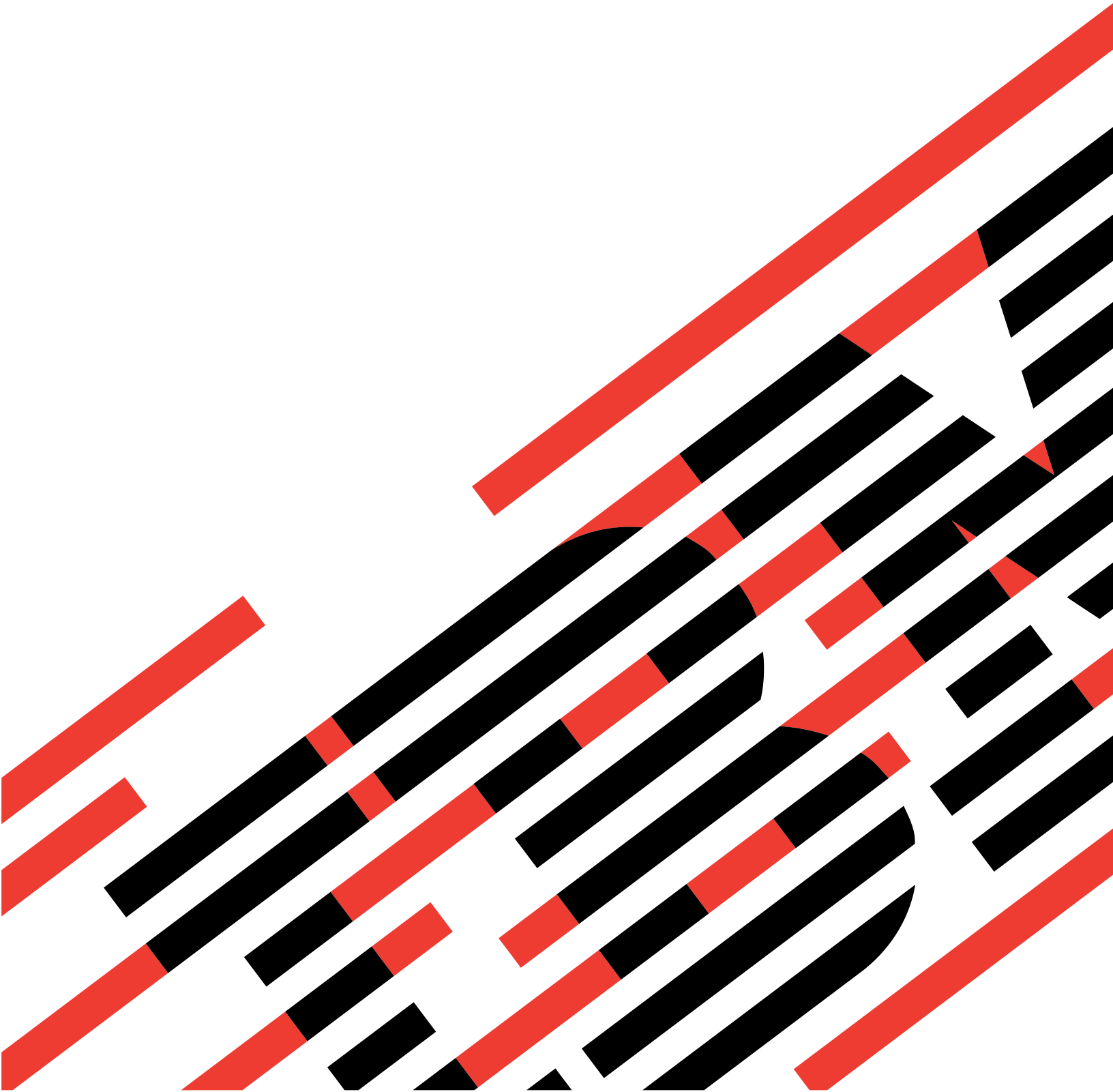
IBM

eserver

iSeries

EIM (Enterprise Identity Mapping)



IBM

@server

iSeries

EIM (Enterprise Identity Mapping)

Indice

EIM (Enterprise Identity Mapping)

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 (Enterprise Identity Mapping) consente soluzioni economiche per una gestione più semplice di più registri utenti e identità utente nella propria società.

EIM è un meccanismo per la messa in corrispondenza (associazione) di una persona o entità alle identità utente appropriate nei vari registri per tutta la società. EIM fornisce API per la creazione e la gestione di queste relazioni di messa in corrispondenza dell'identità, come pure API che vengono utilizzate dalle applicazioni per interrogare tali informazioni. Inoltre, OS/400(R) utilizza le capacità EIM e Kerberos per fornire un ambiente a collegamento singolo.

iSeries Navigator, la GUI di iSeries, fornisce wizard per configurare e gestire EIM. Inoltre, gli amministratori possono gestire le relazioni EIM per i profili utente tramite iSeries Navigator.

Il server iSeries(TM) utilizza EIM per consentire alle interfacce OS/400 di autenticare gli utenti tramite il servizio di autenticazione di rete. Le applicazioni, come pure OS/400, possono accettare ticket Kerberos ed utilizzare EIM per trovare il profilo utente che rappresenta la stessa persona rappresentata dal ticket Kerberos.

Gli argomenti riportati di seguito forniscono informazioni specifiche su EIM:

Stampa di questo argomento
Stampa di una versione PDF di questo argomento di EIM e di altri argomenti correlati.

Panoramica su EIM (Enterprise Identity Mapping)
Informazioni sui problemi che possono essere risolti tramite EIM, approcci aziendali a tali problemi e il motivo per cui l'approccio EIM si rivela la migliore soluzione.

Concetti relativi a EIM
Informazioni sui concetti EIM necessari per comprendere pienamente l'implementazione di EIM.

Concetti LDAP relativi a EIM
Informazioni sui concetti LDAP (Lightweight Directory Access Protocol) necessari per comprendere pienamente l'implementazione di EIM.

Abilitazione di un collegamento singolo
Informazioni sui benefici forniti da EIM nella semplificazione del collegamento utente.

Pianificazione per EIM
Assicurarsi che tutti i servizi e le applicazioni necessari siano configurati prima di configurare EIM.

Configurazione di EIM
Utilizzo del wizard Configurazione EIM (Enterprise Identity Mapping) (in seguito si farà riferimento a tale wizard con il nome Configurazione EIM) per iniziare con EIM.

Gestione EIM
Gestione delle proprietà EIM, dei domini EIM, dei registri utenti, delle autorizzazioni utente EIM e così via.

API relative a EIM
Utilizzo delle API relative ad EIM nelle applicazioni e nella rete.

Risoluzione dei problemi di EIM
Ricerca delle soluzioni ai problemi e agli errori comuni che si verificano quando si utilizza EIM nella rete.

Informazioni correlative relative a EIM
Collegamento alle informazioni correlate relative a EIM.

Stampa di questo argomento

Per visualizzare o scaricare la versione PDF, selezionare EIM (Enterprise Identity Mapping)

(circa 390 KB o 50 pagine).

Altre informazioni

E' possibile visualizzare o scaricare questi argomenti correlati:

- Servizi di autenticazione di rete (circa 199 KB o 60 pagine) contiene le informazioni su come configurare il servizio di autenticazione di rete insieme ad EIM per creare un ambiente a collegamento singolo.
- Servizi indirizzario (LDAP) (circa 323 KB o 66 pagine) contiene informazioni su come configurare il server LDAP, che può essere utilizzato come unità di controllo del dominio EIM, insieme alle informazioni sulla configurazione LDAP avanzata.

Salvataggio del file PDF

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

1. Aprire il PDF nel browser (fare clic sul collegamento riportato sopra).
2. Nel menu del browser, fare clic su **File**.
3. Fare clic su **Salva con nome...**
4. Spostarsi nell'indirizzario in cui si desidera salvare il PDF.
5. Fare clic su **Salva**.

Scaricamento di Adobe Acrobat Reader

Se si necessita di Adobe Acrobat Reader per visualizzare o stampare questi PDF, è possibile scaricarne una copia dal sito web di Adobe (www.adobe.com/prodindex/acrobat/readstep.html)

.

Panoramica su EIM (Enterprise Identity Mapping)

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 (Enterprise Identity Mapping) è una tecnologia di infrastruttura IBM

che consente agli amministratori e agli sviluppatori di applicazioni di indirizzare 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 costo amministrativo e aumentando potenzialmente la verosomiglianza dell'esposizione della 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 collegamento singolo. 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 soluzioni economiche per gestire in modo più semplice diversi registri utenti e identità utente in una società. EIM costituisce un'architettura per la descrizione delle relazioni tra singoli o entità (come i server file e i server di stampa) nella società e le molte identità che li rappresentano all'interno della società. Inoltre, EIM fornisce una serie di API che consentono alle applicazioni di effettuare domande su queste relazioni.

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 è stato autenticato con un'identità utente ed è possibile mettere in corrispondenza tale identità con l'identità appropriata presente in un altro registro utenti, l'utente non deve fornire di nuovo le credenziali per l'autenticazione. L'utente è già noto ed è necessario sapere solo quale identità utente rappresenta tale utente in un altro registro utenti. Quindi, EIM fornisce una funzione di messa in corrispondenza dell'identità generalizzata per la società.

La capacità di mettere in corrispondenza le identità dell'utente in diversi registri utenti fornisce molti benefici. Innanzitutto, indica che le applicazioni sono flessibili nell'utilizzo di un registro utenti per l'autenticazione e dell'utilizzo di un altro registro completamente diverso per l'autorizzazione. Ad esempio, un amministratore può mettere in corrispondenza un'identità SAP (o meglio, SAP potrebbe effettuare tale operazione da sola) per accedere alle risorse SAP.

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

1. Creare identificativi EIM che rappresentino le persone o entità della società.
2. Creare definizioni di registro EIM che descrivono i registri utenti esistenti nella società.
3. Definire la relazione tra le identità utente presenti in tali registri e gli identificativi EIM che sono stati creati.

Nei registri utenti esistenti non sono necessarie modifiche al codice. L'amministratore non deve avere le corrispondenze per tutte le identità presenti in un registro utenti. EIM consente corrispondenze uno-molti (in altri termini, un singolo utente con più identità in un singolo registro utenti). EIM consente inoltre corrispondenze molti-uno (in altri termini, più utenti condividono una singola identità utente in un singolo registro utenti, il che sebbene supportato non è consigliato). Un amministratore può rappresentare un qualsiasi registro utenti di un qualsiasi tipo in EIM.

EIM è un'architettura aperta che gli amministratori possono utilizzare per rappresentare le relazioni di corrispondenza identità per qualsiasi registro. Non richiede che i dati vengano copiati in un nuovo contenitore e che si tenti di tenere le copie sincronizzate. Gli unici dati che vengono introdotti da EIM sono le informazioni sulla relazione. Gli amministratori gestiscono questi dati in un indirizzario LDAP, il quale fornisce la flessibilità di gestione dei dati in un'unica ubicazione e di disporre di repliche dovunque 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.

Concetti su 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 possono differire a seconda delle piattaforme, i concetti su EIM sono comuni tra le piattaforme IBM

@server

.

