna definire è il numero ed il tipo di responsabili per il proprio dominio EIM. Tutto il personale con mansioni e autorizzazioni di amministratore deve essere coinvolto nel processo di pianificazione di EIM come membri del team di implementazione di EIM.

Nota: i responsabili di EIM hanno un ruolo importante in un'organizzazione, considerato il fatto che ad essi è consentito creare identità utente sui sistemi. Quando creano delle associazioni EIM per le identità utente, essi determinano chi sono gli utenti che possono accedere ai sistemi di computer e quali privilegi hanno quando accedono. IBM consiglia di dare quest'autorità a persone di fiducia, sulla base della normativa di sicurezza dell'azienda.

La seguente tabella elenca i potenziali ruoli dei membri del team e le attività e le competenze richieste per configurare e gestire EIM.

Nota: se una singola persona in un'organizzazione sarà responsabile per tutte le attività di configurazione e di amministrazione di EIM, è necessario che ad essa siano assegnati il ruolo e le autorizzazioni di un amministratore di EIM.

Tabella 10. Ruoli, attività e competenze per la configurazione di EIM

Ruolo	Attività autorizzate	Competenze richieste
Amministratore EIM	• Coordinamento delle operazioni di dominio • Aggiunta, rimozione e modifica di definizioni di registro, identificativi EIM ed associazioni per le identità utente • Autorizzazione di sovrindentende per i dati in un dominio EIM	Conoscenza degli strumenti di amministrazione di EIM
Amministratore identificativi EIM	• Creazione e modifica degli identificativi EIM • Aggiunta e rimozione di associazioni amministrative e di origine (non può aggiungere o rimuovere associazioni di destinazione)	Conoscenza degli strumenti di amministrazione di EIM
Amministratore registri EIM	Gestione di tutte le definizioni di registro EIM: • Aggiunta e rimozione delle associazioni di destinazione (non può aggiungere o rimuovere associazioni amministrative e di origine) • Aggiornamento delle definizioni di registro EIM	Conoscenza di: • Tutti i registri utente definiti per il dominio EIM (come le informazioni sulle identità utente) • Gli strumenti di amministrazione di EIM

Tabella 10. Ruoli, attività e competenze per la configurazione di EIM (Continua)

Ruolo	Attività autorizzate	Competenze richieste
Amministratore registro X EIM	Gestione di una specifica definizione di registro EIM: • Aggiunta e rimozione di associazioni di destinazione per uno specifico registro utente (ad esempio, registro X) • Aggiornamento di una specifica definizione di registro EIM	Conoscenza di: • Lo specifico registro utente definito per il dominio EIM (come le informazioni sulle identità utente) • Gli strumenti di amministrazione di EIM
Amministratore del server di indirizzario (LDAP)	• Installazione e configurazione di un server di indirizzario (se necessario) • Personalizzazione della configurazione del server d indirizzario per EIM • Creazione di un dominio EIM (vedere nota) • Definizione di utenti che sono autorizzati ad accedere all'unità di controllo del dominio EIM • Facoltativo: Definizione del primo amministratore di EIM **Nota:** l'amministratore del server di indirizzario può fare tutto quello che può fare un amministratore di EIM.	Conoscenza di: • Installazione, configurazione e personalizzazione del server di indirizzario • Strumenti di amministrazione EIM
Amministratore del registro utenti	• Impostazione dei profili utente o delle identità utente per uno specifico registro utenti • Facoltativo: Funzione di amministratore di registro EIM per il registro utenti specificato	Conoscenza di: • Strumenti per l'amministrazione del registro utenti • Strumenti di amministrazione EIM
Programmatore di sistema o amministratore di sistema	Installazione dei prodotti software necessari (potrebbe includere l'installazione di EIM)	Conoscenza di: • Programmazione di sistema o competenze amministrative • Procedure di installazione per la piattaforma
Programmatore di applicazioni	Compilazione di applicazioni che utilizzano le API EIM	Conoscenza di: • Piattaforma • Competenze di programmazione • Compilazione di programmi

Concetti correlati

"Controllo di accesso EIM" a pagina 39
Un utente EIM è un utente che possiede il controllo di accesso EIM in base all'appartenenza ad un gruppo utenti LDAP (Lightweight Directory Access Protocol) predefinito per uno specifico dominio.

Pianificazione di un dominio EIM

Parte del processo di pianificazione dell'implementazione di EIM (Enterprise Identity Mapping) iniziale richiede che l'utente definisca un dominio EIM. Per sfruttare appieno i vantaggi comportati dall'avere un archivio centralizzato di informazioni di corrispondenza, è necessario pianificare la condivisione del dominio tra molte applicazioni e molti sistemi.

La consultazione dell'argomento relativo alla pianificazione di EIM consentirà di raccogliere le informazioni necessarie per definire il dominio e di registrarle sui fogli di lavoro per la pianificazione. Le sezioni di esempio dai fogli di lavoro possono essere di ausilio per l'utente nella raccolta e la registrazione di queste informazioni a ciascuno stadio della pianificazione in questo argomento.

La seguente tabella elenca le informazioni che è necessario raccogliere quando si pianifica il proprio dominio e suggerisce il ruolo o i ruoli del team di implementazione di EIM che potrebbero essere responsabili per ciascun elemento di informazione necessario.

Nota: anche se la tabella elenca un ruolo specifico come suggerimento per l'assegnazione della responsabilità di raccogliere le informazioni descritte, assegnare i ruoli sulla base delle esigenze e della normativa di sicurezza della propria organizzazione. In un'organizzazione più piccola, ad esempio, è possibile che l'utente preferisca designare una sola persona come amministratore di EIM responsabile di tutte le attività di pianificazione, configurazione e gestione di EIM.

Tabella 11. Informazioni necessarie per la pianificazione del dominio EIM

Informazioni necessarie	Ruolo
1. Se esiste un dominio esistente da utilizzare adatto alle proprie esigenze o se occorre crearne uno.	Amministratore EIM
2. Quale server di indirizzario fungerà da unità di controllo del dominio EIM. (Consultare "Pianificazione di un'unità di controllo del dominio EIM" per informazioni dettagliate sulla selezione di un'unità di controllo del dominio.)	Amministratore del server di indirizzario (LDAP) o amministratore di EIM
3. Un nome per il dominio. È anche possibile fornire una descrizione facoltativa.	Amministratore EIM
4. Dove, nell'indirizzario, memorizzare i dati di dominio EIM. **Nota:** in base alla scelta del sistema che deve contenere il server di indirizzario ed alla scelta di un indirizzario per la memorizzazione dei dati di dominio EIM, è possibile che occorra eseguire alcune attività di configurazione dei servizi di indirizzario prima che possa essere creato il dominio.	Sia l'amministratore del server di indirizzario (LDAP) che l'amministratore di EIM
5. Le applicazioni e i sistemi operativi che parteciperanno al dominio. Se si sta configurando il primo dominio, questo primo gruppo potrebbe essere limitato ad un solo sistema. (Consultare "Sviluppo di un piano di denominazione delle definizioni di registro EIM" a pagina 62 per ulteriori informazioni.)	Team di EIM
6. Le persone e le entità che parteciperanno al dominio. **Nota:** per semplificare la verifica iniziale, limitare il numero di partecipanti a uno o due.	Team di EIM

Pianificazione di un'unità di controllo del dominio EIM

Quando si raccolgono le informazioni per definire un dominio EIM (Enterprise Identity Mapping), occorre determinare quale prodotto server di indirizzario fungerà da unità di controllo del dominio EIM.

EIM richiede che l'unità di controllo del dominio si trovi in un server indirizzario che supporta LDAP (Lightweight Directory Access Protocol) Versione 3. Inoltre, il prodotto server indirizzario deve essere in grado di accettare lo schema LDAP e le altre considerazioni per EIM e comprendere alcuni attributi ed alcune classi di oggetto.

Se la propria azienda possiede più di un server di indirizzario che può ospitare un'unità di controllo del dominio EIM, considerare anche se utilizzare delle unità di controllo del dominio replicate secondarie. Se

si prevede, ad esempio, che si verificherà un numero notevole di operazioni di ricerca di corrispondenze EIM, le repliche possono migliorare le prestazioni delle operazioni di ricerca.

Considerare inoltre se rendere la propria unità di controllo del dominio *locale* oppure *remota* in relazione al sistema che si prevede eseguirà il numero maggiore di operazioni di ricerca di corrispondenze. Un'unità di controllo del dominio locale per il sistema per volumi elevati può migliorare le prestazioni delle operazioni di ricerca per il sistema locale. Utilizzare i fogli di lavoro per la pianificazione per registrare queste decisioni di pianificazione, quelle relative al proprio dominio e le altre informazioni sugli indirizzari.

Dopo avere determinato quale server di indirizzario nella propria azienda ospiterà la propria unità di controllo del dominio EIM, occorre prendere alcune decisioni in merito all'accesso all'unità di controllo del dominio.

Pianificazione dell'accesso all'unità di controllo del dominio

Occorre pianificare la modalità di accesso, propria e dei sistemi operativi e delle applicazioni abilitati a EIM, al server di indirizzario che ospita l'unità di controllo del dominio EIM. Per accedere ad un dominio EIM, occorre:

1. Essere in grado di eseguire un'associazione all'unità di controllo del dominio EIM
2. Accertarsi che il soggetto dell'associazione sia un membro del gruppo di controllo di accesso di EIM oppure che sia l'amministratore LDAP. Per ulteriori informazioni, consultare la sezione relativa alla gestione del controllo di accesso EIM.

Selezione del tipo di collegamento EIM

La API EIM supportano vari meccanismi differenti per stabilire una connessione, indicata anche come collegamento, all'unità di controllo del dominio EIM. Ciascun tipo di meccanismo di collegamento fornisce un livello differente di autenticazione e codifica per la connessione. Le scelte possibili sono:

Collegamenti semplici
Un collegamento semplice è una connessione LDAP dove un client LDAP fornisce un DN (distinguished name) del collegamento ed una parola d'ordine del collegamento al server LDAP per l'autenticazione. Il DN e la parola d'ordine del collegamento sono definiti dall'amministratore di LDAP nell'indirizzario LDAP. Questa è la forma più debole di autenticazione e quella meno sicura poiché il DN e la parola d'ordine del collegamento vengono inviati senza essere codificati e potrebbero essere intercettati da utenti non autorizzati. Utilizzare CRAM-MD5 (meccanismo di autenticazione tramite risposta a domande di identificazione) per aggiungere un ulteriore livello di protezione per la parola d'ordine del collegamento. Con il protocollo CRAM-MD5, il client invia un valore di cui è stato eseguito l'hashing invece della parola d'ordine non codificata al server per l'autenticazione.

Autenticazione server con SSL (Secure Sockets Layer) - autenticazione lato server
Un server LDAP può essere configurato per le connessioni SSL o TLS (Transport Layer Security). Il server LDAP utilizza un certificato digitale per autenticare se stesso presso il client LDAP e stabilisce una sessione di comunicazioni codificata tra loro. Solo il server LDAP è autenticato tramite un certificato. L'utente finale è autenticato tramite un DN ed una parola d'ordine del collegamento. Il livello di autenticazione è uguale a quello del collegamento semplice, ma tutti i dati (compresi il DN e la parola d'ordine) sono codificati per ragioni di riservatezza.

Autenticazione client con SSL
Un server LDAP può essere configurato per richiedere che l'utente finale sia autenticato tramite un certificato digitale invece che tramite un DN ed una parola d'ordine del collegamento per le connessioni sicure SSL o TLS al server LDAP. Sia il client che il server sono autenticati e la sessione è codificata. Quest'opzione fornisce un livello maggiore di autenticazione utente e fornisce la riservatezza di tutti i dati trasmessi.

Autenticazione Kerberos

Un client LDAP può essere autenticato presso il server utilizzando un certificato Kerberos come una sostituzione facoltativa per il DN e la parola d'ordine del collegamento. (Kerberos), che è un sistema di autenticazione di rete di terze parti attendibile, consente ad un principal (utente o servizio) di dimostrare la propria identità ad un altro servizio nell'ambito di una rete non protetta. L'autenticazione dei principal è completata tramite un server centralizzato detto KDC (key distribution center/centro distribuzione chiavi). Il KDC autentica un utente con un certificato Kerberos. Questi certificati dimostrano l'identità del principal ad altri servizi nella rete. Dopo che un principal è stato autenticato tramite questi certificati, il principal ed il servizio possono scambiare dati codificati con un servizio di destinazione. Quest'opzione fornisce un livello maggiore di autenticazione client e protegge la riservatezza delle informazioni di autenticazione.

La selezione di un meccanismo di collegamento è basata sul livello di sicurezza richiesto dall'applicazione abilitata a EIM e sui meccanismi di autenticazione supportati dal server LDAP che ospita il dominio EIM.

Potrebbe inoltre essere necessario eseguire delle attività di configurazione aggiuntive per il server LDAP per abilitare il meccanismo di autenticazione che si sceglie di utilizzare. Consultare la documentazione per il server LDAP che ospita l'unità di controllo del dominio per determinare quali altre attività di configurazione potrebbe essere necessario eseguire.

Foglio di lavoro di esempio per la pianificazione: informazioni sull'unità di controllo del dominio

Dopo avere preso le proprie decisioni in merito all'unità di controllo del dominio EIM, utilizzare i fogli di lavoro per la pianificazione per registrare le informazioni sull'unità di controllo del dominio EIM richieste dalle proprie applicazioni e dai propri sistemi operativi abilitati a EIM. Le informazioni raccolte come parte di questo processo possono essere utilizzate dall'amministratore di LDAP per definire l'identità di collegamento dell'applicazione o del sistema operativo al server di indirizzario LDAP che ospita l'unità di controllo del dominio EIM.

La seguente parte campione dei fogli di lavoro per la pianificazione mostra il tipo di informazioni che bisogna raccogliere. Include inoltre dei valori di esempio che è possibile utilizzare quando si configura l'unità di controllo del dominio EIM.

Tabella 12. Informazioni sul dominio e sull'unità di controllo del dominio per il foglio di lavoro per la pianificazione di EIM

Informazioni richieste per configurare il dominio e l'unità di controllo del dominio EIM	**Risposte di esempio**
Un nome significativo per il dominio. Questo potrebbe essere il nome di una società, di un reparto oppure di un'applicazione che utilizza il dominio.	`MyDomain`
Facoltativo: Se si sta configurando un dominio EIM in un indirizzario LDAP già esistente, specificare un DN (distinguished name) principale per il dominio. Questo è il DN che rappresenta la voce immediatamente precedente alla voce del nome dominio nella gerarchia con struttura ad albero delle informazioni dell'indirizzario, ad esempio `o=ibm,c=us`.	`o=ibm,c=us`

Tabella 12. Informazioni sul dominio e sull'unità di controllo del dominio per il foglio di lavoro per la pianificazione di EIM (Continua)

Informazioni richieste per configurare il dominio e l'unità di controllo del dominio EIM	**Risposte di esempio**
Il DN di dominio EIM completo risultante. Questo è il nome completo del dominio EIM che descrive la posizione dell'indirizzario per i dati del dominio EIM. Il DN completo è formato, come minimo, dal DN di dominio (`ibm-eimDomainName=`), più il nome dominio specificato dall'utente. Se si sceglie di specificare un DN principale per il dominio, il DN di dominio completo sarà formato dal DN di dominio relativo (`ibm-eimDomainName=`), dal nome dominio (MyDomain) e dal DN principale (`o=ibm,c=us`). **Nota:**	Uno dei seguenti, in base al fatto che si scelga o meno un DN principale: • `ibm-eimDomainName=MyDomain` • `ibm-eimDomainName=MyDomain,o=ibm,c=us`
L'indirizzo di collegamento per l'unità di controllo del dominio. Consiste nel tipo di collegamento (ldap di base o ldap sicuro, ad esempio `ldap://` o `ldaps://`) più le seguenti informazioni:	`ldap://`
• Facoltativo: Il nome host o l'indirizzo IP • Facoltativo: Il numero di porta	• `some.ldap.host` • `389`
L'indirizzo di collegamento completo per l'unità di controllo del dominio risultante	`ldap://some.ldap.host:389`
Il meccanismo di collegamento richiesto dalle applicazioni o dai sistemi. Le scelte includono: • Collegamento semplice • CRAM MD5 • Autenticazione server • Autenticazione client • Kerberos	Kerberos

Se il proprio team di amministrazione e di configurazione di EIM è formato da più membri del team, occorrerà determinare l'identità ed il meccanismo di collegamento che ciascun membro del team utilizzerà per accedere al dominio EIM in base al suo ruolo. Occorrerà inoltre determinare l'identità ed il meccanismo di collegamento per gli utenti finali dell'applicazione EIM. Il seguente foglio di lavoro potrebbe risultare utile come un esempio per la raccolta di queste informazioni.

Tabella 13. Foglio di lavoro di esempio per la pianificazione delle identità di collegamento

Autorizzazione o ruolo EIM	**Identità di associazione**	**Meccanismo di associazione**	**Per cosa è richiesto**
Amministratore EIM	eimadmin@krbrealm1.com	kerberos	configurare e gestire EIM
Amministratore LDAP	cn=administrator	collegamento semplice	Configurare l'unità di controllo del dominio EIM
Amministratore registro X EIM	cn=admin2	CRAM MD5	gestire una specifica definizione di registro
Ricerca di corrispondenze EIM	cn=MyApp,c=US	collegamento semplice	eseguire operazioni di ricerca di corrispondenze applicazione

Sviluppo di un piano di denominazione delle definizioni di registro EIM

Per utilizzare EIM (Enterprise Identity Mapping)) per mettere in corrispondenza l'identità utente in un registro con un'identità utente equivalente in un altro registro, entrambi i registri utenti devono essere definiti per EIM.

È necessario creare una definizione di registro EIM per ciascun registro utenti di applicazione o sistema operativo che parteciperà al dominio EIM. I registri utenti possono rappresentare dei registri di sistema operativo come Resource Access Control Facility (RACF) o i5/OS, un registro distribuito come Kerberos oppure un sottoinsieme di un registro di sistema utilizzato esclusivamente da un'applicazione.

Un dominio EIM può contenere delle definizioni di registro per i registri utente esistenti su qualsiasi piattaforma. Ad esempio, un dominio gestito da un'unità di controllo del dominio su i5/OS potrebbe contenere delle definizioni di registro per piattaforme non i5/OS (come un registro AIX). Sebbene sia possibile definire un qualsiasi registro utente su un dominio EIM, è necessario definire i registri utente per quelle applicazioni e sistemi operativi abilitati all'EIM.

È possibile denominare una definizione di registro EIM come si desidera, a condizione che il nome sia univoco nel dominio EIM. È ad esempio possibile denominare la definizione di registro EIM in base al nome del sistema sul quale si trova il registro utenti. Se questo non è sufficiente per distinguere una definizione di registro da definizioni simili, è possibile utilizzare un punto (.) oppure un segno di sottolineatura (_) per aggiungere il tipo di registro utenti che si sta definendo. Indipendentemente dai criteri che si sceglie di utilizzare, sarebbe opportuno sviluppare una convenzione di denominazione per le proprie definizioni di registro EIM. Questo assicurerebbe che i nomi delle definizioni sono congruenti nell'ambito del dominio e che descrivono in modo adeguato il tipo e l'istanza del registro utenti definito ed il modo in cui è utilizzato. È ad esempio possibile scegliere il nome di ciascuna definizione di registro utilizzando una combinazione del nome dell'applicazione o del sistema operativo utilizzati dal registro e della posizione fisica del registro utenti all'interno della propria azienda.

Un'applicazione compilata per utilizzare EIM può specificare un alias di registro di origine, un alias di registro di destinazione, oppure degli alias per entrambi. Quando si creano delle definizioni di registro EIM, è necessario controllare la documentazione per le applicazioni per determinare se occorre specificare uno o più alias per le definizioni di registro. Quando si assegnano questi alias alle definizioni dei registri, l'applicazione può eseguire una ricerca alias per rilevare la definizione o le definizioni di registro EIM corrispondenti agli alias presenti nell'applicazione.

La seguente parte campione del foglio di lavoro per la pianificazione potrebbe risultare utile per registrare le informazioni sui registri utenti partecipanti. È possibile utilizzare il foglio di lavoro effettivo per specificare un nome di definizione di registro per ciascun registro utenti, per specificare se utilizza un alias e per descrivere la posizione del registro utenti ed il suo utilizzo. La documentazione relativa all'installazione ed alla configurazione per l'applicazione fornirà alcune delle informazioni di cui si ha bisogno per il foglio di lavoro.

Tabella 14. Foglio di lavoro di esempio per la pianificazione delle informazioni sulle definizioni di registro EIM

Nome definizione di registro	**Tipo registro utenti**	**Alias della definizione di registro**	**Descrizione del registro**
System_C	Registro utenti di sistema i5/OS	Consultare la documentazione dell'applicazione	Registro utenti principale per i5/OS sul Sistema C
System_A_WAS	LTPA WebSphere	app_23_alias_source	Registro utenti LTPA WebSphere sul Sistema A
System_B	Linux	Consultare la documentazione dell'applicazione	Registro utenti Linux sul Sistema B

Tabella 14. Foglio di lavoro di esempio per la pianificazione delle informazioni sulle definizioni di registro EIM (Continua)

Nome definizione di registro	Tipo registro utenti	Alias della definizione di registro	Descrizione del registro
System_A	Registro utenti di sistema i5/OS	app_23_alias_target app_xx_alias_target	Registro utenti di sistema principale per i5/OS sul Sistema A
System_D	Registro utenti Kerberos	app_xx_alias_source	Dominio Kerberos legal.mydomain.com
System_4	Registro utenti Windows 2000	Consultare la documentazione dell'applicazione	Registro utenti dell'applicazione per la gestione del personale sul Sistema 4

Nota: i tipi di associazione per ciascun registro verranno determinati successivamente nel processo di pianificazione.

Dopo avere completato questa sezione del foglio di lavoro di pianificazione, sviluppare il proprio piano di corrispondenze delle identità per determinare se utilizzare associazioni di identificativi, associazioni normativa o entrambi i tipi di associazioni per creare le corrispondenze di cui si ha bisogno per le identità utente in ciascun registro utenti definito.

Sviluppo di un piano di corrispondenza delle identità

Una parte critica del processo di pianificazione dell'implementazione di EIM (Enterprise Identity Mapping) iniziale richiede che l'utente determini come desidera utilizzare la corrispondenza delle identità nella propria azienda.

Ci sono due metodi che è possibile utilizzare per la corrispondenza delle identità in EIM:

- Le **associazioni di identificativi** descrivono le relazioni tra un identificativo EIM e le identità utente nei registri utenti che rappresentano detta persona. Un'associazione di identificativi crea una corrispondenza uno-a-uno diretta tra un identificativo EIM ed una specifica identità utente. È possibile utilizzare le associazioni di identificativi per definire indirettamente una relazione tra identità utente tramite l'identificativo EIM.

  Se la propria normativa di sicurezza richiede un alto grado di responsabilità dettagliata, è possibile che occorra utilizzare quasi esclusivamente le associazioni di identificativi per la propria implementazione di corrispondenze delle identità. Poiché si utilizzano le associazioni di identità per creare delle corrispondenze uno-a-uno per le identità utente di proprietà degli utenti, è sempre possibile determinare esattamente chi ha eseguito un'azione su un oggetto o su quale sistema.
- Le **associazioni normativa** descrivono una relazione tra più identità utente ed una singola identità utente in un registro utenti. Le associazioni normativa utilizzano il supporto normativa corrispondenze EIM per creare corrispondenze molti-ad-uno tra identità utente senza coinvolgere un identificativo EIM.

  Le associazioni normativa possono essere utili quando si hanno uno o più grossi gruppi di utenti che devono accedere a sistemi o applicazioni nella propria azienda dove non si desidera che essi abbiano delle identità utente specifiche per accedere. Si ponga ad esempio il caso che si abbia un'applicazione Web che accede ad una specifica applicazione interna. Si potrebbe non volere impostare centinaia di migliaia di identità utente per autenticare gli utenti per quest'applicazione interna. In questa situazione, è possibile configurare la corrispondenza delle identità in modo tale che tutti gli utenti di quest'applicazione Web vengono messi in corrispondenza con una singola identità utente con il livello minimo di autorizzazione richiesto per eseguire l'applicazione. È possibile eseguire questo tipo di corrispondenza delle identità utilizzando le associazioni normativa.

L'utente potrebbe decidere di utilizzare le associazioni di identificativi per fornire il miglior controllo delle identità utente nella propria azienda ottenendo al tempo stesso il massimo grado di gestione semplificata delle parole d'ordine. In alternativa, potrebbe decidere di utilizzare una combinazione di associazioni normativa e associazioni di identificativi per semplificare l'SSO, dove appropriato, conservando al tempo stesso il controllo specifico sulle identità utente per gli amministratori. Indipendentemente dal tipo di corrispondenza delle identità che si decide risponda meglio alle proprie esigenze aziendali e meglio si adatti alla propria normativa di sicurezza, è necessario creare un piano di corrispondenza delle identità per assicurarsi di implementare la corrispondenza delle identità in modo appropriato.

Per creare un piano di corrispondenza delle identità, è necessario procedere nel seguente modo:

Concetti correlati

"Creazione di associazioni EIM" a pagina 108
È possibile creare due tipi di associazioni EIM diverse. È possibile creare un'associazione identificativo o un'associazione normativa.

"Creazione di un'associazione normativa" a pagina 110
Un'associazione normativa fornisce un metodo per definire direttamente una relazione tra più identità utente in uno o più registri ed una singola identità utente di destinazione in un altro registro.

Pianificazione delle associazioni di EIM:

Le associazioni sono delle voci che l'utente crea in un dominio EIM (Enterprise Identity Mapping) per definire una relazione tra le identità utente in registri utenti differenti.

È possibile creare due tipi di associazioni in EIM: le associazioni identificativo, per definire delle associazioni uno-a-uno, e le associazioni normativa, per definire delle associazioni molti-a-uno. È possibile utilizzare associazioni normativa invece di, oppure insieme ad, associazioni identificativo.

I tipi specifici di associazioni che si sceglie di creare dipendono da come un utente utilizza una specifica identità utente e della propria pianificazione delle associazioni di identità generale.

È possibile creare uno qualsiasi dei seguenti tipi di associazioni identificativo:

- **Associazioni di destinazione**

  Si definiscono delle associazioni di destinazione per gli utenti che di norma accedono a questo sistema colo come un server da qualche altro sistema client. Questo tipo di associazione viene utilizzato quando un'applicazione esegue delle operazioni di ricerca di corrispondenze.
- **Associazioni di origine**

  Si definiscono delle associazioni di origine quando l'identità utente è la prima che un utente fornisce per collegarsi al sistema o alla rete. Questo tipo di associazione viene utilizzato quando un'applicazione esegue delle operazioni di ricerca di corrispondenze.
- **Associazioni amministrative**

  Si definiscono delle associazioni amministrative quando si desidera potere tenere traccia del fatto che l'identità utente appartenga ad uno specifico utente ma non si desidera che l'identità utente sia disponibile per le operazioni di ricerca di corrispondenze. È possibile utilizzare questo tipo di associazione per tenere traccia di tutte le identità utente utilizzate da una persona nell'azienda.

Un'**associazione normativa** definisce sempre un'associazione di destinazione.

Una singola definizione di registro può avere più di un tipo di associazione, in base al modo in cui è utilizzato il registro utenti cui fa riferimento. Anche se non ci sono limiti né al numero né alle combinazioni di associazioni che è possibile definire, tenere questo numero al minimo per semplificare l'amministrazione del proprio dominio EIM.

Di norma, un'applicazione fornirà delle indicazioni su quali definizioni di registro prevede per i registri di origine e di destinazione, ma non sui tipi di associazione. Ciascun utente finale dell'applicazione deve essere messo in corrispondenza con l'applicazione da almeno un'associazione. Quest'associazione può essere una messa in corrispondenza uno-a-uno tra il loro identificativo EIM univoco ed un'identità utente nel registro di destinazione richiesto oppure una messa in corrispondenza molti-a-uno tra un registro di origine di cui l'identità utente è un membro e il registro di destinazione richiesto. Il tipo di associazione utilizzato dipende dai propri requisiti di messa in corrispondenza delle identità e dai criteri forniti dall'applicazione.

In precedenza, come parte del processo di pianificazione, si sono completati due fogli di lavoro per la pianificazione per le identità utente nella propria organizzazione con le informazioni sugli identificativi EIM e le definizioni di registro EIM necessari. È adesso necessario associare queste informazioni specificando i tipi di associazione che si desidera utilizzare per mettere in corrispondenza le identità utente nella propria azienda. È necessario determinare se definire un'associazione normativa per una specifica applicazione e per il relativo registro di utenti oppure se definire delle associazioni di identificativi specifiche (di origine, di destinazione e amministrative) per ciascuna identità utente nel registro applicazione o di sistema. È possibile farlo registrando le informazioni sui tipi di associazione richiesti sia nel foglio di lavoro per la pianificazione delle definizioni di registro che nelle corrispondenti righe del foglio di lavoro di ciascuna associazione.

Per completare il proprio piano di messa in corrispondenza delle identità, è possibile utilizzare i seguenti fogli di lavoro di esempio come un ausilio nella registrazione delle informazioni sulle associazioni di cui si ha bisogno per descrivere un quadro completo di come si pianifica l'implementazione della messa in corrispondenza delle identità.

Tabella 15. Foglio di lavoro di esempio per la pianificazione delle informazioni sulle definizioni di registro EIM

Nome definizione di registro	**Tipo registro utenti**	**Alias della definizione di registro**	**Descrizione del registro**	**Tipi di associazione**
System_C	Registro utenti di sistema i5/OS	Consultare la documentazione dell'applicazione	Registro utenti principale per i5/OS sul Sistema C	Destinazione
System_A_WAS	LTPA WebSphere	app_23_alias_source	Registro utenti LTPA WebSphere sul Sistema A	Principalmente di origine
System_B	Linux	Consultare la documentazione dell'applicazione	Registro utenti Linux sul Sistema B	Di origine e di destinazione
System_A	Registro utenti di sistema i5/OS	app_23_alias_target app_xx_alias_target	Registro utenti di sistema principale per i5/OS sul Sistema A	Destinazione
System_D	Registro utenti Kerberos	app_xx_alias_source	Dominio Kerberos legal.mydomain.com	Origine
System_4	Registro utenti Windows 2000	Consultare la documentazione dell'applicazione	Registro utenti dell'applicazione per la gestione del personale sul Sistema 4	Amministrativa
order.mydomain.com	Registro utenti Windows 2000		Registro di accesso principale per i dipendenti del reparto ordini	Normativa registro predefinita (registro di origine)

Tabella 15. Foglio di lavoro di esempio per la pianificazione delle informazioni sulle definizioni di registro EIM (Continua)

Nome definizione di registro	Tipo registro utenti	Alias della definizione di registro	Descrizione del registro	Tipi di associazione
System_A_order_app	Applicazione reparto ordini		Registro specifico per l'applicazione per gli aggiornamenti degli ordini	Normativa registro predefinita (registro di destinazione)
System_C_order_app	Applicazione reparto ordini		Registro specifico per l'applicazione per gli aggiornamenti degli ordini	Normativa registro predefinita (registro di destinazione)

Tabella 16. Foglio di lavoro di esempio della pianificazione degli identificativi EIM

Nome identificativo univoco	Descrizione identificativo o identità utente	Alias identificativo
John S Day	Responsabile della gestione del personale	app_23_admin
John J Day	Dipartimento legale	app_xx_admin
Sharon A. Jones	Amministratore reparto ordini	

Tabella 17. Foglio di lavoro di esempio per la pianificazione delle associazioni di identificativi

Nome univoco identificativo: _____John S Day_____		
Registro utente	**Identità utente**	**Tipi di associazione**
Sistema A WAS su Sistema A	johnday	Origine
Linux su Sistema B	jsd1	Di origine e di destinazione
i5/OS su Sistema C	JOHND	Destinazione
Registro 4 su Windows 2000 sistema di gestione del personale	JDAY	Amministrativa

Tabella 18. Foglio di lavoro di esempio per la pianificazione delle associazioni normativa

Tipo di associazione normativa	Registro utenti origine	Registro utenti di destinazione	Identità utente	Descrizione
Registro predefinito	order.mydomain.com	System_A_order_app	SYSUSERA	Mette in corrispondenza l'utente del reparto ordini autenticato Windows con l'appropriata identità utente applicazione
Registro predefinito	order.mydomain.com	System_C_order_app	SYSUSERB	Mette in corrispondenza l'utente del reparto ordini autenticato Windows con l'appropriata identità utente applicazione

Sviluppo di un piano di denominazione degli identificativi EIM:

In fase di pianificazione delle proprie esigenze di corrispondenza di identità EIM, è possibile creare degli identificativi EIM univoci per gli utenti di applicazioni e di sistemi operativi abilitati a EIM nella propria azienda quando si desidera creare delle corrispondenze uno-a-uno tra le identità utente per un utente. Utilizzando le associazioni di identificativi per creare delle corrispondenze uno-a-uno, è possibile ottimizzare i vantaggi della gestione delle parole d'ordine fornita da EIM.

La pianificazione delle denominazioni in fase di sviluppo dipende dalle proprie esigenze e preferenze aziendali; il solo requisito per i nomi di identificativo EIM è che devono essere univoci. Alcune società potrebbero volere utilizzare il nome completo, legale, di una persona; altre società potrebbero preferire utilizzare un tipo diverso di dati, come ad esempio il numero impiegato di ciascuna persona. Se si desidera creare dei nomi di identificativo EIM basati sul nome completo di ciascuna persona, è possibile anticipare possibili duplicazioni di nomi. Il modo in cui si gestiscono i potenziali nomi identificativo duplicati è una questione di preferenze personali. È possibile che l'utente desideri gestire ciascun caso manualmente aggiungendo una stringa di caratteri predeterminata al ciascun nome identificativo per assicurare l'univocità; l'utente potrebbe ad esempio decidere di aggiungere il numero del reparto di ciascuna persona.

Come parte dello sviluppo di un piano di denominazione degli identificativi EIM, è necessario decidere il proprio piano di corrispondenza identità generale. Questo aiuta a decidere quando occorre utilizzare gli identificativi e le associazioni di identificativi invece delle associazioni normativa per le corrispondenze di identità nell'ambito della propria azienda. Per sviluppare il proprio piano di denominazione degli identificativi EIM, è possibile utilizzare il foglio di lavoro qui di seguito come ausilio nella raccolta delle informazioni sulle identità utente nella propria organizzazione e nella pianificazione degli identificativi EIM per le identità utente. Il foglio di lavoro rappresenta il tipo di informazioni di cui l'amministratore EIM deve essere a conoscenza quando crea gli identificativi EIM oppure le associazioni normativa per gli utenti di un'applicazione.

Tabella 19. Foglio di lavoro di esempio della pianificazione degli identificativi EIM

Nome identificativo univoco	**Descrizione identificativo o identità utente**	**Alias identificativo**
John S Day	Responsabile della gestione del personale	app_23_admin
John J Day	Dipartimento legale	app_xx_admin
Sharon A. Jones	Amministratore reparto ordini	

Un'applicazione scritta per utilizzare l'EIM può specificare un alias da essa utilizzato per trovare l'identificativo EIM appropriato, che può essere utilizzato dall'applicazione stessa per determinare a sua volta una specifica identità utente da utilizzare. Controllare la documentazione relativa alle proprie applicazioni per determinare se sia necessario specificare uno o più alias per l'identificativo. I campi relativi alla descrizione dell'identificativo EIM o dell'identità utente sono in formato libero e possono essere utilizzati per fornire delle informazioni descrittive sull'utente.

Non è necessario creare degli identificativi EIM per tutti i membri della propria azienda in una sola volta. Dopo avere creato un identificativo EIM iniziale e dopo averlo utilizzato per verificare la propria configurazione di EIM, è possibile creare degli identificativi EIM aggiuntivi basati sui fini della propria azienda inerenti l'utilizzo di EIM. È ad esempio possibile aggiungere degli identificativi EIM su una base dipartimentale o areale. In alternativa, è possibile aggiungere degli identificativi EIM quando si distribuiscono ulteriori applicazioni EIM.

Dopo avere raccolto le informazioni necessarie per sviluppare un piano di denominazione degli identificativi EIM, è possibile pianificare le associazioni per le proprie identità utente.

Fogli di lavoro per la pianificazione dell'implementazione di EIM

Durante l'esecuzione del processo di pianificazione di EIM (Enterprise Identity Mapping), potrebbe risultare utile servirsi di questi fogli di lavoro per raccogliere le informazioni che saranno necessarie per configura re ed utilizzare EIM nella propria azienda. Esempi di sezioni completate di questi fogli di lavoro sono forniti nelle pagine di pianificazione come appropriato.

Questi fogli di lavoro sono forniti come un esempio dei tipi di fogli di lavoro di cui si ha bisogno per creare il proprio piano di implementazione di EIM. Il numero di voci fornito è inferiore al numero che sarà probabilmente necessario per le proprie informazioni su EIM. È possibile modificare questi fogli di lavoro per adeguarli alla propria situazione.

Tabella 20. Foglio di lavoro delle informazioni sul dominio e sull'unità di controllo del dominio

Informazioni richieste per configurare il dominio e l'unità di controllo del dominio EIM	**Risposte**
Un nome significativo per il dominio. Questo potrebbe essere il nome di una società, di un reparto oppure di un'applicazione che utilizza il dominio.	
Facoltativo: Un DN (Distinguished Name) principale per il dominio. Questo è il DN che rappresenta la voce immediatamente precedente alla voce del nome dominio nella gerarchia con struttura ad albero delle informazioni dell'indirizzario, ad esempio `o=ibm,c=us`.	
Il DN di dominio EIM completo risultante. Questo è il nome completo del dominio EIM che descrive la posizione dell'indirizzario per i dati del dominio EIM. Il DN completo è formato, come minimo, dal DN di dominio (`ibm-eimDomainName=`), più il nome dominio specificato dall'utente. Se si sceglie di specificare un DN principale per il dominio, il DN di dominio completo sarà formato dal DN di dominio relativo (`ibm-eimDomainName=`), dal nome dominio (MyDomain) e dal DN principale (`o=ibm,c=us`).	
L'indirizzo di collegamento per l'unità di controllo del dominio. Consiste nel tipo di collegamento (ldap di base o ldap sicuro, ad esempio `ldap://` o `ldaps://`) più le seguenti informazioni:	
• Facoltativo: Il nome host o l'indirizzo IP • Facoltativo: Il numero di porta	
L'indirizzo di collegamento completo per l'unità di controllo del dominio risultante	
Il meccanismo di collegamento richiesto dalle applicazioni o dai sistemi. Le scelte includono: • Collegamento semplice • CRAM MD5 • Autenticazione server • Autenticazione client • Kerberos	

Consultare Pianificazione di un'unità di controllo del dominio EIM per un esempio di come utilizzare questo foglio di lavoro.

Tabella 21. Foglio di lavoro per la pianificazione delle identità di collegamento

Autorizzazione o ruolo EIM	Identità di associazione	Meccanismo di associazione	Per cosa è richiesto

Consultare Pianificazione di un'unità di controllo del dominio EIM per un esempio di come utilizzare questo foglio di lavoro.

Tabella 22. Foglio di lavoro per la pianificazione delle informazioni sulle definizioni di registro

Nome definizione di registro	Tipo registro utenti	Alias della definizione di registro	Descrizione del registro	Tipi di associazione

Consultare Sviluppo di un piano di denominazione delle definizioni di registro EIM per un esempio di come utilizzare questo foglio di lavoro.

Tabella 23. Foglio di lavoro per la pianificazione degli identificativi EIM

Nome identificativo univoco	Descrizione identificativo o identità utente	Alias identificativo

Tabella 23. Foglio di lavoro per la pianificazione degli identificativi EIM (Continua)

Consultare Sviluppo di un piano di denominazione degli identificativi EIM per un esempio di come utilizzare questo foglio di lavoro.

Tabella 24. Foglio di lavoro per la pianificazione delle associazioni di identificativi

Nome univoco identificativo: _____John S Day_____		
Registro utente	Identità utente	Tipi di associazione

Consultare Pianificazione delle associazioni EIM per un esempio di come utilizzare questo foglio di lavoro.

Tabella 25. Foglio di lavoro per la pianificazione delle associazioni normativa

Tipo di associazione normativa	Registro utenti di origine	Registro utenti di destinazione	Identità utente	Descrizione

Consultare Pianificazione delle associazioni EIM per un esempio di come utilizzare questo foglio di lavoro.

Pianificazione dello sviluppo delle applicazioni EIM

Per consentire ad un'applicazione di utilizzare EIM (Enterprise Identity Mapping) e partecipare ad un dominio, l'applicazione deve essere in grado di utilizzare le API EIM.

Consultare la documentazione relativa alle API EIM e la documentazione EIM specifica per la piattaforma per determinare se ci sono delle considerazioni di pianificazione speciali che è necessario comprendere quando si scrivono o si adattano delle applicazioni per utilizzare le API EIM. Ci potrebbero essere ad esempio delle considerazioni relative alla compilazione, e di altra natura, per le applicazioni C o C++ che eseguono delle chiamate alle API EIM. In base alla piattaforma dell'applicazione, ci potrebbero anche essere delle considerazioni di modifica dei collegamenti, o di altra natura.

Attività correlate

"API di EIM" a pagina 133
EIM (Enterprise Identity Mapping) fornisce il mezzo per la gestione delle identità degli utenti tra più

piattaforme. EIM dispone di più API (application programming interface) che possono essere utilizzate dalle applicazioni per eseguire operazioni EIM al posto dell'applicazione o di un'applicazione utente.

Pianificazione di Enterprise Identity Mapping per i5/OS

Ci sono più tecnologie e servizi che EIM (Enterprise Identity Mapping) comprende sulla piattaforma System i. Prima di configurare EIM sul proprio server, è necessario decidere la funzionalità che si desidera implementare utilizzando le capacità di EIM e di SSO.

Prima di implementare EIM, è necessario decidere i requisiti di sicurezza di base per la rete e aver implementato tali misure di sicurezza. EIM fornisce gli amministratori e agli utente una gestione dell'identità più semplice nell'ambito della società. Quando viene utilizzato con il servizio di autenticazione di rete, EIM fornisce alla società capacità di SSO.

Se si pianifica l'utilizzo di Kerberos per autenticare gli utenti come parte di un'implementazione con SSO, è necessario configurare anche il servizio di autenticazione di rete.

Per ulteriori informazioni su come pianificare la configurazione EIM dei propri sistemi, consultare le seguenti informazioni:

Informazioni correlate

Pianificazione del servizio di autenticazione di rete

Prerequisiti di installazione di EIM per i5/OS

Il foglio di lavoro per la pianificazione identifica i servizi da installare prima di configurare EIM.

Tabella 26. Foglio di lavoro per la pianificazione dell'installazione di EIM

Foglio di lavoro per la pianificazione dei prerequisiti di EIM	**Risposte**
Sul sistema è in esecuzione i5/OS V5R4, o successiva?	
Le opzioni ed i prodotti su licenza di seguito indicati sono installati sul sistema? • i5/OS Host Servers (5761-SS1 Opzione 12) • System i Access per Windows (5761-XE1) • Qshell Interpreter (5761-SS1 Opzione 30) Necessario se si intende configurare il servizio di autenticazione di rete e EIM. **Nota:** 5722 è il codice prodotto delle opzioni e dei prodotti i5/OS, precedenti a V6R1.	
System i Navigator è installato sul PC dell'amministratore, compresi i seguenti sottocomponenti? • Rete • Sicurezza(Necessaria se si intende configurare il servizio di autenticazione di rete e EIM)	
Si è installato il service pack System i Access per Windows più recente? Per il service pack più recente, consultare System i Access	
Se un server di indirizzario, ad esempio IBM Tivoli Directory Server per i5/OS è attualmente configurato e si desidera utilizzarlo come unità di controllo del dominio EIM, si conoscono la parola d'ordine e il DN (distinguished name) amministratore LDAP?	
Se un server di indirizzario è attualmente configurato, può essere temporaneamente arrestato? (Ciò richiederà il completamento del processo di configurazione di EIM.)	
Si dispone delle autorizzazioni speciali *SECADM, *ALLOBJ e *IOSYSCFG?	
Sono state applicate le ultime PTF?	

Installazione delle opzioni System i Navigator richieste

Per abilitare un ambiente con SSO con EIM (Enterprise Identity Mapping) e il servizio di autenticazione di rete, è necessario installare sia l'opzione **Rete** che l'opzione **Sicurezza** di System i Navigator.

EIM si trova nell'opzione **Rete** e il servizio di autenticazione di rete si trova nell'opzione **Sicurezza**. Se non si pianifica l'utilizzo del servizio di autenticazione di rete nella propria rete, non è necessario installare l'opzione **Sicurezza** di System i Navigator.

Per installare l'opzione Rete di System i Navigator o per verificare che questa opzione sia attualmente installata, assicurarsi che System i Access per Windows sia installato sul PC che si sta utilizzando per amministrare il modello System i .

Per installare l'opzione **Rete**:

1. Fare clic su **Avvia > Programmi > System i Access per Windows > Installazione selettiva**.
2. Seguire le istruzioni riportate sulla finestra di dialogo. Sulla finestra di dialogo **Selezione componente**, espandere **System i Navigator** e poi selezionare l'opzione **Rete**. Se si intende utilizzare il servizio di autenticazione di rete, è necessario selezionare anche l'opzione **Sicurezza**.
3. Continuare con il resto dell'**Installazione selettiva**.

Informazioni correlate

Servizio di autenticazione di rete (NAS)

Considerazioni sulla copia di riserva ed il ripristino per EIM

Occorre sviluppare un piano per la copia di riserva ed il ripristino per i dati EIM (Enterprise Identity Mapping) per assicurare che i dati EIM siano protetti e possano essere ripristinati nel caso in cui si verifichi un problema con il server indirizzario dove si trova l'unità di controllo di dominio EIM. Ci sono anche delle informazioni sulla configurazione EIM necessarie per comprendere come eseguire il ripristino.

Informazioni correlate

Replica server indirizzario

Attività di replica

Considerazioni sul ripristino e il salvataggio del server indirizzario

Copia di riserva e ripristino dei dati di dominio EIM:

Il modo in cui si salvano i dati EIM dipende da come si decide di gestire quest'aspetto del server di indirizzario che funge da unità di controllo del dominio per i propri dati EIM.

Un modo per eseguire la copia di riserva dei dati, soprattutto ai fini di un ripristino di emergenza, consiste nel salvare la libreria dei database. Per impostazione predefinita, questa è `QUSRDIRDB`. Se `changelog` è abilitato, bisogna salvare anche la libreria `QUSRDIRCL`. Il server di indirizzario sul sistema dove si desidera ripristinare la libreria deve avere lo stesso schema e la stessa configurazione LDAP del server di indirizzario originale. I file che memorizzano queste informazioni si trovano in `/QIBM/UserData/OS400/DirSrv`. I dati di configurazione aggiuntivi si trovano in `QUSRSYS/QGLDCFG` (oggetto `*USRSPC`) e `QUSRSYS/QGLDVLDL` (oggetto `*VLDL`). Per disporre di una copia di riserva completa di tutto per il server di indirizzario, è necessario salvare entrambe le librerie, i file IFS (Integrated System File) e gli oggetti `QUSRSYS`.

È ad esempio possibile utilizzare un file LDIF per salvare integralmente o parzialmente il contenuto del server di indirizzario. Per eseguire la copia di riserva delle informazioni sul dominio per un IBM Tivoli Directory Server per un'unità di controllo del dominio per i5/OS, attenersi alla seguente procedura:

1. In System i Navigator, espandere **Rete > Server > TCP/IP**.
2. Fare clic con il tasto destro del mouse su **Server indirizzario**, selezionare **Strumenti** e selezionare quindi **Esporta file** per visualizzare una pagina che consente di specificare quali parti del contenuto del server di indirizzario esportare in un file.

3. Trasferire il file di esportazione sulla piattaforma System i che si desidera utilizzare come server di indirizzario di riserva.
4. In System i Navigator sul server di riserva, espandere **Rete > Server > TCP/IP**.
5. Fare clic con il tasto destro del mouse su **Server indirizzario**, selezionare **Strumenti** e selezionare quindi **Importa** per caricare il contenuto del file trasferito sul nuovo server di indirizzario.

Un altro metodo da prendere in considerazione per salvare i propri dati di dominio EIM consiste nel configurare ed utilizzare un server di indirizzario di replica. Tutte le modifiche apportati ai dati di dominio EIM vengono automaticamente inoltrate al server di indirizzario di replica; in questo modo, se si verifica un malfunzionamento del server di indirizzario dove si trova l'unità di controllo di dominio oppure se detto server perde dei dati EIM, è possibile richiamare i dati dal server di replica.

Come configurare ed utilizzare un server di indirizzario di replica varia in base al tipo di modello di replica che sceglie di utilizzare.

Copia di riserva e ripristino delle informazioni di configurazione di EIM:

Se si verifica un malfunzionamento del sistema, potrebbe essere necessario ripristinare le relative informazioni di configurazione EIM. Queste informazioni non possono essere salvate e ripristinate facilmente da un sistema all'altro.

L'utente dispone di queste opzioni per salvare e ripristinare la configurazione EIM:

- Utilizzare il comando di salvataggio dei dati di sicurezza (SAVSECDTA) su ciascun sistema per salvare le informazioni di configurazione EIM e altre importanti informazioni di configurazione. Ripristinare quindi l'oggetto di profilo utente QSYS su ciascun sistema.

  Nota: è necessario utilizzare il comando SAVSECDTA e ripristinare l'oggetto di profilo utente QSYS su ciascun sistema con una configurazione EIM singolarmente. È possibile che si verifichino dei problemi se si tenta di recuperare l'oggetto di profilo utente QSYS su un sistema se è stato salvato su un sistema differente.
- Eseguire nuovamente il wizard di Configurazione di EIM oppure aggiornare manualmente le proprietà della cartella relativa alla configurazione di EIM. Per semplificare questo processo, salvare i fogli di lavoro per la pianificazione dell'implementazione di EIM oppure eseguire una registrazione delle informazioni di configurazione EIM per ciascun sistema.

Occorre inoltre valutare e pianificare come eseguire la copia di riserva ed il ripristino dei dati del servizio di autenticazione di rete se si è configurato questo servizio come parte dell'implementazione di un ambiente con SSO.

Configurazione di EIM

Il Wizard di configurazione EIM consente di completare in modo facile e rapido, una configurazione EIM di base per il sistema. Il wizard fornisce tre opzioni di configurazione del sistema EIM.

La modalità di utilizzo del wizard per la configurazione di EIM su un sistema specifico varia a seconda della gestione totale di EIM all'interno dell'azienda e delle proprie necessità di configurazione di EIM. Ad esempio, molti amministratori desiderano utilizzare EIM insieme al servizio di autenticazione di rete per creare un ambiente con SSO tra più sistemi e piattaforme senza dovere modificare le normative di sicurezza sottostanti. Di conseguenza, il wizard di configurazione di EIM consente di configurare il servizio di autenticazione di rete come parte della configurazione EIM. Tuttavia, la configurazione e l'utilizzo del servizio di autenticazione di rete non è un prerequisito o un requisito per la configurazione e l'utilizzo di EIM.

Prima di iniziare il processo di configurazione EIM per uno o più sistemi, pianificare la propria implementazione di EIM per raccogliere le informazioni necessarie. Ad esempio, è necessario prendere decisioni sui seguenti punti:

- Quale piattaforma System i si desidera configurare come unità di controllo dominio EIM per il dominio EIM? Utilizzare il wizard Configurazione EIM per creare un nuovo dominio prima su questo sistema, quindi utilizzare il wizard per configurare tutti i sistemi aggiuntivi da unire a questo dominio.
- Si desidera configurare il servizio di autenticazione di rete su ogni sistema che si configura per EIM? In questo caso, è possibile utilizzare il wizard Configurazione EIM per creare una configurazione servizio di autenticazione di rete di base su ogni modello System i. Tuttavia, è necessario eseguire altre attività per completare la configurazione del servizio autenticazione di rete.

Dopo aver utilizzato il wizard di configurazione di EIM per creare una configurazione di base per ciascuna piattaforma System i, è necessario ancora effettuare alcune operazioni di configurazione EIM per disporre di una configurazione EIM completa. Consultare Scenario: Abilitazione dell'SSO per un esempio che illustra come una società fittizia ha configurato un ambiente con SSO utilizzando il servizio di autenticazione di rete e EIM.

Per configurare EIM, è necessario disporre di tutte le seguenti autorizzazioni speciali:

- Responsabile della sicurezza (*SECADM).
- Tutti gli oggetti (*ALLOBJ).
- Configurazione di sistema (*IOSYSCFG).

Prima di utilizzare il wizard di configurazione di EIM, è necessario avere completato tutti i "Pianificazione di EIM (Enterprise Identity Mapping)" a pagina 53 passi per determinare esattamente come si utilizzerà EIM. Se si sta configurando EIM come parte della creazione di un ambiente con SSO, completare anche tutta la pianificazione dell'SSO.

Per accedere al wizard di configurazione di EIM, seguire i passi riportati di seguito:

1. Avviare System i Navigator.
2. Collegarsi al sistema per cui si desidera configurare EIM. Se si sta configurando EIM per più di un sistema, iniziare con quello su cui si desidera configurare l'unità di controllo del dominio per EIM.
3. Espandere **Rete → EIM (Enterprise Identity Mapping)**.
4. Fare clic con il tasto destro del mouse su **Configurazione** e selezionare **Configura** per avviare il wizard Configurazione EIM.
5. Selezionare un'opzione di configurazione EIM e seguire le istruzioni fornite per completare il wizard.
6. Fare clic su **?**, se necessario, per determinare le informazioni da specificare durante l'esecuzione del wizard.

Dopo avere completato la propria pianificazione, è possibile utilizzare il wizard di configurazione di EIM per creare una delle tre configurazioni EIM di base. È possibile utilizzare il wizard per unire un dominio esistente o per creare e partecipare a un nuovo dominio. Quando si utilizza il wizard di configurazione di EIM per creare ed unire un nuovo dominio, è possibile scegliere se configurare un'unità di controllo dominio EIM su un sistema locale o remoto. Le seguenti informazioni forniscono istruzioni per la configurazione di EIM in base al tipo di configurazione EIM di base di cui si ha bisogno:

Informazioni correlate

Servizio di autenticazione di rete (NAS)

SSO (Single sign-on)

Creazione e partecipazione ad un nuovo dominio locale

Quando si utilizza il wizard di configurazione di EIM per creare e partecipare a un nuovo dominio, è possibile scegliere di configurare l'unità di controllo del dominio EIM sul sistema locale come parte della creazione della configurazione EIM.

Se necessario, il wizard di configurazione di EIM assicura che verranno fornite le informazioni di configurazione di base del server indirizzario. Inoltre, se Kerberos non è attualmente configurato sulla piattaforma System i, il wizard richiede l'avvio del wizard Configurazione servizio autenticazione di rete.

Dopo avere completato il wizard di configurazione di EIM, è possibile eseguire le seguenti attività:
- Creare un nuovo dominio EIM.
- Configurare un server di indirizzario locale che agisca come un'unità di controllo del dominio EIM.
- Configurare il servizio di autenticazione di rete per il sistema.
- Creare le definizioni di registro EIM per il registro locale i5/OS ed il registro Kerberos.
- Configurare il sistema in modo che partecipi al nuovo dominio EIM.

Per configurare il sistema in modo da creare e partecipare a un nuovo dominio EIM, è necessario disporre di tutte le seguenti autorizzazioni speciali:
- Responsabile della sicurezza (*SECADM).
- Tutti gli oggetti (*ALLOBJ).
- Configurazione di sistema (*IOSYSCFG).

Per utilizzare il wizard di configurazione di EIM per creare e partecipare a un nuovo dominio locale, effettuare le seguenti operazioni:

1. In System i Navigator, selezionare il sistema per cui si desidera configurare EIM ed espandere **Rete > EIM (Enterprise Identity Mapping)**.
2. Fare clic con il tasto destro del mouse su **Configurazione** e selezionare **Configura** per per avviare il wizard Configurazione EIM.

   Nota: quest'opzione è etichettata **Riconfigura** se EIM è stato configurato precedentemente sul sistema.
3. Sulla pagina di **Benvenuto** del wizard, selezionare **Creazione e collegamento di un nuovo dominio** e fare clic su **Avanti**.
4. Nella pagina **Specifica ubicazione dominio EIM**, selezionare **Sul server dell'indirizzario locale** e fare clic su **Avanti**.

   Nota: questa opzione configura il server indirizzario locale in modo che agisca come unità di controllo dominio EIM. Poiché questo server indirizzario memorizza tutti i dati EIM per il dominio, deve essere attivo e rimanere attivo per supportare le ricerche di corrispondenze EIM ed altre operazioni.

   Se il servizio di autenticazione di rete non è attualmente configurato sulla piattaforma System i, o se sono richieste ulteriori informazioni di configurazione dell'autenticazione di rete per configurare un ambiente a collegamento singolo (SSO), viene visualizzata la pagina **Configurazione servizi autenticazione di rete**. Questa pagina consente di avviare il wizard Configurazione servizio autenticazione di rete con il quale l'utente può configurare il servizio di autenticazione di rete. È anche possibile configurare il Sevizio autenticazione di rete in un secondo momento utilizzando il wizard di configurazione per questo servizio tramite System i Navigator. Una volta completata la configurazione del servizio di autenticazione di rete, il wizard di configurazione di EIM proseguirà.
5. Per configurare il servizio di autenticazione di rete, attenersi alla seguente procedura:
   a. Sulla pagina **Configura servizio di autenticazione di rete**, selezionare **Sì** per avviare il wizard Configurazione servizio autenticazione di rete. In questo wizard, è possibile configurare varie interfacce e vari servizi i5/OS in modo che partecipino ad un dominio Kerberos e configurare un ambiente a collegamento singolo (SSO) che utilizza sia EIM che il servizio di autenticazione di rete.

b. Sulla pagina **Specifica di informazioni sul dominio**, specificare il nome del dominio predefinito nel campo **Dominio predefinito**. Se si sta utilizzando l'autenticazione Microsoft Active Directory per Kerberos, selezionare **Microsoft Active Directory viene utilizzato per l'autenticazione Kerberos** e fare clic su **Avanti**.

c. Sulla pagina **Specifica informazioni KDC**, specificare il nome completo del server Kerberos per quest'ambito nel campo **KDC**, specificare 88 nel campo **Porta** e fare clic su **Avanti**.

d. Sulla pagina **Specifica informazioni server parola d'ordine**, selezionare **Sì** o **No** per impostare un server parola d'ordine. Il server parola d'ordine consente ai principal di modificare le parole d'ordine sul server Kerberos. Se si seleziona **Sì**, immettere il nome del server parola d'ordine nel campo **Server parola d'ordine**. Nel campo **Porta**, accettare il valore predefinito di 464 e fare clic su Avanti.

e. Sulla pagina **Selezione voci keytab**, selezionare **Autenticazione Kerberos i5/OS** e fare clic su **Avanti**.

   Nota: è inoltre possibile creare delle voci keytab per IBM Tivoli Directory Server per i5/OS, i5/OS NetServer e IBM HTTP Server per i5/OS if se si desidera che questi servizi utilizzino l'autenticazione Kerberos. È possibile che occorra eseguire delle operazioni di configurazione aggiuntive per questi servizi per consentire loro di potere utilizzare l'autenticazione Kerberos.

f. Sulla pagina **Creazione voce keytab i5/OS**, immettere e confermare la parola d'ordine e fare clic su **Avanti**. Questa è la stessa parola d'ordine che si utilizzerà quando si aggiungeranno i principal i5/OS al server Kerberos.

g. Opzionale: Sulla pagina **Creazione file batch**, selezionare **Sì**, specificare le seguenti informazioni e fare clic su **Avanti**:

   - Nel campo **File batch**, aggiornare il percorso di indirizzario. Fare clic su **Sfoglia** per individuare il percorso di indirizzario appropriato oppure modificare il percorso nel campo **File batch**.
   - Nel campo **Includi parola d'ordine**, selezionare **Sì**. Questo assicura che tutte le parole d'ordine associate al principal di servizio i5/OS siano incluse nel file batch. È importante notare che le parole d'ordine sono visualizzate senza essere crittografate e possono essere lette da chiunque disponga di accesso in lettura al file batch. È pertanto essenziale cancellare il file batch dal server Kerberos e dal PC immediatamente dopo averlo utilizzato. Se non si include la parola d'ordine, all'utente verrà richiesta quando si esegue il file batch.

     Nota: è anche possibile aggiungere manualmente i principal di servizio generati dal wizard a Microsoft Active Directory. Per ulteriori informazioni su come eseguire quest'operazione, consultare la sezione relativa all' Aggiunta di principal i5/OS al server Kerberos

   - Sulla pagina **Riepilogo**, controllare i dettagli della configurazione del servizio di autenticazione di rete e fare clic su **Fine** per tornare al wizard di configurazione di EIM.

6. Se il server indirizzario locale non è attualmente configurato, verrà visualizzata la pagina **Configura server indirizzario** quando riprenderà il wizard di configurazione di EIM. Fornire le seguenti informazioni per configurare il server indirizzario locale:

   Nota: se si configura il server indirizzario locale prima di utilizzare il wizard di configurazione di EIM, verrà invece visualizzata la pagina **Specifica l'utente per la connessione**. Utilizzare questa pagina per specificare il DN e la parola d'ordine per l'amministratore LDAP per assicurarsi che il wizard disponga delle autorizzazioni sufficienti per amministrare il dominio EIM e gli oggetti in esso e continuare con il passo successivo in questa procedura. Fare clic su **?**, se necessario, per determinare quali informazioni fornire per questa pagina.

   a. Nel campo **Porta**, accettare il numero porta predefinito 389 oppure specificare un numero porta diverso da utilizzare per comunicazioni EIM non sicure con il server indirizzario.

b. Nel campo **DN**, specificare il DN LDAP che identifica l'amministratore LDAP per il server indirizzario. Il wizard di configurazione di EIM crea questo DN di amministratore LDAP e lo utilizza per configurare il server indirizzario come unità di controllo del nuovo dominio che si sta creando.
c. Nel campo **Parola d'ordine**, specificare la parola d'ordine dell'amministratore LDAP.
d. Nel campo **Conferma parola d'ordine**, specificare di nuovo la parola d'ordine per convalidarla.
e. Fare clic su **Avanti**.

7. Sulla pagina **Specifica il dominio**, fornire le seguenti informazioni:
   a. Nel campo **Dominio**, specificare il nome del dominio EIM che si desidera creare. Accettare il nome predefinito di `EIM` oppure utilizzare una qualsiasi stringa di caratteri di senso compiuto per l'utente. Tuttavia, non è possibile utilizzare caratteri speciali come `= + < > , # ; \` e *.
   b. Nel campo **Descrizione**, inserire il testo per descrivere il dominio.
   c. Fare clic su **Avanti**.
8. Sulla pagina **Specifica DN principale per il dominio**, selezionare **Sì** per specificare un DN principale per il dominio che si sta creando oppure specificare **No** per fare in modo che i dati EIM vengano memorizzati in un'ubicazione indirizzario con un suffisso il cui nome è derivato dal nome di dominio EIM.

   Nota: quando si crea un dominio su un server indirizzario locale, il DN principale è facoltativo. Specificando un DN principale, è possibile specificare dove devono trovarsi i dati EIM dello spazio del nome LDAP locale. Quando non si specifica un DN principale, i dati EIM si trovano nel proprio suffisso nello spazio del nome. Se si seleziona **Sì**, utilizzare la casella di elenco per selezionare il suffisso LDAP locale da utilizzare come DN principale oppure immettere il testo per creare e denominare un nuovo DN principale. Non è necessario specificare un DN principale per il nuovo dominio. Fare clic su **?** per ulteriori informazioni sull'utilizzo di un DN principale.
9. Sulla pagina **Informazioni sul registro**, specificare se aggiungere i registri utenti locali al dominio EIM come definizioni di registro. Selezionare uno di questi tipi di registri utenti oppure entrambi:

   Nota: non è necessario creare le definizioni di registro adesso. Se si sceglie di creare le definizioni di registro in un secondo momento, occorre aggiungere le definizioni di registro di sistema e aggiornare le proprietà di configurazione di EIM.
   a. Selezionare **i5/OS locale** per aggiungere una definizione di registro per il registro locale. Nel campo fornito, accettare il valore predefinito per il nome di definizione di registro oppure specificare un valore differente. Il nome registro EIM è una stringa arbitraria che rappresenta il tipo di registro e l'istanza specifica di tale registro.
   b. Selezionare **Kerberos** per aggiungere una definizione di servizio per un registro Kerberos. Nel campo fornito, accettare il valore predefinito per il nome di definizione di registro oppure specificare un valore differente. Il nome di definizione di registro predefinito è lo stesso del nome di dominio. Accettando il nome predefinito ed utilizzando lo stesso nome di registro Kerberos del nome di dominio, è possibile migliorare le prestazioni nel richiamo delle informazioni dal registro. Selezionare **Le identità utente Kerberos sono sensibili al maiuscolo e minuscolo**, se necessario.
   c. Fare clic su **Avanti**.
10. Sulla pagina **Specifica l'utente di sistema EIM**, selezionare un **Tipo utente** che si desidera venga utilizzato dal sistema quando vengono eseguite operazioni EIM per conto delle funzioni di sistema operativo. Queste operazioni includono le ricerche delle corrispondenze e la cancellazione delle associazioni quando si cancella un profilo utente i5/OS locale. È possibile selezionare uno dei seguenti tipi di utente: **DN e parola d'ordine**, **File keytab e principal Kerberos** oppure **Principal e parola d'ordine Kerberos**. Il tipo di utente da selezionare varia a seconda della configurazione del sistema corrente. Ad esempio, se non è stato configurato il Servizio di autenticazione di rete (NAS-Network Authentication Service) per il sistema, è possibile che i tipi di utente Kerberos non

siano disponibili per la selezione. Il tipo di utente selezionato determina le altre informazioni che devono essere fornite per completare la pagina come segue:

Nota: è necessario specificare un utente correntemente definito nel server indirizzario che contiene l'unità di controllo dominio EIM. L'utente specificato deve disporre di privilegi per eseguire almeno la ricerca delle corrispondenze e la gestione registro di un registro utenti locale. Se l'utente specificato non dispone di tali privilegi, alcune funzioni del sistema operativo relative all'utilizzo del collegamento singolo (SSO) e alla cancellazione dei profili utente potrebbero avere esito negativo.

Se non si è creato il server indirizzario prima di eseguire questo wizard, il solo tipo utente che è possibile selezionare e **DN e parola d'ordine** ed il solo DN che è possibile specificare è il DN dell'amministratore LDAP.