La Figura 1 fornisce un esempio di implementazione di EIM in una società. Tre server operano come client EIM e contengono le applicazioni abilitate da EIM che richiedono dati EIM utilizzando le operazioni di ricerca EIM

6

. L'unità di controllo del dominio

1

memorizza le informazioni sul dominio EIM

2

, che includono un identificativo EIM

3

, le associazioni

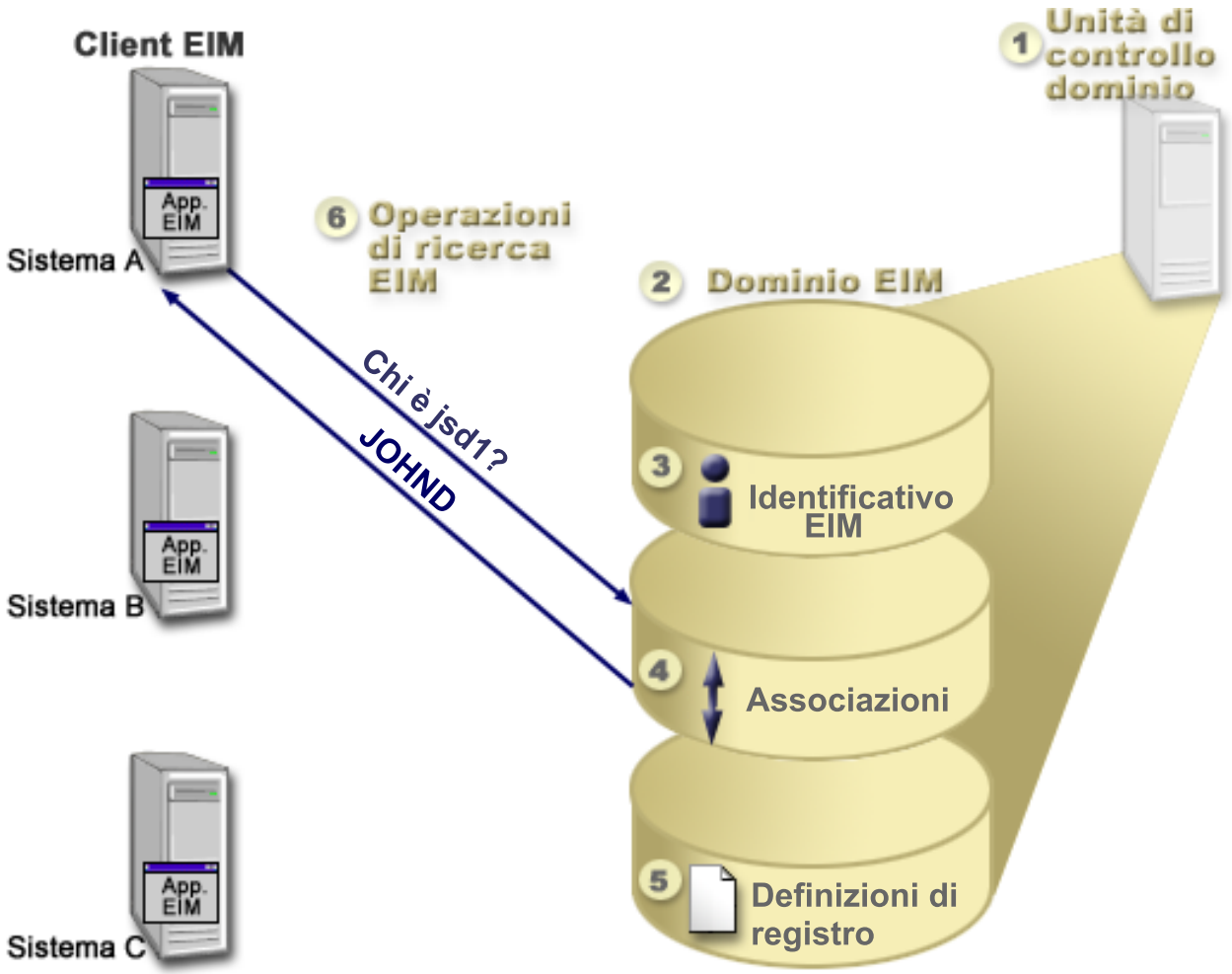
4

tra questi identificativi EIM e le identità utente e le definizioni di registro EIM

5

.

Figura 1: Un esempio di implementazione EIM



Rivedere le informazioni riportate di seguito per meglio comprendere questi concetti su EIM:

- Unità di controllo del dominio EIM
- Dominio EIM
- Identificativo EIM
- Definizioni di registro EIM
- Associazioni EIM
- Operazioni di ricerca EIM
- Autorizzazioni EIM

Unità di controllo del dominio EIM

L'*unità di controllo del dominio EIM* è un server LDAP (Lightweight Directory Access Protocol) configurato per gestire almeno un dominio EIM. Un *dominio EIM* è un indirizzario LDAP composto da tutti gli identificativi EIM, le associazioni EIM e i registri utenti definiti in tale dominio. I sistemi (client EIM) fanno parte del dominio EIM utilizzando i dati del dominio relativi alle operazioni di ricerca EIM. Nella società deve essere presente minimo un'unità di controllo del dominio EIM.

Attualmente, è possibile configurare alcune piattaforme IBM

in modo che operino come un'unità di controllo del dominio EIM. Qualsiasi sistema che supporta le API relative ad EIM può partecipare come client nel dominio. Questi sistemi client utilizzano le API relative ad EIM per contattare un'unità di controllo del dominio EIM per eseguire operazioni di ricerca EIM.

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. E' invece *remota* se il client EIM è in esecuzione su un sistema separato dall'unità di controllo del dominio.

Dominio EIM

Un *dominio EIM* è un indirizzario presente nel server LDAP (Lightweight Directory Access Protocol) che contiene i dati EIM di una società. Un dominio EIM è una raccolta di tutti gli identificativi EIM, delle associazioni EIM e dei registri utenti definiti in tale dominio. I sistemi (client EIM) fanno parte del dominio utilizzando i dati del dominio relativi alle operazioni di ricerca EIM.

Un dominio EIM è diverso da un registro utenti. Un registro utenti definisce una serie di identità utente note e sicure da una particolare istanza di un sistema operativo o applicazione. Un registro utenti contiene anche le informazioni necessarie per autenticare l'utente dell'identità. Inoltre, tale registro spesso contiene altri attributi come le preferenze utente, i privilegi di sistema o le informazioni personali su tale 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. Poiché EIM tiene traccia solo delle informazioni sulla relazione, non esistono elementi da sincronizzare tra i registri utenti e EIM.

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 le persone o le entità rappresentate da tali identità nella società.

Figura 2: Dominio EIM e dati memorizzati nel dominio

I dati EIM includono:

- **Identificativi EIM.** Ogni identificativo EIM creato rappresenta una persona o un'entità (ad esempio un server di stampa o un server file) all'interno di una società. Consultare Identificativo EIM per ulteriori informazioni.
- **Definizioni di registro EIM.** Ogni definizione di registro EIM creata rappresenta un registro utenti reale (e le informazioni sull'identità utente in esso contenute) presente su un sistema all'interno della società. Una volta definito uno specifico registro utenti in EIM, tale registro può entrare a far parte del dominio EIM. Consultare Definizioni di registro EIM per ulteriori informazioni.
- **Associazioni EIM.** Ogni associazione EIM creata rappresenta la relazione tra un identificativo EIM e un'identità associata all'interno di una società. Le associazioni vengono create per le identità presenti nei registri utenti che fanno parte del dominio EIM. Le associazioni forniscono le informazioni che collegano un identificativo EIM ad una specifica identità utente in un determinato registro utenti. Di conseguenza, le associazioni devono essere definite in modo tale che i client EIM possano utilizzare le API relative ad EIM per eseguire operazioni di ricerca EIM con esito positivo. Queste operazioni di ricerca EIM cercano in un dominio EIM le associazioni tra gli identificativi EIM e le identità utente nei registri utenti riconosciuti. Consultare Operazioni di ricerca EIM per ulteriori informazioni.

Una volta creati gli identificativi EIM, le definizioni di registro e le associazioni, è possibile iniziare ad utilizzare EIM per organizzare e gestire in maniera più semplice le identità utente all'interno della società.

Identificativo EIM

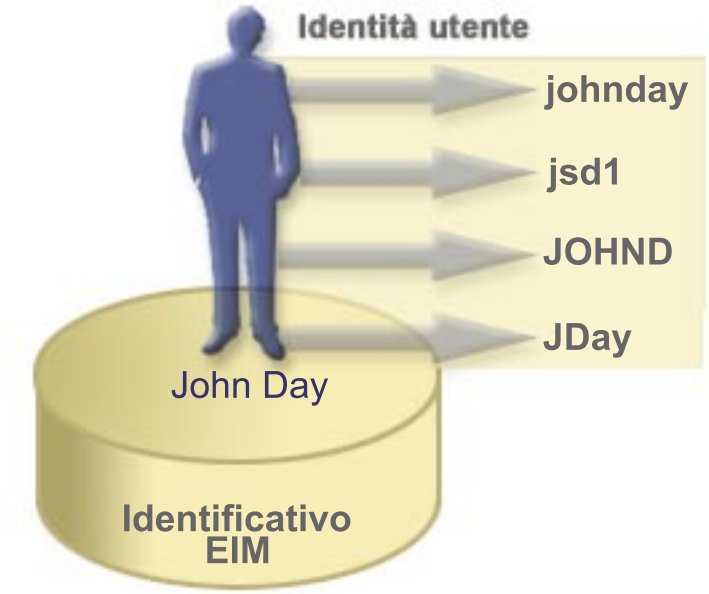
Un *identificativo EIM* rappresenta una persona o un'entità in una società. Una tipica rete è composta da diverse applicazioni e piattaforme hardware e dai registri utenti associati. La maggior parte delle piattaforme e molte delle applicazioni utilizzano registri utenti specifici della piattaforma o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

Quando si crea un identificativo EIM e lo si associa a diverse identità utente relative ad una persona o entità, diventa più semplice creare applicazioni multi-livello eterogenee, ad esempio, un ambiente a collegamento singolo. Quando si crea un identificativo EIM e le associazioni, risulta più semplice anche creare ed utilizzare strumenti che semplifichino l'amministrazione implicata nella gestione di ogni identità di cui dispone una persona o un'entità all'interno della società.

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 quattro diversi registri utenti: `johnday`, `jsd1`, `JOHND` e `JDay`.

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

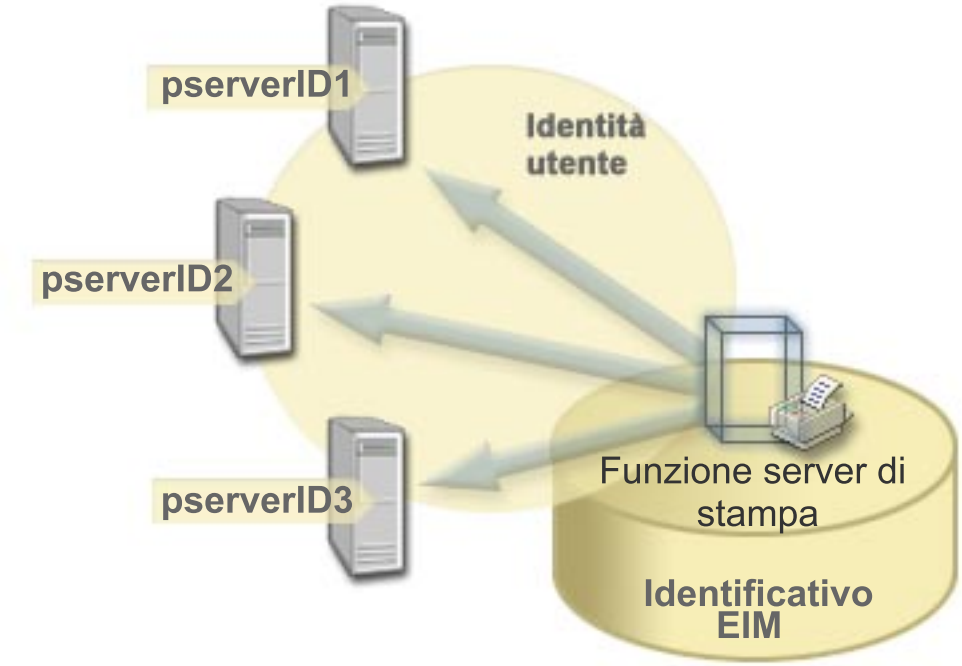


In EIM, è possibile creare associazioni che definiscono le relazioni tra l'identificativo `John Day` e ognuna delle diverse identità utente di *John Day*. Creando queste associazioni per definire queste relazioni, è possibile scrivere delle applicazioni che utilizzino le API relative ad EIM per ricercare 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. In questo esempio, l'identificativo EIM `funzione server di stampa` rappresenta l'entità reale della funzione del server di stampa nella società. Le associazioni create per definire le relazioni tra l'identificativo EIM (`funzione server di stampa`) e ognuna delle entità utente di 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.

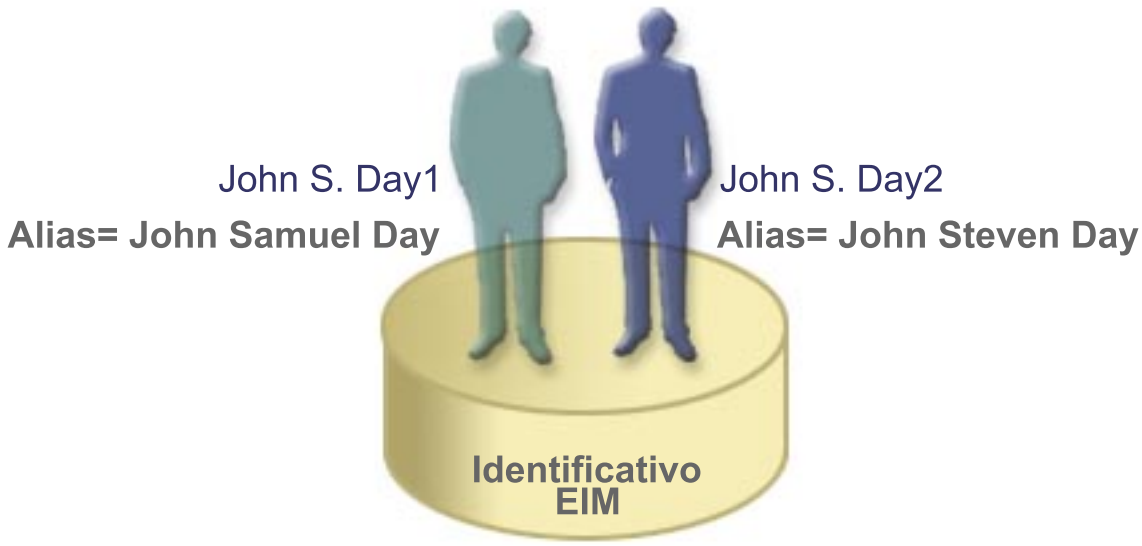
Alias e identificativi EIM

Per gli identificativi EIM possono essere creati anche degli alias. Questi ultimi possono essere di aiuto nella localizzazione di uno specifico identificativo EIM nel momento in cui viene eseguita 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 di un dominio EIM. Gli alias possono aiutare a risolvere le situazioni in cui l'utilizzo di nomi identificativi univoci possa rivelarsi difficile. Ad esempio, diversi individui all'interno di una società possono condividere lo stesso nome, ciò può creare confusione se si stanno utilizzando 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 diversi identificativi EIM per distinguerli: `John S. Day1` e `John S. Day2`. Tuttavia, non è immediatamente comprensibile quale *John S. Day* sia rappresentato da ognuno di questi identificativi.

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



Utilizzando gli alias, l'amministratore EIM può fornire ulteriori informazioni sull'individuo di ciascun identificativo EIM. Queste informazioni possono essere utilizzate anche in un'operazione di ricerca EIM per distinguere tra gli utenti rappresentati dall'identificativo. Ad esempio, l'alias di `John S. Day1` potrebbe essere `John Samuel Day` e l'alias di `John S. Day2` potrebbe essere `John Steven Day`.

Ogni identificativo EIM può avere più alias per identificare quale *John S. Day* è rappresentato dall'identificativo EIM. L'amministratore EIM potrebbe aggiungere un altro alias ad ogni identificativo EIM dei due individui per distinguerli ulteriormente. Ad esempio, gli alias aggiuntivi potrebbero contenere il numero impiegato, il numero settore, la qualifica o altri attributi distinti dell'utente.

Definizioni di registro EIM

Una *definizione di registro EIM* rappresenta il registro utenti reale presente su un sistema all'interno della società. Un registro utenti funziona come un indirizzario e contiene una lista di identità utente valide per un determinato sistema o applicazione. Un registro utenti di base contiene identità utente e le relative parole d'ordine. Un esempio di registro utenti è costituito dal registro z/OS Security Server Resource Access Control Facility (RACF(R)). I registri utenti possono contenere anche altre informazioni. Ad esempio, un indirizzario LDAP (Lightweight Directory Access Protocol) contiene i DN, le parole d'ordine e i controlli di accesso ai dati memorizzati in LDAP. Altri esempi di registri utenti comuni sono KDC (key distribution center) di Kerberos e il registro profili utente OS/400.

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

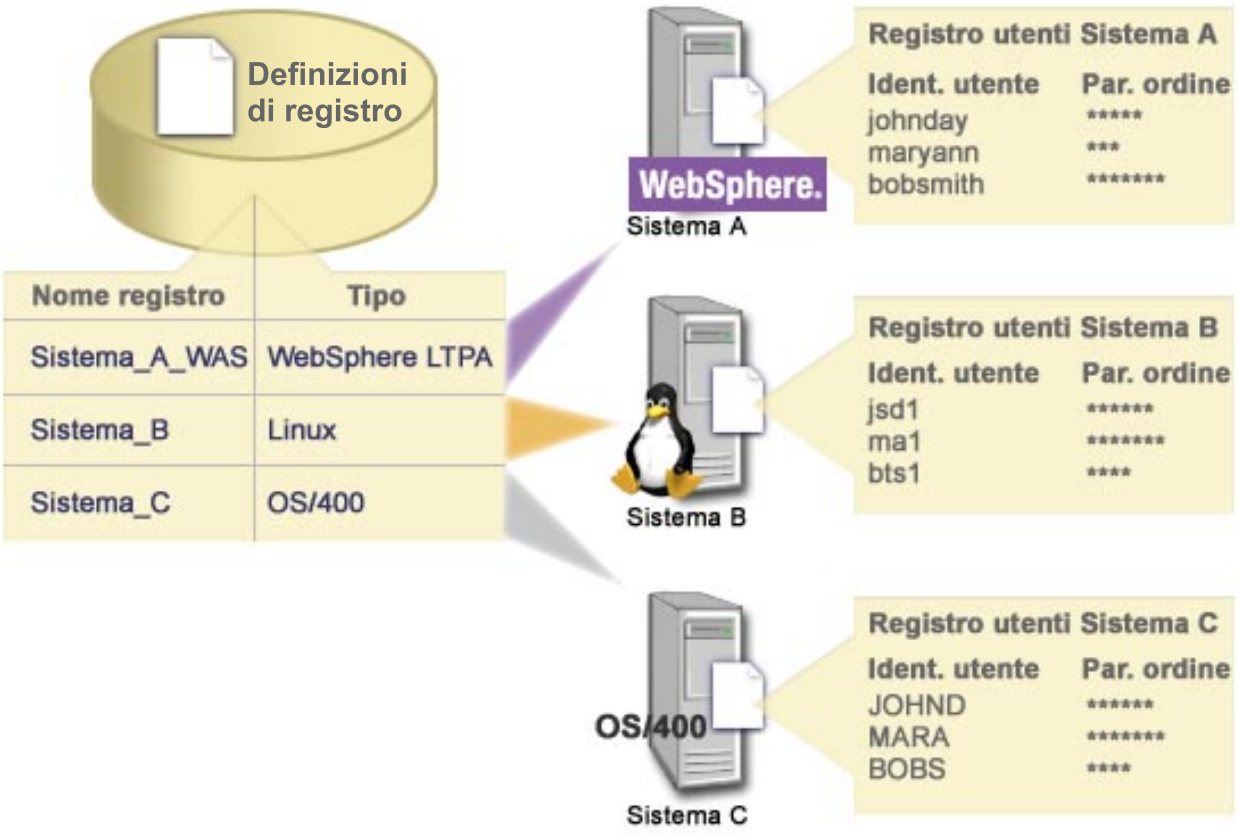
- Un nome registro EIM arbitrario e univoco
- Il tipo di registro utenti

Ogni definizione di registro rappresenta un'istanza specifica 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 di un registro utenti di sistema oppure il nome host combinato con il nome dell'applicazione di un registro utenti applicazione. Per creare nomi definizione di registro EIM univoci, è possibile utilizzare una qualsiasi combinazione di caratteri alfanumerici, di caratteri misti e spazi.

Nella Figura 6, l'amministratore ha creato definizioni di registro EIM per registri utenti che rappresentano il Sistema A, il Sistema B e il Sistema C. Ad esempio, il Sistema A contiene un registro utenti relativo a WebSphere LTPA (Lightweight Third-Party Authentication). Il nome definizione di registro utilizzato

dall'amministratore è di aiuto nell'identificazione della ricorrenza specifica del tipo di registro utenti. Ad esempio, spesso un indirizzo IP o un nome host è sufficiente per molti tipi di registri utenti. In questo esempio, l'amministratore identifica l'istanza specifica del registro utenti utilizzando `Sistema_A_WAS` come nome definizione di registro. In aggiunta al nome, l'amministratore ha fornito anche il tipo di registro `WebSphere LTPA`.

Figura 6: Definizioni di registro EIM per tre registri utenti in una società



E' inoltre possibile definire i registri utenti che sono presenti all'interno di altri registri utenti. Ad esempio, il registro z/OS Security Server (RACF) può contenere specifici registri utenti che costituiscono una sottoserie di utenti all'interno di un registro utenti RACF globale. Per un esempio più dettagliato su come funziona quanto riportato sopra, consultare Definizioni di registro di sistema e dell'applicazione.

Alias e definizioni di registro EIM

E' possibile creare anche alias per definizioni di registro EIM. E' possibile utilizzare tipi di alias predefiniti oppure definire i propri tipi di alias da utilizzare. I tipi di alias predefiniti includono:

- Nome host DNS (Domain Name System)
- Dominio Kerberos
- DN mittente
- DN root
- Indirizzo TCP/IP
- Nome host DNS LDAP

Questo supporto alias consente ai programmatori di scrivere le applicazioni senza dover conoscere in anticipo il nome registro EIM arbitrario scelto dall'amministratore che ha sviluppato l'applicazione. La documentazione dell'applicazione può fornire l'amministratore EIM con il nome alias utilizzato dall'applicazione. Utilizzando queste informazioni, l'amministratore EIM può assegnare questo nome alias alla definizione di registro EIM che rappresenta il registro utenti reale che l'amministratore desidera venga utilizzato dall'applicazione.

Quando l'amministratore aggiunge l'alias alla definizione di registro EIM, l'applicazione può eseguire una ricerca alias per trovare il nome registro EIM durante l'inizializzazione. La ricerca alias consente all'applicazione di determinare il nome o i nomi registro EIM da utilizzare come immissione nelle API che eseguono le operazioni di ricerca EIM.

Definizioni di sistema e del registro applicazioni

Alcune applicazioni utilizzano una sottoserie di identità utente all'interno di una singola istanza di un registro utenti. EIM consente agli amministratori di modellare questo scenario fornendo due tipi di definizioni di registro EIM: sistema e applicazione.

Una **definizione di registro di sistema** rappresenta un registro distinto all'interno di una stazione di lavoro o di un server. Una definizione di registro di sistema può essere creata quando il registro nella società dispone di uno dei seguenti tratti:

- Il registro viene fornito da un sistema operativo, ad esempio AIX(R), OS/400(R) o da un prodotto di gestione della sicurezza come z/OS Security Server Resource Access Control Facility (RACF(R)).
- Il registro contiene identità utente univoche in una specifica applicazione, ad esempio Lotus Notes(R).
- Il registro contiene identità utente distribuite, ad esempio i principal Kerberos o i DN LDAP (Lightweight Directory Access Protocol).