- Se si seleziona **DN e parola d'ordine**, fornire le seguenti informazioni:
  - Nel campo **DN**, specificare il DN LDAP che identifica l'utente che verrà utilizzato dal sistema quando eseguirà le operazioni EIM.
  - Nel campo **Parola d'ordine**, specificare la parola d'ordine per il DN.
  - Nel campo **Conferma parola d'ordine**, specificare di nuovo la parola d'ordine per verificarla.
- Se si seleziona **Principal Kerberos e parola d'ordine**, fornire le seguenti informazioni:
  - Nel campo **Principal**, specificare il nome di principal Kerberos che verrà utilizzato dal sistema quando eseguirà le operazioni EIM
  - Nel campo **Dominio**, specificare il nome completo del dominio Kerberos di cui è membro il principal. Il nome del principal e del dominio identificano in modo univoco gli utenti Kerberos nel file keytab. Ad esempio, il principal `jsmith` nell'ambito `ordept.myco.com` è rappresentato nel file keytab come `jsmith@ordept.myco.com`.
  - Nel campo **Parola d'ordine**, immettere la parola d'ordine dell'utente.
  - Nel campo **Conferma parola d'ordine**, specificare di nuovo la parola d'ordine per verificarla.
- Se si seleziona **File keytab e principal Kerberos**, fornire le seguenti informazioni:
  - Nel campo **File keytab**, specificare il nome file keytab e il percorso completo in cui si trova il principal Kerberos che verrà utilizzato dal sistema quando eseguirà le operazioni EIM. In alternativa, fare clic su **Sfoglia** per ricercare negli indirizzari dell'IFS System i e selezionare un file keytab.
  - Nel campo **Principal**, specificare il nome di principal Kerberos che verrà utilizzato dal sistema quando eseguirà le operazioni EIM.
  - Nel campo **Dominio**, specificare il nome completo del dominio Kerberos di cui è membro il principal. Il nome del principal e del dominio identificano in modo univoco gli utenti Kerberos nel file keytab. Ad esempio, il principal `jsmith` nell'ambito `ordept.myco.com` è rappresentato nel file keytab come `jsmith@ordept.myco.com`.
- Fare clic su **Verifica connessione** per accertarsi che il wizard possa utilizzare le informazioni utente specificate per stabilire correttamente una connessione all'unità di controllo di dominio EIM.
- Fare clic su **Avanti**.

11. Nel pannello **Riepilogo**, rivedere le informazioni di configurazioni fornite. Se tutte le informazioni sono corrette, fare clic su **Fine**.

Finalizzazione della configurazione EIM per il dominio

Dopo essere stato completato, il wizard aggiunge il nuovo dominio alla cartella **Gestione domini** e si è creata una configurazione EIM di base per questo server. Tuttavia, è necessario completare queste attività per finalizzare la configurazione di EIM per il dominio:

1. Utilizzare il wizard di configurazione di EIM su ciascun server aggiuntivo che si desidera partecipi al dominio.

2. Aggiungere definizioni registro EIM al dominio EIM, se necessario, per altre piattaforme e applicazioni non System i che si desidera partecipino al dominio EIM. Queste definizioni del registro fanno riferimento ai registri utenti reali che devono far parte del dominio. È possibile aggiungere delle definizioni di registro di sistema oppure aggiungere delle definizioni di registro applicazione sulla base delle esigenze della propria implementazione EIM.
3. A seconda dell'implementazione EIM necessaria, stabilire se:
   - Creare identificativi EIM per ogni utente o entità univoci nel dominio e creare associazioni di identificativi per essi.
   - Creare delle associazioni normative per associare un gruppo di utenti ad una singola identità utente di destinazione.
   - Creare un combinazione di entrambe le opzioni.
4. Utilizzare la funzione Verifica di una corrispondenza di EIM per verificare la associazioni di identità per la propria configurazione EIM.
5. Se il solo utente EIM definito è il DN per l'amministratore LDAP, l'utente EIM ha un elevato livello di autorizzazione a tutti i dati sul server indirizzario. Si potrebbe pertanto considerare la possibilità di creare uno o più DN come utenti aggiuntivi che hanno un controllo accesso più appropriato e limitato per i dati EIM. Per ulteriori informazioni su come creare dei DN per il server indirizzario, consultare DN (Distinguished name) ini5/OS Information Center. Il numero di utenti EIM aggiuntivi definito dipende dall'enfasi posta dalla propria normativa di sicurezza sulla separazione dei doveri e delle responsabilità inerenti la sicurezza. Di norma, è possibile creare almeno i seguenti due tipi di DN:
   - **Un utente che ha un controllo accesso di amministratore EIM**

     Questo DN di amministratore EIM fornisce l'appropriato livello di autorizzazione per un amministratore responsabile per la gestione del dominio EIM. Questo DN di amministratore EIM potrebbe essere utilizzato quando si stabilisce una connessione all'unità di controllo di dominio quando si gestiscono tutti gli aspetti del del dominio EIM tramite System i Navigator.
   - **Almeno un utente che ha uno dei seguenti controlli accesso**:
     – Amministratore identificativo
     – Amministratore registro
     – Operazioni di corrispondenza EIM

     Quest'utente fornisce l'appropriato livello di controllo accesso richiesto per l'utente di sistema che esegue le operazioni EIM per conto del sistema operativo.

   Nota: per utilizzare questo nuovo DN per l'utente di sistema invece del DN di amministratore LDAP, occorre modificare le proprietà di configurazione di EIM per la piattaforma System i. Consultare Gestione delle proprietà di configurazione di EIM per ulteriori informazioni su come modificare il DN dell'utente di sistema.

Inoltre, l'utente può utilizzare SSL (Secure Sockets Layer) o TLS (Transport Layer Security) per configurare una connessione sicura all'unità di controllo del dominio EIM per proteggere la trasmissione di dati EIM. Se si abilita SSL per il server indirizzario, occorre aggiornare le proprietà di configurazione di EIM per specificare che la piattaforma System i utilizza una connessione SSL sicura. Occorre inoltre aggiornare le proprietà per il dominio per specificare che EIM utilizza le connessioni SSL per gestire il dominio tramite System i Navigator.

Nota: Potrebbe essere necessario eseguire attività aggiuntive se si è creata una configurazione di servizio di autenticazione di rete di base, specialmente se si sta implementando un ambiente a collegamento singolo (SSO). È possibile ottenere informazioni su questi passi aggiuntivi consultando i passi di configurazione completi dimostrati dallo scenario di abilitazione del collegamento singolo (SSO) per i5/OS.

Creazione e partecipazione ad un nuovo dominio remoto

Quando si utilizza il wizard di configurazione di EIM per creare ed unire un nuovo dominio, è possibile scegliere di configurare un server indirizzario su un sistema remoto in modo che agisca come unità di controllo dominio EIM come parte della creazione della propria configurazione EIM.

È necessario specificare le informazioni appropriate per stabilire un collegamento al server indirizzario remoto per potere configurare EIM. Se Kerberos non è attualmente configurato sulla piattaforma System i, il wizard richiede l'avvio del wizard Configurazione servizio autenticazione di rete.

Nota: il server indirizzario sul sistema remoto deve fornire il supporto EIM. EIM richiede che l'unità di controllo dominio abbia come host un server indirizzario che supporta LDAP (Lightweight Directory Access Protocol) Versione 3. Inoltre, il prodotto server indirizzario deve avere lo schema EIM configurato. Ad esempio, IBM Directory Server V5.1 fornisce questo supporto. Per informazioni più dettagliate sui requisiti dell'unità di controllo del dominio EIM, consultare "Pianificazione di un'unità di controllo del dominio EIM" a pagina 58.

Dopo avere completato il wizard di configurazione di EIM, è possibile eseguire le seguenti attività:

- Creare un nuovo dominio EIM.
- Configurare un server di indirizzario remoto che agisca come un'unità di controllo del dominio EIM.
- Configurare il servizio di autenticazione di rete per il sistema.
- Creare le definizioni di registro EIM per il registro locale i5/OS ed il registro Kerberos.
- Configurare il sistema in modo che partecipi al nuovo dominio EIM.

Per configurare il sistema in modo da creare e partecipare a un nuovo dominio EIM, è necessario disporre di tutte le seguenti autorizzazioni speciali:

- Responsabile della sicurezza (*SECADM).
- Tutti gli oggetti (*ALLOBJ).
- Configurazione di sistema (*IOSYSCFG).

Per utilizzare il Wizard di configurazione EIM per creare e partecipare a un dominio in un sistema remoto, completare le seguenti operazioni:

1. Verificare che il server dell'indirizzario sul sistema remoto sia attivo.
2. In System i Navigator, selezionare il sistema per cui si desidera configurare EIM ed espandere **Rete > EIM (Enterprise Identity Mapping)**.
3. Fare clic con il tasto destro del mouse su **Configurazione** e selezionare **Configura** per per avviare il wizard Configurazione EIM.

   Nota: quest'opzione è etichettata **Riconfigura** se EIM è stato configurato precedentemente sul sistema.
4. Sulla pagina di **Benvenuto** del wizard, selezionare **Creazione e collegamento di un nuovo dominio** e fare clic su **Avanti**.
5. Nella pagina **Specifica ubicazione dominio EIM**, selezionare **Sul server dell'indirizzario locale** e fare clic su **Avanti**.

   Nota: questa opzione configura il server indirizzario locale in modo che agisca come unità di controllo dominio EIM. Poiché questo server indirizzario memorizza tutti i dati EIM per il dominio, deve essere attivo e rimanere attivo per supportare le ricerche di corrispondenze EIM ed altre operazioni.

   Se il servizio di autenticazione di rete non è attualmente configurato sulla piattaforma System i, o se sono richieste ulteriori informazioni di configurazione dell'autenticazione di rete per configurare un ambiente a collegamento singolo (SSO), viene visualizzata la pagina **Configurazione servizi autenticazione di rete**. Questa pagina consente di avviare il wizard Configurazione servizio

autenticazione di rete con il quale l'utente può configurare il servizio di autenticazione di rete. È anche possibile configurare il Sevizio autenticazione di rete in un secondo momento utilizzando il wizard di configurazione per questo servizio tramite System i Navigator. Una volta completata la configurazione del servizio di autenticazione di rete, il wizard di configurazione di EIM proseguirà.

6. Per configurare il servizio di autenticazione di rete, attenersi alla seguente procedura:
   a. Sulla pagina **Configura servizio di autenticazione di rete**, selezionare **Sì** per avviare il wizard Configurazione servizio autenticazione di rete. In questo wizard, è possibile configurare varie interfacce e vari servizi i5/OS in modo che partecipino ad un dominio Kerberos e configurare un ambiente a collegamento singolo (SSO) che utilizza sia EIM che il servizio di autenticazione di rete.
   b. Sulla pagina **Specifica di informazioni sul dominio**, specificare il nome del dominio predefinito nel campo **Dominio predefinito**. Se si sta utilizzando l'autenticazione Microsoft Active Directory per Kerberos, selezionare **Microsoft Active Directory viene utilizzato per l'autenticazione Kerberos** e fare clic su **Avanti**.
   c. Sulla pagina **Specifica informazioni KDC**, specificare il nome completo del server Kerberos per quest'ambito nel campo **KDC**, specificare 88 nel campo **Porta** e fare clic su **Avanti**.
   d. Sulla pagina **Specifica informazioni server parola d'ordine**, selezionare **Sì** o **No** per impostare un server parola d'ordine. Il server parola d'ordine consente ai principal di modificare le parole d'ordine sul server Kerberos. Se si seleziona **Sì**, immettere il nome del server parola d'ordine nel campo **Server parola d'ordine**. Nel campo **Porta**, accettare il valore predefinito di 464 e fare clic su Avanti.
   e. Sulla pagina **Selezione voci keytab**, selezionare **Autenticazione Kerberos i5/OS** e fare clic su **Avanti**.

      Nota: è inoltre possibile creare delle voci keytab per IBM Tivoli Directory Server per i5/OS, i5/OS NetServer e il server IBM HTTP Server per i5/OS se si desidera che questi servizi utilizzino l'autenticazione Kerberos. È possibile che occorra eseguire delle operazioni di configurazione aggiuntive per questi servizi per consentire loro di potere utilizzare l'autenticazione Kerberos.
   f. Sulla pagina **Creazione voce keytab i5/OS**, immettere e confermare la parola d'ordine e fare clic su **Avanti**. Questa è la stessa parola d'ordine che si utilizzerà quando si aggiungeranno i principal i5/OS al server Kerberos.
   g. Opzionale: Sulla pagina **Creazione file batch**, selezionare **Sì**, specificare le seguenti informazioni e fare clic su **Avanti**:
      - Nel campo **File batch**, aggiornare il percorso di indirizzario. Fare clic su **Sfoglia** per individuare il percorso di indirizzario appropriato oppure modificare il percorso nel campo **File batch**.
      - Nel campo **Includi parola d'ordine**, selezionare **Sì**. Questo assicura che tutte le parole d'ordine associate al principal di servizio i5/OS siano incluse nel file batch. È importante notare che le parole d'ordine sono visualizzate senza essere crittografate e possono essere lette da chiunque disponga di accesso in lettura al file batch. È pertanto essenziale cancellare il file batch dal server Kerberos e dal PC immediatamente dopo averlo utilizzato. Se non si include la parola d'ordine, all'utente verrà richiesta quando si esegue il file batch.

        Nota: è anche possibile aggiungere manualmente i principal di servizio generati dal wizard a Microsoft Active Directory. Per ulteriori informazioni su come eseguire quest'operazione, consultare la sezione relativa all' Aggiunta di principal i5/OS al server Kerberos.
      - Sulla pagina **Riepilogo**, controllare i dettagli della configurazione del servizio di autenticazione di rete e fare clic su **Fine** per tornare al wizard di configurazione di EIM.
7. Utilizzare la pagina **Specifica l'unità di controllo del dominio EIM** per specificare le informazioni di connessione per l'unità di controllo del dominio EIM che si desidera configurare:
   a. Nel campo **Nome unità di controllo del dominio**, specificare il nome del server di indirizzario remoto che si desidera configurare come unità di controllo del dominio EIM per il dominio che si

sta creando. Il nome dell'unità di controllo del dominio EIM può essere il nome dominio e host TCP/IP del server indirizzario o l'indirizzo del server indirizzario.

b. Specificare le informazioni sulla connessione all'unità di controllo del dominio nel seguente modo:
   - Selezionare **Utilizza connessione protetta (SSL o TLS)** se si desidera utilizzare una connessione protetta all'unità di controllo del dominio EIM. Se selezionata, la connessione utilizza SSL (Secure Sockets Layer) o TLS (Transport Layer Security) per stabilire una connessione protetta per proteggere la trasmissione di dati EIM su una rete non affidabile, ad esempio Internet.

     Nota: è necessario verificare se l'unità di controllo del dominio EIM è configurata per utilizzare una connessione protetta. Altrimenti, il collegamento all'unità di controllo del dominio può avere esito negativo.
   - Nel campo **Porta**, specificare la porta TCP/IP su cui è in ascolto il server indirizzario. Se è stata selezionata **Utilizza connessione sicura**, la porta predefinita è `636`; altrimenti, la porta predefinita è `389`.

c. Fare clic su **Verifica connessione** per verificare che il wizard possa utilizzare le informazioni specificate per stabilire correttamente una connessione all'unità di controllo di dominio EIM remota.

d. Fare clic su **Avanti**.

8. Sulla pagina **Specifica l'utente per la connessione**, selezionare un **Tipo utente** per la connessione. È possibile selezionare uno dei seguenti tipi di utente: **DN e parola d'ordine**, **File keytab e principal Kerberos**, **Principal e parola d'ordine Kerberos**, oppure **Profilo utente e parola d'ordine**. I due tipi utente Kerberos sono disponibili solo se il servizio di autenticazione di rete è configurato per la piattaforma System i locale. Il tipo di utente selezionato determina le altre informazioni che devono essere fornite per completare la finestra di dialogo come segue:

   Nota: per assicurarsi che il wizard disponga delle autorizzazioni necessarie per creare gli oggetti EIM necessari nell'indirizzario, selezionare **DN e parola d'ordine** come tipo utente e specificare il DN e la parola d'ordine dell'amministratore LDAP come utente.

   È possibile specificare un utente differente per la connessione; tuttavia, l'utente specificato deve disporre di autorizzazioni equivalenti a quelle dell'amministratore LDAP per il server di indirizzario remoto.

   a. Se si seleziona **DN e parola d'ordine**, fornire le seguenti informazioni:
      - Nel campo **DN** specificare il DN e la parola d'ordine dell'amministratore LDAP per assicurarsi che il wizard disponga di autorizzazioni sufficienti per amministrare il dominio EIM e gli oggetti in esso contenuti.
      - Nel campo **Parola d'ordine**, specificare la parola d'ordine per il DN.
      - Nel campo **Conferma parola d'ordine**, specificare di nuovo la parola d'ordine per convalidarla.

   b. Se si seleziona **File keytab e principal Kerberos**, fornire le seguenti informazioni:
      - Nel campo **File keytab**, specificare il nome file keytab e il percorso completo in cui si trova il principal Kerberos che il wizard utilizzerà in fase di connessione al dominio EIM. In alternativa, fare clic su **Sfoglia** per ricercare negli indirizzari dell'IFS i5/OS e selezionare un file keytab.
      - Nel campo **Principal**, specificare il nome del principal Kerberos da utilizzare per identificare l'utente.
      - Nel campo **Dominio**, specificare il nome completo del dominio Kerberos di cui è membro il principal. Il nome del principal e del dominio identificano in modo univoco gli utenti Kerberos nel file keytab. Ad esempio, il principal `jsmith` nel dominio `ordept.myco.com`, è rappresentato nel file keytab come `jsmith@ordept.myco.com`.

   c. Se si seleziona **Principal Kerberos e parola d'ordine**, fornire le seguenti informazioni:

- Nel campo **Principal**, specificare il nome del principal Kerberos che il wizard utilizzerà in fase di connessione al dominio EIM.
- Nel campo **Dominio**, specificare il nome completo del dominio Kerberos di cui è membro il principal. Il nome del principal e del dominio identificano in modo univoco gli utenti Kerberos nel file keytab. Ad esempio, il principal `jsmith` nell'ambito `ordept.myco.com` è rappresentato nel file keytab come `jsmith@ordept.myco.com`.
- Nel campo **Parola d'ordine**, specificare la parola d'ordine per il principal Kerberos.
- Nel campo **Conferma parola d'ordine**, specificare di nuovo la parola d'ordine per convalidarla.

d. Se si seleziona **Profilo utente e parola d'ordine**, fornire le seguenti informazioni:
- Nel campo **Profilo utente**, specificare il nome di profilo utente che il wizard utilizzerà in fase di connessione al dominio EIM.
- Nel campo **Parola d'ordine**, specificare la parola d'ordine per il profilo utente.
- Nel campo **Conferma parola d'ordine**, specificare di nuovo la parola d'ordine per convalidarla.

e. Fare clic su **Verifica connessione** per verificare che il wizard possa utilizzare le informazioni utente specificate per stabilire correttamente una connessione all'unità di controllo di dominio EIM.

f. Fare clic su **Avanti**.

9. Sulla pagina **Specifica il dominio**, fornire le seguenti informazioni:
   a. Nel campo **Dominio**, specificare il nome del dominio EIM che si desidera creare. Accettare il nome predefinito di `EIM` oppure utilizzare una qualsiasi stringa di caratteri di senso compiuto per l'utente. Tuttavia, non è possibile utilizzare caratteri speciali come **= + < > , # ;** \ e *.
   b. Nel campo **Descrizione**, inserire il testo per descrivere il dominio.
   c. Fare clic su **Avanti**.
10. Nella finestra di dialogo **Specifica il DN principale per il dominio**, selezionare **Sì** per specificare il DN principale che deve essere utilizzato dal wizard per l'ubicazione del dominio EIM che si sta creando. Corrisponde al DN che rappresenta la voce immediatamente precedente alla voce del nome dominio nella gerarchia ad albero delle informazioni dell'indirizzario. Altrimenti, specificare **No** per fare in modo che i dati EIM vengano memorizzati in un'ubicazione indirizzario con un suffisso il cui nome è derivato dal nome di dominio EIM.

    Nota: quando si utilizza il wizard per configurare un dominio su un'unità di controllo dominio remota è necessario specificare un DN principale appropriato per il dominio. Poiché è necessario che siano già presenti tutti gli oggetti di configurazione necessari per il DN principale, altrimenti la configurazione EIM non riesce, è opportuno utilizzare l'opzione Sfoglia per risalire al DN principale appropriato piuttosto che immettere manualmente le informazioni. Fare clic su **?** per ulteriori informazioni sull'utilizzo di un DN principale.
11. Sulla pagina **Informazioni sul registro**, specificare se aggiungere dei registri utenti locali al dominio EIM come definizioni di registro. Selezionare uno di questi tipi di registri utenti oppure entrambi:

    Nota: non è necessario creare le definizioni di registro adesso. Se si sceglie di creare le definizioni di registro in un secondo momento, consultare Aggiunta di una definizione del registro di sistema e Proprietà di configurazione EIM.

    a. Selezionare **i5/OS locale** per aggiungere una definizione di registro per il registro locale. Nel campo fornito, accettare il valore predefinito per il nome di definizione di registro oppure specificare un valore differente. Il nome registro EIM è una stringa arbitraria che rappresenta il tipo di registro e l'istanza specifica di tale registro.
    b. Selezionare **Kerberos** per aggiungere una definizione di servizio per un registro Kerberos. Nel campo fornito, accettare il valore predefinito per il nome di definizione di registro oppure specificare un valore differente. Il nome di definizione di registro predefinito è lo stesso del nome di dominio. Accettando il nome predefinito ed utilizzando lo stesso nome di registro Kerberos del

nome di dominio, è possibile migliorare le prestazioni nel richiamo delle informazioni dal registro. Selezionare **Le identità utente Kerberos sono sensibili al maiuscolo e minuscolo**, se necessario.

c. Fare clic su **Avanti**.

12. Sulla pagina **Specifica l'utente di sistema EIM**, selezionare un **Tipo utente** che si desidera venga utilizzato dal sistema quando vengono eseguite operazioni EIM per conto delle funzioni di sistema operativo. Queste operazioni includono le ricerche delle corrispondenze e la cancellazione delle associazioni quando si cancella un profilo utente i5/OS locale. È possibile selezionare uno dei seguenti tipi di utente: **DN e parola d'ordine**, **File keytab e principal Kerberos** oppure **Principal e parola d'ordine Kerberos**. Il tipo di utente da selezionare varia a seconda della configurazione del sistema corrente. Ad esempio, se non è stato configurato il Servizio di autenticazione di rete (NAS-Network Authentication Service) per il sistema, è possibile che i tipi di utente Kerberos non siano disponibili per la selezione. Il tipo di utente selezionato determina le altre informazioni che devono essere fornite per completare la pagina come segue:

    Nota: è necessario specificare un utente correntemente definito nel server indirizzario che contiene l'unità di controllo dominio EIM. L'utente specificato deve disporre di privilegi per eseguire almeno la ricerca delle corrispondenze e la gestione registro di un registro utenti locale. Se l'utente specificato non dispone di tali privilegi, alcune funzioni del sistema operativo relative all'utilizzo del collegamento singolo (SSO) e alla cancellazione dei profili utente potrebbero avere esito negativo.

    Se non si è creato il server indirizzario prima di eseguire questo wizard, il solo tipo utente che è possibile selezionare e **DN e parola d'ordine** ed il solo DN che è possibile specificare è il DN dell'amministratore LDAP.

    a. Se si seleziona **DN e parola d'ordine**, fornire le seguenti informazioni:
        - Nel campo **DN**, specificare il DN LDAP che identifica l'utente che verrà utilizzato dal sistema quando eseguirà le operazioni EIM.
        - Nel campo **Parola d'ordine**, specificare la parola d'ordine per il DN.
        - Nel campo **Conferma parola d'ordine**, specificare di nuovo la parola d'ordine per verificarla.

    b. Se si seleziona **Principal Kerberos e parola d'ordine**, fornire le seguenti informazioni:
        - Nel campo **Principal**, specificare il nome di principal Kerberos che verrà utilizzato dal sistema quando eseguirà le operazioni EIM
        - Nel campo **Dominio**, specificare il nome completo del dominio Kerberos di cui è membro il principal. Il nome del principal e del dominio identificano in modo univoco gli utenti Kerberos nel file keytab. Ad esempio, il principal `jsmith` nell'ambito `ordept.myco.com` è rappresentato nel file keytab come `jsmith@ordept.myco.com`.
        - Nel campo **Parola d'ordine**, immettere la parola d'ordine dell'utente.
        - Nel campo **Conferma parola d'ordine**, specificare di nuovo la parola d'ordine per verificarla.

    c. Se si seleziona **File keytab e principal Kerberos**, fornire le seguenti informazioni:
        - Nel campo **File keytab**, specificare il nome file keytab e il percorso completo in cui si trova il principal Kerberos che verrà utilizzato dal sistema quando eseguirà le operazioni EIM. In alternativa, fare clic su **Sfoglia** per ricercare negli indirizzari dell'IFS System i e selezionare un file keytab.
        - Nel campo **Principal**, specificare il nome di principal Kerberos che verrà utilizzato dal sistema quando eseguirà le operazioni EIM.
        - Nel campo **Dominio**, specificare il nome completo del dominio Kerberos di cui è membro il principal. Il nome del principal e del dominio identificano in modo univoco gli utenti Kerberos nel file keytab. Ad esempio, il principal `jsmith` nell'ambito `ordept.myco.com` è rappresentato nel file keytab come `jsmith@ordept.myco.com`.

d. Fare clic su **Verifica connessione** per accertarsi che il wizard possa utilizzare le informazioni utente specificate per stabilire correttamente una connessione all'unità di controllo di dominio EIM.

e. Fare clic su **Avanti**.

13. Nel pannello **Riepilogo**, rivedere le informazioni di configurazioni fornite. Se tutte le informazioni sono corrette, fare clic su **Fine**.

Finalizzazione della configurazione EIM per il dominio

Dopo essere stato completato, il wizard aggiunge il nuovo dominio alla cartella **Gestione domini** e si è creata una configurazione EIM di base per questo server. Tuttavia, è necessario completare queste attività per finalizzare la configurazione di EIM per il dominio:

1. Utilizzare il wizard di configurazione di EIM su ciascun server aggiuntivo che si desidera partecipi al dominio esistente. Consultare l'argomento "Partecipazione ad un dominio esistente" a pagina 86 per ulteriori informazioni.
2. Aggiungere definizioni registro EIM al dominio EIM, se necessario, per altre piattaforme e applicazioni non System i che si desidera partecipino al dominio EIM.Tali definizioni fanno riferimento ai registri utenti reali che devono partecipare al dominio. In base alle esigenze della propria implementazione EIM, consultare "Aggiunta di una definizione del registro di sistema" a pagina 98 oppure "Aggiunta di una definizione del registro dell'applicazione" a pagina 98.
3. A seconda dell'implementazione EIM necessaria, stabilire se:
   a. "Creazione di un identificativo EIM" a pagina 105 per ogni utente o entità univoci nel dominio e "Creazione di un'associazione identificativo EIM" a pagina 109 per essi.
   b. "Creazione di un'associazione normativa" a pagina 110 per mettere in corrispondenza un gruppo di utenti ad una singola identità utente di destinazione.
   c. Creare un combinazione di entrambe le opzioni.
4. Utilizzare la funzione "Verifica delle corrispondenze" a pagina 94 di EIM per verificare le corrispondenze di identità per la propria configurazione EIM.
5. Se il solo utente EIM definito è il DN per l'amministratore LDAP, l'utente EIM ha un elevato livello di autorizzazione a tutti i dati sul server indirizzario. Si potrebbe pertanto considerare la possibilità di creare uno o più DN come utenti aggiuntivi che hanno un controllo accesso più appropriato e limitato per i dati EIM. Per ulteriori informazioni su come creare dei DN per il server indirizzario, consultare DN (Distinguished name) ini5/OS Information Center. Il numero di utenti EIM aggiuntivi definito dipende dall'enfasi posta dalla propria normativa di sicurezza sulla separazione dei doveri e delle responsabilità inerenti la sicurezza. Di norma, è possibile creare almeno i seguenti due tipi di DN:
   - **Un utente che ha un controllo accesso di amministratore EIM**

     Questo DN di amministratore EIM fornisce l'appropriato livello di autorizzazione per un amministratore responsabile per la gestione del dominio EIM. Questo DN di amministratore EIM potrebbe essere utilizzato quando si stabilisce una connessione all'unità di controllo di dominio quando si gestiscono tutti gli aspetti del del dominio EIM tramite System i Navigator.
   - **Almeno un utente che ha uno dei seguenti controlli accesso**:
     – Amministratore identificativo
     – Amministratore registro
     – Operazioni di corrispondenza EIM

     Quest'utente fornisce l'appropriato livello di controllo accesso richiesto per l'utente di sistema che esegue le operazioni EIM per conto del sistema operativo.

   Nota: per utilizzare questo nuovo DN per l'utente di sistema invece del DN di amministratore LDAP, occorre modificare le proprietà di configurazione di EIM per la piattaforma System i. Consultare la sezione relativa alla "Gestione delle proprietà di configurazione EIM" a pagina 125 per ulteriori informazioni su come modificare il DN dell'utente di sistema.

Potrebbe essere necessario eseguire attività aggiuntive se si è creata una configurazione di servizio di autenticazione di rete di base, specialmente se si sta implementando un ambiente a collegamento singolo (SSO). È possibile ottenere informazioni su questi passi aggiuntivi consultando i passi di configurazione completi dimostrati dallo scenario di abilitazione del collegamento singolo (SSO) per i5/OS.

Partecipazione ad un dominio esistente

Utilizzare il wizard di configurazione EIM (Enterprise Identity Mapping) su una piattaforma System i per configurare un'unità di controllo del dominio e per creare un dominio EIM, quindi utilizzare il wizard per configurare altri sistemi in modo che partecipino al dominio.

Dopo aver creato un dominio EIM e configurato un'unità di controllo dominio controller su un sistema, è possibile configurare tutte le piattaforme System i aggiuntive da unire al dominio EIM esistente. Durante l'esecuzione del wizard, è necessario fornire informazioni sul dominio, incluse le informazioni sul collegamento all'unità di controllo del dominio EIM. Quando si utilizza il wizard di configurazione di EIM per unire un dominio esistente, il wizard fornisce ancora all'utente l'opzione per avviare il wizard Configurazione servizio autenticazione di rete se si sceglie di configurare Kerberos come parte della configurazione EIM sul sistema.

Dopo avere completato il wizard di configurazione di EIM per partecipare ad un dominio esistente, è possibile eseguire le seguenti attività:

- Configurare il servizio di autenticazione di rete per il sistema.
- Creare le definizioni di registro EIM per il registro locale i5/OS ed il registro Kerberos.
- Configurare il sistema per partecipare a un dominio EIM esistente.

Per configurare il sistema in modo da poter partecipare a un dominio EIM esistente, è necessario disporre di tutte le seguenti autorizzazioni speciali:

- Responsabile della sicurezza (*SECADM).
- Tutti gli oggetti (*ALLOBJ).

Per avviare ed utilizzare il wizard di configurazione di EIM per partecipare ad un dominio EIM esistente, completare i passi riportati di seguito:

1. Verificare che il server dell'indirizzario sul sistema remoto sia attivo.
2. In System i Navigator, selezionare il sistema per cui si desidera configurare EIM ed espandere **Rete > EIM (Enterprise Identity Mapping)**.
3. Fare clic con il tasto destro del mouse su **Configurazione** e selezionare **Configura...** per avviare il wizard di configurazione di EIM.

   Nota: quest'opzione è etichettata **Riconfigura...** se EIM è stato configurato precedentemente sul sistema.
4. Sulla pagina di **Benvenuti** del wizard, selezionare **Partecipa a un dominio esistente** e fare clic su **Avanti**.

   Nota: Se il servizio di autenticazione di rete non è attualmente configurato sul modello System i, o se sono richieste ulteriori informazioni di configurazione dell'autenticazione di rete per configurare un ambiente a collegamento singolo (SSO), viene visualizzata la pagina **Configurazione servizi autenticazione di rete**. Questa pagina consente di avviare il wizard Configurazione servizio autenticazione di rete con il quale l'utente può configurare il servizio di autenticazione di rete. È anche possibile configurare il Sevizio autenticazione di rete in un secondo momento utilizzando il wizard di configurazione per questo servizio tramite System i Navigator. Una volta completata la configurazione del servizio di autenticazione di rete, il wizard di configurazione di EIM proseguirà.
5. Per configurare il servizio di autenticazione di rete, attenersi alla seguente procedura:

a. Sulla pagina **Configura servizio di autenticazione di rete**, selezionare **Sì** per avviare il wizard Configurazione servizio autenticazione di rete. In questo wizard, è possibile configurare varie interfacce e vari servizi i5/OS in modo che partecipino ad un dominio Kerberos e configurare un ambiente a collegamento singolo (SSO) che utilizza sia EIM che il servizio di autenticazione di rete.

b. Sulla pagina **Specifica di informazioni sul dominio**, specificare il nome del dominio predefinito nel campo **Dominio predefinito**. Se si sta utilizzando l'autenticazione Microsoft Active Directory per Kerberos, selezionare **Microsoft Active Directory viene utilizzato per l'autenticazione Kerberos** e fare clic su **Avanti**.

c. Sulla pagina **Specifica informazioni KDC**, specificare il nome completo del server Kerberos per quest'ambito nel campo **KDC**, specificare 88 nel campo **Porta** e fare clic su **Avanti**.

d. Sulla pagina **Specifica informazioni server parola d'ordine**, selezionare **Sì** o **No** per impostare un server parola d'ordine. Il server parola d'ordine consente ai principal di modificare le parole d'ordine sul server Kerberos. Se si seleziona **Sì**, immettere il nome del server parola d'ordine nel campo **Server parola d'ordine**. Nel campo **Porta**, accettare il valore predefinito di 464 e fare clic su Avanti.

e. Sulla pagina **Selezione voci keytab**, selezionare **Autenticazione Kerberos i5/OS** e fare clic su **Avanti**.

   Nota: è inoltre possibile creare delle voci keytab per IBM Tivoli Directory Server per i5/OS, i5/OS NetServer e IBM HTTP Server per i5/OS if se si desidera che questi servizi utilizzino l'autenticazione Kerberos. È possibile che occorra eseguire delle operazioni di configurazione aggiuntive per questi servizi per consentire loro di potere utilizzare l'autenticazione Kerberos.

f. Sulla pagina **Creazione voce keytab i5/OS**, immettere e confermare la parola d'ordine e fare clic su **Avanti**. Questa è la stessa parola d'ordine che si utilizzerà quando si aggiungeranno i principal i5/OS al server Kerberos.

g. Opzionale: Sulla pagina **Creazione file batch**, selezionare **Sì**, specificare le seguenti informazioni e fare clic su **Avanti**:

   - Nel campo **File batch**, aggiornare il percorso di indirizzario. Fare clic su **Sfoglia** per individuare il percorso di indirizzario appropriato oppure modificare il percorso nel campo **File batch**.
   - Nel campo **Includi parola d'ordine**, selezionare **Sì**. Questo assicura che tutte le parole d'ordine associate al principal di servizio i5/OS siano incluse nel file batch. È importante notare che le parole d'ordine sono visualizzate senza essere crittografate e possono essere lette da chiunque disponga di accesso in lettura al file batch. È pertanto essenziale cancellare il file batch dal server Kerberos e dal PC immediatamente dopo averlo utilizzato. Se non si include la parola d'ordine, all'utente verrà richiesta quando si esegue il file batch.