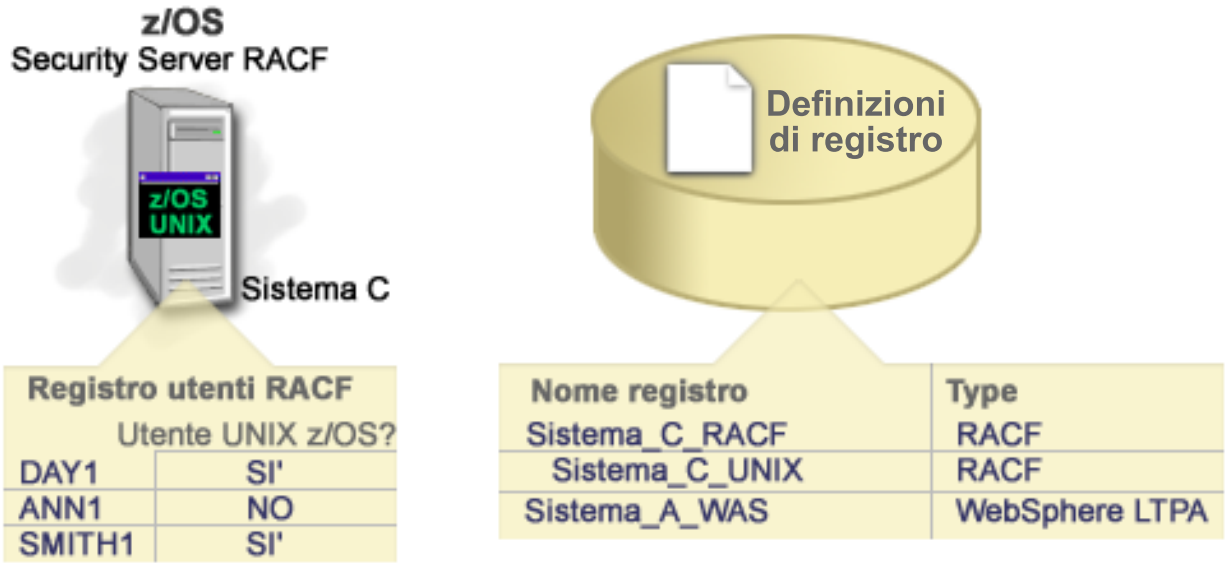
Una **definizione di registro dell'applicazione** rappresenta una sottoserie delle identità utente definite in un registro di sistema. Queste identità utente condividono una serie comune di attributi o caratteristiche che consentono loro di utilizzare una particolare applicazione o serie di applicazioni. E' possibile creare una definizione di registro quando le identità utente hanno i seguenti tratti:

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

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.

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 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 UNIX z/OS sul Sistema C. Queste identità utente sono realmente identità RACF con attributi univoci che li identificano come utenti UNIX z/OS. All'interno delle definizioni di registro EIM, l'amministratore EIM ha definito `Sistema_C_RACF` per rappresentare il registro utenti RACF generale. L'amministratore ha inoltre definito `Sistema_C_UNIX` per rappresentare le identità utente che hanno attributi UNIX z/OS.

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



Associazioni EIM

Un'*associazione EIM* è una relazione tra un identificativo EIM che rappresenta una specifica persona ed una singola identità utente in un registro utenti che rappresenta anche tale persona. Quando si creano associazioni tra un identificativo EIM e tutte le identità utente della persona o dell'entità, l'utente fornisce una delucidazione singola e completa di come tale persona o entità utilizza le risorse in una società. EIM fornisce API che consentono alle applicazioni di trovare un'identità utente sconosciuta in uno specifico registro utenti (destinazione) fornendo un'identità utente nota in altri registri utenti (origine). Questo processo viene detto *corrispondenza identità*.

Prima di poter creare un'associazione, è necessario innanzitutto creare l'identificativo EIM e la definizione di registro EIM appropriati 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

Un amministratore può creare diversi tipi di associazioni tra un identificativo EIM e un'identità utente in base a come viene utilizzata l'identità utente. Le identità utente possono essere utilizzate per l'autenticazione, l'autorizzazione o per entrambe.

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 utente 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 identità utente presenti in un registro utenti per l'autenticazione mentre possono utilizzarne di diverse presenti in un altro registro per l'autorizzazione.

In EIM, esistono tre tipi di associazioni, che possono essere definite da un amministratore, tra un identificativo EIM e un'identità. Questi tipi sono associazioni origine, di destinazione e amministrativa.

Associazione origine

Quando un'identità utente viene utilizzata per l'*autenticazione*, tale identità deve disporre di un'associazione origine ad un identificativo EIM. Un'associazione origine consente di utilizzare l'identità utente come origine in un'operazione di ricerca EIM per trovare un'identità utente diversa che sia associata allo stesso identificativo EIM. Se in un'operazione di ricerca EIM, come identità di destinazione viene utilizzata un'identità utente con una sola associazione origine, non verrà restituita alcuna identità associata.

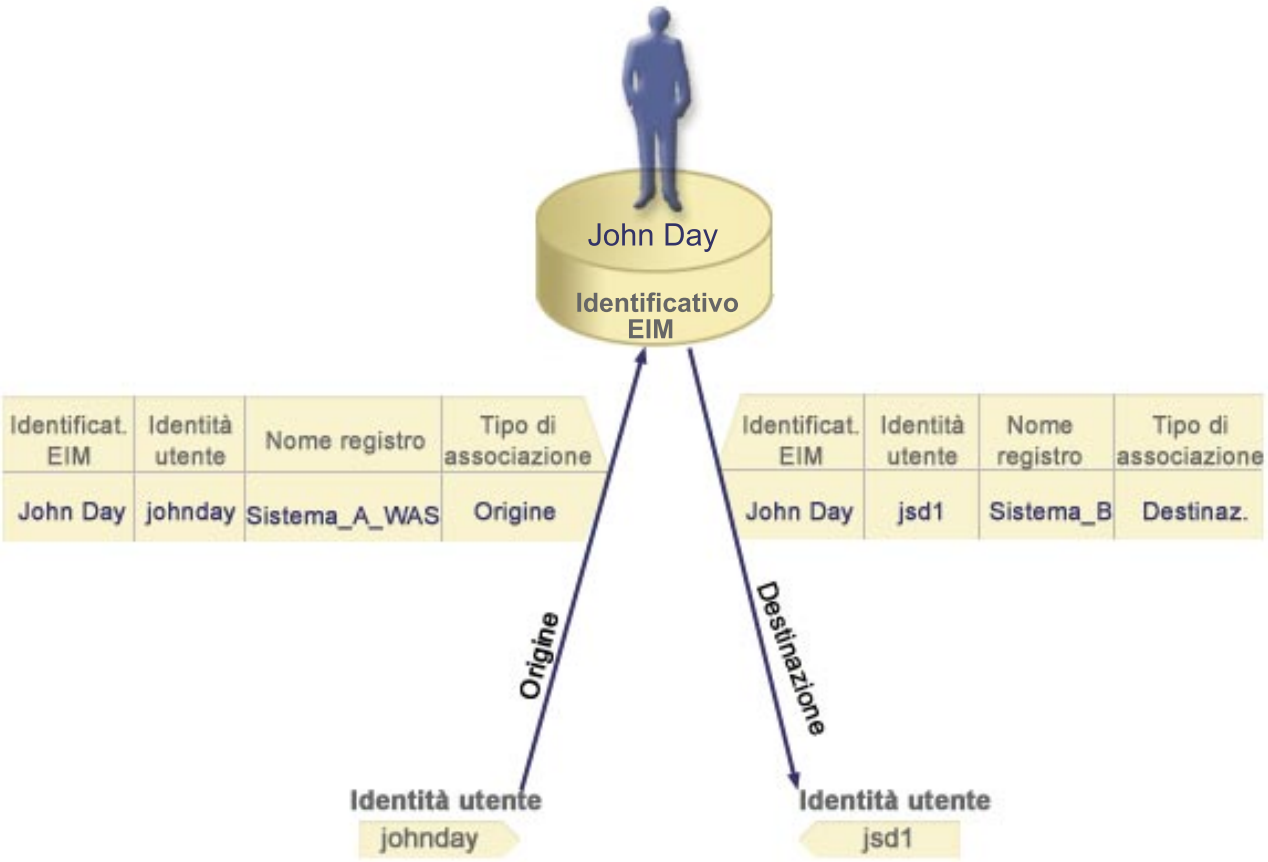
Associazione di destinazione

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. Un'associazione di destinazione consente all'identità utente di essere restituita come risultato di un'operazione di ricerca EIM. Se in un'operazione di ricerca EIM, come identità origine viene utilizzata un'identità utente con una sola associazione di destinazione, non verrà restituita alcuna identità associata.

Per una singola identità utente potrebbe essere necessario creare sia un'associazione di destinazione che origine. Ciò si rivela necessario per un utente utilizza un singolo sistema sia come client che come server oppure per utenti che hanno funzione di amministratori. Ad esempio, normalmente un utente esegue l'autenticazione su una piattaforma Windows ed esegue applicazioni che accedono ad un server AIX. A causa delle responsabilità di lavoro dell'utente, quest'ultimo deve, occasionalmente, collegarsi direttamente ad un server AIX. In questa situazione potrebbero essere create sia associazioni origine che di destinazione tra l'identità utente AIX e l'identificativo EIM della persona. Le identità utente che rappresentano gli utenti finali normalmente necessitano solo di un'associazione di destinazione.

La Figura 6 illustra un esempio di un'associazione origine e di un'associazione di destinazione. In questo esempio, l'amministratore ha creato due associazioni per l'identificativo EIM `John Day` per definire la relazione tra questo identificativo e le due identità utente associate. L'amministratore ha creato un'associazione origine per `johnday`, l'identità utente WebSphere LTPA (Lightweight Third-Party Authentication) nel registro utenti `Sistema_A_WAS`. L'amministratore ha creato anche un'associazione di destinazione per `jsd1`, il profilo utente OS/400 nel registro utenti Sistema B. Queste associazioni forniscono un mezzo tramite il quale le applicazioni ottengono un'identità utente sconosciuta (la destinazione, `jsd1`) in base ad un'identità utente nota (l'origine, `johnday`) come parte di un'operazione di ricerca EIM.

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



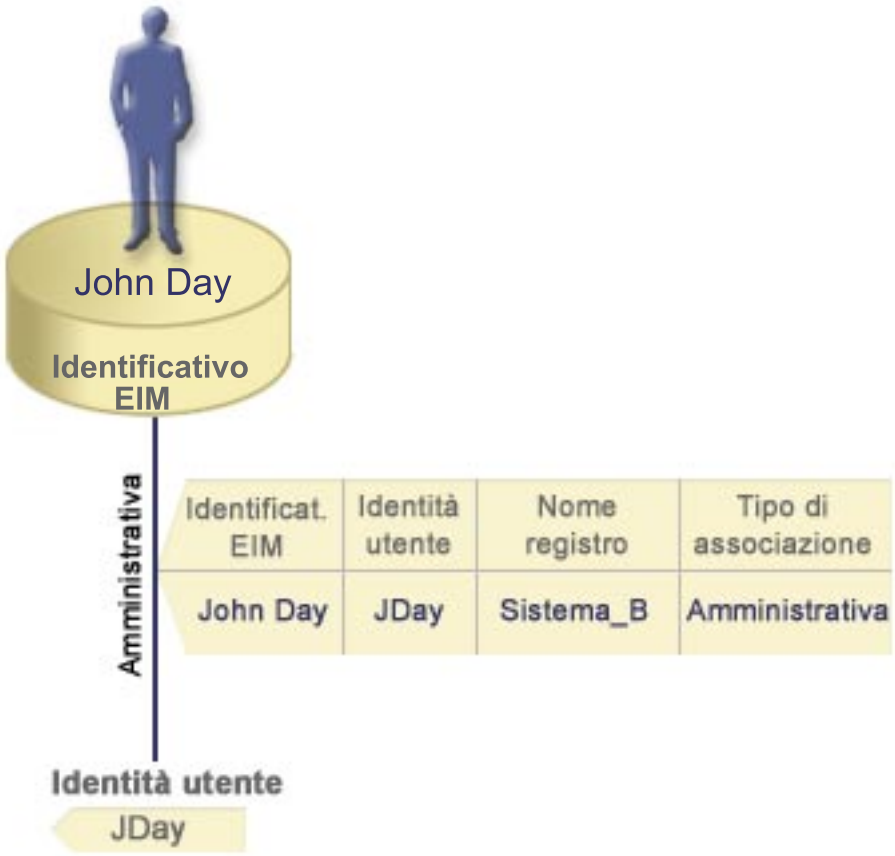
Associazione amministrativa

Un'associazione amministrativa di un identificativo EIM viene normalmente utilizzata per mostrare che la persona o l'entità rappresentata dall'identificativo EIM possiede un'identità utente che necessita di speciali considerazioni per un sistema specificato. Questo tipo di associazione può essere utilizzato, ad esempio, con registri utenti molto delicati.

A causa della natura di ciò che rappresenta un'associazione amministrativa, un'operazione di ricerca EIM che fornisce un'identità utente origine con un'associazione amministrativa non restituisce risultati. Allo stesso modo, 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, `John Day` dispone di un'identità utente sul Sistema A e di un'altra identità sul Sistema B, che costituisce un sistema altamente sicuro. L'amministratore di sistema desidera assicurarsi che gli utenti vengano autenticati nel Sistema B utilizzando solo il registro utenti locale di questo sistema. L'amministratore non desidera consentire che un'applicazione autentichi `John Day` nel sistema utilizzando meccanismi di autenticazione esterni. Utilizzando un'associazione amministrativa per l'identità utente `JDay` sul Sistema B, l'amministratore EIM può vedere che John Day dispone di 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, esse non possono trovare le identità utente che dispongono di associazioni amministrative.

Figura 7: Associazione amministrativa EIM per l'identificativo EIM `John Day`



Operazioni di ricerca EIM

Un'*operazione di ricerca EIM* è un processo tramite il quale un'applicazione o il sistema operativo trova un'identità utente associata sconosciuta in uno specifico registro di destinazione fornendo alcune informazioni note e sicure. Le applicazioni che utilizzano le API relative ad EIM possono eseguire queste operazioni di ricerca EIM sulle informazioni solo se tali informazioni sono memorizzate nel dominio EIM. Un'applicazione può eseguire uno dei due tipi di operazioni di ricerca EIM in base al tipo di informazioni fornite dall'applicazione come origine dell'operazione di ricerca EIM: un'identità utente o un identificativo EIM.

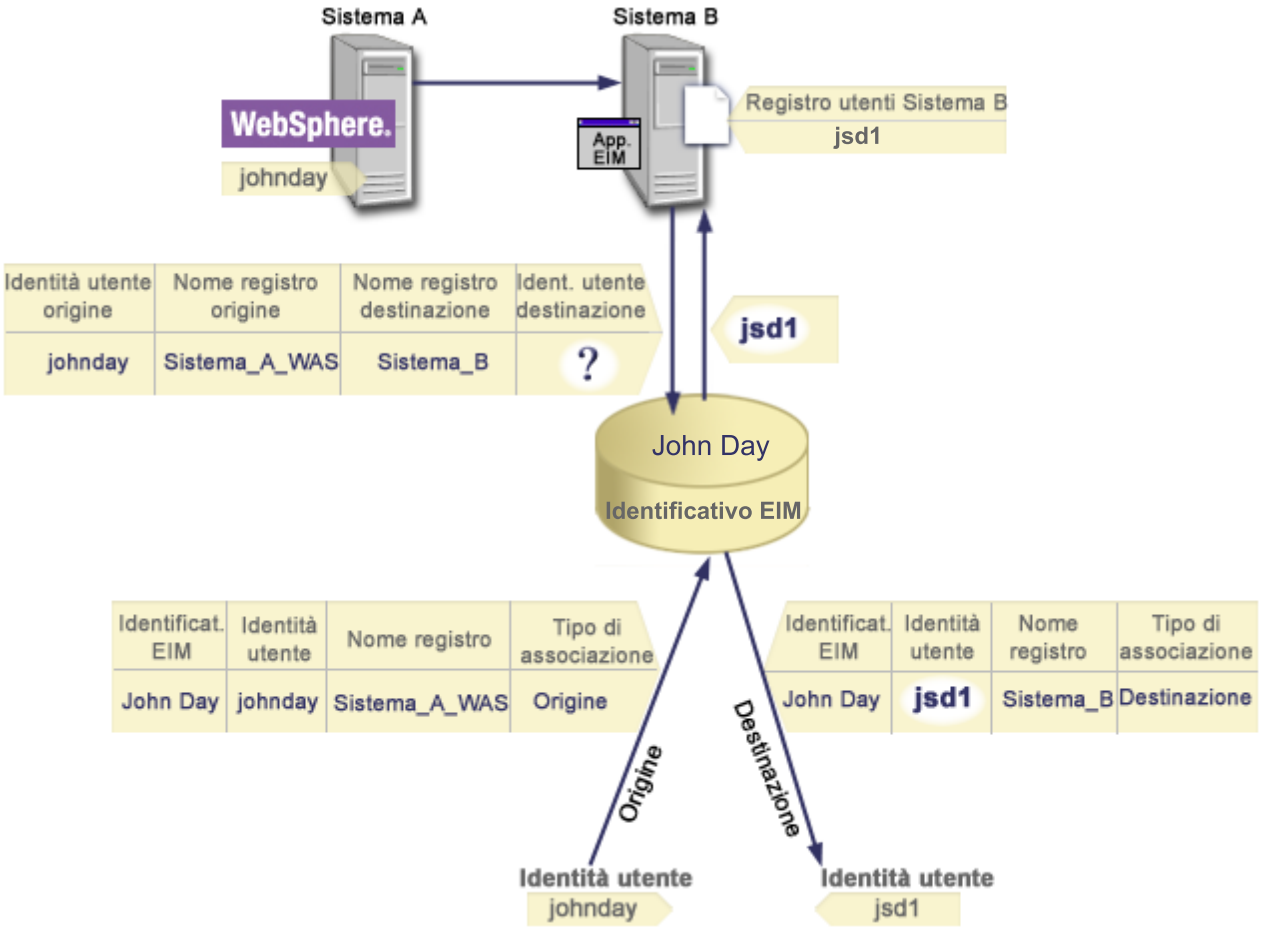
Quando un'applicazione fornisce un'*identità utente come origine*, l'applicazione deve fornire anche il nome definizione del registro EIM per l'identità utente di origine e il nome definizione del registro EIM costituisce la destinazione dell'operazione di ricerca EIM. Per essere utilizzata come origine in un'operazione di ricerca EIM, un'identità utente deve disporre di un'associazione origine definita per essa.

Quando un'applicazione fornisce un *identificativo EIM come origine* dell'operazione di ricerca EIM, l'applicazione deve fornire anche il nome definizione registro EIM che costituisce la destinazione dell'operazione di ricerca EIM. Affinché un'identità utente venga restituita come destinazione di entrambi i tipi di operazione di ricerca EIM, l'identità utente deve disporre di un'associazione definita per essa.

Le informazioni fornite vengono inoltrate all'unità di controllo del dominio EIM in cui sono memorizzate tutte le informazioni EIM e l'operazione di ricerca EIM ricercherà l'associazione origine che corrisponde alle informazioni fornite. In base all'identificativo EIM (fornito nell'API o determinato dalle informazioni dell'associazione origine), l'operazione di ricerca EIM ricercherà poi un'associazione di destinazione per tale identificativo che corrisponda al nome definizione del registro EIM.

Nella Figura 10, l'identità utente `johnday` si autentica in Websphere Application Server utilizzando LPTA (Lightweight Third-Party Authentication) sul Sistema A. Websphere Application Server sul Sistema A richiama il programma nativo sul Sistema B per accedere ai dati sul Sistema B. Il programma nativo utilizza un'API relativa ad 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, `Sistema_A_WAS` come nome definizione del registro EIM di origine e `Sistema_B` come nome definizione del registro EIM di destinazione. Queste informazioni di origine vengono inoltrate all'unità di controllo del dominio EIM e l'operazione di ricerca EIM trova un'associazione origine che corrisponde alle informazioni. Utilizzando il nome identificativo EIM, l'operazione di ricerca EIM cerca un'associazione di destinazione per l'identificativo `John Day` che corrisponde al nome definizione del registro EIM di destinazione per `Sistema_B`. Quando viene rilevata l'associazione di destinazione corrispondente, l'operazione di ricerca EIM restituirà l'identità utente `jsd1` all'applicazione.

Figura 10: Operazione di ricerca EIM basata sull'identità utente nota `johnday`



Autorizzazioni EIM

Le *autorizzazioni EIM* consentono ad un utente di eseguire specifiche attività amministrative o operazioni di ricerca EIM. Solo gli utenti con autorizzazione di amministratore EIM possono concedere o revocare le autorizzazioni degli altri utenti. Le autorizzazioni EIM vengono concesse solo alle identità utente note all'unità di controllo del dominio EIM.

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

- **Amministratore LDAP (Lightweight Directory Access Protocol).** Questa autorizzazione consente all'utente di configurare un nuovo dominio EIM. Un utente con questa autorizzazione può eseguire le funzioni riportate di seguito:
  - Creazione di un dominio
  - Cancellazione di un dominio
  - Creazione ed eliminazione degli identificativi EIM
  - Creazione ed eliminazione di una definizione di registro EIM
  - Creazione ed eliminazione delle associazioni origine, di destinazione e amministrative
  - Esecuzione delle operazioni di ricerca EIM
  - Richiamo di associazioni, identificativi EIM e definizioni di registro EIM
  - Aggiunta, eliminazione ed elenco delle informazioni di autorizzazione EIM
- **Amministratore EIM.** Questa autorizzazione consente all'utente di gestire tutti i dati EIM all'interno di questo dominio EIM. Un utente con questa autorizzazione può eseguire le funzioni riportate di seguito:
  - Cancellazione di un dominio
  - Creazione ed eliminazione degli identificativi EIM
  - Creazione ed eliminazione di una definizione di registro EIM
  - Creazione ed eliminazione delle associazioni origine, di destinazione e amministrative
  - Esecuzione delle operazioni di ricerca EIM
  - Richiamo di associazioni, identificativi EIM e definizioni di registro EIM
  - Aggiunta, eliminazione ed elenco delle informazioni di autorizzazione EIM
- **Amministratore identificativi EIM.** Questa autorizzazione consente all'utente di aggiungere e modificare gli identificativi EIM e di gestire le associazioni origine e amministrative. Un utente con questa autorizzazione può eseguire le funzioni riportate di seguito:
  - Creazione di un identificativo EIM
  - Aggiunta ed eliminazione di associazioni origine
  - Aggiunta ed eliminazione di associazioni amministrative
  - Esecuzione delle operazioni di ricerca EIM
  - Richiamo di associazioni, identificativi EIM e definizioni di registro EIM
- **Ricerca delle corrispond. EIM.** Questa autorizzazione consente all'utente di eseguire operazioni di ricerca EIM. Un utente con questa autorizzazione può eseguire le funzioni riportate di seguito:
  - Esecuzione delle operazioni di ricerca EIM
  - Richiamo di associazioni, identificativi EIM e definizioni di registro EIM
- **Amministratore registri EIM.** Questa autorizzazione consente all'utente di gestire tutte le definizioni di registro EIM. Un utente con questa autorizzazione può eseguire le funzioni riportate di seguito:
  - Aggiunta ed eliminazione delle associazioni di destinazione
  - Esecuzione delle operazioni di ricerca EIM
  - Richiamo di associazioni, identificativi EIM e definizioni di registro EIM
- **Amministratore registro X EIM.** Questa autorizzazione consente all'utente di gestire una specifica definizione di registro EIM. Questa autorizzazione consente ad un utente di eseguire le funzioni riportate di seguito:
  - Aggiunta ed eliminazione delle associazioni di destinazione per la definizione di registro EIM
  - Esecuzione delle operazioni di ricerca EIM
  - Richiamo di associazioni, identificativi EIM e definizioni di registro EIM

Ognuna delle tabelle riportate di seguito è organizzata in base all'attività EIM che viene eseguita dall'API. Ogni tabella visualizza ogni API relative ad EIM, le diverse autorizzazioni EIM e l'accesso di ogni autorizzazione a specifiche funzioni EIM.