     Nota: è anche possibile aggiungere manualmente i principal di servizio generati dal wizard a Microsoft Active Directory. Per ulteriori informazioni su come eseguire quest'operazione, consultare la sezione relativa all' Aggiunta di principal i5/OS al server Kerberos

   - Sulla pagina **Riepilogo**, controllare i dettagli della configurazione del servizio di autenticazione di rete e fare clic su **Fine** per tornare al wizard di configurazione di EIM.

6. Sulla pagina **Specifica unità di controllo del dominio**, fornire le seguenti informazioni:

   Nota: il server indirizzario che agisce da unità di controllo del dominio deve essere attivo perché il completamento di questa configurazione EIM abbia esito positivo.

   a. Nel campo **Nome unità di controllo del dominio**, specificare il nome del sistema che opera come unità di controllo del dominio EIM a cui si desidera partecipi la piattaforma System i .

   b. Fare clic su **Utilizza connessione protetta (SSL o TLS)** se si desidera utilizzare una connessione protetta all'unità di controllo del dominio EIM. Se selezionata, la connessione utilizza SSL (Secure

Sockets Layer) o TLS (Transport Layer Security) per stabilire una connessione protetta per proteggere la trasmissione di dati EIM su una rete non affidabile, ad esempio Internet.

Nota: è necessario verificare se l'unità di controllo del dominio EIM è configurata per utilizzare una connessione protetta. Altrimenti, il collegamento all'unità di controllo del dominio può avere esito negativo.

c. Nel campo **Porta**, specificare la porta TCP/IP su cui è in ascolto il server indirizzario. Se è stata selezionata **Utilizza connessione sicura**, la porta predefinita è `636`; altrimenti, la porta predefinita è `389`.

d. Fare clic su **Verifica connessione** per verificare che il wizard possa utilizzare le informazioni specificate per stabilire correttamente una connessione all'unità di controllo di dominio EIM.

e. Fare clic su **Avanti**.

7. Sulla pagina **Specifica l'utente per la connessione**, selezionare un **Tipo utente** per la connessione. È possibile selezionare uno dei seguenti tipi di utenti: **DN e parola d'ordine**, **File keytab e principal Kerberos**, **Principal e parola d'ordine Kerberos**, oppure **Profilo utente e parola d'ordine**. I due tipi utente Kerberos sono disponibili solo se il servizio di autenticazione di rete è configurato per la piattaforma System i locale. Il tipo di utente selezionato determina le altre informazioni che devono essere fornite per completare la finestra di dialogo come segue:

   Nota: per assicurarsi che il wizard disponga delle autorizzazioni necessarie per creare gli oggetti EIM necessari nell'indirizzario, selezionare **DN e parola d'ordine** come tipo utente e specificare il DN e la parola d'ordine dell'amministratore LDAP come utente.

   È possibile specificare un utente differente per la connessione; tuttavia, l'utente specificato deve disporre di autorizzazioni equivalenti a quelle dell'amministratore LDAP per il server di indirizzario remoto.

   - Se si seleziona **DN e parola d'ordine**, fornire le seguenti informazioni:
     - Nel campo **DN**, specificare il DN LDAP che identifica l'utente autorizzato a creare oggetti nello spazio del nome locale del server LDAP. Se questo wizard è stato utilizzato per configurare il server LDAP in un passo precedente, è necessario inserire il DN dell'amministratore LDAP creato durante tale passo.
     - Nel campo **Parola d'ordine**, specificare la parola d'ordine per il DN.
     - Nel campo **Conferma parola d'ordine**, specificare di nuovo la parola d'ordine per convalidarla.
   - Se si seleziona **File keytab e principal Kerberos**, fornire le seguenti informazioni:
     - Nel campo **File keytab**, specificare il nome file keytab e il percorso completo in cui si trova il principal Kerberos che il wizard utilizzerà in fase di connessione al dominio EIM. In alternativa, fare clic su **Sfoglia...** per ricercare negli indirizzari dell'IFS System i per selezionare un file keytab.
     - Nel campo **Principal**, specificare il nome del principal Kerberos da utilizzare per identificare l'utente.
     - Nel campo **Dominio**, specificare il nome completo del dominio Kerberos di cui è membro il principal. Il nome del principal e del dominio identificano in modo univoco gli utenti Kerberos nel file keytab. Ad esempio, il principal `jsmith` nel dominio `ordept.myco.com`, è rappresentato nel file keytab come `jsmith@ordept.myco.com`.
   - Se si seleziona **Principal Kerberos e parola d'ordine**, fornire le seguenti informazioni:
     - Nel campo **Principal**, specificare il nome del principal Kerberos che il wizard utilizzerà in fase di connessione al dominio EIM.
     - Nel campo **Dominio**, specificare il nome completo del dominio Kerberos di cui è membro il principal. Il nome del principal e del dominio identificano in modo univoco gli utenti Kerberos nel file keytab. Ad esempio, il principal `jsmith` nell'ambito `ordept.myco.com` è rappresentato nel file keytab come `jsmith@ordept.myco.com`.
     - Nel campo **Parola d'ordine**, specificare la parola d'ordine per il principal Kerberos.

- Nel campo **Conferma parola d'ordine**, specificare di nuovo la parola d'ordine per convalidarla.

- Se si seleziona **Profilo utente e parola d'ordine**, fornire le seguenti informazioni:
  - Nel campo **Profilo utente**, specificare il nome di profilo utente che il wizard utilizzerà in fase di connessione al dominio EIM.
  - Nel campo **Parola d'ordine**, specificare la parola d'ordine per il profilo utente.
  - Nel campo **Conferma parola d'ordine**, specificare di nuovo la parola d'ordine per convalidarla.
- Fare clic su **Verifica connessione** per verificare che il wizard possa utilizzare le informazioni utente specificate per stabilire correttamente una connessione all'unità di controllo di dominio EIM.
- Fare clic su **Avanti**.

8. Sulla pagina **Specifica dominio**, selezionare il nome del dominio che si desidera collegare e fare clic su **Avanti**.
9. Sulla pagina **Informazioni sul registro**, specificare se aggiungere dei registri utenti locali al dominio EIM come definizioni di registro. Selezionare uno di questi tipi di registri utenti oppure entrambi:
   - Selezionare **i5/OS locale** per aggiungere una definizione di registro per il registro locale. Nel campo fornito, accettare il valore predefinito per il nome di definizione di registro oppure specificare un valore differente. Il nome registro EIM è una stringa arbitraria che rappresenta il tipo di registro e l'istanza specifica di tale registro.

     Nota: non è necessario creare la definizione di registro i5/OS locale adesso. Se si sceglie di creare la definizione di registro i5/OS in un secondo momento, occorre aggiungere la definizione di registro di sistema e aggiornare le proprietà di configurazione di EIM.
   - Selezionare **Kerberos** per aggiungere una definizione di servizio per un registro Kerberos. Nel campo fornito, accettare il valore predefinito per il nome di definizione di registro oppure specificare un valore differente. Il nome di definizione di registro predefinito è lo stesso del nome di dominio. Accettando il nome predefinito ed utilizzando lo stesso nome di registro Kerberos del nome di dominio, è possibile migliorare le prestazioni nel richiamo delle informazioni dal registro. Selezionare **Le identità utente Kerberos sono sensibili al maiuscolo e minuscolo**, se necessario.

     Nota: se si è utilizzato il wizard di configurazione di EIM oppure un altro sistema per aggiungere una definizione di registro per il registro Kerberos per cui questo modello System i dispone di un principal di servizio, non occorre aggiungere una definizione di registro Kerberos come parte di questa configurazione. Occorrerà tuttavia specificare il nome di detto registro Kerberos nelle proprietà di configurazione per questo sistema dopo avere completato il wizard.
   - Fare clic su **Avanti**.
10. Sulla pagina **Specifica l'utente di sistema EIM**, selezionare un **Tipo utente** che si desidera venga utilizzato dal sistema quando vengono eseguite operazioni EIM per conto delle funzioni di sistema operativo. Queste operazioni includono le ricerche delle corrispondenze e la cancellazione delle associazioni quando si cancella un profilo utente i5/OS locale. È possibile selezionare uno dei seguenti tipi di utente: **DN e parola d'ordine**, **File keytab e principal Kerberos** oppure **Principal e parola d'ordine Kerberos**. Il tipo di utente da selezionare varia a seconda della configurazione del sistema corrente. Ad esempio, se non è stato configurato il Servizio di autenticazione di rete (NAS-Network Authentication Service) per il sistema, è possibile che i tipi di utente Kerberos non siano disponibili per la selezione. Il tipo di utente selezionato determina le altre informazioni che devono essere fornite per completare la pagina come segue:

    Nota: è necessario specificare un utente correntemente definito nel server indirizzario che contiene l'unità di controllo dominio EIM. L'utente specificato deve disporre di privilegi per eseguire almeno la ricerca delle corrispondenze e la gestione registro di un registro utenti locale. Se l'utente specificato non dispone di tali privilegi, alcune funzioni del sistema operativo relative all'utilizzo del collegamento singolo (SSO) e alla cancellazione dei profili utente potrebbero avere esito negativo.

- Se si seleziona **DN e parola d'ordine**, fornire le seguenti informazioni:
  - Nel campo **DN**, specificare il DN LDAP che identifica l'utente che verrà utilizzato dal sistema quando eseguirà le operazioni EIM.
  - Nel campo **Parola d'ordine**, specificare la parola d'ordine per il DN.
  - Nel campo **Conferma parola d'ordine**, specificare di nuovo la parola d'ordine per verificarla.
- Se si seleziona **Principal Kerberos e parola d'ordine**, fornire le seguenti informazioni:
  - Nel campo **Principal**, specificare il nome di principal Kerberos che verrà utilizzato dal sistema quando eseguirà le operazioni EIM
  - Nel campo **Dominio**, specificare il nome completo del dominio Kerberos di cui è membro il principal. Il nome del principal e del dominio identificano in modo univoco gli utenti Kerberos nel file keytab. Ad esempio, il principal `jsmith` nell'ambito `ordept.myco.com` è rappresentato nel file keytab come `jsmith@ordept.myco.com`.
  - Nel campo **Parola d'ordine**, immettere la parola d'ordine dell'utente.
  - Nel campo **Conferma parola d'ordine**, specificare di nuovo la parola d'ordine per verificarla.
- Se si seleziona **File keytab e principal Kerberos**, fornire le seguenti informazioni:
  - Nel campo **File keytab**, specificare il nome file keytab e il percorso completo in cui si trova il principal Kerberos che verrà utilizzato dal sistema quando eseguirà le operazioni EIM. In alternativa, fare clic su **Sfoglia...** per ricercare negli indirizzari dell'IFS System i per selezionare un file keytab.
  - Nel campo **Principal**, specificare il nome di principal Kerberos che verrà utilizzato dal sistema quando eseguirà le operazioni EIM.
  - Nel campo **Dominio**, specificare il nome completo del dominio Kerberos di cui è membro il principal. Il nome del principal e del dominio identificano in modo univoco gli utenti Kerberos nel file keytab. Ad esempio, il principal `jsmith` nell'ambito `ordept.myco.com` è rappresentato nel file keytab come `jsmith@ordept.myco.com`.
- Fare clic su **Verifica connessione** per accertarsi che il wizard possa utilizzare le informazioni utente specificate per stabilire correttamente una connessione all'unità di controllo di dominio EIM.
- Fare clic su **Avanti**.

11. Nel pannello **Riepilogo**, rivedere le informazioni di configurazioni fornite. Se tutte le informazioni sono corrette, fare clic su **Fine**.

Finalizzazione della configurazione EIM per il dominio

Dopo essere stato completato, il wizard aggiunge il dominio alla cartella **Gestione domini** e si è creata una configurazione EIM di base per questo server. Tuttavia, potrebbe essere necessario completare queste attività per finalizzare la configurazione di EIM per il dominio:

1. Aggiungere definizioni registro EIM al dominio EIM, se necessario, per i sistemi su cui sono in esecuzione sistemi i5/OS e le applicazioni che si desidera partecipino al dominio EIM. Queste definizioni del registro fanno riferimento ai registri utenti reali che devono far parte del dominio. È possibile aggiungere delle definizioni di registro di sistema oppure aggiungere delle definizioni di registro applicazione sulla base delle esigenze della propria implementazione EIM.
2. A seconda dell'implementazione EIM necessaria, stabilire se:
   - Creare identificativi EIM per ogni utente o entità univoci nel dominio e creare associazioni di identificativi per essi.
   - Creare delle associazioni normative per associare un gruppo di utenti ad una singola identità utente di destinazione.
   - Creare un combinazione di entrambe le opzioni.
3. Utilizzare la funzione Verifica di una corrispondenza di EIM per verificare la associazioni di identità per la propria configurazione EIM.
4. Se il solo utente EIM definito è il DN per l'amministratore LDAP, l'utente EIM ha un elevato livello di autorizzazione a tutti i dati sul server indirizzario. Si potrebbe pertanto considerare la possibilità di

creare uno o più DN come utenti aggiuntivi che hanno un controllo accesso più appropriato e limitato per i dati EIM. Per ulteriori informazioni su come creare dei DN per il server indirizzario, consultare DN (Distinguished name) ini5/OS Information Center. Il numero di utenti EIM aggiuntivi definito dipende dall'enfasi posta dalla propria normativa di sicurezza sulla separazione dei doveri e delle responsabilità inerenti la sicurezza. Di norma, è possibile creare almeno i seguenti due tipi di DN:

- **Un utente che ha un controllo accesso di amministratore EIM**

  Questo DN di amministratore EIM fornisce l'appropriato livello di autorizzazione per un amministratore responsabile per la gestione del dominio EIM. Questo DN di amministratore EIM potrebbe essere utilizzato quando si stabilisce una connessione all'unità di controllo di dominio quando si gestiscono tutti gli aspetti del del dominio EIM tramite System i Navigator.
- **Almeno un utente che ha uno dei seguenti controlli accesso**:
  - Amministratore identificativo
  - Amministratore registro
  - Operazioni di corrispondenza EIM

  Quest'utente fornisce l'appropriato livello di controllo accesso richiesto per l'utente di sistema che esegue le operazioni EIM per conto del sistema operativo.

Nota: per utilizzare questo nuovo DN per l'utente di sistema invece del DN di amministratore LDAP, occorre modificare le proprietà di configurazione di EIM per la piattaforma System i. Consultare Gestione delle proprietà di configurazione di EIM per ulteriori informazioni su come modificare il DN dell'utente di sistema.

Potrebbe essere necessario eseguire attività aggiuntive se si è creata una configurazione di servizio di autenticazione di rete di base, specialmente se si sta implementando un ambiente a collegamento singolo (SSO). È possibile ottenere informazioni su questi passi aggiuntivi consultando i passi di configurazione completi dimostrati dallo scenario di abilitazione del collegamento singolo (SSO) per i5/OS.

Configurazione di una connessione sicura all'unità di controllo del dominio EIM

È possibile utilizzare il protocollo SSL (Secure Sockets Layer) o TLS (Transport Layer Security) per stabilire una connessione sicura all'unità di controllo del dominio EIM per proteggere la trasmissione di dati EIM.

Per configurare SSL o TLS per EIM, è necessario completare le attività riportate di seguito:

1. Se necessario, utilizzare DCM (Digital Certificate Manager) per creare un certificato per un server di indirizzario da utilizzare per SSL.
2. Abilitare SSL per il server di indirizzario locale che ospita l'unità di controllo del dominio EIM.
3. Aggiornare le proprietà di configurazione di EIM per specificare che il modello System i utilizza una connessione SSL sicura. Per aggiornare le proprietà di configurazione di EIM, attenersi alla seguente procedura:
   a. In System i Navigator, selezionare il sistema su cui è stato configurato EIM ed espandere **Rete** → **EIM (Enterprise Identity Mapping)**.
   b. Fare clic con il tasto destro del mouse su **Configurazione** e selezionare **Proprietà**.
   c. Sulla pagina **Dominio**, selezionare **Utilizza connessione protetta (SSL o TLS)**, specificare la porta sicura su cui è in ascolto il server di indirizzario oppure accettare il valore predefinito 636 nel campo **Porta** e fare clic su **OK**.
4. Aggiornare le proprietà del dominio EIM per ciascun dominio EIM per specificare che EIM utilizza una connessione SSL nella gestione del dominio tramite System i Navigator. Per aggiornare le proprietà del dominio EIM, attenersi alla seguente procedura:
   a. In System i Navigator, selezionare il sistema su cui è stato configurato EIM ed espandere **Rete** → **EIM (Enterprise Identity Mapping)** → **Gestione domini**.

b. Selezionare il dominio EIM in cui si desidera lavorare.
   - Se il dominio EIM che si desidera gestire non è elencato in **Gestione domini**, consultare Aggiunta di un dominio EIM a Gestione domini.
   - Se attualmente non si è collegati al dominio EIM in cui si desidera lavorare, consultare Connessione all'unità di controllo del dominio EIM.

c. Fare clic con il tasto destro del mouse sul dominio EIM a cui si è connessi e selezionare **Proprietà**.

d. Sulla pagina **Dominio**, selezionare **Utilizza connessione protetta (SSL o TLS)**, specificare la porta sicura su cui è in ascolto il server di indirizzario oppure accettare il valore predefinito 636 nel campo **Porta** e fare clic su **OK**.

Gestione di EIM

Dopo avere configurato EIM (Enterprise Identity Mapping) sulla propria piattaforma System i, ci potrebbero essere delle attività amministrative che occorrerà eseguire nel corso del tempo per gestire il proprio dominio EIM ed i dati per il dominio.

Per ulteriori informazioni sulla gestione di EIM nella propria azienda, consultare queste pagine.

Gestione dei domini EIM

Utilizzare System i Navigator per gestire tutti i domini EIM.

Per gestire un dominio EIM, è necessario che esso sia elencato all'interno della cartella **Gestione domini** sotto la cartella **Rete** in System i Navigator; in caso contrario, è necessario aggiungerlo. Quando si utilizza il wizard di configurazione EIM per creare e configurare un nuovo dominio EIM, il dominio viene aggiunto automaticamente alla cartella **Gestione domini** in modo da poter gestire il dominio e le informazioni nel dominio stesso.

È possibile utilizzare una qualsiasi connessione System i per gestire un dominio EIM che risiede in una qualsiasi ubicazione della stessa rete, anche nel caso in cui il sistema che si sta utilizzando non partecipi al dominio.

È possibile eseguire le seguenti attività di gestione per un dominio:

Aggiunta di un dominio EIM alla cartella Gestione domini

Per aggiungere un dominio EIM alla cartella Gestione domini, è necessario disporre dell'autorizzazione speciale *SECADM e il dominio che si desidera aggiungere deve esistere prima di aggiungerlo alla cartella Gestione domini.

Per aggiungere un dominio EIM (Enterprise Identity Mapping) esistente alla cartella **Gestione domini**, attenersi alla seguente procedura:

1. Espandere **Rete >EIM (Enterprise Identity Mapping)**.
2. Fare clic con il tasto destro del mouse su **Gestione domini** e selezionare **Aggiungi dominio**.
3. Nella finestra di dialogo **Aggiungi dominio**, specificare il dominio e le informazioni di connessione richieste. Oppure, fare clic su **Sfoglia** per visualizzare un elenco di domini che l'unità di controllo dominio specificata gestisce.

   Nota: se si fa clic su **Sfoglia**, viene visualizzata la finestra di dialogo **Connetti all'unità di controllo dominio EIM**. Per visualizzare l'elenco dei domini, è necessario connettersi all'unità di controllo dominio con il controllo di accesso amministratore LDAP oppure con il controllo di accesso amministratore EIM. Il contenuto dell'elenco di domini varia in base al controllo accesso EIM di cui si dispone. Se si ha un controllo accesso amministratore LDAP, è possibile visualizzare un elenco di tutti i domini che l'unità di controllo dominio gestisce. Altrimenti l'elenco contiene solo quei domini per i quali si dispone del controllo accesso amministratore EIM.

4. Fare clic su **?**, se necessario, per determinare le informazioni da specificare per ciascun campo.
5. Fare clic su **OK** per aggiungere il dominio.

Connessione a un dominio EIM

Prima di potere lavorare con un dominio EIM (Enterprise Identity Mapping), è necessario connettersi all'unità di controllo del dominio EIM per il dominio. È possibile connettersi ad un dominio EIM anche se il proprio modello System i non è attualmente configurato per partecipare a questo dominio.

Per connettersi all'unità di controllo del dominio EIM è necessario che l'utente con cui ci si sia membro di un gruppo di di controllo accesso EIM. L'appartenenza al gruppo controllo accesso EIM determina quali attività è possibile eseguire nel dominio e quali dati EIM è possibile visualizzare o modificare.

Per collegarsi ad un dominio EIM, completare i passi riportati di seguito:

1. Espandere **Rete > EIM (Enterprise Identity Mapping) > Gestione domini**.
2. Fare clic con il tasto destro del mouse sul dominio con il quale si desidera stabilire il collegamento.

   Nota: se il dominio con il quale si desidera lavorare non è elencato in **Gestione domini**, è necessario aggiungere un dominio EIM alla cartella relativa alla gestione domini.
3. Fare clic con il tasto destro del mouse sul dominio EIM a cui si desidera effettuare la connessione e selezionare **Connetti**.
4. Nella finestra di dialogo **Collega all'unita di controllo del dominio EIM**, specificare il **Tipo di utente**, fornire le informazioni di identificazione necessarie all'utente e selezionare un'opzione parola d'ordine per connettersi all'unità di controllo del dominio.
5. Fare clic su **?**, se necessario, per determinare quali informazioni specificare per ciascun campo nella finestra di dialogo.
6. Fare clic su **OK** per connettersi all'unità di controllo del dominio.

Abilitare le associazioni normativa per un dominio

Un'associazione normativa consente di creare corrispondenze molte a una in situazioni in cui non esistono associazioni tra identità utente e un identificativo EIM.

È possibile utilizzare un'associazione normativa per mettere in corrispondenza una serie di origine di diverse identità utente (invece che una singola identità utente) con una singola identità utente di destinazione all'interno di un registro utente di destinazione specificato. Prima di poter utilizzare le associazioni normativa, tuttavia, è necessario innanzitutto accertarsi che l'utente abiliti il dominio all'utilizzo di associazioni normativa per operazioni di ricerca corrispondenze.

Per abilitare il supporto normativa corrispondenze ad utilizzare le associazioni normativa per un dominio, è necessario essere connessi al dominio EIM in cui si desidera lavorare e bisogna avere il controllo di accesso amministratore EIM.

Per abilitare il supporto di ricerca delle corrispondenze per utilizzare le associazioni normativa per un dominio, completare le seguenti operazioni:

1. Espandere **Rete > EIM (Enterprise Identity Mapping) > Gestione domini**.
2. Fare clic con il tasto destro del mouse sul dominio EIM in cui si desidera lavorare e selezionare **Normativa corrispondenza**.
   - Se il dominio EIM che si desidera gestire non è elencato in **Gestione domini**, è necessario aggiungere un dominio EIM alla cartella relativa alla gestione domini.
   - Se attualmente non si è connessi al dominio EIM in cui si desidera lavorare, è necessario connettersi all'unità di controllo del dominio EIM. (L'opzione **Normativa corrispondenza** non è disponibile fino a quando non ci si connette al dominio.)
3. Sulla pagina **Generale**, selezionare **Abilita ricerche di corrispondenza tramite associazioni normativa per dominio**.

4. Fare clic su **OK**.

Nota: È necessario abilitare le ricerche di corrispondenze l'uso di associazioni normativa per ogni definizione registro destinazione per cui sono state specificate associazioni normativa. Se non si abilitano le ricerche di corrispondenza per la definizione di registro di destinazione, tale registro non può partecipare alle operazioni di ricerca corrispondenze EIM. Se non si specifica che il registro destinazione può utilizzare associazioni normativa, qualsiasi associazione normativa definita per tale registro viene ignorata dalle operazioni di ricerca corrispondenze EIM.

Concetti correlati

"Abilitazione e supporto normativa corrispondenze EIM" a pagina 38
Il supporto normativa corrispondenze EIM (Enterprise Identity Mapping) consente di utilizzare le associazioni normativa ed anche delle specifiche associazioni di identificativi in un dominio EIM. È possibile utilizzare le associazioni normativa invece di, oppure insieme ad, associazioni di identificativi.

Verifica delle corrispondenze

La verifica delle corrispondenze EIM (Enterprise Identity Mapping) consente di eseguire le operazioni di ricerca di corrispondenze EIM nella configurazione EIM. È possibile utilizzare la verifica per controllare che una specifica identità utente di origine corrisponda esattamente all'identità utente di destinazione appropriata. La verifica assicura che le operazioni di ricerca delle corrispondenze EIM possano restituire l'identità utente destinazione corretta in base alle informazioni specificate.

Per utilizzare la funzione di verifica delle corrispondenze per la verifica della configurazione EIM, è necessario essere connessi al dominio EIM in cui si desidera lavorare ed è necessario disporre del controllo di accesso EIM a uno dei seguenti livelli:

- Amministratore EIM
- Amministratore identificativo
- Amministratore registro
- Operazioni di ricerca corrispondenza EIM

Per utilizzare il supporto di verifica delle corrispondenze per controllare la configurazione EIM, completare le seguenti operazioni:

1. Espandere **Rete > EIM (Enterprise Identity Mapping) > Gestione domini**.
2. Selezionare il dominio EIM in cui si desidera lavorare.
   - Se il dominio EIM che si desidera gestire non è elencato in **Gestione domini**, consultare Aggiunta di un dominio EIM a Gestione domini.
   - Se attualmente non si è collegati al dominio EIM in cui si desidera lavorare, consultare Connessione all'unità di controllo del dominio EIM.
3. Fare clic con il tasto destro del mouse sul dominio EIM a cui si è connessi e selezionare **Verifica una corrispondenza**
4. Nella finestra di dialogo **Verifica una corrispondenza**, specificare le seguenti informazioni:
   a. Nel campo **Registro di origine**, inserire il nome della definizione del registro che fa riferimento al registro utente da utilizzare come origine dell'operazione di ricerca della corrispondenza per la verifica.
   b. Nel campo **Utente di origine**, immettere il nome dell'identità utente da utilizzare come origine dell'operazione di ricerca della corrispondenza per la verifica.
   c. Nel campo **Registro di destinazione**, immettere il nome della definizione del registro che fa riferimento al registro utente da utilizzare come destinazione dell'operazione di ricerca della corrispondenza per la verifica.
   d. Facoltativo: nel campo **Informazioni di ricerca**, inserire le informazioni di ricerca definite per l'utente di destinazione.

5. Fare clic su **?**, se necessario, per ulteriori dettagli sulle informazioni necessarie per ciascun campo nella finestra di dialogo.
6. Fare clic su **Verifica** e rivedere i risultati dell'operazione di ricerca delle corrispondenze, una volta visualizzati.

   Nota: se l'operazione di ricerca definizione restituisce risultati ambigui, la finestra di dialogo Verifica una corrispondenza - - Risultati viene visualizzata con un messaggio di errore e un elenco di utenti di destinazione rilevato dall'operazione di ricerca.

   a. Per risolvere i problemi dovuti a risultati ambigui, selezionare un utente di destinazione e fare clic su **Dettagli**.
   b. La finestra di dialogo Verifica una corrispondenza - Risultati viene visualizzata con informazioni relative ai risultati dell'operazione di ricerca definizione per l'utente di destinazione specificato. Fare clic su ? per informazioni dettagliate sui risultati dell'operazione di ricerca definizione.
   c. Fare clic su **Chiudi** per uscire dalla finestra di dialogo **Verifica una corrispondenza - Risultati**.
7. Procedere con la verifica della configurazione oppure fare clic su **Chiudi** per uscire.

Concetti correlati

"Risoluzione dei problemi di corrispondenza EIM" a pagina 130
Ci sono vari problemi comuni che possono determinare un mancato funzionamento o un funzionamento imprevisto delle corrispondenze EIM (Enterprise Identity Mapping). Consultare la seguente tabella per trovare informazioni relative al problema che potrebbe essere la causa di un malfunzionamento delle corrispondenze EIM e sulle potenziali soluzioni per detto problema. Se si sta verificando un malfunzionamento delle corrispondenze EIM, è possibile che occorra verificare ciascuna delle soluzioni contenute nella tabella per essere sicuri di trovare e risolvere il problema o i problemi che stanno determinando il malfunzionamento delle corrispondenze.

Gestione dei risultati della verifica e risoluzione dei problemi:

Quando si esegue una verifica, viene restituita un'identità utente di destinazione se la verifica rileva un'associazione tra l'identità utente di origine e il registro utente di destinazione fornito dall'amministratore. La verifica inoltre indica il tipo di associazione rilevata tra le due identità utente. Quando l'operazione di verifica non rileva alcuna associazione sulla base delle informazioni fornite, viene restituita un'identità utente di destinazione `none`.

La verifica, come qualsiasi altra operazione di ricerca corrispondenze EIM, ricerca e restituisce la prima identità utente di destinazione appropriata, effettuando la ricerca nel seguente ordine:

1. Associazione identificativo specifica
2. Associazione normative filtro certificato
3. Associazione normativa registro predefinita
4. Associazione normativa dominio predefinita

In alcuni casi, la verifica non restituisce alcun risultato di identità utente di destinazione, anche se ci sono delle associazioni configurate per il dominio. Verificare di avere fornito le informazioni corrette per la verifica. Se le informazioni sono corrette e la verifica non restituisce alcun risultato, il problema potrebbe essere stato causato da uno dei seguenti fattori:

- Il supporto delle associazioni normativa non è abilitato a livello del dominio. È possibile che occorra abilitare le associazioni normativa per un dominio.
- Il supporto di ricerca corrispondenze o il supporto di associazioni normativa non è abilitato a livello di singolo registro. Potrebbe essere necessario abilitare il supporto di ricerca di corrispondenze e l'utilizzo delle associazioni normativa per il registro di destinazione.
- Un'associazione di destinazione o di origine per un identificativo EIM non è configurata correttamente. Non esiste, ad esempio, un'associazione di origine per il principal Kerberos (o per l'utente Windows)

oppure essa non è corretta. Questo potrebbe anche essere dovuto al fatto che l'associazione di destinazione specifica un'identità utente non corretta. Visualizzare tutte le associazioni di identificativi per un identificativo EIM per verificare le associazioni per uno specifico identificativo.
- Un'associazione normativa non è configurata correttamente. Visualizzare tutte le associazioni normativa per un dominio per verificare le informazioni di destinazione e di origine per tutte le associazioni normativa definite nel dominio.
- La definizione di registro e le identità utente non corrispondono perché sono sensibili al maiuscolo/minuscolo. È possibile cancellare e creare nuovamente il registro oppure cancellare e creare nuovamente le associazioni utilizzando la corretta sequenza di maiuscole/minuscole.

In altri casi la verifica può restituire dei risultati ambigui. In questo caso, viene visualizzato un messaggio di errore. La verifica risulta ambigua quando più di un'identità utente di destinazione corrisponde ai criteri di verifica specificati. Un'operazione di ricerca corrispondenze può restituire più identità utente destinazione quando si verificano una o più delle seguenti situazioni:
- Un identificativo EIM ha più associazioni di destinazione singole per lo stesso registro destinazione.
- Più di un identificativo EIM ha la stessa identità utente specificata in un'associazione di origine e ciascuno di questi identificativi EIM ha un'associazione di destinazione allo stesso registro di destinazione, anche se l'identità utente specificata per ciascuna associazione di destinazione potrebbe essere differente.
- Più di un'associazione normativa di dominio predefinita ha lo stesso registro di destinazione.
- Più di un'associazione normativa di registro predefinita specifica lo stesso registro di origine e lo stesso registro di destinazione.
- Più di un'associazione normativa filtro certificato specifica lo stesso registro X.509 di origine, lo stesso filtro di certificati e lo stesso registro di destinazione.

Un'operazione di ricerca corrispondenze che restituisce più di una identità utente di destinazione può creare problemi per applicazioni abilitate a EIM, inclusi applicazioni e prodotti i5/OS. Di conseguenza, bisogna determinare la causa dei risultati ambigui e quale azione deve essere eseguita per risolvere la situazione. In base alla causa, è possibile procedere in uno o più dei seguenti modi:
- La verifica restituisce più identità di destinazione indesiderate. Questo indica che la configurazione delle associazioni per il dominio non è corretta, per una delle seguenti cause:
  - Un'associazione di destinazione o di origine per un identificativo EIM non è configurata correttamente. Non esiste, ad esempio, un'associazione di origine per il principal Kerberos (o per l'utente Windows) oppure essa non è corretta. Questo potrebbe anche essere dovuto al fatto che l'associazione di destinazione specifica un'identità utente non corretta. Visualizzare tutte le associazioni di identificativi per un identificativo EIM per verificare le associazioni per uno specifico identificativo.
  - Un'associazione normativa non è configurata correttamente. Visualizzare tutte le associazioni normativa per un dominio per verificare le informazioni di destinazione e di origine per tutte le associazioni normativa definite nel dominio.
- La verifica restituisce più identità utente di destinazione e questi risultati sono appropriati per il modo in cui si sono configurate le associazioni ma si ha bisogno di specificare delle informazioni di ricerca per ciascuna identità utente di destinazione. Bisogna definire informazioni di ricerca univoche per tutte le identità utente di destinazione che hanno la stessa origine (un identificativo EIM per associazioni di identificativi o un registro utenti di origine per le associazioni normativa). Definendo delle informazioni di ricerca per ciascuna identità utente di destinazione, si assicura che un'operazione di ricerca restituisca una singola identità utente di destinazione invece di tutte le possibili identità utente di destinazione. Consultare Aggiunta informazioni di ricerca ad un'identità utente di destinazione. È necessario specificare queste informazioni di ricerca relative all'operazione di ricerca corrispondenze.