Tabella 1: Gestione domini

API EIM	Amministratore LDAP	Amministratore EIM	Amministratore identificativi EIM	Ricerca di corrispond. EIM	Amministratore registri EIM	Amministratore registro X EIM
eimChangeDomain	X	X	-	-	-	-
eimCreateDomain	X	-	-	-	-	-
eimDeleteDomain	X	X	-	-	-	-
eimListDomains	X	X	-	-	-	-

Tabella 2: Gestione identificativi

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

Tabella 3: Gestione registri

API EIM	Amministratore LDAP	Amministratore EIM	Amministratore identificativi EIM	Ricerca di corrispond. EIM	Amministratore registri EIM	Amministratore registro X EIM
eimAddApplicationRegistry	X	X	-	-	-	-
eimAddSystemRegistry	X	X	-	-	-	-
eimChangeRegistry	X	X	-	-	X	X
eimChangeRegistryUser	X	X	-	-	X	X
eimChgRegistryAlias	X	X	-	-	X	X
eimGetRegistryFromAlias	X	X	X	X	X	X
eimListRegistries	X	X	X	X	X	X
eimListRegistryAliases	X	X	X	X	X	X
eimListRegistryUsers	X	X	X	X	X	X
eimRemoveRegistry	X	X	-	-	-	-

Tabella 4: Gestione associazioni

Per le API eimAddAssociation() e eimRemoveAssociation() esistono 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	Amministratore LDAP	Amministratore EIM	Amministratore identificativi EIM	Ricerca di corrispond. EIM	Amministratore registri EIM	Amministratore 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 corrispondenze

API EIM	Amministratore LDAP	Amministratore EIM	Amministratore identificativi EIM	Ricerca di corrispond. EIM	Amministratore registri EIM	Amministratore 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 6: Gestione accesso

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

Concetti LDAP relativi a EIM

EIM (Enterprise Identity Mapping) utilizza un server LDAP (Lightweight Directory Access Protocol) come un'unità di controllo del dominio EIM per memorizzare i dati EIM. E' possibile utilizzare i DN LDAP nella configurazione di EIM per il proprio server iSeries e come mezzo di autenticazione nell'unità di controllo del dominio EIM.

Per utilizzare i DN LDAP durante la configurazione e la gestione di EIM, è necessario comprendere i seguenti concetti relativi a LDAP:

- DN LDAP
- DN principale LDAP

DN LDAP

Un DN LDAP è una voce LDAP (Lightweight Directory Access Protocol) che identifica e descrive un utente autorizzato di un server LDAP. E' possibile utilizzare il wizard Configurazione EIM per configurare il server

LDAP affinché memorizzi le informazioni sul dominio EIM. E' possibile utilizzare i DN LDAP come mezzi per accedere e richiamare questi dati EIM in modo tale che il proprio server iSeries possa far parte di un ambiente a collegamento singolo.

I DN sono composti dal nome della voce stessa come pure dai nomi, nell'ordine dal basso verso l'alto, degli oggetti che la precedono nell'indirizzario LDAP. Un esempio di un DN LDAP completo potrebbe essere `cn=Tim Jones, o=IBM, c=US`. Ogni voce contiene almeno un attributo che viene utilizzato per rappresentare la voce. Questo attributo di denominazione viene chiamato DN relativo della voce (RDN). La voce che si trova prima di un determinato RDN viene detta DN principale LDAP. In questo esempio, `cn=Tim Jones` denomina la voce, costituisce quindi l'RDN. `o=IBM, c=US` è il DN principale di `cn=Tim Jones`. Consultare DN principale LDAP per ulteriori informazioni su come EIM utilizza tali DN.

Poiché EIM utilizza il server LDAP per memorizzare i dati EIM, è possibile utilizzare i DN LDAP come mezzo di autenticazione nell'unità di controllo del dominio EIM. E' possibile utilizzare i DN LDAP anche quando si configura EIM per il proprio server iSeries. Ad esempio, è possibile utilizzare i DN LDAP quando:

- Si configura il server LDAP per operare come unità di controllo del dominio EIM. Ciò viene effettuato creando ed utilizzando il DN LDAP che identifica l'amministratore LDAP del server LDAP. Se il server LDAP non è stato precedentemente configurato, è possibile configurarlo quando si utilizza il wizard Configurazione EIM per creare e collegare un nuovo dominio.
- Si utilizza il wizard Configurazione 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 LDAP deve rappresentare un utente autorizzato a creare oggetti nello spazio del nome locale del server LDAP.
- Si utilizza il wizard Configurazione 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 OS/400 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.

Per ulteriori informazioni sui DN e su come LDAP li utilizza, consultare Basi di LDAP.

DN principale LDAP

Un DN principale LDAP è una voce nello spazio del nome del server indirizzari Lightweight Directory Access Protocol (LDAP). 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 un DN principale quando si trova ad un livello superiore dello spazio del nome del server LDAP.

Un esempio di un DN LDAP completo potrebbe essere `cn=Tim Jones, o=IBM, c=US`. Ogni voce contiene almeno un attributo che viene utilizzato per denominare la voce. Questo attributo di denominazione viene chiamato DN relativo della voce (RDN). La voce che si trova prima di un determinato RDN viene detta DN principale. In questo esempio, `cn=Tim Jones` denomina la voce, costituisce quindi l'RDN. `o=IBM, c=US` è il DN principale di `cn=Tim Jones`.

Poiché EIM utilizza il server LDAP per memorizzare i dati EIM, è possibile utilizzare i DN LDAP come mezzo di autenticazione nell'unità di controllo del dominio EIM. I DN LDAP e i DN principali possono essere utilizzati anche quando si configura EIM per il proprio server iSeries. Ad esempio, quando si utilizza il wizard Configurazione EIM per creare e collegare un nuovo dominio, è possibile specificare un DN principale per il dominio che si sta creando. Utilizzando un DN principale, è possibile specificare dove devono risiedere i dati EIM del dominio nello spazio del nome LDAP locale. Quando non si specifica un DN principale, i dati EIM si trovano nel proprio suffisso nello spazio del nome.

Per ulteriori informazioni sui DN e su come vengono utilizzati, consultare Basi di LDAP.

Abilitazione di un collegamento singolo tramite EIM

EIM fornisce un meccanismo economico per l'abilitazione del collegamento singolo nell'ambito di una società. L'implementazione OS/400 di EIM e Kerberos fornisce un ambiente a collegamento singolo multilivello ed eterogeneo. Di seguito vengono riportati i benefici per gli utenti, gli amministratori e gli sviluppatori di applicazioni quando, in una società, è disponibile un ambiente a collegamento singolo:

Benefici per gli utenti
In un ambiente a collegamento singolo, l'autenticazione si verifica ogniqualvolta gli utenti tentano di accedere ad un nuovo sistema; tuttavia, a tali utenti non verranno richieste le parole d'ordine. EIM riduce la necessità di tenere traccia e di gestire più nomi utente e parole d'ordine per accedere ad altri sistemi nella rete. Una volta che l'utente è stato autenticato sulla rete, può accedere ai servizi e alle applicazioni presenti nella società senza la necessità di disporre di differenti parole d'ordine per questi diversi sistemi.

Benefici per gli amministratori
Per un amministratore, un collegamento singolo semplifica la gestione della sicurezza globale della società. Senza il collegamento singolo, gli utenti e le applicazioni potrebbero memorizzare nella cache le parole d'ordine su diversi sistemi, ciò potrebbe compromettere la sicurezza dell'intera rete. Gli amministratori impiegano tempo e denaro per soluzioni che riducono questi rischi di sicurezza. Il collegamento singolo riduce i costi amministrativi nella gestione dell'autenticazione mentre viene mantenuta sicura l'intera rete. Inoltre, tale collegamento riduce i costi amministrativi relativi alla reimpostazione delle parole d'ordine dimenticate.

Benefici per gli sviluppatori di applicazioni
Per gli sviluppatori di applicazioni che devono essere eseguite su rete eterogenee, EIM fornisce l'infrastruttura per sviluppare le applicazioni che operano tra le piattaforme. Utilizzando le API di EIM, i programmatori possono scrivere applicazioni che utilizzano il registro utenti esistente più appropriato per l'autenticazione mentre ne utilizzano un altro per l'autorizzazione. Gli sviluppatori di applicazioni non devono supportare registri utenti specifici della piattaforma all'interno delle applicazioni che essi creano, perché è EIM che fornisce l'infrastruttura per creare le applicazioni che mettono in corrispondenza le identità presenti in tali registri con un singolo identificativo EIM. Inoltre, EIM consente ai programmatori di conservare queste applicazioni senza modificare la semantica di sicurezza associata, e la sicurezza a livello dell'applicazione riduce in modo significativo il costo dell'implementazione delle applicazioni tra piattaforme multilivello.

Abilitazione iSeries di un collegamento singolo
Per abilitare un ambiente a collegamento singolo, l'IBM utilizza due tecnologie che interagiscono tra loro: EIM e servizio di autenticazione di rete, che costituisce l'implementazione IBM di Kerberos e delle API GSS. Configurando queste due tecnologie, un amministratore può abilitare un ambiente a collegamento singolo. Windows 2000, XP, AIX e zSeries utilizzano il protocollo Kerberos per autenticare gli utenti su una rete. Kerberos comporta l'uso di un centro di distribuzione chiavi, sicuro e basato sulla rete che autentica i principal (utenti Kerberos) sulla rete. Un utente riceve un ticket Kerberos da un centro di distribuzione chiavi centralizzato. Questo ticket autentica l'utente in un altro servizio nella società. Un ticket può essere inoltrato da un utente ad un servizio che accetta i ticket. Il servizio che accetta un ticket lo utilizza per determinare chi dichiara di essere l'utente (all'interno del dominio e del registro utenti Kerberos) e che gli utenti siano realmente coloro che dichiarano di essere.

Mentre un servizio di autenticazione di rete consente ad un server iSeries di far parte di un dominio Kerberos, EIM fornisce un meccanismo per associare questi principal Kerberos ad un singolo identificativo EIM che rappresenta tale utente all'interno dell'intera società. Anche altre identità utente, come ad esempio un nome utente OS/400, possono essere associate a questo identificativo EIM. In base a queste associazioni, EIM fornisce un meccanismo per OS/400 e per le applicazioni per determinare quale profilo utente OS/400 rappresenta la persona o l'entità identificata dal principal Kerberos. E' possibile pensare alle informazioni contenute in EIM come ad un albero con un identificativo EIM come radice e alla lista delle identità utente associate all'identificativo EIM come rami.

Utilizzando la figura riportata di seguito come esempio, immaginare che un utente, ad esempio John Smith, si colleghi alla rete tramite il suo PC Windows ed acceda ad un'istanza di OS/400 per accedere alle applicazioni abilitate da Kerberos. A John non viene richiesto il suo nome utente OS/400. Queste applicazioni possono consultare l'applicazione presente nell'identificativo EIM di John per trovare il nome utente OS/400. John Smith non necessita più di una parola d'ordine nel suo profilo utente OS/400 in quanto quest'ultimo non viene utilizzato per l'autenticazione, ma utilizzato solo per l'autorizzazione.

Figura 1. Ambiente a collegamento singolo

L'argomento, Scenario: Abilitazione di un collegamento singolo, fornisce un esempio su come un amministratore configura il servizio di autenticazione di rete ed EIM per abilitare un ambiente a collegamento singolo.

Tramite un collegamento singolo è possibile accedere alle seguenti applicazioni:

- iSeries Navigator
- Emulazione PC5250
- Distributed Relational Database Architecture (TM)(DRDA)(R)
- NetServer
- QFileSvr.400

Pianificazione per EIM

Sul server iSeries, EIM comprende molte tecnologie e servizi. Prima di configurare EIM sul proprio server, è necessario decidere la funzionalità che si desidera implementare utilizzando EIM e le capacità di collegamento singolo.

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 collegamento singolo.

Il foglio di lavoro di pianificazione di seguito riportato identifica i servizi da installare prima di configurare EIM.

Foglio di lavoro di pianificazione	**Risposte**
La versione del proprio OS/400 è V5R2 (5722-SS1) o successiva?	
Cryptographic Access Provider (5722-AC3) è installato sui propri server iSeries?	
iSeries Access per Windows (5722-XE1) è installato sui PC appropriati sulla rete (i PC utilizzati per gestire i server iSeries) e sui propri server iSeries?	
Il componente secondario Rete di iSeries Navigator è installato su tutti i PC della rete e sui propri sistemi iSeries?	
Se un server LDAP è attualmente configurato e si desidera utilizzarlo come unità di controllo del dominio EIM, si conoscono il DN amministratore LDAP e la parola d'ordine?	
Se un server LDAP 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?	

Se si pianifica l'utilizzo di Kerberos per autenticare gli utenti, è necessario configurare anche il servizio di autenticazione di rete. Consultare Pianificazione del servizio di autenticazione di rete per un foglio di lavoro completo della pianificazione di tale servizio.

Se si sta configurando il servizio di autenticazione di rete ed EIM per abilitare il collegamento singolo, vedere lo Scenario: Abilitazione collegamento singolo che illustra la modalità con cui una società ha configurato entrambi i prodotti.

Installazione delle opzioni iSeries Navigator richieste

Per abilitare un ambiente a collegamento singolo con EIM e il servizio di autenticazione di rete, è necessario installare sia l'opzione Rete che l'opzione Sicurezza di iSeries Navigator. EIM si trova all'interno dell'opzione Rete e il servizio di autenticazione di rete di trova nell'opzione Sicurezza. Se non si intende utilizzare il servizio di autenticazione di rete nella propria rete, non è necessario installare l'opzione Sicurezza di iSeries Navigator.

Per installare l'opzione Rete di iSeries Navigator oppure per verificare che questa opzione sia attualmente installata, assicurarsi che iSeries Access per Windows sia installato sul PC e che lo si stia utilizzando per gestire il server iSeries.

Per installare l'opzione Rete:

1. Fare clic su **Start —> Programmi —> IBM iSeries Access per Windows —> Installazione selettiva**.

2. Seguire le istruzioni riportate sulla finestra di dialogo. Sulla finestra di dialogo **Selezione componente**, espandere **iSeries 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 la parte rimanente dell'installazione selettiva.

Configurazione del servizio di autenticazione di rete

Servizio di autenticazione di rete consente di utilizzare l'autenticazione Kerberos sul proprio server iSeries. Questo servizio non è un prerequisito per l'utilizzo di EIM sul proprio server; tuttavia, utilizzare l'autenticazione Kerberos per la sicurezza nella propria società, fornisce molti benefici.

Il servizio di autenticazione di rete, quando utilizzato insieme a EIM, fornisce un mezzo per abilitare un ambiente a collegamento singolo. Un ambiente a collegamento singolo si rivela utile per gli utenti e gli amministratori. Gli utenti dispongono di meno nomi utente e parole d'ordine da gestire e gli amministratori devono tenere traccia di meno informazioni per ogni utente. Poiché l'abilitazione di un collegamento singolo è di aiuto nel colmare il divario tra le diverse piattaforme e i diversi sistemi all'interno della società, lo sviluppo dell'applicazione e i costi generali di gestione possono essere ridotti.

Se attualmente non si dispone di un servizio di autenticazione di rete configurato sul server iSeries o su tutti i server della rete, consultare Pianificazione del servizio di autenticazione di rete per la pianificazione delle informazioni per poter iniziare. Se si conosce il servizio di autenticazione di rete, consultare Configurazione del servizio di autenticazione di rete per iniziare con il processo di configurazione.

Configurazione di EIM

Per abilitare un ambiente a collegamento singolo su più piattaforme senza dover modificare le normative di riservatezza sottostanti, è necessario configurare EIM come pure il servizio di autenticazione di rete. 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.

Per iniziare il processo di configurazione di EIM affinché il server iSeries faccia parte di un ambiente a collegamento singolo, utilizzare il wizard Configurazione EIM. A seconda delle necessità di configurazione, il wizard può essere utilizzato per collegare un dominio esistente oppure per crearne e collegarne uno nuovo.

Il wizard Configurazione EIM consente di completare facilmente una configurazione di base di EIM. Ad esempio, se non è stato ancora configurato un server LDAP oppure se il servizio di autenticazione di rete non è configurato, il wizard Configurazione EIM costituisce un aiuto nell'esecuzione di queste attività.

Una volta utilizzato il wizard per eseguire la configurazione di base di EIM, è necessario eseguire alcuni passi di configurazione aggiuntivi prima di poter utilizzare l'ambiente a collegamento singolo. Consultare Scenario: Abilitazione di un collegamento singolo per un esempio che illustra come una società fittizia ha configurato un ambiente a collegamento singolo utilizzando il servizio di autenticazione di rete e EIM.

Prima di utilizzare il wizard Configurazione EIM, devono essere stati completati tutti i passi di pianificazione per determinare esattamente come verranno utilizzati EIM e il servizio di autenticazione di rete per abilitare un ambiente a collegamento singolo. Una volta completata la pianificazione, è possibile utilizzare il wizard per configurare EIM per il proprio server iSeries in uno dei due seguenti modi: creare nuovi domini o collegarne di esistenti. Gli argomenti riportati di seguito forniscono istruzioni per la configurazione di EIM:

Creazione e collegamento di un nuovo dominio
Scegliere questa attività per creare un dominio EIM per la propria rete e per configurare il server iSeries entrare a farne parte. Il wizard crea il nuovo dominio e configura il server LDAP locale in modo che sia l'unità di controllo del nuovo dominio. Inoltre, se Kerberos non è attualmente

configurato sul server iSeries, il wizard richiede all'utente l'avvio del wizard Configurazione servizio di autenticazione di rete. Una volta completata questa attività, è possibile configurare altri server iSeries in modo che facciano parte del dominio. Per eseguire tale operazione, collegarsi ad essi ed utilizzare il wizard Configurazione EIM per configurare un server in modo da collegare un dominio EIM esistente.

Collegamento di un dominio esistente
Una volta utilizzato il wizard Configurazione EIM per configurare un'unità di controllo del dominio e un dominio EIM, scegliere questa attività per configurare altri server iSeries in modo che entrino a far parte del dominio. Questa attività deve essere completata per ogni server iSeries presente nella rete che utilizzerà EIM. Una volta completato il wizard, è necessario fornire le informazioni sul dominio che si sta collegando, incluse le informazioni di collegamento (ad esempio il numero porta e se utilizzare Transport Layer Security (TLS)/Secure Sockets Layer (SSL) all'unità di controllo del dominio EIM. Se Kerberos non è attualmente configurato sul server iSeries, il wizard richiede all'utente di avviare il wizard Configurazione servizio di autenticazione di rete.

Come accedere al wizard Configurazione EIM

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

1. Avviare iSeries Navigator.
2. Collegarsi al server iSeries per il quale si desidera configurare EIM.
   Se si sta configurando EIM per più di un server iSeries, iniziare con quello su cui si desidera configurare l'unità di controllo del dominio relativo a EIM.
3. Espandere **Rete —> EIM (Enterprise Identity Mapping)**.
4. Fare clic con il tastino destro del mouse su **Configurazione** e selezionare **Configura...** per avviare il wizard Configurazione EIM.
5. Selezionare il percorso **Collegamento di un dominio esistente** o **Creazione e collegamento di un nuovo dominio**.

Una volta terminato l'utilizzo del wizard Configurazione EIM per creare l'unità di controllo del dominio e per configurare i propri server iSeries in modo che facciano parte del dominio, è necessario completare le attività riportate di seguito per finalizzare la propria configurazione di EIM:

1. Aggiunta di registri EIM al dominio EIM per i server e le applicazioni non iSeries che si desidera facciano parte del dominio EIM.
2. Creazione di identificativi EIM nel dominio per ogni entità o utente univoco per i sistemi che fanno parte del dominio EIM.
3. Creazione di associazioni tra diverse identità utente della persona o entità e questi identificativi EIM.

Creazione e collegamento di un nuovo dominio

E' possibile utilizzare il wizard Configurazione EIM per configurare il server LDAP sul server iSeries in modo che sia l'unità di controllo del dominio EIM per il nuovo dominio. Se necessario, il wizard Configurazione EIM assicura che verranno fornite le informazioni di configurazione di base del server LDAP.

Inoltre, se Kerberos non è attualmente configurato sul server iSeries, il wizard richiede all'utente l'avvio del wizard Configurazione servizio di autenticazione di rete. Una volta completato questo wizard, è stato configurato un nuovo dominio EIM, il proprio server iSeries è configurato per collegare il nuovo dominio e i registri utenti specificato sono stati aggiunti al dominio.

Per utilizzare il wizard per completare questa attività, è necessario disporre dell'autorizzazione speciale Amministratore della sicurezza (*SECADM), Tutti gli oggetti (*ALLOBJ) e Configurazione di sistema (*IOSYSCFG).

Per avviare ed utilizzare il wizard Configurazione EIM per creare e collegare un nuovo dominio EIM, completare i passi riportati di seguito da iSeries Navigator:

Nota: Questo wizard configura anche il server LDAP locale come la nuova unità di controllo del dominio EIM.

1. Espandere **Rete** —> **EIM (Enterprise Identity Mapping)**.
2. Fare clic con il tastino destro del mouse su **Configurazione** e selezionare **Configura...** per avviare il wizard Configurazione EIM.
3. Sulla pagina di **Benvenuto** del wizard, selezionare **Creazione e collegamento di un nuovo dominio** e fare clic su **Avanti**.
4. Se il servizio di autenticazione di rete non è attualmente configurato sul server iSeries, verrà visualizzata la finestra di dialogo **Configurazione servizi autenticazione di rete**. Questa finestra di dialogo richiede di selezionare se configurare il servizio di autenticazione di rete. Se si seleziona **Sì**, viene avviato il wizard Configurazione servizi di autenticazione di rete. Una volta completata la configurazione del servizio di autenticazione di rete, il wizard Configurazione EIM proseguirà.
5. Se il server LDAP non è attualmente configurato, verrà visualizzata la finestra di dialogo **Configurazione server indirizzari**. Sulla finestra di dialogo, fornire le seguenti informazioni per configurare il server LDAP locale:
   - Nel campo **Porta**, accettare il numero porta predefinito **389** oppure immettere un numero porta diverso da utilizzare per comunicazioni EIM non sicure con il server indirizzari.
   - Nel campo **DN**, immettere il DN LDAP che identifica l'amministratore LDAP per il server LDAP. Il wizard Configurazione EIM crea questo DN amministratore LDAP e lo utilizza per configurare il server LDAP come unità di controllo del dominio che si sta creando.
   - Nel campo **Parola d'ordine**, immettere la parola d'ordine dell'amministratore LDAP.
   - Nel campo **Conferma parola d'ordine**, immettere di nuovo la parola d'ordine.
   - Fare clic su **Avanti**.
6. Sulla finestra di dialogo **Specifica unità di controllo del dominio**, fornire le seguenti informazioni:
   - 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 i caratteri speciali come = + < > , # ; \ e *.
   - Nel campo **Descrizione**, inserire il testo per descrivere il dominio.
   - Fare clic su **Avanti**.
7. Sulla finestra di dialogo **Specifica DN principale dominio**, selezionare se specificare un DN principale per il dominio che si sta creando. 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.
8. Sulla finestra di dialogo **Specifica utente per collegamento**, selezionare un **tipo di utente** per il collegamento. E' possibile selezionare uno dei seguenti tipi di utenti: DN e parola d'ordine, file keytab e principal Kerberos oppure principal Kerberos e parola d'ordine. I due tipi di utenti Kerberos sono disponibili solo se il servizio di autenticazione di rete è configurato per il sistema iSeries locale. Il tipo di utente selezionato determina le altre informazioni che devono essere fornite per completare la finestra di dialogo come segue:
   - Se si seleziona **DN e parola d'ordine**, fornire le seguenti informazioni:
     – Nel campo **DN**, immettere 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**, immettere la parola d'ordine dell'utente.

– Nel campo **Conferma parola d'ordine**, immettere di nuovo la parola d'ordine.

- Se si seleziona **File keytab e principal Kerberos**, fornire le seguenti informazioni:
  – Nel campo **File Keytab**, inserire il nome del file keytab presente sul server iSeries che identifica l'utente autorizzato a creare gli oggetti nel nome dello spazio locale del server LDAP. Oppure, è possibile fare clic su **Sfoglia** per selezionare il file keytab.
  – Nel campo **Principal**, inserire il nome del principal Kerberos da utilizzare per identificare l'utente.
  – Nel campo **Dominio**, inserire il nome del dominio Kerberos del 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**, immettere il nome del principal Kerberos che identifica l'utente autorizzato a creare gli oggetti nel nome dello spazio locale del server LDAP.
  – Nel campo **Dominio**, inserire il nome del dominio Kerberos del principal.
  – Nel campo **Parola d'ordine**, immettere la parola d'ordine dell'utente.
  – Nel campo **Conferma parola d'ordine**, immettere di nuovo la parola d'ordine. 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 viene rappresentato nel file keytab come jsmith@ordept.myco.com.
- Fare clic su **Verifica collegamento** per verificare le informazioni di configurazione del collegamento all'unità di controllo del dominio.
- Fare clic su **Avanti**.