  Nota: tale approccio funziona solo se l'applicazione può utilizzare le informazioni di ricerca. Tuttavia, le applicazioni base i5/OS come System i Access per Windows non possono utilizzare le informazioni di ricerca per distinguere tra più identità utenti di destinazione restituite da

un'operazione di ricerca. Di conseguenza, è possibile prendere in considerazione il ridefinire le associazioni per il dominio per assicurare che un'operazione di ricerca di corrispondenze possa restituire una singola identità utente di destinazione per assicurare che le applicazioni i5/OS di base possano eseguire correttamente le operazioni di ricerca e eseguire messe in corrispondenza di identità.

Eliminazione di un dominio EIM dalla cartella Gestione domini

È possibile eliminare un dominio EIM che non si desidera più gestire dalla cartella **Gestione domini**. Tuttavia, rimuovere il dominio dalla cartella **Gestione domini non** equivale a cancellare il dominio e non cancella i dati del dominio dall'unità di controllo del dominio.

Non è necessario disporre di alcun controllo di accesso EIM per eliminare un dominio.

Per rimuovere un dominio EIM che non si desidera più gestire dalla cartella **Gestione domini**, attenersi alla seguente procedura:

1. Espandere **Rete >EIM (Enterprise Identity Mapping)**.
2. Fare clic con il tasto destro del mouse su **Gestione domini** e selezionare **Elimina dominio**.
3. Selezionare il dominio EIM che si desidera eliminare da **Gestione domini**.
4. Fare clic su **OK** per eliminare il dominio.

Attività correlate

"Cancellazione di un dominio EIM e di tutti gli oggetti di configurazione"
Prima di potere cancellare un dominio EIM, è necessario cancellare tutte le definizioni di registro e tutti gli identificativi EIM (Enterprise Identity Mapping) nel dominio. Se non si desidera cancellare il dominio e tutti i dati relativi, ma non si desidera più gestirlo, è possibile scegliere di eliminare il dominio.

Cancellazione di un dominio EIM e di tutti gli oggetti di configurazione

Prima di potere cancellare un dominio EIM, è necessario cancellare tutte le definizioni di registro e tutti gli identificativi EIM (Enterprise Identity Mapping) nel dominio. Se non si desidera cancellare il dominio e tutti i dati relativi, ma non si desidera più gestirlo, è possibile scegliere di eliminare il dominio.

Per cancellare un dominio EIM, è necessario disporre del controllo di accesso EIM a uno di questi livelli:

- Amministratore LDAP.
- Amministratore EIM.

1. Espandere **Rete > EIM (Enterprise Identity Mapping) > Gestione domini**.
2. Se necessario, cancellare tutte le definizioni di registro dal dominio EIM.
3. Se necessario, eliminare tutti gli identificativi EIM dal dominio EIM.
4. Fare clic con il tasto destro del mouse sul dominio che si desidera cancellare e selezionare **Cancella**.
5. Fare clic su **Sì** sulla finestra di dialogo **Conferma cancellazione**.

Nota: la finestra di dialogo relativa all'eliminazione in corso viene visualizzata per indicare lo stato dell'eliminazione del dominio fino al completamento del processo.

Attività correlate

"Eliminazione di un dominio EIM dalla cartella Gestione domini"
È possibile eliminare un dominio EIM che non si desidera più gestire dalla cartella **Gestione domini**. Tuttavia, rimuovere il dominio dalla cartella **Gestione domini non** equivale a cancellare il dominio e non cancella i dati del dominio dall'unità di controllo del dominio.

Gestione delle definizioni di registro di EIM

Per fare in modo che i registri utenti e le identità utenti in essi contenute partecipino a un dominio EIM (Enterprise Identity Mapping), è necessario creare definizioni di registro per essi. Sarà quindi possibile gestire la modalità di partecipazione ad EIM dei registri utenti e delle relative identità, semplicemente gestendo queste definizioni di registro.

È possibile effettuare le seguenti attività di gestione per le definizioni dei registri:

Concetti correlati

"Creazione di un'associazione normativa" a pagina 110
Un'associazione normativa fornisce un metodo per definire direttamente una relazione tra più identità utente in uno o più registri ed una singola identità utente di destinazione in un altro registro.

Attività correlate

"Cancellazione di un'associazione normativa" a pagina 124
Per eliminare un'associazione normativa, è necessario essere connessi al dominio EIM (Enterprise Identity Mapping) in cui si desidera lavorare e bisogna disporre del controllo di accesso EIM come Amministratore registro oppure come amministratore EIM.

Aggiunta di una definizione del registro di sistema

Per creare una definizione registro sistema, è necessario essere connessi al dominio EIM (Enterprise Identity Mapping) in cui si desidera lavorare e disporre del controllo di accesso dell'amministratore EIM.

Per aggiungere una definizione di registro di sistema ad un dominio EIM, attenersi alla seguente procedura:

1. Espandere **Rete > EIM (Enterprise Identity Mapping) > Gestione domini**.
2. Selezionare il dominio EIM in cui si desidera lavorare.
   - Se il dominio EIM con il quale si desidera lavorare non è elencato in Gestione domini, consultare "Aggiunta di un dominio EIM alla cartella Gestione domini" a pagina 92.
   - Se attualmente non si è connessi al dominio EIM in cui si desidera lavorare, consultare "Connessione a un dominio EIM" a pagina 93.
3. Espandere il dominio EIM a cui si è ora collegati.
4. Fare clic con il tasto destro del mouse su **Registri utente**, selezionare **Aggiungi registro** e selezionare quindi **Sistema**.
5. Nella casella di dialogo **Aggiungi registro di sistema**, fornire le informazioni relative alla definizione del registro di sistema come segue:
   a. Un nome per la definizione del registro di sistema.
   b. Un tipo di definizione del registro.
   c. Una descrizione della definizione del registro di sistema.
   d. (Facoltativo.) L'URL registro utenti.
   e. Uno o più alias per la definizione del registro di sistema, se necessari.
6. Fare clic su **OK** per salvare le informazioni e aggiungere la definizione del registro al dominio EIM.

Aggiunta di una definizione del registro dell'applicazione

Per creare una definizione registro applicazione, è necessario essere connessi al dominio EIM (Enterprise Identity Mapping) in cui si desidera lavorare e disporre del controllo di accesso dell'amministratore EIM.

Per aggiungere una definizione di registro applicazioni a un dominio EIM, completare le seguenti operazioni:

1. Espandere **Rete > EIM (Enterprise Identity Mapping) > Gestione domini**.
2. Selezionare il dominio EIM in cui si desidera lavorare.
   - Se il dominio EIM con il quale si desidera lavorare non è elencato in Gestione domini, consultare "Aggiunta di un dominio EIM alla cartella Gestione domini" a pagina 92.

- Se attualmente non si è connessi al dominio EIM in cui si desidera lavorare, consultare "Connessione a un dominio EIM" a pagina 93.

3. Espandere il dominio EIM a cui si è ora collegati.
4. Fare clic con il tasto destro del mouse su **registri utente**, selezionare **Aggiungi Registro** e selezionare quindi **Applicazione**.
5. Nella finestra di dialogo **Aggiungi registro applicazione**, fornire le informazioni sulla definizione del registro applicazioni, come di seguito illustrato:
   a. Un nome per la definizione del registro applicazioni.
   b. Il nome della definizione registro sistema di cui il registro utenti applicazione che si sta definendo è una sottoserie. La definizione di registro di sistema che si specifica deve esistere già in EIM, altrimenti la creazione della definizione di registro applicazione ha esito negativo.
   c. Un tipo di definizione del registro.
   d. Una descrizione della definizione del registro dell'applicazione.
   e. Uno o più alias per la definizione del registro dell'applicazione, se necessari.
6. Fare clic su **?**, se necessario, per stabilire le informazioni da specificare per ciascun campo.
7. Fare clic su **OK** per salvare le informazioni e aggiungere la definizione del registro al dominio EIM.

Concetti correlati

"Definizioni registro utenti" a pagina 14
Una definizione di registro di sistema è una voce che si crea in EIM per rappresentare e descrivere un registro utenti distinto in una rete o in un server.

Aggiunta di una definizione del registro di gruppo

Per creare una definizione registro gruppo, è necessario essere connessi al dominio EIM in cui si desidera operare ed è necessario disporre del controllo di accesso dell'amministratore EIM.

Per aggiungere una definizione del registro di gruppo a un dominio EIM, completare le seguenti operazioni:

1. Espandere **Rete → EIM (Enterprise Identity Mapping) → Gestione domini.**
2. Selezionare il dominio EIM in cui si desidera lavorare.
   a. Se il dominio EIM che si desidera gestire non è elencato in Gestione domini, consultare la sezione relativa all'aggiunta di un dominio EIM a Gestione domini.
   b. Se attualmente non si è conness al dominio EIM in cui si desidera lavorare, consultare Connessione all'unità di controllo del dominio EIM.
3. Espandere il dominio EIM a cui si è connessi.
4. Fare clic con il tasto destro del mouse su **registri utenti**, selezionare **Aggiungi registro**, quindi selezionare **Gruppo.**
5. Nella finestra di dialogo Aggiungi registro di gruppo, fornire le informazioni sulla definizione di tale registro, nel seguente modo:
   a. Un nome per la definizione del registro di gruppo.
   b. Selezionare **I membri del registro di gruppo sono sensibili al maiuscolo/minuscolo** se tutti i membri della definizione del registro di gruppo sono sensibili al maiuscolo/minuscolo.
   c. Una descrizione della definizione del registro di gruppo.
   d. Uno o più alias per la definizione del registro di gruppo, se necessari.
6. Fare clic su **?**, se necessario, per stabilire le informazioni da specificare per ciascun campo.
7. Fare clic su **OK** per salvare le informazioni e aggiungere la definizione del registro al dominio EIM.

Aggiunta di un alias ad una definizione di registro

L'utente, o lo sviluppatore dell'applicazione, può specificare delle informazioni di distinzione aggiuntive per una definizione di registro. È possibile eseguire quest'operazione creando un alias per la definizione di registro. L'alias per la definizione di registro può essere poi utilizzato per meglio distinguere un registro utenti da un altro.

Gli alias permettono ai programmatori di scrivere applicazioni senza dover conoscere in anticipo il nome di definizione del registro EIM arbitrario scelto dall'amministratore che distribuisce l'applicazione. La documentazione dell'applicazione può fornire all'amministratore EIM il nome alias utilizzato dall'applicazione. Utilizzando queste informazioni, l'amministratore EIM può assegnare questo nome alias alla definizione del registro EIM che rappresenta il vero registro utente che l'amministratore desidera venga utilizzato dall'applicazione.

Per aggiungere un alias a una definizione di registro, è necessario essere connessi al dominio EIM in cui si desidera lavorare ed è necessario disporre del controllo di accesso EIM a uno di questi livelli:

- Amministratore di registro.
- Amministratore dei registri selezionati (per il registro che si sta modificando).
- Amministratore EIM.

Per aggiungere un alias ad una definizione registro EIM, completare le seguenti operazioni:

1. Espandere **Rete > EIM (Enterprise Identity Mapping) > Gestione domini**.
2. Selezionare il dominio EIM in cui si desidera lavorare.
   - Se il dominio EIM con il quale si desidera lavorare non è elencato in Gestione domini, consultare "Aggiunta di un dominio EIM alla cartella Gestione domini" a pagina 92.
   - Se attualmente non si è connessi al dominio EIM in cui si desidera lavorare, consultare "Connessione a un dominio EIM" a pagina 93.
3. Espandere il dominio EIM a cui si è ora collegati.
4. Fare clic su **Registri utenti** per visualizzare l'elenco di definizioni di registro all'interno del dominio.

   Nota: se si ha il livello Amministratore per il controllo accesso ai registri selezionati, l'elenco contiene solo quelle definizioni registro per cui si dispone di specifica autorizzazione.
5. Fare clic con il tasto destro del mouse sulla definizione di registro per cui si desidera aggiungere un alias e selezionare **Proprietà**.
6. Selezionare la pagina **Alias** e specificare il nome ed il tipo di alias che si desidera aggiungere.

   Nota: è possibile specificare un tipo di alias che non è presente nell'elenco dei tipi.
7. Fare clic su **?**, se necessario, per determinare le informazioni da specificare per ciascun campo.
8. Fare clic su **Aggiungi**.
9. Fare clic su **OK** per salvare le modifiche apportate alla definizione di registro.

Definizione di un tipo di registro utente privato in EIM

Quando si crea una definizione di registro EIM (Enterprise Identity Mapping) è possibile specificare uno dei vari tipi di registro utenti predefiniti per rappresentare un effettivo registro utenti che esiste su un sistema all'interno della propria azienda.

I tipi di definizione di registro predefiniti abbracciano la maggior parte dei registri utenti di sistema operativo; è possibile che occorra creare una definizione di registro per cui EIM non include un tipo di registro predefinito. In questo caso esistono due opzioni. È possibile utilizzare una definizione di registro esistente che corrisponde alle caratteristiche del proprio registro utenti oppure è possibile definire un tipo di registro utenti privato.

Per definire un tipo di registro privato che EIM non riconosce come predefinito, è necessario utilizzare un OID (object identity - identità oggetto) per specificare il tipo di registro nel formato **IdentificativoOggetto-normalizzazione**, dove **IdentificativoOggetto** è un identificativo oggetto decimale puntato, ad esempio 1.2.3.4.5.6.7, e **normalizzazione** è il valore **caseExact** o il valore **caseIgnore**. Ad esempio, l'OID (object identifier) per System i è `1.3.18.0.2.33.2-caseIgnore`.

Ottenere gli OID necessari dalle autorità di registrazione OID legittimate per accertarsi di creare ed utilizzare OID univoci. Gli OID univoci sono di ausilio per evitare potenziali conflitti con gli OID creati da altre organizzazioni o applicazioni.

Esistono due modi per ottenere gli OID:

- **Registrare gli oggetti con un'autorizzazione**. Questo metodo si rivela una buona scelta quando si necessita di un piccolo numero di OID corretti per rappresentare le informazioni. Ad esempio, questi OID potrebbero rappresentare le normative di certificazione per gli utenti nella società.
- **Ottenere un'assegnazione di partenza da un'autorità di registrazione ed assegnare i propri OID come necessario**. Questo metodo, che costituisce un'assegnazione di intervallo identificativo oggetto decimale puntato, si rivela una buona scelta se si necessita di un ampio numero di OID oppure se le proprie assegnazioni OID sono soggette a modifica. L'assegnazione di partenza è composta da numeri decimali puntati iniziali su cui basare il proprio **IdentificativoOggetto**. Ad esempio, l'assegnazione di partenza potrebbe essere `1.2.3.4.5.`. È quindi possibile creare gli OID aumentando questo identificativo di partenza di base. Ad esempio, è possibile creare gli OID nel formato `1.2.3.4.5.x.x.x)`.

Ulteriori informazioni sulla registrazione dei propri OID tramite un'autorità di registrazione possono essere reperite sulle seguenti risorse Internet:

- ANSI (American National Standards Institute) costituisce l'autorità di registrazione negli Stati Uniti per i nomi di organizzazione nel processo di registrazione globale stabilito da ISO (International Standards Organization) e ITU (International Telecommunication Union). Un modulo in formato Microsoft Word per richiedere un RID (Registered Application Provider Identifier) si trova nel sito Web della ANSI Public Document Library, all'indirizzo http://public.ansi.org/ansionline/Documents/. È possibile trovare il modulo selezionando **Other Services > Registration Programs**. L'identificativo OID di partenza ANSI per le organizzazioni è `2.16.840.1`. ANSI addebita una tariffa per le assegnazioni dell'identificativo OID di partenza. È necessario attendere circa due settimane prima di ricevere l'identificativo OID di partenza assegnato dall'ANSI. ANSI assegnerà un numero (NEWNUM) per creare un nuovo identificativo OID di partenza; ad esempio `2.16.840.1.NEWNUM`.
- Nella maggior parte dei paesi o regioni, l'associazione degli standard nazionale conserva un registro di OID. Come con gli identificativi ANSI di partenza, questi sono di norma degli identificativi di partenza assegnati sotto l'OID `2.16`. Potrebbero essere necessarie delle ricerche per individuare l'autorità OID di un particolare paese o regione. Gli indirizzi per gli organi ISO nazionali si trovano all'indirizzo http://www.wssn.net/WSSN/listings/links_national.html. Le informazioni includono l'indirizzo postale e l'indirizzo di posta elettronica. In molti casi, viene specificato anche un indirizzo web.
- IANA (Internet Assigned Numbers Authority) assegna numeri privati per la società, ossia OID, all'identificativo di partenza `1.3.6.1.4.1`. IANA ha assegnato identificativi di partenza a più di 7.500 società fino ad oggi. La pagina per la richiesta si trova all'indirizzo http://www.iana.org/cgi-bin/enterprise.pl, sotto Private Enterprise Numbers. IANA impiega generalmente una settimana. Un OID proveniente da IANA è gratuito. IANA assegnerà un numero (NEWNUM) in modo che il nuovo identificativo OID di partenza sarà `1.3.6.1.4.1.NEWNUM`.
- Il Governo Federale degli Stati Uniti gestisce il CSOR (Computer Security Objects Registry). Il CSOR è l'autorità di denominazione per l'identificativo di partenza `2.16.840.1.101.3` e attualmente registra gli oggetti per le etichette di sicurezza, gli algoritmi crittografici e le normative di certificazione. Gli OID della normativa di certificazione sono definiti nell'identificativo di partenza `2.16.840.1.101.3.2.1`. Il

CSOR fornisce gli OID normativa alle agenzie del Governo Federale Statunitense. Per ulteriori informazioni sul CSOR, consultare http://www.csrc.nist.gov/pki/CSOR/csor.html .

Concetti correlati

"Definizioni di registro EIM" a pagina 11
Una definizione registro EIM (Enterprise Identity Mapping) è una voce all'interno di EIM che si crea per rappresentare un registro utenti effettivo che esiste su un sistema all'interno della propria azienda. Un registro utenti funziona come un indirizzario e contiene un elenco di identità utente valide per un determinato sistema o applicazione.

Abilitazione del supporto di ricerca corrispondenze e dell'uso di associazioni normativa per un registro destinazione

Il supporto normativa di corrispondenza EIM (Enterprise Identity Mapping) permette di utilizzare le associazioni normativa come un mezzo per la creazione di corrispondenze di tipo 'molti a uno' in situazioni in cui non esistono associazioni tra delle identità utente e un identificativo EIM. È possibile utilizzare un'associazione normativa per mettere in corrispondenza una serie origine di più identità utente (piuttosto che una singola identità utente) con una singola identità utente di destinazione in un registro utenti di destinazione specificato.

Prima di poter utilizzare le associazioni normativa, tuttavia, è necessario innanzitutto accertarsi che l'utente abiliti ricerche di corrispondenze tramite associazioni normativa per il dominio. È necessario anche abilitare una o due impostazioni per ogni registro:

- **Abilita ricerche di corrispondenze per il registro** Selezionare questa opzione per assicurarsi che il registro possa partecipare alle operazioni di ricerca corrispondenze EIM, indipendentemente dal fatto che sia stata definita qualche associazione normativa per il registro.
- **Utilizza associazioni normativa** Selezionare quest'opzione per consentire a questo registro di essere il registro di destinazione di un'associazione normativa e garantire che possa partecipare alle operazioni di ricerca corrispondenze EIM.

Se non si abilitano le ricerche di corrispondenza per il registro, questo non può partecipare affatto alle operazioni di ricerca corrispondenze EIM. Se non si specifica che il registro utilizza associazioni normativa, le operazioni di ricerca corrispondenze EIM ignorano qualsiasi associazione normativa per il registro quando il registro è la destinazione dell'operazione.

Per abilitare le ricerche di corrispondenze all'utilizzo di associazioni normativa per un registro di destinazione, è necessario essere collegati al dominio EIM in cui si desidera lavorare e bisogna avere "Controllo di accesso EIM" a pagina 39 ad uno di questi livelli:

- Amministratore EIM
- Amministratore registro
- Amministratore per registri selezionati (per i registri che si desidera abilitare)

Per abilitare il supporto di ricerca delle corrispondenze in generale, e per consentire l'utilizzo delle associazioni normativa nello specifico, per un registro di destinazione, completare le seguenti operazioni:

1. Espandere **Rete > EIM (Enterprise Identity Mapping) > Gestione domini**.
2. Selezionare il dominio EIM in cui si desidera lavorare.
   - Se il dominio EIM con il quale si desidera lavorare non è elencato in **Gestione domini**, consultare "Aggiunta di un dominio EIM alla cartella Gestione domini" a pagina 92.
   - Se attualmente non si è collegati al dominio EIM in cui si desidera lavorare, consultare Connessione all'unità di controllo del dominio EIM.
3. Selezionare **Registri utenti** per visualizzare un elenco delle definizioni di registro per il dominio.

   Nota: se si ha il livello Amministratore per il controllo accesso ai registri selezionati, l'elenco contiene solo quelle definizioni registro per cui si dispone di specifica autorizzazione.

4. Fare clic con il tasto destro del mouse sulla definizione di registro per cui si desidera abilitare il supporto normativa di corrispondenza per associazioni normativa e selezionare **Normativa corrispondenza**
5. Nella pagina **Generale**, selezionare **Abilita ricerche di corrispondenza per il registro**. Selezionando questa opzione si consente al registro di partecipare alle operazioni di ricerca corrispondenze EIM. Se questa opzione non è selezionata, un'operazione di ricerca non può restituire i dati per il registro, indipendentemente dal fatto che il registro sia il registro di origine o il registro destinazione nell'operazione di ricerca.
6. Selezionare **Utilizza associazioni normativa**. Selezionando questa opzione si consente alle operazioni di ricerca di utilizzare associazioni normativa come basi per la restituzione di dati quando il registro è la destinazione dell'operazione di ricerca.
7. Fare clic su **OK** per salvare le modifiche.

Nota: prima che qualsiasi registro possa utilizzare le associazioni normativa, è necessario anche assicurarsi di abilitare le associazioni normativa per un dominio.

Concetti correlati

"Abilitazione e supporto normativa corrispondenze EIM" a pagina 38
Il supporto normativa corrispondenze EIM (Enterprise Identity Mapping) consente di utilizzare le associazioni normativa ed anche delle specifiche associazioni di identificativi in un dominio EIM. È possibile utilizzare le associazioni normativa invece di, oppure insieme ad, associazioni di identificativi.

Cancellazione di una definizione di registro

Quando si cancella una definizione di registro da un dominio EIM (Enterprise Identity Mapping), non viene coinvolto il registro utente a cui fa riferimento la definizione del registro ma tale registro utenti non potrà più partecipare al dominio EIM.

È necessario considerare questi fattori quando si cancella una definizione di registro:

- Quando si cancella una definizione di registro, si perdono tutte le associazioni per detto registro utenti. Se si definisce nuovamente il registro per il dominio, bisogna creare nuovamente le associazioni necessarie.
- Quando si cancella una definizione di registro X.509, si perdono anche tutti i filtri di certificati definiti per detto registro. Se si definisce nuovamente il registro X.509 per il dominio, è necessario creare nuovamente i filtri certificato necessari.
- Non è possibile cancellare una definizione di registro di sistema se sono presenti definizioni di registro applicazione che specificano la definizione di registro di sistema come un registro principale.

Per creare una definizione registro, è necessario essere connessi al dominio EIM in cui si desidera lavorare ed è necessario disporre del controllo di accesso dell'amministratore EIM.

Per cancellare una definizione del registro EIM, completare le seguenti operazioni:

1. Espandere **Rete > EIM (Enterprise Identity Mapping) > Gestione domini**.
2. Selezionare il dominio EIM in cui si desidera lavorare.
   - Se il dominio EIM con il quale si desidera lavorare non è elencato in **Gestione domini**, consultare "Aggiunta di un dominio EIM alla cartella Gestione domini" a pagina 92.
   - Se attualmente non si è collegati al dominio EIM in cui si desidera lavorare, consultare Connessione all'unità di controllo del dominio EIM.
3. Espandere il dominio EIM a cui si è connessi.
4. Fare clic su **Registri utenti** per visualizzare un elenco delle definizioni di registro per il dominio.

   Nota: se si ha il livello Amministratore per il controllo accesso ai registri selezionati, l'elenco contiene solo quelle definizioni registro per cui si dispone di specifica autorizzazione.

5. Fare clic con il tasto destro del mouse sul registro utenti che si desidera cancellare e selezionare **Cancella**.
6. Fare clic su **Sì** sulla finestra di dialogo **Conferma** per cancellare la definizione di registro.

Eliminazione di un alias da una definizione di registro

Per eliminare un alias da una definizione di registro EIM (Enterprise Identity Mapping), è necessario essere connessi al dominio EIM in cui si desidera lavorare e bisogna disporre del controllo di accesso EIM come Amministratore registro, Amministratore dei registri selezionati o amministratore EIM.

Per eliminare un alias da una definizione di registro EIM, effettuare le seguenti operazioni:

1. Espandere **Rete > EIM (Enterprise Identity Mapping) > Gestione domini**.
2. Selezionare il dominio EIM in cui si desidera lavorare.
   - Se il dominio EIM con il quale si desidera lavorare non è elencato in **Gestione domini**, consultare "Aggiunta di un dominio EIM alla cartella Gestione domini" a pagina 92.
   - Se attualmente non si è collegati al dominio EIM in cui si desidera lavorare, consultare Connessione all'unità di controllo del dominio EIM.
3. Espandere il dominio EIM a cui si è connessi.
4. Fare clic su **Registri utenti** per visualizzare un elenco delle definizioni di registro per il dominio.

   Nota: se si ha il livello Amministratore per il controllo accesso ai registri selezionati, l'elenco contiene solo quelle definizioni registro per cui si dispone di specifica autorizzazione.
5. Fare clic con il tasto destro del mouse su una definizione di registro e selezionare **Proprietà**.
6. Selezionare la pagina **Alias**.
7. Selezionare l'alias che si desidera eliminare e fare clic su **Elimina**.
8. Fare clic su **OK** per salvare le modifiche.

Aggiunta di un membro ad una definizione registro di gruppo

Per aggiungere un membro a una definizione del registro di gruppo, è necessario essere connessi al dominio EIM in cui si desidera lavorare e bisogna disporre del controllo di accesso EIM come amministratore EIM, Amministratore registro, Amministratore per i registri selezionati (sia per la definizione di registro del gruppo cui si desidera aggiungere il membro sia per la definizione di registro del gruppo cui si desidera aggiungere il membro sia per il membro individuale che si intende aggiungere).

Per aggiungere un membro a una definizione del registro di gruppo, completare le seguenti operazioni:

1. **Espandere Rete → EIM (Enterprise Identity Mapping) → Gestione domini.**
2. Selezionare il dominio EIM in cui si desidera lavorare.
   a. Se il dominio EIM che si desidera gestire non è elencato in Gestione domini, consultare la sezione relativa all'aggiunta di un dominio EIM a Gestione domini.
   b. Se attualmente non si è connessi al dominio EIM in cui si desidera lavorare, consultare Connessione all'unità di controllo del dominio EIM.
3. Espandere il dominio EIM a cui si è connessi.
4. Fare clic su **Registri utenti** per visualizzare l'elenco di definizioni di registro nel dominio.
5. 5. Fare clic con il tasto destro del mouse sulla definizione del registro di gruppo a cui si desidera aggiungere un membro e selezionare **Proprietà.**
6. Selezionare la pagina **Membri**e fare clic su **Aggiungi**.
7. Nella **finestra di dialogo Aggiungi membro del registro di gruppo EIM**, selezionare una o più definizioni di registro e fare clic su **OK**. Il contenuto dell'elenco varia in base al tipo di controllo accesso EIM che si desidera ed è limitato alle definizioni di registro con la stessa sensibilità al maiuscolo/minuscolo degli altri membri del gruppo.
8. Fare clic su **OK** per uscire.

Gestione degli identificativi EIM (Enterprise Identity Mapping)

Utilizzare queste informazioni per comprendere le modalità di creazione e gestione degli identificativi EIM per un dominio.

La creazione e l'utilizzo di identificativi EIM che rappresentano gli utenti nella propria rete può essere di notevole aiuto per tenere traccia di quale persona è proprietaria di una specifica identità utente. Gli utenti di un'azienda cambiano spesso; alcuni vengono assunti, altri licenziati e altri ancora vengono spostati da un reparto ad un altro. Queste modifiche aumentano il continuo problema amministrativo di tenere traccia delle identità e delle parole d'ordine degli utenti per i sistemi e le applicazioni nella rete. Inoltre, la gestione delle parole d'ordine in un'azienda richiede molto tempo. Creando degli identificativi EIM (Enterprise Identity Mapping) ed associandoli con le identità utente per ciascun utente, è possibile semplificare il processo di tenere traccia di chi è proprietario di una specifica identità utente. Questo semplifica anche la gestione delle parole d'ordine.

L'implementazione dell'ambiente con SSO semplifica inoltre il processo di gestione delle identità utente per gli utenti, soprattutto quando vengono spostati in un altro reparto o in un'altra area all'interno dell'azienda. L'abilitazione dell'SSO può eliminare la necessità, per questi utenti, di ricordare nuovi nomi utente e parole d'ordine per i nuovi sistemi.

Nota: il modo in cui si creano e si utilizzano degli identificativi EIM dipende dalle esigenze della propria organizzazione. Per ulteriori informazioni, consultare "Sviluppo di un piano di denominazione degli identificativi EIM" a pagina 66.

È possibile gestire gli identificativi EIM per qualsiasi dominio EIM disponibile nella cartella **Gestione domini**. È possibile eseguire tutte le operazioni seguenti, per la gestione degli identificativi EIM in un dominio EIM:

Informazioni correlate

SSO (Single sign-on)

Creazione di un identificativo EIM

Per creare un identificativo EIM, è necessario essere connessi al dominio EIM (Enterprise Identity Mapping) in cui si desidera lavorare e bisogna disporre del controllo di accesso EIM come Amministratore identificativo o amministratore EIM.

Per creare un identificativo EIM per una persona o un'entità nella propria azienda, attenersi alla seguente procedura:

1. Espandere **Rete > EIM (Enterprise Identity Mapping) > Gestione domini**.
2. Selezionare il dominio EIM in cui si desidera lavorare.
   - Se il dominio EIM con il quale si desidera lavorare non è elencato in **Gestione domini**, consultare "Aggiunta di un dominio EIM alla cartella Gestione domini" a pagina 92.
   - Se attualmente non si è connessi al dominio EIM in cui si desidera lavorare, consultare "Connessione a un dominio EIM" a pagina 93.
3. Espandere il dominio EIM a cui si è connessi.
4. Fare clic con il tasto destro del mouse su **Identificativi** e selezionare **Nuovo identificativo**.
5. Nella finestra di dialogo **Nuovo identificativo EIM**, fornire informazioni sull'identificativo EIM, nel modo seguente:
   a. Un nome per l'identificativo.
   b. Eventuale creazione di un nome univoco da parte del sistema, se necessario.
   c. Una descrizione dell'identificativo.
   d. Uno o più alias per l'identificativo, se necessario.
6. Fare clic su **?**, se necessario, per determinare le informazioni da specificare per ciascun campo.
7. Una volta inserite le informazioni richieste, fare clic su **OK** per creare l'identificativo EIM.

Nota: se si crea un gran numero di identificativi EIM, potrebbe a volte volerci del tempo per la visualizzazione dell'elenco di identificativi quando si espande la cartella **Identificativi**. Per migliorare le prestazioni quando si ha un gran numero di identificativi EIM, consultare "Personalizzazione della vista degli identificativi EIM" a pagina 107.

Aggiunta di un alias ad un identificativo EIM

È possibile creare un alias per fornire ulteriori informazioni di distinzione per un identificativo EIM. Questi ultimi possono essere di aiuto nella localizzazione di uno specifico identificativo EIM (Enterprise Identity Mapping) quando si esegue un'operazione di ricerca EIM. Ad esempio, gli alias possono essere utili nelle situazioni in cui il nome legale di un utente sia diverso dal nome con cui è conosciuto.

I nomi identificativo EIM devono essere univoci all'interno del dominio EIM. Gli alias possono risolvere situazioni in cui l'utilizzo di nomi identificativi univoci può risultare difficoltoso. Ad esempio, diversi soggetti di un'azienda possono condividere lo stesso nome; ciò può creare confusione se si utilizzano i nomi propri come identificativi EIM. Ad esempio, se ci sono due utenti che si chiamano John J. Johnson, è possibile creare un alias John Joseph Johnson per un utente e un alias John Jeffrey Johnson per rendere più semplice la distinzione dell'identità di ogni utente. Gli alias aggiuntivi possono contenere il codice impiegato dell'utente, il numero del reparto, la qualifica o altri attributi che lo contraddistinguono.

Per aggiungere un alias ad un identificativo EIM, bisogna essere collegati al dominio EIM in cui si desidera lavorare e bisogna avere "Controllo di accesso EIM" a pagina 39 ad uno di questi livelli:

- Amministratore EIM.
- Amministratore identificativo.

Per aggiungere un alias ad un identificativo EIM, completare i passi riportati di seguito.

1. Espandere **Rete > EIM (Enterprise Identity Mapping) > Gestione domini**.
2. Selezionare il dominio EIM in cui si desidera lavorare.
   - Se il dominio EIM con il quale si desidera lavorare non è elencato in **Gestione domini**, consultare "Aggiunta di un dominio EIM alla cartella Gestione domini" a pagina 92.
   - Se attualmente non si è connessi al dominio EIM in cui si desidera lavorare, consultare "Connessione a un dominio EIM" a pagina 93.
3. Espandere il dominio EIM a cui si è connessi.
4. Fare clic su **Identificativi** per visualizzare, nel pannello di destra, un elenco di identificativi disponibili nel dominio.

   Nota: quando si tenta di espandere la cartella **Identificativi**, è possibile che si impieghi parecchio tempo prima di vedere visualizzato l'elenco degli identificativi. Per migliorare le prestazioni quando si ha un gran numero di identificativi EIM nel dominio, consultare "Personalizzazione della vista degli identificativi EIM" a pagina 107.
5. Fare clic con il tasto destro del mouse sull'identificativo EIM per cui si desidera aggiungere un alias e selezionare **Proprietà**.
6. Nel campo **Alias**, specificare il nome dell'alias che si desidera aggiungere a questo identificativo EIM e fare clic su **Aggiungi**.
7. Fare clic su **OK** per salvare le modifiche apportate all'identificativo EIM.

Eliminazione di un alias da un identificativo EIM

Per eliminare un alias da un identificativo EIM (Enterprise Identity Mapping), è necessario essere connessi al dominio EIM in cui si desidera lavorare e bisogna disporre del controllo di accesso EIM come Amministratore identificativo o amministratore EIM.

Per eliminare un alias da un identificativo EIM, completare queste operazioni:

1. Espandere **Rete > EIM (Enterprise Identity Mapping) > Gestione domini**.
2. Selezionare il dominio EIM in cui si desidera lavorare.

- Se il dominio EIM con il quale si desidera lavorare non è elencato in **Gestione domini**, consultare "Aggiunta di un dominio EIM alla cartella Gestione domini" a pagina 92.
- Se attualmente non si è connessi al dominio EIM in cui si desidera lavorare, consultare "Connessione a un dominio EIM" a pagina 93.

3. Espandere il dominio EIM a cui si è connessi.
4. Fare clic su **Identificativi** per visualizzare, nel pannello di destra, un elenco di identificativi disponibili nel dominio.

   Nota: quando si tenta di espandere la cartella **Identificativi**, è possibile che si impieghi parecchio tempo prima di vedere visualizzato l'elenco degli identificativi. Per migliorare le prestazioni quando si ha un gran numero di identificativi EIM nel dominio, consultare "Personalizzazione della vista degli identificativi EIM".
5. Fare clic con il tasto destro del mouse sull'identificativo EIM per cui si desidera aggiungere un alias e selezionare **Proprietà**.
6. Selezionare l'alias che si desidera eliminare e fare clic su **Elimina**.
7. Fare clic su **OK** per salvare le modifiche.

Cancellazione di un identificativo EIM

Per cancellare un identificativo EIM, è necessario essere connessi al dominio EIM (Enterprise Identity Mapping) in cui si desidera lavorare e disporre del controllo di accesso di amministratore EIM.

Per cancellare un identificativo EIM, effettuare le seguenti operazioni:

1. Espandere **Rete > EIM (Enterprise Identity Mapping) > Gestione domini**.
2. Selezionare il dominio EIM in cui si desidera lavorare.
   - Se il dominio EIM con il quale si desidera lavorare non è elencato in **Gestione domini**, consultare "Aggiunta di un dominio EIM alla cartella Gestione domini" a pagina 92.
   - Se attualmente non si è collegati al dominio EIM in cui si desidera lavorare, consultare Connessione all'unità di controllo del dominio EIM.
3. Espandere il dominio EIM a cui si è ora collegati.
4. Fare clic su **Identificativi**.

   Nota: quando si tenta di espandere la cartella **Identificativi**, è possibile che si impieghi parecchio tempo prima di vedere visualizzato l'elenco degli identificativi. Per migliorare le prestazioni quando si ha un gran numero di identificativi EIM nel dominio, è possibile eseguire la "Personalizzazione della vista degli identificativi EIM".
5. Selezionare l'identificativo EIM che si desidera cancellare. Per cancellare più identificativi, premere il tasto **Ctrl** quando si selezionano gli identificativi EIM.
6. Fare clic con il tasto destro del mouse sugli identificativi EIM selezionati e selezionare **Cancella**.
7. Nella finestra di dialogo **Conferma cancellazione**, fare clic su **Sì** per cancellare gli identificativi EIM selezionati.

Personalizzazione della vista degli identificativi EIM

A volte, quando si tenta di espandere la cartella Identificativi è necessario attendere molto prima che venga visualizzato l'elenco di identificativi. Per migliorare le prestazioni quando si ha un gran numero di identificativi EIM (Enterprise Identity Mapping) nel dominio, è possibile personalizzare la modalità di visualizzazione della cartella Identificativi.

Per personalizzare la vista della cartella **Identificativi**, seguire questi passi:

1. Espandere **Rete —> EIM (Enterprise Identity Mapping) —> Gestione domini**.
2. Selezionare il dominio EIM in cui si desidera lavorare.
   - Se il dominio EIM con il quale si desidera lavorare non è elencato in **Gestione domini**, consultare "Aggiunta di un dominio EIM alla cartella Gestione domini" a pagina 92.

- Se attualmente non si è connessi al dominio EIM in cui si desidera lavorare, consultare "Connessione a un dominio EIM" a pagina 93.

3. Fare clic con il tasto destro del mouse sulla cartella **Identificativi** e selezionare **Personalizza questa vista**.
4. Specificare i criteri che si vogliono utilizzare per visualizzare gli identificativi EIM nel dominio. Per restringere il numero di identificativi EIM visualizzati, specificare i caratteri che si desidera utilizzare per ordinare gli identificativi. È possibile specificare uno o più caratteri jolly (*) nel nome identificativo. È ad esempio possibile immettere `*JOHNSON*` come criterio di ordinamento nel campo **Identificativi**. Il risultato restituirà tutti gli identificativi EIM dove è definita la stringa di caratteri `JOHNSON` come parte del nome di identificativo EIM e restituirà anche gli identificativi EIM dove è definita la stringa di caratteri `JOHNSON` come parte dell'alias per un identificativo EIM.
5. Fare clic su **OK** per salvare le modifiche.

Gestione di associazioni EIM

EIM consente di creare e gestire due tipi di associazioni che definiscono delle relazioni dirette o indirette tra le identità utente: associazioni di identificativi e associazioni normativa. EIM consente di creare e gestire delle associazioni di identificativi tra gli identificativi EIM e le loro identità utente; queste consentono di definire singole relazioni, indirette ma specifiche, tra identità utente.

EIM consente inoltre di creare delle associazioni normativa per descrivere una relazione tra più identità utente in uno o più registri ed una singola identità utente di destinazione in un altro registro. Le associazioni normativa utilizzano il supporto normativa corrispondenze EIM per creare corrispondenze molti-ad-uno tra identità utente senza coinvolgere un identificativo EIM. Poiché entrambi i tipi di associazioni definiscono le relazioni tra le identità utente in un'azienda, la gestione delle associazioni si rivela estremamente importante nella gestione di EIM.

Mantenere le associazioni in un dominio è la chiave per semplificare le attività amministrative richieste per tenere traccia di quali utenti hanno degli account sui vari sistemi nella rete. Quando si implementa una rete con SSO sicura, è necessario tenere aggiornate le associazioni di identificativi e le associazioni normativa.

È possibile eseguire le seguenti attività di gestione per le associazioni:

Creazione di associazioni EIM

È possibile creare due tipi di associazioni EIM diverse. È possibile creare un'associazione identificativo o un'associazione normativa.

È possibile creare un'associazione identificativo per definire indirettamente una relazione tra due identità utente utilizzate da una sola persona. Un'associazione identificativo descrive una relazione tra un identificativo EIM ed un'identità utente in un registro utenti. Le associazioni di identificativi consentono di creare corrispondenze uno ad uno tra un identificativo EIM e ciascuna delle varie identità utente relative all'utente che l'identificativo EIM rappresenta.

È possibile creare un'associazione normativa per definire direttamente una relazione tra più identità utente in uno o più registri e ed una singola identità utente di destinazione in un altro registro. Le associazioni normativa utilizzano il supporto normativa corrispondenze EIM per creare corrispondenze molti-ad-uno tra identità utente senza coinvolgere un identificativo EIM. Le associazioni normativa consentono di creare velocemente un gran numero di corrispondenze tra identità utente correlate in differenti registri utenti.

Decidere di creare associazioni di identificativi, creare associazioni normativa o utilizzare un insieme di entrambi i metodi dipende dalle proprie esigenze di implementazione EIM.

Concetti correlati

"Sviluppo di un piano di corrispondenza delle identità" a pagina 63
Una parte critica del processo di pianificazione dell'implementazione di EIM (Enterprise Identity Mapping) iniziale richiede che l'utente determini come desidera utilizzare la corrispondenza delle identità nella propria azienda.

"Creazione di un'associazione normativa" a pagina 110
Un'associazione normativa fornisce un metodo per definire direttamente una relazione tra più identità utente in uno o più registri ed una singola identità utente di destinazione in un altro registro.

Attività correlate

"Creazione di un'associazione identificativo EIM"
Le associazioni di identificativi definiscono una relazione tra un identificativo EIM (Enterprise Identity Mapping) ed un'identità utente nella propria azienda per la persona o l'entità cui fa riferimento l'identificativo EIM.

Creazione di un'associazione identificativo EIM:

Le associazioni di identificativi definiscono una relazione tra un identificativo EIM (Enterprise Identity Mapping) ed un'identità utente nella propria azienda per la persona o l'entità cui fa riferimento l'identificativo EIM.

È possibile creare tre tipi di associazione identificativo: destinazione, origine e amministrativa. Per prevenire potenziali problemi con le associazioni e con il modo in cui mettono in corrispondenza le identità, consultare "Sviluppo di un piano di corrispondenza delle identità" a pagina 63.

Per creare un'associazione identificativo, è necessario essere connessi al dominio EIM in cui si desidera lavorare ed è necessario disporre del controllo di accesso EIM richiesto dal tipo di associazione che si desidera creare.

Per creare un'associazione di origine o un'associazione amministrativa, è necessario avere il controllo accesso EIM ad uno di questi livelli:
- Amministratore identificativo.
- Amministratore EIM.

Per creare un'associazione destinazione, è necessario avere il controllo accesso EIM ad uno di questi livelli:
- Amministratore di registro.
- Amministratore per registri selezionati (per la definizione di registro che fa riferimento al registro utenti che contiene l'identità utente di destinazione)
- Amministratore EIM.

Per creare un'associazione identificativo, attenersi alla seguente procedura:
1. Espandere **Rete > EIM (Enterprise Identity Mapping) > Gestione domini**.
2. Selezionare il dominio EIM in cui si desidera lavorare.
   - Se il dominio EIM con il quale si desidera lavorare non è elencato in **Gestione domini**, consultare "Aggiunta di un dominio EIM alla cartella Gestione domini" a pagina 92.
   - Se attualmente non si è connessi al dominio EIM in cui si desidera lavorare, consultare "Connessione a un dominio EIM" a pagina 93.
3. Espandere il dominio EIM a cui si è ora collegati.
4. Fare clic su **Identificativi** per visualizzare l'elenco di identificativi EIM del dominio.

   Nota: quando si tenta di espandere la cartella **Identificativi**, è possibile che si impieghi parecchio tempo prima di vedere visualizzato l'elenco degli identificativi. Per migliorare le prestazioni quando si ha un gran numero di identificativi EIM nel dominio, consultare "Personalizzazione della vista degli identificativi EIM" a pagina 107.

5. Fare clic con il tasto destro del mouse sull'identificativo EIM per il quale si desidera creare un'associazione e selezionare **Proprietà...**
6. Selezionare la pagina **Associazioni** e fare clic su **Aggiungi...**.
7. Nella finestra di dialogo **Aggiungi associazione**, fornire le informazioni per definire l'associazione, come di seguito riportato:
   - Il nome del registro contenente l'identità utente che si desidera associare all'identificativo EIM. Specificare il nome esatto di una definizione registro esistente o scorrere per selezionarne una.
   - Il nome dell'identità utente che si desidera associare all'identificativo EIM.
   - Il tipo di associazione. È possibile creare uno di questi tre diversi tipi di associazioni:
     – Amministrativa
     – Origine
     – Destinazione
8. Fare clic su **?**, se necessario, per determinare le informazioni da specificare per ciascun campo.
9. Facoltativo. Per un'associazione di destinazione, fare clic su **Avanzate...** per visualizzare la finestra di dialogo **Aggiungi associazione - Avanzate**. Specificare le informazioni di ricerca per l'identità utente di destinazione e fare clic su **OK** per ritornare alla finestra di dialogo **Aggiungi associazione**.
10. Una volta fornite le informazioni necessarie, fare clic su **OK** per creare l'associazione.

Concetti correlati

"Creazione di associazioni EIM" a pagina 108
È possibile creare due tipi di associazioni EIM diverse. È possibile creare un'associazione identificativo o un'associazione normativa.

Creazione di un'associazione normativa:

Un'associazione normativa fornisce un metodo per definire direttamente una relazione tra più identità utente in uno o più registri ed una singola identità utente di destinazione in un altro registro.

Le associazioni normativa utilizzano il supporto normativa corrispondenze EIM per creare corrispondenze molti-ad-uno tra identità utente senza coinvolgere un identificativo EIM. Poiché è possibile utilizzare le associazioni normativa in diversi modi che si sovrappongono, è necessario avere una conoscenza approfondita del supporto normativa di corrispondenza EIM prima di creare e utilizzare le associazioni normativa. Inoltre, per prevenire potenziali problemi con le associazioni e con il modo in cui mettono in corrispondenza le identità, è necessario sviluppare un piano di corrispondenza di identità generale per la propria azienda prima di iniziare a definire le associazioni.

Decidere di creare associazioni di identificativi, creare associazioni normativa o utilizzare un insieme di entrambi i metodi dipende dalle proprie esigenze di implementazione EIM.

La modalità di creazione di un'associazione normativa varia in base al tipo di associazione normativa. Per maggiori informazioni sulla creazione di un'associazione normativa, consultare:

Concetti correlati

"Gestione delle definizioni di registro di EIM" a pagina 98
Per fare in modo che i registri utenti e le identità utenti in essi contenute partecipino a un dominio EIM (Enterprise Identity Mapping), è necessario creare definizioni di registro per essi. Sarà quindi possibile gestire la modalità di partecipazione ad EIM dei registri utenti e delle relative identità, semplicemente gestendo queste definizioni di registro.

"Creazione di associazioni EIM" a pagina 108
È possibile creare due tipi di associazioni EIM diverse. È possibile creare un'associazione identificativo o un'associazione normativa.

"Abilitazione e supporto normativa corrispondenze EIM" a pagina 38
Il supporto normativa corrispondenze EIM (Enterprise Identity Mapping) consente di utilizzare le

associazioni normativa ed anche delle specifiche associazioni di identificativi in un dominio EIM. È possibile utilizzare le associazioni normativa invece di, oppure insieme ad, associazioni di identificativi.

"Sviluppo di un piano di corrispondenza delle identità" a pagina 63
Una parte critica del processo di pianificazione dell'implementazione di EIM (Enterprise Identity Mapping) iniziale richiede che l'utente determini come desidera utilizzare la corrispondenza delle identità nella propria azienda.

Creare un'associazione normativa di dominio predefinita:

Per creare un'associazione normativa di dominio predefinita, è necessario essere connessi al dominio EIM (Enterprise Identity Mapping) in cui si desidera lavorare e bisogna disporre del controllo di accesso dell'Amministratore registro o dell'amministratore EIM .

un'associazione normativa descrive una relazione tra una più identità utente di origine e una singola identità utente in un registro utenti di destinazione. È possibile utilizzare un'associazione normativa per descrivere una relazione tra una serie di più identità utente di origine e una singola identità utente di destinazione nel registro utenti di destinazione specificato. Le associazioni normativa utilizzano il supporto normativa corrispondenze EIM per creare corrispondenze molti-ad-uno tra identità utente senza coinvolgere un identificativo EIM.

Nota: Poiché è possibile utilizzare le associazioni normativa in diversi modi che si sovrappongono, è necessario conoscere approfonditamente il supporto normativa corrispondenze EIM prima di creare e utilizzare le associazioni normativa. Inoltre, per prevenire potenziali problemi con le associazioni e con il modo in cui associano le identità, è necessario sviluppare un piano di associazione di identità generale per la propria azienda prima di iniziare a definire le associazioni.

In un'associazione normativa dominio predefinita, tutti gli utenti nel dominio rappresentano l'origine dell'associazione normativa e vengono messi in corrispondenza con un singolo registro di destinazione ed utente destinazione. È possibile definire un'associazione normativa del dominio predefinito per ciascun registro nel dominio. Se due o più associazioni normativa dominio fanno riferimento allo stesso registro di destinazione, è possibile definire informazioni di ricerca univoche per ognuna di queste associazioni normativa per garantire che le operazioni di ricerca corrispondenze possano distinguere tra esse. In caso contrario, le operazioni di ricerca delle corrispondenze possono restituire più identità utente di destinazione. Come conseguenza di questi risultati ambigui, le applicazioni che si basano su EIM potrebbero non essere in grado di stabilire l'esatta identità di destinazione da utilizzare.

Per creare un'associazione normativa dei domini predefinita, completare queste operazioni:

1. Espandere **Rete > EIM (Enterprise Identity Mapping) > Gestione domini**.
2. Fare clic con il tasto destro del mouse sul dominio EIM in cui si desidera lavorare e selezionare **Normativa corrispondenza**
   - Se il dominio EIM con il quale si desidera lavorare non è elencato in **Gestione dominio**, consultare "Aggiunta di un dominio EIM alla cartella Gestione domini" a pagina 92.
   - Se attualmente non si è collegati al dominio EIM in cui si desidera lavorare, consultare Collegamento all'unità di controllo del dominio EIM.
3. Selezionare **Abilita ricerche di corrispondenza tramite associazioni normativa per il dominio** sulla pagina `Generale`.
4. Selezionare la pagina **Dominio** e fare clic su **Aggiungi**.
5. Nella finestra di dialogo **Aggiungi associazione normativa dei domini predefinita**, specificare le seguenti informazioni necessarie:
   - Il nome della definizione del registro del **Registro di destinazione** per l'associazione normativa.
   - Il nome dell'identità utente dell'**Utente di destinazione** per l'associazione normativa.

6. Fare clic su **?**, se necessario, per ulteriori dettagli su come completare questa e le finestre di dialogo successive.
7. Facoltativo. Fare clic su **Avanzate** per visualizzare la finestra di dialogo **Aggiungi associazione - Avanzate**. Specificare **Informazioni di ricerca** per l'associazione normativa e fare clic su **OK** per tornare alla finestra di dialogo **Associazione normativa dominio predefinita**.

   Nota: se due o più associazioni normativa dominio predefinite fanno riferimento allo stesso registro di destinazione, è necessario definire informazioni di ricerca univoche per ogni identità utente di destinazione in queste associazioni normativa. Definendo informazioni di ricerca per ogni identità utente di destinazione in questa situazione, si garantisce che le operazioni di ricerca della corrispondenza possano differenziarle. In caso contrario, le operazioni di ricerca delle corrispondenze possono restituire più identità utente di destinazione. Come conseguenza di questi risultati ambigui, le applicazioni che si basano su EIM potrebbero non essere in grado di stabilire l'esatta identità di destinazione da utilizzare.
8. Fare clic su **OK** per creare la nuova associazione normativa e ritornare alla pagina **Dominio**. La nuova associazione normativa è adesso visualizzata nella tabella **Associazioni normativa predefinite** table.
9. Verificare che la nuova associazione delle normative sia abilitata per il registro di destinazione.
10. Fare clic su **OK** per salvare le modifiche ed uscire dalla finestra di dialogo **Normativa di corrispondenza**.

Nota: Verificare che il supporto normativa di corrispondenze e l'utilizzo di associazioni normativa per un registro di destinazione siano abilitate in modo corretto. In caso contrario, l'associazione normativa potrebbe non avere effetto.

Creazione di un'associazione normativa di registro predefinita:

Per creare un'associazione normativa di registro predefinita, è necessario essere connessi al dominio EIM (Enterprise Identity Mapping) in cui si desidera lavorare e bisogna disporre del controllo di accesso EIM come Amministratore registro oppure come amministratore EIM.

un'associazione normativa descrive una relazione tra una più identità utente di origine e una singola identità utente in un registro utenti di destinazione. È possibile utilizzare un'associazione normativa per descrivere una relazione tra una serie di più identità utente di origine e una singola identità utente di destinazione nel registro utenti di destinazione specificato. Le associazioni normativa utilizzano il supporto normativa corrispondenze EIM per creare corrispondenze molti-ad-uno tra identità utente senza coinvolgere un identificativo EIM.

Nota: Poiché è possibile utilizzare le associazioni normativa in diversi modi che si sovrappongono, è necessario conoscere approfonditamente il supporto normativa corrispondenze EIM prima di creare e utilizzare le associazioni normativa. Inoltre, per prevenire potenziali problemi con le associazioni e con il modo in cui mettono in corrispondenza le identità, è necessario sviluppare un piano di corrispondenza di identità generale per la propria azienda prima di iniziare a definire le associazioni.

All'interno di un'associazione normativa del registro predefinito, tutti gli utenti in un singolo registro sono l'origine dell'associazione normativa e vengono messi in corrispondenza con un singolo registro di destinazione e un utente di destinazione. Quando si abilita l'associazione normativa del registro predefinito per il registro di destinazione, l'associazione normativa assicura che tutte queste identità utente di origine possano essere messe in corrispondenza con un singolo registro utente di destinazione e un utente di destinazione specificati.

Per creare un'associazione normativa dei registri predefinita, completare queste operazioni:

1. Espandere **Rete > EIM (Enterprise Identity Mapping) > Gestione domini**.
2. Selezionare il dominio EIM in cui si desidera lavorare.

- Se il dominio EIM con il quale si desidera lavorare non è elencato in **Gestione domini**, consultare "Aggiunta di un dominio EIM alla cartella Gestione domini" a pagina 92.
- Se attualmente non si è collegati al dominio EIM in cui si desidera lavorare, consultare Connessione all'unità di controllo del dominio EIM.

3. Selezionare **Abilita ricerche di corrispondenza tramite associazioni normativa per il dominio** sulla pagina `Generale`.
4. Selezionare **Abilita ricerche di corrispondenza tramite associazioni normativa per il dominio** sulla pagina `Generale`.
5. Nella finestra di dialogo **Aggiungi associazione normativa dei registri predefinita**, specificare le seguenti informazioni necessarie:
   - Il nome della definizione del registro del **Registro di origine** per l'associazione normativa.
   - Il nome della definizione del registro del **Registro di destinazione** per l'associazione normativa.
   - Il nome dell'identità utente dell'**Utente di destinazione** per l'associazione normativa.
6. Fare clic su **?**, se necessario, per ulteriori dettagli su come completare questa e le finestre di dialogo successive.
7. Facoltativo. Fare clic su **Avanzate** per visualizzare la finestra di dialogo **Aggiungi associazione - Avanzate**. Specificare le **informazioni per la ricerca** per l'associazione normativa e fare clic su **OK** per ritornare alla finestra di dialogo **Aggiungi associazione normativa dei registri predefinita**. se due o più associazioni normativa con lo stesso registro di origine fanno riferimento allo stesso registro destinazione, è necessario definire informazioni di ricerca univoche per ogni identità utente di destinazione in queste associazioni normativa. Definendo informazioni di ricerca per ogni identità utente di destinazione in questa situazione, si garantisce che le operazioni di ricerca della corrispondenza possano differenziarle. In caso contrario, le operazioni di ricerca delle corrispondenze possono restituire più identità utente di destinazione. Come conseguenza di questi risultati ambigui, le applicazioni che si basano su EIM potrebbero non essere in grado di stabilire l'esatta identità di destinazione da utilizzare.
8. Fare clic su **OK** per creare la nuova associazione normativa e ritornare alla pagina **Registro**. La nuova associazione normativa registro predefinita ora viene visualizzata in **Associazioni normativa predefinite**.
9. Verificare che la nuova associazione delle normative sia abilitata per il registro di destinazione.
10. Fare clic su **OK** per salvare le modifiche ed uscire dalla finestra di dialogo **Normativa di corrispondenza**.

    Nota: Verificare che il supporto normativa di corrispondenze e l'utilizzo di associazioni normativa per un registro di destinazione siano abilitate in modo corretto. In caso contrario, l'associazione normativa potrebbe non avere effetto.

Creazione di un'associazione normativa filtro certificato:

Per creare un'associazione normativa filtro certificato, è necessario essere connessi al dominio EIM (Enterprise Identity Mapping) in cui si desidera lavorare e bisogna disporre del controllo di accesso EIM come Amministratore registro oppure come amministratore EIM.

un'associazione normativa descrive una relazione tra una serie di più identità utente di origine e una singola identità utente di destinazione nel registro utenti di destinazione specificato. Le associazioni normativa utilizzano il supporto normativa corrispondenze EIM per creare corrispondenze molti-ad-uno tra identità utente senza coinvolgere un identificativo EIM.

Nota: Poiché è possibile utilizzare le associazioni normativa in diversi modi che si sovrappongono, è necessario conoscere approfonditamente il supporto normativa corrispondenze EIM prima di creare e utilizzare le associazioni normativa. Inoltre, per prevenire potenziali problemi con le associazioni

e con il modo in cui mettono in corrispondenza le identità, è necessario sviluppare un piano di corrispondenza di identità generale per la propria azienda prima di iniziare a definire le associazioni.

In un'associazione normativa filtro certificato, è necessario specificare una serie di certificati in un singolo registro X.509 come origine dell'associazione normativa. Questi certificati vengono messi in corrispondenza con un singolo registro di destinazione e con un utente di destinazione specificati. A differenza di un'associazione normativa registro predefinita in cui tutti gli utenti in un singolo registro rappresentano l'origine dell'associazione normativa, l'ambito di un'associazione normativa filtro certificato è più flessibile. È possibile specificare una sottoserie di certificati nel registro come origine. Il filtro certificato specificato per l'associazioni normativa determina il relativo ambito.

Nota: creare e utilizzare un'associazione normative del registro predefinito quando si desidera mettere in corrispondenza tutti i certificati contenuti in un registro utente X.509 con una singola identità utente di destinazione.

Il filtro certificato controlla la modalità in base alla quale un'associazione normativa filtro certificato mette in corrispondenza una serie di origine di identità utente, in questo caso certificati digitali, con una specifica identità utente di destinazione. Il filtro di certificati che si desidera utilizzare deve esistere, quindi, prima di poter creare un'associazione normativa filtro certificato.

Prima di poter creare un'associazione normativa filtro certificato, è necessario creare un filtro certificato da utilizzare come base dell'associazione normativa.

Per creare un'associazione normativa filtro certificato, completare le seguenti operazioni:

1. Espandere **Rete > EIM (Enterprise Identity Mapping) > Gestione domini**.
2. Fare clic con il tasto destro del mouse sul dominio EIM in cui si desidera lavorare e selezionare **Normativa corrispondenza**
   - Se il dominio EIM con il quale si desidera lavorare non è elencato in **Gestione domini**, consultare "Aggiunta di un dominio EIM alla cartella Gestione domini" a pagina 92.
   - Se attualmente non si è collegati al dominio EIM in cui si desidera lavorare, consultare Connessione all'unità di controllo del dominio EIM.
3. Selezionare **Abilita ricerche di corrispondenza tramite associazioni normativa per il dominio** sulla pagina `Generale`.
4. Selezionare la pagina **Filtro certificato** e fare clic su **Aggiungi** per visualizzare la finestra di dialogo **Aggiungi associazione normativa filtro certificato** dialog.
5. Fare clic su **?**, se necessario, per ulteriori dettagli su come completare questa e le finestre di dialogo successive.
6. Specificare le seguenti informazioni necessarie per la definizione dell'associazione normativa:
   a. Immettere il nome definizione di registro di un registro utenti X.509 da utilizzare come **Registro X.509 di origine** per l'associazione normativa. Oppure, fare clic su **Sfoglia** per selezionarne una da un elenco di definizioni di registro per il dominio
   b. Fare clic su **Seleziona** per visualizzare la finestra di dialogo **Seleziona filtro certificato** e selezionare un filtro certificato esistente da utilizzare come base per la nuova associazione normativa del filtro del certificato.

      Nota: si **deve** utilizzare un filtro certificato esistente. Se il filtro certificato che si desidera utilizzare non è elencato, fare clic su **Aggiungi** per creare un nuovo filtro certificato.
   c. Specificare il nome della definizione di registro del **Registro destinazione** o fare clic su **Sfoglia** per selezionarne una da un elenco di definizioni registro esistenti per il dominio.
   d. Specificare il nome dell'**utente di destinazione** con cui mettere in corrispondenza tutti i certificati nel **Registro X.509 di origine** che soddisfa il filtro certificato. Oppure, fare clic su **Sfoglia** per selezionarne uno da un elenco di utenti riconosciuti nel dominio.

e. Facoltativo. Fare clic su **Avanzate** per visualizzare la finestra di dialogo **Aggiungi associazione - Avanzate**. Specificare **Informazioni di ricerca** per l'identità utente di destinazione e fare clic su **OK** per tornare alla finestra di dialogo **Aggiungi associazione normativa filtro certificato**.

   Nota: se due o più associazioni normativa con lo stesso registro X.509 di origine e gli stessi criteri filtro certificato fanno riferimento allo stesso registro destinazione, l'utente deve definire informazioni di ricerca univoche per le identità utente di destinazione in ognuna di queste associazioni normativa. Definendo informazioni di ricerca per ogni identità utente di destinazione in questa situazione, si garantisce che le operazioni di ricerca della corrispondenza possano differenziarle. In caso contrario, le operazioni di ricerca delle corrispondenze possono restituire più identità utente di destinazione. Come conseguenza di questi risultati ambigui, le applicazioni che si basano su EIM potrebbero non essere in grado di stabilire l'esatta identità di destinazione da utilizzare.

7. Fare clic su **OK** per creare l'associazione normativa filtro certificato e ritornare alla pagina **Filtro certificato**. Nell'elenco viene visualizzata la nuova associazione normativa.
8. Verificare che la nuova associazione normativa sia abilitata per il registro di destinazione.
9. Fare clic su **OK** per salvare le modifiche ed uscire dalla finestra di dialogo **Normativa di corrispondenza**.

Nota: Verificare che il supporto normativa di corrispondenze e l'utilizzo di associazioni normativa per un registro di destinazione siano abilitate in modo corretto. In caso contrario, l'associazione normativa potrebbe non avere effetto.

Creazione di un filtro certificato:

Un filtro del certificato definisce una serie di attributi del certificato DN (distinguished name) simili per un gruppo di certificati utente in un registro utenti X.509 di origine. È possibile utilizzare il filtro certificato come base per un'associazione normativa filtro certificato.

Il filtro certificato in un'associazione normativa determina i certificati nel registro X.509 di origine specificato da corrispondere all'utente di destinazione specificato. I certificati per cui le informazioni sul DN soggetto e sul DN emittente che soddisfano i criteri del filtro vengono messi in corrispondenza con l'utente di destinazione specificato durante le operazioni di ricerca della corrispondenza EIM.

Per creare un filtro certificato, è necessario essere collegati al dominio EIM in cui si desidera lavorare e bisogna avere "Controllo di accesso EIM" a pagina 39 ad uno di questi livelli:

- Amministratore EIM
- Amministratore registro
- Amministratore per registri selezionati (per la definizione registro che fa riferimento al registro utenti X.509 per cui si desidera creare il filtro certificato)

Un filtro certificato viene creato in base a specifiche informazioni sul DN (distinguished name) provenienti da un certificato digitale. Le informazioni DN specificate possono essere il DN soggetto, che designa il proprietario del certificato, oppure il DN emittente, che designa l'emittente del certificato. È possibile specificare informazioni DN complete o parziali per un filtro certificato.

Quando si aggiunge il filtro certificato a un'associazione normativa filtro certificato, il filtro certificato stabilisce quali dei certificati presenti in un registro X.509 vengono messi in corrispondenza con l'identità utente di destinazione specificata dall'associazione normativa. Quando un certificato digitale è l'identità utente di origine in un'operazione di ricerca corrispondenza EIM (dopo che l'applicazione richiedente utilizza l'API EIM `eimFormatUserIdentity()` per formattare il nome identità utente) e si applica l'associazione normativa filtro certificato, EIM mette a confronto le informazioni DN nel certificato con le informazioni DN o DN parziale specificate nel filtro. Se le informazioni DN nel certificato corrispondono al filtro, EIM restituisce un'identità utente di destinazione specificata dall'associazione normativa filtro certificato.

Quando si crea il filtro certificato è possibile fornire le informazioni DN (distinguished name) richieste in uno di questi tre modi:

- È possibile immettere i DN completo o parziale di uno specifico certificato per il **DN soggetto**, il **DN emittente** o entrambi.
- È possibile copiare le informazioni da un certificato specifico negli appunti ed utilizzarle per creare un elenco di candidati filtro certificato in base alle informazioni DN (distinguished name) nel certificato. Quindi è possibile selezionare quali DN utilizzare per il filtro certificato.

  Nota: se si desidera generare le informazioni sul DN necessarie per creare un filtro del certificato, è necessario copiare le informazioni del certificato sugli Appunti prima di eseguire questa attività. Inoltre, il certificato deve avere un formato con codifica base64. Per ulteriori dettagliate informazioni sui metodi necessari per ottenere un certificato nel formato adeguato, consultare Filtro certificato.
- È possibile creare un elenco di candidati filtro certificato in base alle informazioni DN (distinguished name) da un certificato digitale per cui vi è un'associazione di origine esistente con un identificativo EIM. Quindi è possibile selezionare quali DN utilizzare per il filtro certificato.

Per creare un filtro certificato da utilizzare come base per l'associazione normativa filtro certificato, completare le seguenti operazioni:

1. Espandere **Rete > EIM (Enterprise Identity Mapping) > Gestione domini**.
2. Fare clic con il tasto destro del mouse sul dominio EIM in cui si desidera lavorare e selezionare **Normativa corrispondenza**
   - Se il dominio EIM con il quale si desidera lavorare non è elencato in **Gestione dominio**, consultare "Aggiunta di un dominio EIM alla cartella Gestione domini" a pagina 92.
   - Se attualmente non si è collegati al dominio EIM in cui si desidera lavorare, consultare Collegamento all'unità di controllo del dominio EIM.
3. Selezionare la pagina **Filtro certificato** e fare clic su **Filtri certificato** per visualizzare la finestra di dialogo **Filtri certificato**.

   Nota: Se si fa clic su **Filtri certificato** senza selezionare un'associazione normativa, viene visualizzata la finestra di dialogo **Sfoglia registri EIM**. Questa finestra di dialogo consente di selezionare un registro X.509 da un elenco di definizioni dei registri X.509 nel dominio per il quale si desidera visualizzare i filtri certificato. Il contenuto dell'elenco varia in base al tipo di controllo accesso EIM che si desidera.
4. Fare clic su **Aggiungi** per visualizzare la finestra di dialogo **Aggiungi filtro certificato**.
5. Nella finestra di dialogo **Aggiungi filtro certificato**, è necessario selezionare se aggiungere o meno un singolo filtro certificato oppure generare un filtro certificato basato su uno specifico certificato digitale. Fare clic su **?**, se necessario, per ulteriori dettagli su come completare questa e le finestre di dialogo successive.
   a. Se si seleziona **Aggiungi un singolo filtro certificato**, è possibile immettere informazioni specifiche sul **DN soggetto** completo o parziale, il **DN emittente** completo o parziale o entrambi. Fare clic su **OK** per creare il filtro certificato e ritornare alla finestra di dialogo **Filtri certificato**. Il filtro viene ora visualizzato nell'elenco.
   b. Se si seleziona **Crea filtro certificato da certificato digitale**, fare clic su **OK** per visualizzare la finestra di dialogo **Crea filtri certificato**.
      1) Incollare la versione con codifica base64 delle informazioni dei certificati, precedentemente copiate negli appunti, nel campo **Informazioni sui certificati**.
      2) Fare clic su **OK** per creare un elenco di potenziali filtri certificato in base al **DN soggetto** e al **DN emittente** del certificato.
      3) Dalla finestra di dialogo **Sfoglia filtri certificato**, selezionare uno o più di questi filtri certificato. Fare clic su **OK** per tornare alla finestra di dialogo **Seleziona filtri certificato** dove vengono ora visualizzati i filtri certificato selezionati.

c. Se si seleziona **Crea filtro certificato da un'associazione origine per un utente X.509**, fare clic su **OK** per visualizzare la finestra di dialogo **Crea filtri certificato**. Questa finestra di dialogo visualizza un elenco di identità utente X.509 che hanno un'associazione di origine con un identificativo EIM nel dominio.
   1) Selezionare l'identità utente X.509 il cui certificato digitale si desidera utilizzare per generare uno o più candidati filtro certificato e fare clic su **OK**.
   2) Fare clic su **OK** per creare un elenco di potenziali filtri certificato in base al **DN soggetto** e al **DN emittente** del certificato.
   3) Dalla finestra di dialogo **Sfoglia filtri certificato**, selezionare uno o più di questi potenziali filtri certificato. Fare clic su **OK** per tornare alla finestra di dialogo **Seleziona filtri certificato** dove vengono ora visualizzati i filtri certificato selezionati.

Ora è possibile utilizzare il nuovo filtro del certificato come base per la creazione di un'associazione normativa del filtro del certificato.

Aggiunta di informazioni di ricerca ad un'identità utente di destinazione

Le informazioni di ricerca sono dati identificativi univoci facoltativi per l'identità utente di destinazione definita in un'associazione. Questa associazione può essere un'associazione di destinazione individuale o un'associazione normativa.

Le informazioni di ricerca sono necessarie solo quando un'operazione di ricerca corrispondenze può restituire più di un'identità utente di destinazione. Questa situazione può creare dei problemi per le applicazioni abilitate ad EIM, comprese le applicazioni e i prodotti i5/OS, che non sono stati concepiti per gestire questi risultati ambigui.

Quando necessario, è possibile aggiungere informazioni di ricerca univoche per ogni identità utente di destinazione per fornire informazioni di identificazione più dettagliate che descrivano ulteriormente ogni identità utente di destinazione. Se si definiscono le informazioni di ricerca per un'identità utente di destinazione, queste informazioni di ricerca devono essere fornite nell'operazione di ricerca corrispondenze per garantire che l'operazione possa restituire un'identità utente destinazione univoca. Altrimenti, applicazioni che si basano su EIM potrebbero non essere in grado di stabilire l'esatta identità di destinazione da utilizzare.

Nota: se non si desidera che le operazioni di ricerca di EIM siano in grado di restituire più di una identità utente di destinazione, correggere la propria configurazione delle associazioni EIM invece di utilizzare le informazioni di ricerca per risolvere la situazione. Consultare "Risoluzione dei problemi di corrispondenza EIM" a pagina 130 per informazioni più dettagliate.

Il modo in cui si aggiungono informazioni di ricerca per definire ulteriormente un'identità utente di destinazione varia in base al fatto che l'identità utente di destinazione sia definita in un'associazione identificativo oppure in un'associazione di destinazione. Indipendentemente dal metodo che si utilizza per aggiungere le informazioni di ricerca, le informazioni specificate sono legate all'identità utente di destinazione, non alle associazioni di identificativi o alle associazioni normativa in cui viene trovata detta identità utente.

Aggiunta di informazioni di ricerca ad un'identità utente di destinazione in un'associazione identificativo:

Per aggiungere delle informazioni di ricerca all'identità utente di destinazione in un'associazione identificativo, è necessario essere connessi al dominio EIM in cui si desidera lavorare e bisogna avere "Controllo di accesso EIM" a pagina 39 ad uno di questi livelli:

- Amministratore di registro.
- Amministratore per i registri selezionati (per la definizione del registro che fa riferimento al registro utenti contenente l'identità utente di destinazione).
- Amministratore EIM.

Per aggiungere informazioni di ricerca all'identità utente di destinazione in un'associazione identificativo, completare questi passi:

1. Espandere **Rete > EIM (Enterprise Identity Mapping) > Gestione domini**.
2. Selezionare il dominio EIM in cui si desidera lavorare.
   - Se il dominio EIM con il quale si desidera lavorare non è elencato in **Gestione domini**, consultare "Aggiunta di un dominio EIM alla cartella Gestione domini" a pagina 92.
   - Se attualmente non si è collegati al dominio EIM in cui si desidera lavorare, consultare Connessione all'unità di controllo del dominio EIM.
3. Espandere il dominio EIM a cui si è connessi.
4. Fare clic su **Identificativi** per visualizzare l'elenco di identificativi EIM del dominio.

   Nota: quando si tenta di espandere la cartella **Identificativi**, è possibile che si impieghi parecchio tempo prima di vedere visualizzato l'elenco degli identificativi. Per migliorare le prestazioni quando si ha un gran numero di identificativi EIM nel dominio, è possibile eseguire la personalizzazione della vista della cartella **Identificativi** limitando il criterio di ricerca utilizzato per la visualizzazione degli identificativi. Fare clic con il tasto destro del mouse su **Identificativi**, selezionare **Personalizza questa vista > Includi**, e specificare i criteri di visualizzazione da utilizzare per generare l'elenco di identificativi EIM da includere nella vista.
5. Fare clic con il tasto destro del mouse su un identificativo EIM e selezionare **Proprietà**.
6. Selezionare la pagina **Associazioni**, quindi l'associazione di destinazione a cui si desidera aggiungere le informazioni di ricerca e fare clic su **Dettagli**. Fare clic su **?**, se necessario, per determinare le informazioni da specificare per ciascun campo.
7. Nella finestra di dialogo **Associazione - Dettagli**, specificare le **informazioni di ricerca** che si desidera utilizzare per un'ulteriore identificazione dell'identità utente di destinazione in questa associazione e fare clic su **Aggiungi**.
8. Ripetere questa operazione per ogni voce delle informazioni di ricerca che si desidera aggiungere all'associazione.
9. Fare clic su **OK** per salvare le modifiche e tornare alla finestra di dialogo **Associazione - Dettagli**.
10. Fare clic su **OK** per uscire.

Aggiunta di informazioni di ricerca ad un'identità utente di destinazione in un'associazione normativa:

Per aggiungere delle informazioni di ricerca all'identità utente di destinazione in un'associazione normativa, è necessario essere collegati al dominio EIM in cui si desidera lavorare e bisogna avere "Controllo di accesso EIM" a pagina 39 ad uno di questi livelli:

- Amministratore di registro.
- Amministratore dei registri selezionati (per la definizione di registro che fa riferimento al registro utente contenente l'ID utente di destinazione).
- Amministratore EIM.

Per aggiungere informazioni di ricerca all'identità utente di destinazione in un'associazione normativa, attenersi alla seguente procedura:

1. Espandere **Rete > EIM (Enterprise Identity Mapping) > Gestione domini**.
2. Selezionare il dominio EIM in cui si desidera lavorare.
   - Se il dominio EIM con il quale si desidera lavorare non è elencato in **Gestione domini**, consultare "Aggiunta di un dominio EIM alla cartella Gestione domini" a pagina 92.
   - Se attualmente non si è collegati al dominio EIM in cui si desidera lavorare, consultare Connessione all'unità di controllo del dominio EIM.

3. Nella finestra di dialogo **Normativa corrispondenza**, utilizzare le pagine per visualizzare le associazioni normativa per il dominio.
4. Trovare e selezionare l'associazione normativa per il registro di destinazione che contiene l'identità utente di destinazione per cui si desidera aggiungere informazioni di ricerca.
5. Fare clic su **Dettagli** per visualizzare la finestra di dialogo **Associazione normativa - Dettagli** appropriata per il tipo di associazione normativa selezionata. Fare clic su **?**, se necessario, per determinare le informazioni da specificare per ciascun campo.
6. Specificare le **Informazioni di ricerca** che si desidera utilizzare per identificare ulteriormente l'identità utente di destinazione in questa associazione normativa e fare clic su **Aggiungi**. Ripetere questa operazione per ogni voce delle informazioni di ricerca che si desidera aggiungere all'associazione.
7. Fare clic su **OK** per salvare le modifiche e tornare alla finestra di dialogo **Associazione normativa - Dettagli** originale.
8. Fare clic su **OK** per uscire.

Eliminazione delle informazioni di ricerca da un'identità utente di destinazione

Le informazioni di ricerca sono dati identificativi univoci facoltativi per l'identità utente di destinazione definita in un'associazione. Questa associazione può essere un'associazione di destinazione individuale o un'associazione normativa.

Le informazioni di ricerca sono necessarie solo quando un'operazione di ricerca corrispondenze può restituire più di un'identità utente di destinazione. Questa situazione può creare dei problemi per le applicazioni abilitate ad EIM, comprese le applicazioni e i prodotti i5/OS, che non sono stati concepiti per gestire questi risultati ambigui.

Queste informazioni di ricerca devono essere fornite nell'operazione di ricerca corrispondenze per garantire che l'operazione possa restituire un'identità utente destinazione univoca. Tuttavia, se delle informazioni di ricerca definite in precedenza non sono più necessarie, procedere alla loro rimozione, in modo tale che non sia più necessario fornirle per le operazioni di ricerca.

Il modo in cui si rimuovono informazioni di ricerca da un'identità utente di destinazione varia in base al fatto che l'identità utente di destinazione sia definita in un'associazione identificativo oppure in un'associazione di destinazione. Le informazioni di ricerca sono legate all'identità utente di destinazione, non alle associazioni di identificativi o alle associazioni normativa in cui viene trovata detta identità utente. Di conseguenza, quando si cancella l'ultima associazione identificativo o associazione normativa che definisce detta identità utente di destinazione, sia l'identità utente che le informazioni di ricerca vengono cancellate dal dominio EIM.

Rimozione delle informazioni di ricerca per un'identità utente di destinazione in un'associazione identificativo:

Per rimuovere le informazioni di ricerca per l'identità utente di destinazione in un'associazione identificativo, è necessario essere collegati al dominio EIM in cui si desidera lavorare e bisogna avere "Controllo di accesso EIM" a pagina 39 ad uno di questi livelli:

- Amministratore di registro.
- Amministratore per i registri selezionati (per la definizione del registro che fa riferimento al registro utenti contenente l'identità utente di destinazione).
- Amministratore EIM.

Per rimuovere le informazioni di ricerca per l'identità utente di destinazione in un'associazione identificativo, attenersi alla seguente procedura:

1. Espandere **Rete > EIM (Enterprise Identity Mapping) > Gestione domini**.
2. Selezionare il dominio EIM in cui si desidera lavorare.

- Se il dominio EIM con il quale si desidera lavorare non è elencato in **Gestione domini**, consultare "Aggiunta di un dominio EIM alla cartella Gestione domini" a pagina 92.
- Se attualmente non si è collegati al dominio EIM in cui si desidera lavorare, consultare Connessione all'unità di controllo del dominio EIM.

3. Espandere il dominio EIM a cui si è connessi.
4. Fare clic su **Identificativi** per visualizzare l'elenco di identificativi EIM del dominio.

   Nota: quando si tenta di espandere la cartella **Identificativi**, è possibile che si impieghi parecchio tempo prima di vedere visualizzato l'elenco degli identificativi. Per migliorare le prestazioni quando si ha un gran numero di identificativi EIM nel dominio, è possibile eseguire la personalizzazione della vista della cartella **Identificativi** limitando il criterio di ricerca utilizzato per la visualizzazione degli identificativi. Fare clic con il tasto destro del mouse su **Identificativi**, selezionare **Personalizza questa vista > Includi**, e specificare i criteri di visualizzazione da utilizzare per generare l'elenco di identificativi EIM da includere nella vista.
5. Fare clic con il tasto destro del mouse su un identificativo EIM e selezionare **Proprietà**.
6. Selezionare la pagina **Associazioni**, quindi l'associazione di destinazione per l'identità utente per cui si desidera eliminare le informazioni di ricerca e fare clic su **Dettagli**.
7. Nella finestra di dialogo **Associazione - Dettagli**, selezionare le informazioni di ricerca che si desidera eliminare dall'identità utente di destinazione e fare clic su **Elimina**.

   Nota: non viene visualizzata alcuna richiesta di conferma quando si fa clic su **Elimina**.
8. Fare clic su **OK** per salvare le modifiche e tornare alla finestra di dialogo **Associazione - Dettagli**.
9. Fare clic su **OK** per uscire.

Rimozione delle informazioni di ricerca per un'identità utente di destinazione in un'associazione normativa:

Per eliminare delle informazioni di ricerca dall'identità utente di destinazione in un'associazione normativa, è necessario essere collegati al dominio EIM in cui si desidera lavorare e bisogna avere "Controllo di accesso EIM" a pagina 39 ad uno di questi livelli:

- Amministratore di registro.
- Amministratore dei registri selezionati (per la definizione di registro che fa riferimento al registro utente contenente l'ID utente di destinazione).
- Amministratore EIM.

Per eliminare informazioni di ricerca dall'identità utente di destinazione in un'associazione normativa, attenersi alla seguente procedura:

1. Espandere **Rete > EIM (Enterprise Identity Mapping) > Gestione domini**.
2. Selezionare il dominio EIM in cui si desidera lavorare.
   - Se il dominio EIM con il quale si desidera lavorare non è elencato in **Gestione domini**, consultare "Aggiunta di un dominio EIM alla cartella Gestione domini" a pagina 92.
   - Se attualmente non si è collegati al dominio EIM in cui si desidera lavorare, consultare Connessione all'unità di controllo del dominio EIM.
3. Nella finestra di dialogo **Normativa corrispondenza**, utilizzare le pagine per visualizzare le associazioni normativa per il dominio.
4. Trovare e selezionare l'associazione normativa per il registro di destinazione che contiene l'identità utente di destinazione per cui si desidera eliminare informazioni di ricerca.
5. Fare clic su **Dettagli** per visualizzare la finestra di dialogo **Associazione normativa - Dettagli** appropriata per il tipo di associazione normativa selezionata.
6. Selezionare le informazioni di ricerca che si desidera eliminare dall'identità utente di destinazione e fare clic su **Elimina**.

Nota: non viene visualizzata alcuna richiesta di conferma quando si fa clic su **Elimina**.

7. Fare clic su **OK** per salvare le modifiche e tornare alla finestra di dialogo **Associazione normativa - Dettagli** originale.
8. Fare clic su **OK** per uscire.

Visualizzazione di tutte le associazioni identificativo per un identificativo EIM

Per visualizzare tutte le associazioni per un identificativo EIM (Enterprise Identity Mapping) è necessario essere connessi al dominio EIM in cui si desidera lavorare e bisogna disporre di qualche livello di controllo accesso EIM per eseguire questa attività.

È possibile visualizzare tutte le associazioni con qualsiasi livello di controllo accesso tranne Amministratore per il controllo accesso registri selezionati. Questo livello controllo di accesso consente all'utente di elencare e visualizzare solo quelle associazioni ai registri per cui dispone di esplicita autorizzazione, a meno che non disponga anche del controllo accesso per le operazioni di ricerca corrispondenze EIM.

Per visualizzare tutte le associazioni tra un identificativo EIM e le identità utenti (ID) per le quali sono state definite le associazioni per l'identificativo EIM, completare le seguenti operazioni:

Per visualizzare le associazioni per un identificativo, attenersi alla seguente procedura:

1. Espandere **Rete > EIM (Enterprise Identity Mapping) > Gestione domini**.
2. Selezionare il dominio EIM in cui si desidera lavorare.
   - Se il dominio EIM con il quale si desidera lavorare non è elencato in **Gestione domini**, consultare "Aggiunta di un dominio EIM alla cartella Gestione domini" a pagina 92.
   - Se attualmente non si è collegati al dominio EIM in cui si desidera lavorare, consultare Connessione all'unità di controllo del dominio EIM.
3. Espandere il dominio EIM a cui si è connessi.
4. Fare clic su **Identificativi** per visualizzare l'elenco di identificativi EIM del dominio.

   Nota: quando si tenta di espandere la cartella **Identificativi**, è possibile che si impieghi parecchio tempo prima di vedere visualizzato l'elenco degli identificativi. Per migliorare le prestazioni quando si ha un gran numero di identificativi EIM nel dominio, è possibile eseguire la personalizzazione della vista della cartella **Identificativi** limitando il criterio di ricerca utilizzato per la visualizzazione degli identificativi. Fare clic con il tasto destro del mouse su **Identificativi**, selezionare **Personalizza questa vista > Includi**, e specificare i criteri di visualizzazione da utilizzare per generare l'elenco di identificativi EIM da includere nella vista.
5. Selezionare un identificativo EIM, fare clic con il tasto destro del mouse sull'identificativo EIM e selezionare **Proprietà**.
6. Selezionare la pagina **Associazioni** per visualizzare un elenco di identità utenti associate per l'identificativo EIM selezionato.
7. Fare clic su **OK** per terminare.

Visualizzazione di tutte le associazioni normativa per un dominio

Per visualizzare tutte le associazioni normativa definite per un dominio, è necessario essere connessi al dominio EIM (Enterprise Identity Mapping) in cui si desidera lavorare e bisogna avere un certo livello di controllo di accesso EIM per eseguire questa attività.

È possibile visualizzare tutte le associazioni normativa con qualsiasi livello di controllo accesso tranne Amministratore per il controllo accesso registri selezionati. Questo livello controllo di accesso consente all'utente di elencare e visualizzare solo quelle associazioni ai registri per cui dispone di esplicita autorizzazione. Di conseguenza, con questo controllo accesso non è possibile elencare o visualizzare alcuna associazione normativa dominio predefinita, a meno che non si disponga anche del controllo accesso per le operazioni di ricerca corrispondenze EIM.

Per visualizzare tutte le associazioni normativa per un dominio, completare le seguenti operazioni:

1. Espandere **Rete > EIM (Enterprise Identity Mapping) > Gestione domini**.
2. Fare clic con il tasto destro del mouse sul dominio EIM in cui si desidera lavorare e selezionare **Normativa corrispondenza**
   - Se il dominio EIM con il quale si desidera lavorare non è elencato in **Gestione domini**, consultare "Aggiunta di un dominio EIM alla cartella Gestione domini" a pagina 92.
   - Se attualmente non si è collegati al dominio EIM in cui si desidera lavorare, consultare Connessione all'unità di controllo del dominio EIM.
3. Selezionare una pagina per visualizzare le associazioni normativa definite per il dominio, come di seguito riportato:
   a. Selezionare la pagina **Dominio** per visualizzare le associazioni normativa del dominio predefinito definite per il dominio e per verificare se l'associazione normativa è abilitata al livello del registro.
   b. Selezionare la pagina **Registro** per visualizzare le associazioni normativa del registro predefinito definite per il dominio. Inoltre, è possibile visualizzare i registri utenti e di destinazione coinvolti nelle associazioni normativa.
   c. Selezionare la pagina **Filtro certificato** per visualizzare le associazioni normativa filtro certificato definite e abilitate a livello del registro.
4. Fare clic su **OK** per terminare.

Visualizzazione di tutte le associazioni normativa per una definizione di registro

Per visualizzare tutte le associazioni normativa definite per un registro specifico, è necessario essere connessi al dominio EIM (Enterprise Identity Mapping) in cui si desidera lavorare e bisogna avere un certo livello di controllo di accesso EIM per eseguire questa attività.

È possibile visualizzare tutte le associazioni normativa con qualsiasi livello di controllo accesso tranne Amministratore per il controllo accesso registri selezionati. Questo livello controllo di accesso consente all'utente di elencare e visualizzare solo quelle associazioni ai registri per cui dispone di esplicita autorizzazione. Di conseguenza, con questo controllo accesso non è possibile elencare o visualizzare alcuna associazione normativa dominio predefinita, a meno che non si disponga anche del controllo accesso per le operazioni di ricerca corrispondenze EIM.

Per visualizzare tutte le associazioni normativa per una definizione registro, completare questi passi:

1. Espandere **Rete > EIM (Enterprise Identity Mapping) > Gestione domini**.
2. Selezionare il dominio EIM in cui si desidera lavorare.
   - Se il dominio EIM con il quale si desidera lavorare non è elencato in **Gestione domini**, consultare "Aggiunta di un dominio EIM alla cartella Gestione domini" a pagina 92.
   - Se attualmente non si è collegati al dominio EIM in cui si desidera lavorare, consultare Connessione all'unità di controllo del dominio EIM.
3. Fare clic con il tasto destro del mouse sulla definizione registro che si desidera gestire e selezionare **Normativa corrispondenza**.
4. Selezionare una pagina per visualizzare le associazioni normativa definite per la definizione registro specificata, nel modo seguente:
   - Selezionare la pagina **Dominio** per visualizzare le associazioni normativa dominio predefinite definite per il registro.
   - Selezionare la pagina **Registro** per visualizzare le associazioni normativa registro predefinite specificate ed abilitate per il registro.
   - Selezionare la pagina **Filtro certificato** per visualizzare le associazioni normativa filtro certificato definite ed abilitate per il registro.
5. Fare clic su **OK** per terminare.

Cancellazione di un'associazione identificativo

Per cancellare un' associazione identificativo, è necessario essere connessi al dominio EIM (Enterprise Identity Mapping) in cui si desidera lavorare ed è necessario disporre del controllo di accesso EIM richiesto dal tipo di associazione che si desidera cancellare.

Per cancellare un'associazione origine o un'associazione amministrativa, è necessario avere il controllo accesso EIM ad uno di questi livelli:

- Amministratore identificativo.
- Amministratore EIM.

Per cancellare un'associazione destinazione, è necessario avere il controllo accesso EIM ad uno di questi livelli:

- Amministratore di registro.
- Amministratore per i registri selezionati (per la definizione del registro che fa riferimento al registro utenti contenente l'identità utente di destinazione).
- Amministratore EIM.

Per cancellare un'associazione identificativo, completare i passi riportati di seguito.

1. Espandere **Rete > EIM (Enterprise Identity Mapping) > Gestione domini**.
2. Selezionare il dominio EIM in cui si desidera lavorare.
   - Se il dominio EIM con il quale si desidera lavorare non è elencato in **Gestione domini**, consultare "Aggiunta di un dominio EIM alla cartella Gestione domini" a pagina 92.
   - Se attualmente non si è collegati al dominio EIM in cui si desidera lavorare, consultare Connessione all'unità di controllo del dominio EIM.
3. Espandere il dominio EIM a cui si è connessi.
4. Fare clic su **Identificativi** per visualizzare l'elenco di identificativi EIM del dominio.

   Nota: quando si tenta di espandere la cartella **Identificativi**, è possibile che si impieghi parecchio tempo prima di vedere visualizzato l'elenco degli identificativi. Per migliorare le prestazioni quando si ha un gran numero di identificativi EIM nel dominio, è possibile eseguire la personalizzazione della vista della cartella **Identificativi** limitando i criteri di ricerca utilizzati per la visualizzazione degli identificativi. Fare clic con il tasto destro del mouse su **Identificativi**, selezionare **Personalizza questa vista > Includi**, e specificare i criteri di visualizzazione da utilizzare per generare l'elenco di identificativi EIM da includere nella vista.
5. Selezionare un identificativo EIM, fare clic con il tasto destro del mouse sull'identificativo EIM e selezionare **Proprietà**.
6. Selezionare la pagina **Associazioni** per visualizzare un elenco di identità utenti associate per l'identificativo EIM selezionato.
7. Selezionare l'associazione che si desidera cancellare e fare clic su **Elimina** per cancellare l'associazione.

   Nota: non viene visualizzata alcuna richiesta di conferma quando si fa clic su **Elimina**.
8. Fare clic su **OK** per salvare le modifiche.

Nota: quando si elimina un'associazione di destinazione, qualsiasi operazione di ricerca corrispondenze nel registro di destinazione che dipenda dall'uso dell'associazione cancellata potrebbe dare esito negativo se non esistono altre associazioni (associazioni normativa o associazioni di identificativi) per il registro di destinazione interessato.

Il solo modo di definire un'identità utente in EIM è quando si specifica l'identità utente come parte della creazione di un'associazione, un'associazione identificativo o un'associazione normativa. Di conseguenza, quando si cancella l'ultima associazione di destinazione per un'identità utente (eliminando

un'associazione di destinazione individuale o un'associazione normativa), quella identità utente non è più definita in EIM. Di conseguenza, il nome identità utente e qualsiasi informazione di ricerca per tale identità utente vengono persi.

Cancellazione di un'associazione normativa

Per eliminare un'associazione normativa, è necessario essere connessi al dominio EIM (Enterprise Identity Mapping) in cui si desidera lavorare e bisogna disporre del controllo di accesso EIM come Amministratore registro oppure come amministratore EIM.

Per cancellare un'associazione normativa, completare queste operazioni:

1. Espandere **Rete > EIM (Enterprise Identity Mapping) > Gestione domini**.
2. Selezionare il dominio EIM in cui si desidera lavorare.
   - Se il dominio EIM con il quale si desidera lavorare non è elencato in **Gestione domini**, consultare "Aggiunta di un dominio EIM alla cartella Gestione domini" a pagina 92.
   - Se attualmente non si è collegati al dominio EIM in cui si desidera lavorare, consultare Connessione all'unità di controllo del dominio EIM.
3. Selezionare la pagina appropriata per il tipo di associazione normative che si desidera cancellare.
4. In quella pagina, selezionare l'associazione normativa appropriata e fare clic su **Elimina**.

   Nota: non viene visualizzata alcuna richiesta di conferma quando si fa clic su **Elimina**.
5. Fare clic su **OK** per uscire dalla finestra di dialogo **Normativa corrispondenza** e salvare le modifiche.

Nota: quando si elimina un'associazione normativa di destinazione, qualsiasi operazione di ricerca corrispondenze nel registro di destinazione che dipenda dall'uso dell'associazione normativa cancellata potrebbe dare esito negativo se non esistono altre associazioni (associazioni normativa o associazioni di identificativi) per il registro di destinazione interessato.

Il solo modo di definire un'identità utente in EIM è quando si specifica l'identità utente come parte della creazione di un'associazione, un'associazione identificativo o un'associazione normativa. Di conseguenza, quando si cancella l'ultima associazione di destinazione per un'identità utente (eliminando un'associazione di destinazione individuale o un'associazione normativa), quella identità utente non è più definita in EIM. Di conseguenza, il nome identità utente e qualsiasi informazione di ricerca per tale identità utente vengono persi.

Concetti correlati

"Gestione delle definizioni di registro di EIM" a pagina 98
Per fare in modo che i registri utenti e le identità utenti in essi contenute partecipino a un dominio EIM (Enterprise Identity Mapping), è necessario creare definizioni di registro per essi. Sarà quindi possibile gestire la modalità di partecipazione ad EIM dei registri utenti e delle relative identità, semplicemente gestendo queste definizioni di registro.

Gestione del controllo di accesso utente EIM

Un utente EIM (Enterprise Identity Mapping) è un utente che possiede il controllo di accesso EIM in base all'appartenenza a gruppi utenti LDAP (Lightweight Directory Access Protocol) predefiniti. Specificando il controllo di accesso EIM per un utente, tale utente viene aggiunto a un gruppo di utenti LDAP specifico.

Ogni gruppo LDAP dispone di un 'autorizzazione per eseguire le diverse attività amministrative EIM all'interno di un dominio. Le attività amministrative e il tipo, comprese le operazioni di ricerca, che un utente EIM può eseguire variano in base al gruppo di controllo di accesso a cui appartiene l'utente EIM.

Solo utenti con controllo accesso amministratore LDAP o controllo accesso amministratore EIM possono aggiungere altri utenti ad un gruppo controllo accesso EIM o modificare le impostazioni del controllo accesso per altri utenti. Prima che un utente possa divenire membro di un gruppo di controllo di accesso

EIM, è necessario che tale utente disponga di una voce del server dell'indirizzario che agisca come unità di controllo del dominio EIM. Inoltre, solo determinati tipi di utente possono diventare membri di un gruppo di controllo di accesso EIM: i principal Kerberos, i DN (distinguished name) e i profili utente i5/OS.

Nota: perché sia disponibile il tipo utente Kerberos principal in EIM, è necessario che sia configurato sul sistema il servizio di autenticazione di rete. Perché sia disponibile il tipo profilo utente i5/OS in EIM, è necessario che sia configurato un suffisso oggetto sistema sul server indirizzario. Questo consente al server indirizzario di fare riferimento agli oggetti sistema i5/OS, come ad esempio i profili utente i5/OS.

Per gestire il controllo di accesso per un utente del server indirizzario esistente o per aggiungere un utente del server indirizzario esistente ad un gruppo di controllo di accesso EIM, attenersi alla seguente procedura:

1. Espandere **Rete > EIM (Enterprise Identity Mapping) > Gestione domini**.
2. Selezionare il dominio EIM in cui si desidera lavorare.
   - Se il dominio EIM con il quale si desidera lavorare non è elencato in **Gestione domini**, consultare "Aggiunta di un dominio EIM alla cartella Gestione domini" a pagina 92.
   - Se attualmente non si è collegati al dominio EIM in cui si desidera lavorare, consultare Connessione all'unità di controllo del dominio EIM.
3. Fare clic con il tasto destro del mouse sul dominio EIM a cui si è connessi e selezionare **Controllo di accesso**
4. Nella finestra di dialogo **Modifica controllo di accesso EIM**, selezionare il **Tipo di utente** per visualizzare i campi richiesti per fornire le informazioni di identificazione dell'utente.
5. Immettere le informazioni necessari per identificare l'utente per cui si desidera gestire il controllo di accesso EIM e fare clic su **OK** per aprire la finestra **Modifica controllo accesso EIM**. Fare clic su **?**, se necessario, per determinare le informazioni da specificare per ciascun campo.
6. Selezionare uno o più gruppi di **Controllo di accesso** per l'utente e fare clic su **OK** per aggiungere l'utente ai gruppi selezionati. Fare clic su **?** per informazioni dettagliate sull'autorizzazione di cui ciascun gruppo dispone e per conoscere eventuali requisiti speciali.
7. Una volta fornite le informazioni richieste, fare clic su **OK** per salvare le modifiche apportate.

Concetti correlati

"Controllo di accesso EIM" a pagina 39
Un utente EIM è un utente che possiede il controllo di accesso EIM in base all'appartenenza ad un gruppo utenti LDAP (Lightweight Directory Access Protocol) predefinito per uno specifico dominio.

Informazioni correlate

Servizio di autenticazione di rete (NAS)

Gestione delle proprietà di configurazione EIM

È possibile gestire varie proprietà di configurazione differenti di EIM per il server. Di norma, questa non è un'operazione che occorre eseguire spesso.

Si sono tuttavia delle situazioni che richiedono che l'utente apporti delle modifiche alle proprietà di configurazione. Se ad esempio il sistema si disattiva e bisogna creare nuovamente le proprietà di configurazione di EIM, è possibile eseguire nuovamente il wizard di Configurazione di EIM oppure modificare le proprietà qui. Un altro esempio è se si è scelto di non creare le definizioni di registro per i registri locali quando si è eseguito il wizard di Configurazione di EIM, è possibile aggiornare le informazioni sulle definizioni di registro qui.

Le proprietà che l'utente può modificare comprendono:

- Il dominio EIM al quale partecipa il server.
- Le informazioni di connessione per l'unità di controllo del dominio EIM.

- L'identità utente che il sistema utilizza per eseguire le operazioni EIM per conto delle funzioni del sistema operativo.
- I nomi delle definizioni dei registri che fanno riferimento ai registri utenti reali che il sistema può utilizzare durante le operazioni EIM per conto delle funzioni del sistema operativo. Questi nomi di definizioni di registro fanno riferimento ai registri utenti locali che è possibile creare quando si esegue il wizard di Configurazione di EIM.

  Nota: se si è scelto di non creare i nomi di definizioni dei registri locali quando si è eseguito il wizard di Configurazione di EIM perché i registri erano già definiti per il dominio EIM o perché si è scelto di definirli per il dominio in un secondo momento, è necessario aggiornare le proprietà di configurazione del sistema con questi nomi di definizioni di registro qui. Il sistema ha bisogno di queste informazioni sulle definizioni di registro per eseguire le operazioni EIM per conto delle funzioni del sistema operativo.

Per modificare le proprietà di configurazione di EIM, è necessario disporre di queste autorizzazioni speciali:

- Responsabile della sicurezza (*SECADM).
- Tutti gli oggetti (*ALLOBJ).

Per modificare le proprietà di configurazione di EIM per la piattaforma System i, attenersi alla seguente procedura:

1. Espandere **Rete >EIM (Enterprise Identity Mapping)**.
2. Fare clic con il tasto destro del mouse su **Configurazione** e selezionare **Proprietà**.
3. Apportare le modifiche alle informazioni sulla configurazione EIM.
4. Fare clic su **?**, per determinare le informazioni da specificare per ciascun campo nella finestra di dialogo.
5. Fare clic su **Verifica configurazione** per garantire che tutte le informazioni specificate consentano al sistema di stabilire con esito positivo un collegamento all'unità di controllo dominio EIM.
6. Fare clic su **OK** per salvare le modifiche.

Nota: se non è stato utilizzato il wizard di configurazione EIM per creare o partecipare a un dominio, non tentare di creare una configurazione EIM specificando manualmente le proprietà di configurazione. L'uso del wizard per creare una configurazione EIM di base consente di prevenire potenziali problemi di configurazione, dato che il wizard fa molto di più che configurare semplicemente queste proprietà.

Risoluzione dei problemi di EIM

Utilizzare i seguenti metodi per la risoluzione dei problemi per risolvere alcuni dei problemi di base che potrebbero insorgere durante la configurazione e l'utilizzo di EIM (Enterprise Identity Mapping).

EIM è composto da più tecnologie e da molte applicazioni e funzioni. Di conseguenza, si possono verificare dei problemi in varie aree. Le seguenti informazioni descrivono alcuni problemi ed errori comuni che potrebbero verificarsi quando si utilizza EIM ed alcuni consigli su come correggere questi errori e problemi.

Informazioni correlate

Troubleshoot single signon configuration

Risoluzione dei problemi di connessione all'unità di controllo del dominio

Diversi fattori possono contribuire al verificarsi di problemi di connessione quando si tenta di connettersi all'unità di controllo del dominio. Consultare la seguente tabella per determinare come risolvere potenziali problemi di connessione all'unità di controllo del dominio

Tabella 27. Problemi di connessione all'unità di controllo del dominio EIM comuni e soluzioni

Possibile problema	Possibili soluzioni
Non è possibile stabilire una connessione all'unità di controllo del dominio quando si utilizza System i Navigator per gestire EIM.	Le informazioni sulla connessione all'unità di controllo del dominio potrebbero essere state specificate in modo non corretto per il dominio che si desidera gestire. Completare la seguente procedura per verificare le informazioni sulla connessione al dominio: • Espandere **Rete-->EIM (Enterprise Identity Mapping)-->Rete->Gestione domini**. Fare clic con il tasto destro del mouse sul dominio che si desidera gestire e selezionare **Proprietà**. • Verificare che il nome dell'**Unità di controllo del dominio** sia corretto e che il **DN principale**, se specificato, sia corretto. • Verificare che le informazioni sulla **Connessione** per l'unità di controllo del dominio siano corrette. Assicurarsi che il numero di **Porta** sia corretto. Se è selezionata **Utilizza connessione protetta (SSL o TLS)**, il server di indirizzario deve essere configurato per utilizzare SSL. Fare clic su **Verifica connessione** per verificare che è possibile utilizzare le informazioni specificate per stabilire una connessione all'unità di controllo del dominio correttamente. • Verificare che le informazioni sull'utente nel pannello **Connetti all'unità di controllo dominio** siano corrette.

Tabella 27. Problemi di connessione all'unità di controllo del dominio EIM comuni e soluzioni (Continua)

Possibile problema	Possibili soluzioni
Il sistema operativo o le applicazioni non possono stabilire una connessione al controllo di dominio per accedere ai dati EIM. Si sta ad esempio verificando un malfunzionamento delle operazioni di ricerca di corrispondenze EIM eseguite per conto del sistema. Questo potrebbe verificarsi perché la configurazione di EIM non è corretta sul sistema o sui sistemi.	Verificare la configurazione di EIM. Espandere **Rete-->EIM (Enterprise Identity Mapping)-->Configurazione** sul sistema con il quale si sta tentando l'autenticazione. Fare clic con il tasto destro del mouse sulla cartella **Configurazione**, selezionare **Proprietà** e verificare quanto segue: • Pagina **Dominio** : – Il nome dell'unità di controllo del dominio ed i numeri di porta sono corretti. – Fare clic su **Verifica configurazione** per verificare che l'unità di controllo del dominio sia attiva. – Il nome del registro locale è specificato in modo corretto. – Il nome del registro Kerberos è specificato in modo corretto. – Verificare che sia selezionata **Abilita operazioni EIM per questo sistema**. • pagina **Utente di sistema** : – L'utente specificato ha un controllo di accesso EIM sufficiente per eseguire una ricerca di corrispondenze e la parola d'ordine è valida per l'utente. Consultare la guida in linea per ulteriori informazioni sui vari tipi di credenziali dell'utente. **Nota:** se è stata modificata la parola d'ordine per l'utente di sistema specificato nel server di indirizzario, è necessario modificare la parola d'ordine anche qui. Se queste parole d'ordine non corrispondono, l'utente di sistema non può eseguire le funzioni EIM per il sistema operativo e le operazioni di ricerca di corrispondenze hanno esito negativo. – Fare clic su **Verifica connessione** per confermare che le informazioni sull'utente specificate siano corrette.
Le informazioni sulla configurazione sembrano essere corrette ma non è possibile stabilire una connessione all'unità di controllo del dominio.	• Accertarsi che il server di indirizzario che funge da unità di controllo del dominio EIM sia attivo. Se l'unità di controllo del dominio è una piattaforma System i, è possibile utilizzare System i Navigator e ed attenersi alla seguente procedura: 1. Espandere **Rete > Server > TCP/IP**. 2. Verificare che il Server dell'indirizzario abbia lo stato **Avviato**. Se il server è arrestato, fare clic con il tasto destro del mouse su **Server indirizzario** e selezionare **Avvia**

Dopo avere verificato che le informazioni sulla connessione sono corrette e che il server di indirizzario è attivo, tentare di stabilire una connessione all'unità di controllo del dominio attenendosi alla seguente procedura:

1. Espandere **Rete > EIM (Enterprise Identity Mapping) > Gestione domini**.

2. Fare clic con il tasto destro del mouse sul dominio EIM a cui si desidera effettuare la connessione e selezionare **Connetti**.
3. Specificare il tipo di utente e le informazioni utente necessarie da utilizzare per collegarsi all'unità di controllo del dominio EIM.
4. Fare clic su **OK**.

Risoluzione dei problemi generali di configurazione EIM e dei problemi di dominio

Ci sono vari problemi generali che potrebbero verificarsi durante la configurazione di EIM per il proprio sistema e anche alcuni problemi che potrebbero verificarsi quando si accede ad un dominio EIM. Consultare la seguente tabella per ulteriori informazioni su alcuni problemi comuni e sulle potenziali soluzioni che è possibile applicare per risolverli.

Tabella 28. Problemi comuni di configurazione e di dominio EIM e soluzioni

Possibile problema	Possibili soluzioni
Il wizard di configurazione di EIM sembra bloccarsi durante l'elaborazione finale (**Fine**).	È possibile che il wizard stia attendendo che venga avviata l'unità di controllo del dominio. Controllare che non si siano verificati degli errori durante l'avvio del server di indirizzario. Per le piattaforme System i, verificare la registrazione lavoro per il lavoro `QDIRSRV` nel sottosistema `QSYSWRK`. Per verificare la registrazione lavoro, seguire queste istruzioni: 1. In System i Navigator, espandere **Gestione lavoro > Sottosistemi > Qsyswrk**. 2. Fare clic con il tasto destro del mouse su **Qdirsrv** e selezionare **Registrazione lavoro**.
Mentre si stava utilizzando il wizard di configurazione di EIM per creare un dominio su un sistema remoto, si è ricevuto un messaggio di errore che informa che Il DN (distinguished name) principale immesso non è valido. Il DN deve esistere sul server indirizzario remoto. Specificare o selezionare un DN nuovo o esistente.	Il DN principale specificato per il dominio remoto non esiste. Consultare "Creazione e partecipazione ad un nuovo dominio remoto" a pagina 80 per ulteriori informazioni su come utilizzare il wizard di configurazione di EIM. Consultare inoltre la guida in linea per informazioni dettagliate sulla specifica di un DN principale quando si crea un dominio.
Si riceve un messaggio che indica che il dominio EIM non esiste.	Se non si è creato un dominio EIM, utilizzare il wizard di configurazione di EIM. Questo wizard crea un dominio EIM per conto dell'utente oppure abilita l'utente a configurare un dominio EIM esistente. Se si è creato un dominio EIM, assicurarsi che l'utente specificato sia un membro di un gruppo di "Controllo di accesso EIM" a pagina 39 con autorizzazioni sufficienti per accedere ad esso.
Si riceve un messaggio che indica che non è stato trovato un oggetto EIM (identificativo, registro, associazione, associazione normativa o filtro certificato) o che l'utente non è autorizzato ai dati EIM.	Verificare che l'oggetto EIM esista e se l'utente specificato è un membro di un gruppo di "Controllo di accesso EIM" a pagina 39 con autorizzazioni sufficienti per accedere a detto oggetto.

Tabella 28. Problemi comuni di configurazione e di dominio EIM e soluzioni (Continua)

Possibile problema	Possibili soluzioni
Quando si espande la cartella **Identificativi**, è necessario attendere molto tempo prima che venga visualizzato l'elenco di identificativi.	Questo potrebbe verificarsi se nel dominio c'è un gran numero di identificativi EIM. Per risolvere questo problema, è possibile personalizzare la vista della cartella **Identificativi** restringendo i criteri di ricerca utilizzati per la visualizzazione degli identificativi. Per personalizzare la vista degli identificativi EIM, seguire queste istruzioni: 1. In System i Navigator, espandere **Rete > EIM (Enterprise Identity Mapping) > Gestione domini**. 2. Espandere il dominio in cui si desidera visualizzare gli identificativi EIM. 3. Fare clic con il tasto destro del mouse su **Identificativi** e selezionare **Personalizza questa vista > Includi**. 4. Specificare i criteri di visualizzazione da utilizzare per la creazione dell'elenco di identificativi EIM da inserire nella vista. **Nota:** è possibile utilizzare l'asterisco (*) come carattere jolly. 5. Fare clic su **OK**. Al successivo utilizzo della cartella **Identificativi**, verranno visualizzati solo gli identificativi EIM che corrispondono ai criteri specificati.
Mentre si sta gestendo EIM tramite System i Navigator, si riceve un errore che indica che il gestore EIM non è più valido.	La connessione all'unità di controllo del dominio EIM è stata interrotta. Per ricollegarsi all'unità di controllo del dominio, seguire i passi riportati di seguito: 1. In System i Navigator, espandere **Rete > EIM (Enterprise Identity Mapping) > Gestione domini**. 2. Fare clic con il tasto destro del mouse sul dominio che si desidera gestire e selezionare **Riconnetti**. 3. Specificare le informazioni sul collegamento. 4. Fare clic su **OK**.
Quando si utilizza il protocollo Kerberos per l'autenticazione con EIM, nella registrazione lavoro viene scritto il messaggio diagnostico `CPD3E3F`.	Questo messaggio viene generato ogni volta che le operazioni di autenticazione o di corrispondenza identità hanno esito negativo. Il messaggio di diagnostica contiene i codici di stato principali e secondari necessari per indicare dove si è verificato il problema. Gli errori più comuni vengono documentati nel messaggio insieme alla relativa correzione. Consultare le informazioni di aiuto associate al messaggio di diagnostica per avviare la risoluzione del problema. Potrebbe anche essere utile consultare la sezione Troubleshoot single sign-on configuration.

Risoluzione dei problemi di corrispondenza EIM

Ci sono vari problemi comuni che possono determinare un mancato funzionamento o un funzionamento imprevisto delle corrispondenze EIM (Enterprise Identity Mapping). Consultare la seguente tabella per trovare informazioni relative al problema che potrebbe essere la causa di un malfunzionamento delle corrispondenze EIM e sulle potenziali soluzioni per detto problema. Se si sta verificando un malfunzionamento delle corrispondenze EIM, è possibile che occorra verificare ciascuna delle soluzioni

contenute nella tabella per essere sicuri di trovare e risolvere il problema o i problemi che stanno determinando il malfunzionamento delle corrispondenze.

Tabella 29. Problemi di corrispondenza EIM comuni e soluzioni

Possibile problema	Possibili soluzioni
Le informazioni sulla connessione per l'unità di controllo del dominio potrebbero non essere corrette oppure l'unità di controllo del dominio potrebbe non essere attiva.	Consultare la sezione relativa a problemi di connessione dell'unità di controllo del dominio per informazioni su come verificare le informazioni sulla connessione per l'unità di controllo del dominio e su come verificare che l'unità di controllo del dominio sia attiva.
Si sta verificando un malfunzionamento delle operazioni di ricerca di corrispondenze EIM eseguite per conto del sistema. Questo potrebbe verificarsi perché la configurazione di EIM non è corretta sul sistema o sui sistemi.	Verificare la configurazione di EIM. Espandere **Rete-->EIM (Enterprise Identity Mapping)-->Configurazione** sul sistema con il quale si sta tentando l'autenticazione. Fare clic con il tasto destro del mouse sulla cartella **Configurazione**, selezionare **Proprietà** e verificare quanto segue: • Pagina **Dominio** : – Il nome dell'unità di controllo del dominio ed i numeri di porta sono corretti. – Fare clic su **Verifica configurazione** per verificare che l'unità di controllo del dominio sia attiva. – Il nome del registro locale è specificato in modo corretto. – Il nome del registro Kerberos è specificato in modo corretto. – Verificare che sia selezionata **Abilita operazioni EIM per questo sistema**. • pagina **Utente di sistema** : – L'utente specificato dispone di un controllo di accesso EIM sufficiente per eseguire una ricerca di corrispondenze e la parola d'ordine è valida per l'utente. Consultare la guida in linea per ulteriori informazioni sui vari tipi di credenziali dell'utente. **Nota:** se è stata modificata la parola d'ordine per l'utente di sistema specificato nel server di indirizzario, è necessario modificare la parola d'ordine anche qui. Se queste parole d'ordine non corrispondono, l'utente di sistema non può eseguire le funzioni EIM per il sistema operativo e le operazioni di ricerca di corrispondenze hanno esito negativo. – Fare clic su **Verifica connessione** per confermare che le informazioni sull'utente specificate siano corrette.

Tabella 29. Problemi di corrispondenza EIM comuni e soluzioni (Continua)

Possibile problema	Possibili soluzioni
Un'operazione di ricerche di corrispondenze potrebbe restituire più identità utente di destinazione. Questo si può verificare quando si verifica una (o più) delle seguenti situazioni: • Un identificativo EIM ha più associazioni di destinazione singole per lo stesso registro destinazione. • Più di un identificativo EIM ha la stessa identità utente specificata in un'associazione di origine e ciascuno di questi identificativi EIM ha un'associazione di destinazione allo stesso registro di destinazione, anche se l'identità utente specificata per ciascuna associazione di destinazione potrebbe essere differente. • Più di un'associazione normativa di dominio predefinita ha lo stesso registro di destinazione. • Più di un'associazione normativa di registro predefinita specifica lo stesso registro di origine e lo stesso registro di destinazione. • Più di un'associazione normativa di filtro certificato specifica lo stesso registro X.509 di origine, lo stesso filtro di certificati e lo stesso registro di destinazione.	Usare Verifica definizione EIM per verificare che un'identità utente di origine specifica corrisponda all'appropriata identità utente di destinazione. La soluzione del problema dipende dai risultati della verifica, come indicato di seguito: • La verifica restituisce più identità di destinazione indesiderate per una delle seguenti ragioni: – La configurazione di associazione per il dominio non è corretta per uno di questi motivi: - Un'associazione destinazione o origine per un identificativo EIM non è configurata in modo corretto. Non esiste un'associazione origine per il principal Kerberos (o l'utente Windows) o non è corretta. Oppure l'associazione di destinazione specifica un'identità utente non corretta. Visualizzare tutte le associazioni di identificativi per un identificativo EIM per verificare le associazioni per uno specifico identificativo. - Un'associazione normativa non è configurata in modo corretto. Visualizzare tutte le associazioni normativa per un dominio per verificare le informazioni di origine e destinazione per le associazioni normativa definite nel dominio. – Le definizioni registro di gruppo con membri comuni sono i registri origine o destinazione per associazioni identificativo EIM o normativa. Usare i dettagli dell'operazione di ricerca definizione di verifica per stabilire se i registri di origine o di destinazione sono definizioni del registro di gruppo. In tal caso, verificare le proprietà di definizione del registro di gruppo per stabilire se le definizioni contengono membri comuni. – La verifica restituisce più identità di destinazione e i risultati sono appropriati al modo in cui sono configurate le associazioni. Se questo è il caso, indicare le informazioni di ricerca per ogni identità utente di destinazione, perché un'operazione di ricerca restituisca una sola identità e non tutte quelle possibili. Consultare Aggiunta informazioni di ricerca a un'identità utente di destinazione. **Nota:** questo approccio funziona solo se l'applicazione può usare le informazioni di ricerca. Tuttavia, le applicazioni base i5/OS come System i Access per Windows non possono usare informazioni di ricerca per distinguere tra più identità utente di destinazione restituite da un'operazione di ricerca. Ridefinire, quindi, le associazioni per il dominio in modo che un'operazione di ricerca di corrispondenze restituisca una sola identità utente per assicurare che le applicazioni i5/OS base eseguano in modo corretto operazioni di ricerca e corrispondenze identità.

Tabella 29. Problemi di corrispondenza EIM comuni e soluzioni (Continua)

Possibile problema	Possibili soluzioni
Le operazioni di ricerca EIM non restituiscono risultati e le associazioni sono configurate per il dominio.	Usare la funzione Verifica definizione EIM per verificare che un'identità utente di origine specifica corrisponda all'appropriata identità utente di destinazione. Verificare di aver fornito le informazioni corrette per la verifica. Se valide e la verifica non restituisce risultati, il problema potrebbe essere stato causato da: • La configurazione dell'associazione non è corretta. Verificare tale configurazione usando le informazioni sulla risoluzione dei problemi fornite alla voce precedente. • Il supporto delle associazioni normativa non è abilitato a livello del dominio. È possibile che occorra abilitare le associazioni normativa per un dominio. • Il supporto di ricerca corrispondenze o il supporto di associazioni normativa non è abilitato a livello di singolo registro. Potrebbe essere necessario abilitare il supporto di ricerca di corrispondenze e l'utilizzo delle associazioni normativa per il registro di destinazione. • La definizione di registro e le identità utente non corrispondono perché sono sensibili al maiuscolo/minuscolo. È possibile cancellare e creare nuovamente il registro oppure cancellare e creare nuovamente le associazioni utilizzando la corretta sequenza di maiuscole/minuscole.

Attività correlate

"Verifica delle corrispondenze" a pagina 94
La verifica delle corrispondenze EIM (Enterprise Identity Mapping) consente di eseguire le operazioni di ricerca di corrispondenze EIM nella configurazione EIM. È possibile utilizzare la verifica per controllare che una specifica identità utente di origine corrisponda esattamente all'identità utente di destinazione appropriata. La verifica assicura che le operazioni di ricerca delle corrispondenze EIM possano restituire l'identità utente destinazione corretta in base alle informazioni specificate.

API di EIM

EIM (Enterprise Identity Mapping) fornisce il mezzo per la gestione delle identità degli utenti tra più piattaforme. EIM dispone di più API (application programming interface) che possono essere utilizzate dalle applicazioni per eseguire operazioni EIM al posto dell'applicazione o di un'applicazione utente.

È possibile utilizzare queste API per eseguire le operazioni di ricerca delle corrispondenze, le varie funzioni di configurazione e gestione EIM, le modifiche alle informazioni e le capacità di eseguire le query. Ciascuna di queste API è supportata tra le piattaforme IBM.

Le API relative ad EIM si suddividono in più categorie:

- Operazioni di collegamento e gestore EIM
- Gestione dominio EIM
- Operazioni di registro
- Operazioni identificativo EIM
- Gestione associazione EIM

- Operazioni di ricerca delle corrispondenze EIM
- Gestione autorizzazione EIM

Le applicazioni che utilizzano queste API per gestire o utilizzare le informazioni EIM in un dominio EIM normalmente rientrano nel seguente modello di programmazione:

1. Richiamo di un gestore EIM
2. Collegamento ad un dominio EIM
3. Normale elaborazione dell'applicazione
4. Utilizzo di un'API di gestione EIM o dell'operazione di ricerca delle corrispondenze EIM
5. Normale elaborazione dell'applicazione
6. Prima di terminare, eliminazione del gestore EIM

Concetti correlati

"Pianificazione dello sviluppo delle applicazioni EIM" a pagina 70
Per consentire ad un'applicazione di utilizzare EIM (Enterprise Identity Mapping) e partecipare ad un dominio, l'applicazione deve essere in grado di utilizzare le API EIM.

Informazioni correlate

API EIM (Enterprise Identity Mapping)

Informazioni correlate per EIM

Le pubblicazioni IBM Redbooks altre raccolte di argomenti dell'information center contengono informazioni relative alla raccolta di argomenti su EIM (Enterprise Identity Mapping). È possibile visualizzare o stampare qualsiasi file PDF.

IBM Redbooks

- Windows-based Single Signon and the EIM Framework on the IBM eServer iSeries Server 
- iSeries Access for Windows V5R2 Hot Topics: Tailored Images, Application Administration, SSL, and Kerberos 

Ulteriori informazioni

- SSO (Single signon)
- Servizio autenticazione di rete
- IBM Tivoli Directory Server per i5/OS (LDAP)

Termini e condizioni

Le autorizzazioni per l'utilizzo delle presenti pubblicazioni vengono concesse in base ai seguenti termini e condizioni.

Uso personale: È possibile riprodurre queste pubblicazioni per uso personale, non commerciale a condizione che vengano conservate tutte le indicazioni relative alla proprietà. Non è possibile distribuire, visualizzare o produrre lavori derivati di tali pubblicazioni o di qualsiasi loro parte senza chiaro consenso da parte di IBM.

Uso commerciale: È possibile riprodurre, distribuire e visualizzare queste pubblicazioni unicamente all'interno del proprio gruppo aziendale a condizione che vengano conservate tutte le indicazioni relative alla proprietà. Non è possibile effettuare lavori derivati di queste pubblicazioni o riprodurre, distribuire o visualizzare queste pubblicazioni o qualsiasi loro parte al di fuori del proprio gruppo aziendale senza chiaro consenso da parte di IBM.

Fatto salvo quanto espressamente concesso in questa autorizzazione, non sono concesse altre autorizzazioni, licenze o diritti, espressi o impliciti, relativi alle pubblicazioni o a qualsiasi informazione, dato, software o altra proprietà intellettuale qui contenuta.

IBM si riserva il diritto di ritirare le autorizzazioni qui concesse qualora, a propria discrezione, l'utilizzo di queste pubblicazioni sia a danno dei propri interessi o, come determinato da IBM, qualora non siano rispettate in modo appropriato le suddette istruzioni.

Non è possibile scaricare, esportare o ri-esportare queste informazioni se non in modo pienamente conforme con tutte le leggi e le norme applicabili, incluse le leggi e le norme di esportazione degli Stati Uniti.

IBM NON RILASCIA ALCUNA GARANZIA RELATIVAMENTE AL CONTENUTO DI QUESTE PUBBLICAZIONI. LE PUBBLICAZIONI SONO FORNITE "COSI' COME SONO", SENZA ALCUN TIPO DI GARANZIA, ESPRESSA O IMPLICITA, INCLUSE, A TITOLO ESEMPLIFICATIVO, GARANZIE IMPLICITE DI COMMERCIABILITA' ED IDONEITA' PER UNO SCOPO PARTICOLARE.

Appendice. Informazioni particolari

Queste informazioni sono state progettate per prodotti e servizi offerti negli Stati Uniti.

IBM potrebbe non fornire ad altri paesi prodotti, servizi o funzioni discussi in questo documento. Contattare il rappresentante IBM locale per informazioni sui prodotti e servizi correntemente disponibili nella propria area. Qualsiasi riferimento ad un prodotto, programma o servizio IBM non implica che sia possibile utilizzare soltanto tali prodotti, programmi o servizi IBM. In sostituzione a quanto fornito da IBM, è possibile utilizzare qualsiasi prodotto, programma o servizio funzionalmente equivalente che non violi alcun diritto di proprietà intellettuale di IBM. Tuttavia la valutazione e la verifica dell'uso di prodotti o servizi non IBM ricadono esclusivamente sotto la responsabilità dell'utente.

IBM può avere brevetti o domande di brevetto in corso relativi a quanto trattato nel presente documento. La fornitura di questa pubblicazione non implica la concessione di alcuna licenza su tali brevetti. Chi desiderasse ricevere informazioni relative a licenza può rivolgersi per iscritto a:

Director of Commercial Relations
IBM Europe
Schoenaicher Str. 220
D-7030 Boeblingen
Deutschland

Per le richieste sulla licenza riguardanti informazioni a doppio byte (DBCS), contattare l'IBM Intellectual Property Department del vostro paese o indirizzare eventuali richieste a:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

Le disposizioni contenute nel seguente paragrafo non si applicano al Regno Unito o ad altri paesi nei quali tali disposizioni non siano congruenti con le leggi locali: IBM FORNISCE QUESTA PUBBLICAZIONE "COSI' COM'E'" SENZA ALCUNA GARANZIA, ESPLICITA O IMPLICITA, IVI INCLUSE EVENTUALI GARANZIE DI COMMERCIABILITÀ' ED IDONEITÀ' AD UNO SCOPO PARTICOLARE. Alcuni stati non consentono la recessione da garanzie implicite o esplicite in alcune transazioni, quindi questa specifica potrebbe non essere applicabile in determinati casi.

Queste informazioni possono contenere imprecisioni tecniche o errori tipografici. Alle informazioni di seguito riportate periodicamente vengono apportate delle modifiche; tali modifiche saranno incluse nelle nuove edizioni della presente pubblicazione. IBM si riserva di apportare senza preavviso e in qualsiasi momento miglioramenti e/o modifiche al/i prodotto/i e/o al/i programma/i descritto/i in questa pubblicazione.

Qualsiasi riferimento a siti Web non IBM, contenuto in queste informazioni, viene fornito solo per comodità e non implica in alcun modo l'approvazione di tali siti. I materiali disponibili in questi siti non fanno parte del prodotto e l'utilizzo di questi è a discrezione dell'utente.

IBM può utilizzare o distribuire le informazioni fornite in qualsiasi modo ritenga appropriato senza obblighi verso l'utente.

Sarebbe opportuno che coloro che hanno licenza per questo programma e desiderano avere informazioni su di esso allo scopo di consentire: (i) lo scambio di informazioni tra programmi creati in maniera indipendente e non (compreso questo), (ii) l'uso reciproco di tali informazioni, contattassero:

IBM Corporation

Software Interoperability Coordinator, Department 49XA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Tali informazioni possono essere disponibili secondo i termini e le condizioni appropriate, con il pagamento, in alcuni casi, di un corrispettivo.

Il programma su licenza descritto in questa pubblicazione e tutto il relativo materiale disponibile viene fornito da IBM nei termini dell'IBM Customer Agreement, IBM International Program License Agreement, IBM License Agreement for Machine Code o qualsiasi altro accordo equivalente tra le parti.

Qualsiasi dato sulle prestazioni contenuto in questa pubblicazione è stato stabilito in un ambiente controllato. Quindi i risultati ottenuti in altri ambienti operativi potrebbero variare in modo significativo. È possibile che alcune misurazioni siano state effettuate su sistemi a livello di sviluppo e non esiste alcuna garanzia che tali misurazioni siano le stesse su sistemi generalmente disponibili. Inoltre, è possibile che alcune misurazioni siano state calcolate tramite estrapolazione. I risultati effettivi possono variare. Sarebbe opportuno che gli utenti di questa pubblicazione verificassero i dati applicabili per il relativo ambiente specifico.

Le informazioni riguardanti prodotti non IBM sono ottenute dai fornitori di tali prodotti, dai loro annunci pubblicati o da altre fonti pubblicamente reperibili. IBM non ha testato tali prodotti e non può confermare l'inadeguatezza delle prestazioni, della compatibilità o di altre richieste relative a prodotti non IBM. Domande inerenti alle prestazioni di prodotti non IBM dovrebbero essere indirizzate ai fornitori di tali prodotti.

Tutte le specifiche relative alle direttive o intenti futuri di IBM sono soggette a modifiche o a revoche senza notifica e rappresentano soltanto scopi ed obiettivi.

Tutti i prezzi IBM mostrati sono i prezzi al dettaglio suggeriti da IBM, sono attuali e soggetti a modifica senza preavviso. I prezzi al fornitore possono variare.

Queste informazioni sono solo per scopi di pianificazione. Le presenti informazioni sono soggette a modifiche prima che i prodotti descritti siano resi disponibili.

Queste informazioni contengono esempi di dati e report utilizzati in quotidiane operazioni aziendali. Per illustrarle nel modo più completo possibile, gli esempi includono i nomi di individui, società, marchi e prodotti. Tutti questi nomi sono fittizi e qualsiasi somiglianza con nomi ed indirizzi utilizzati da gruppi aziendali realmente esistenti è puramente casuale.

LICENZA DI COPYRIGHT:

Queste informazioni contengono programmi di applicazione di esempio nella lingua di origine, che illustrano le tecniche di programmazione su varie piattaforme operative. È possibile copiare, modificare e distribuire questi programmi di esempio in qualsiasi formato senza pagare a IBM, allo scopo di sviluppare, utilizzare, commercializzare o distribuire i programmi dell'applicazione conformi all'interfaccia di programmazione dell'applicazione per la piattaforma operativa per cui i programmi di esempio vengono scritti. Questi esempi non sono stati interamente testati in tutte le condizioni. IBM, perciò, non fornisce nessun tipo di garanzia o affidabilità implicita, rispetto alla funzionalità o alle funzioni di questi programmi.

Ogni copia, parte di questi programmi di esempio o lavoro derivato, devono includere un avviso sul copyright, come ad esempio:

© (nome azienda) (anno). Le parti di questo codice provengono da IBM Corp. Sample Programs. © Copyright IBM Corp. _immettere l'anno o gli anni_. Tutti i diritti riservati.

Se si sta utilizzando la versione in formato elettronico di questo manuale, le fotografie e le illustrazioni a colori potrebbero non essere visualizzate.

Marchi

I seguenti termini sono marchi di IBM Corporation negli Stati Uniti e/o negli altri paesi:

AIX
Distributed Relational Database Architecture
Domino
DRDA
eServer
i5/OS
IBM
iSeries
Lotus Notes
NetServer
OS/400
pSeries
RACF
RDN
System i
Tivoli
WebSphere
xSeries
z/OS

Adobe, il logo Adobe, PostScript ed il logo PostScript sono marchi di Adobe Systems Incorporated negli Stati Uniti e/o negli altri paesi.

Linux è un marchio registrato di Linus Torvalds negli Stati Uniti e/o negli altri paesi.

Microsoft, Windows, Windows NT e il logo Windows sono marchi registrati della Microsoft Corporation negli Stati Uniti e/o negli altri paesi.

UNIX è un marchio registrato negli Stati Uniti e in altri paesi con licenza esclusiva di Open Group.

Nomi di altre società, prodotti o servizi possono essere marchi di altre società.

Termini e condizioni

Le autorizzazioni per l'utilizzo delle presenti pubblicazioni vengono concesse in base ai seguenti termini e condizioni.

Uso personale: È possibile riprodurre queste pubblicazioni per uso personale, non commerciale a condizione che vengano conservate tutte le indicazioni relative alla proprietà. Non è possibile distribuire, visualizzare o produrre lavori derivati di tali pubblicazioni o di qualsiasi loro parte senza chiaro consenso da parte di IBM.

Uso commerciale: È possibile riprodurre, distribuire e visualizzare queste pubblicazioni unicamente all'interno del proprio gruppo aziendale a condizione che vengano conservate tutte le indicazioni relative alla proprietà. Non è possibile effettuare lavori derivati di queste pubblicazioni o riprodurre, distribuire o visualizzare queste pubblicazioni o qualsiasi loro parte al di fuori del proprio gruppo aziendale senza chiaro consenso da parte di IBM.

Fatto salvo quanto espressamente concesso in questa autorizzazione, non sono concesse altre autorizzazioni, licenze o diritti, espressi o impliciti, relativi alle pubblicazioni o a qualsiasi informazione, dato, software o altra proprietà intellettuale qui contenuta.

IBM si riserva il diritto di ritirare le autorizzazioni qui concesse qualora, a propria discrezione, l'utilizzo di queste pubblicazioni sia a danno dei propri interessi o, come determinato da IBM, qualora non siano rispettate in modo appropriato le suddette istruzioni.

Non è possibile scaricare, esportare o ri-esportare queste informazioni se non in modo pienamente conforme con tutte le leggi e le norme applicabili, incluse le leggi e le norme di esportazione degli Stati Uniti.

IBM NON RILASCIA ALCUNA GARANZIA RELATIVAMENTE AL CONTENUTO DI QUESTE PUBBLICAZIONI. LE PUBBLICAZIONI SONO FORNITE "COSI' COME SONO", SENZA ALCUN TIPO DI GARANZIA, ESPRESSA O IMPLICITA, INCLUSE, A TITOLO ESEMPLIFICATIVO, GARANZIE IMPLICITE DI COMMERCIABILITA' ED IDONEITA' PER UNO SCOPO PARTICOLARE.

Stampato in Italia