9. Sulla finestra di dialogo **Informazioni registro**, selezionare il tipo di registri utenti che si desidera aggiungere al dominio EIM. Selezionare uno o entrambi i tipi di registro:
   - Selezionare **OS400** per aggiungere un registro utenti che rappresenta il registro locale nel dominio EIM. Nel campo fornito, immettere il nome del registro da creare nel dominio. Il nome registro EIM è una stringa arbitraria che rappresenta il tipo di registro e l'istanza specifica di tale registro.
   - Selezionare **Kerberos** per aggiungere un registro utenti Kerberos al dominio EIM. Nel campo fornito, immettere il nome del registro da creare nel dominio e selezionare **Le identità utente Kerberos sono sensibili al minuscolo e al maiuscolo**, se necessario.
   - Fare clic su **Avanti**.
10. Sulla finestra di dialogo **Specifica utente di sistema EIM**, selezionare il tipo di utente che si desidera venga utilizzato dal sistema quando si eseguono 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 OS/400 locale. E' possibile selezionare uno dei seguenti tipi di utenti: DN e parola d'ordine, file keytab e principal Kerberos oppure principal Kerberos e parola d'ordine. Il tipo di utente selezionato determina le altre informazioni che devono essere fornite per completare la finestra di dialogo come segue:

Nota: 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 al collegamento singolo e alla cancellazione dei profili utente potrebbero avere esito negativo.

11. Se si seleziona **DN e parola d'ordine**, fornire le seguenti informazioni:
    - Nel campo **DN**, immettere il DN LDAP che identifica l'utente di OS/400 da utilizzare quando si contatta l'unità di controllo del dominio EIM.
    - Nel campo **Parola d'ordine**, immettere la parola d'ordine dell'utente.
    - Nel campo **Conferma parola d'ordine**, immettere di nuovo la parola d'ordine.

12. Se si seleziona **Principal Kerberos e parola d'ordine**, fornire le seguenti informazioni:
    - Nel campo **Principal**, inserire il nome del principal Kerberos che identifica l'utente di OS/400 da utilizzare quando si contatta l'unità di controllo del dominio EIM.
    - Nel campo **Dominio**, inserire il nome del dominio Kerberos del principal.
    - Nel campo **Parola d'ordine**, immettere la parola d'ordine dell'utente.
    - Nel campo **Conferma parola d'ordine**, immettere di nuovo la parola d'ordine. 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 viene rappresentato nel file keytab come jsmith@ordept.myco.com.
13. Se si seleziona **File keytab e principal Kerberos**, fornire le seguenti informazioni:
    - Nel campo **File Keytab**, immettere il nome del file keytab sul server iSeries che identifica l'utente di OS/400 da utilizzare quando si contatta l'unità di controllo del dominio EIM. Oppure, è possibile fare clic su **Sfoglia** per selezionare il file keytab.
    - Nel campo **Principal**, inserire il nome del principal Kerberos da utilizzare per identificare l'utente.
    - Nel campo **Dominio**, inserire il nome del dominio Kerberos del 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 viene rappresentato nel file keytab come jsmith@ordept.myco.com.
14. Fare clic su **Verifica collegamento** per verificare il collegamento all'unità di controllo del dominio per il sistema appena creato.
15. Fare clic su **Avanti**.
16. Nel pannello **Riepilogo**, rivedere le informazioni di configurazioni fornite. Se tutte le informazioni sono corrette, fare clic su **Fine**.

Una volta terminato il wizard, è terminata anche la configurazione di base di EIM. Tuttavia, è necessario completare queste attività per finalizzare la configurazione di EIM per questo server:

1. Aggiunta del dominio che è stato creato nella cartella Gestione dominio EIM.
2. Aggiunta dei registri EIM al dominio EIM per gli altri server e applicazioni che si desidera facciano parte del dominio EIM.
3. Creazione di identificativi EIM nel dominio per ogni entità o utente univoco per i sistemi che fanno parte del dominio EIM.
4. Creazione di associazioni tra diverse identità utente della persona o entità e questi identificativi EIM.

Inoltre, l'utente potrebbe voler utilizzare Secure Sockets Layer (SSL) o Transport Layer Security (TLS) per configurare un collegamento sicuro all'unità di controllo del dominio.

Configurazione di un collegamento sicuro all'unità di controllo del dominio EIM

Una volta utilizzato il wizard per creare e collegare un nuovo dominio, l'utente potrebbe voler utilizzare Secure Sockets Layer (SSL) o Transport Layer Security Protocol (TLS) per stabilire un collegamento sicuro all'unità di controllo del dominio EIM. Per configurare SSL o TLS per EIM, è necessario completare le attività riportate di seguito:

1. Abilitazione di SSL per l'unità di controllo del dominio server LDAP.
2. Utilizzo di DCM (Digital Certificate Manager) per creare il certificato di cui necessita il server LDAP per poter utilizzare SSL.
3. Utilizzo di DCM per assegnare il certificato al server LDAP.
4. Aggiornamento delle proprietà di Configurazione EIM per specificare che il server iSeries utilizza un collegamento SSL sicuro.
5. Aggiornamento delle proprietà di Dominio EIM per ogni dominio EIM per specificare che EIM utilizza un collegamento SSL nella gestione del dominio tramite iSeries Navigator.

Collegamento di un dominio esistente

E' possibile utilizzare il wizard Configurazione EIM per collegare un dominio EIM esistente. Utilizzare questa opzione nel wizard Configurazione EIM quando, sulla rete, è già stato configurato un dominio EIM e un'unità di controllo del dominio. Durante l'esecuzione del wizard, è necessario fornire informazioni sul dominio, incluse le informazioni sul collegamento all'unità di controllo del dominio EIM. Il wizard memorizza queste informazioni sul server iSeries e poi le utilizza per collegarsi all'unità di controllo del dominio EIM. Il wizard crea anche un registro utenti EIM che rappresenta il registro profili utente OS/400 su questo server iSeries.

Per utilizzare il wizard per completare questa attività, è necessario disporre dell'autorizzazione speciale Amministratore della sicurezza (*SECADM) e Tutti gli oggetti (*ALLOBJ).

Per avviare ed utilizzare il wizard Configurazione EIM per collegare un dominio EIM esistente, completare i passi riportati di seguito utilizzando iSeries Navigator:

1. Espandere **Rete —> EIM (Enterprise Identity Mapping)**.
2. Fare clic con il tastino destro del mouse su **Configurazione** e selezionare **Configura...** per avviare il wizard Configurazione EIM. Una volta avviato il wizard, fornire le seguenti informazioni man mano che vengono visualizzate le diverse finestre di dialogo.
3. Nella finestra di dialogo di **Benvenuto** del wizard, selezionare **Collegamento di un dominio esistente** e fare clic su **Avanti**.
4. Se il servizio di autenticazione di rete non è attualmente configurato sul server iSeries, verrà visualizzata la finestra di dialogo **Configurazione servizi autenticazione di rete**. Questa finestra di dialogo richiede di selezionare se configurare il servizio di autenticazione di rete. Se si seleziona **Sì**, viene avviato il wizard Configurazione servizi di autenticazione di rete. Una volta completata la configurazione del servizio di autenticazione di rete, il wizard Configurazione EIM proseguirà.
5. Quando viene visualizzata la finestra di dialogo **Specifica unità di controllo del dominio** fornire le seguenti informazioni:
   - Nel campo **Nome unità di controllo del dominio**, specificare il nome del sistema che opera come unità di controllo del dominio per il dominio EIM a cui si desidera si colleghi il server iSeries.
   - Fare clic su **Utilizzare SSL (Secure Sockets Layer)** se si desidera che il richiamo delle informazioni EIM dall'unità di controllo del dominio utilizzi SSL per proteggere la trasmissione dei dati EIM.
   - Fare clic **Verifica collegamento** per verificare le informazioni di configurazione dell'unità di controllo del dominio.

   Nota: Se si è specificato di utilizzare SSL ed è stato ricevuto un messaggio di errore, tale messaggio potrebbe indicare che il server LDAP non è stato configurato per utilizzare SSL.

   - Fare clic su **Avanti**.
6. Sulla finestra di dialogo **Specifica utente per collegamento**, selezionare un **tipo di utente** per il collegamento. E' possibile selezionare uno dei seguenti tipi di utenti: DN e parola d'ordine, file keytab e principal Kerberos oppure principal Kerberos e parola d'ordine. I due tipi di utenti Kerberos sono disponibili solo se il servizio di autenticazione di rete è configurato per il sistema iSeries locale. Il tipo di utente selezionato determina le altre informazioni che devono essere fornite per completare la finestra di dialogo, come segue:
   - Se si seleziona **DN e parola d'ordine**, fornire le seguenti informazioni:
     - Nel campo **DN**, immettere il DN LDAP che identifica l'utente autorizzato a creare oggetti nello spazio del nome locale del server LDAP.
     - Nel campo **Parola d'ordine**, immettere la parola d'ordine dell'utente.
     - Nel campo **Conferma parola d'ordine**, immettere di nuovo la parola d'ordine.
   - Se si seleziona **File keytab e principal Kerberos**, fornire le seguenti informazioni:

- Nel campo **File Keytab**, inserire il nome del file keytab presente sul server iSeries che identifica l'utente autorizzato a creare gli oggetti nel nome dello spazio locale del server LDAP. Oppure, è possibile fare clic su **Sfoglia** per selezionare il file keytab.
- Nel campo **Principal**, inserire il nome del principal Kerberos da utilizzare per identificare l'utente.
- Nel campo **Dominio**, inserire il nome del dominio Kerberos del 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 viene 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**, inserire il nome del principal Kerberos che identifica l'utente autorizzato alla creazione degli oggetti nel nome dello spazio locale del server LDAP.
- Nel campo **Dominio**, inserire il nome del dominio Kerberos del principal.
- Nel campo **Parola d'ordine**, immettere la parola d'ordine dell'utente.
- Nel campo **Conferma parola d'ordine**, immettere di nuovo la parola d'ordine. 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 viene rappresentato nel file keytab come jsmith@ordept.myco.com.

• Fare clic su **Verifica collegamento** per verificare le informazioni di configurazione del collegamento all'unità di controllo del dominio.
• Fare clic su **Avanti**.

7. Sulla pagina **Specifica dominio**, selezionare il nome del dominio che si desidera collegare e fare clic su **Avanti**.
8. Sulla pagina **Informazioni registro**, selezionare il tipo di registri utenti che si desidera aggiungere al dominio EIM. Selezionare uno o entrambi i tipi di registro:
   • Selezionare **OS400** per aggiungere un registro utenti che rappresenta il registro locale nel dominio EIM. Nel campo fornito, immettere il nome del registro da creare nel dominio. Il nome registro EIM è una stringa arbitraria che rappresenta il tipo di registro e l'istanza specifica di tale registro.
   • Selezionare **Kerberos** per aggiungere un registro utenti Kerberos al dominio EIM. Nel campo fornito, immettere il nome del registro da creare nel dominio e selezionare **Le identità utente Kerberos sono sensibili al minuscolo e al maiuscolo** se necessario. E' possibile accettare il valore predefinito; il nome registro Kerberos è lo stesso del nome dominio. Utilizzando lo stesso nome di registro Kerberos del nome dominio, è possibile migliorare le prestazioni nel richiamo delle informazioni dal registro. Per ulteriori informazioni su come è possibile definire i registri utenti all'interno di EIM, consultare Definizioni di registro EIM.
   • Fare clic su **Avanti**.
9. Sulla finestra di dialogo **Specifica utente di sistema EIM**, selezionare il tipo di utente che si desidera venga utilizzato dal sistema quando si eseguono 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 OS/400 locale. E' possibile selezionare uno dei seguenti tipi di utenti: DN e parola d'ordine, file keytab e principal Kerberos oppure principal Kerberos e parola d'ordine. Il tipo di utente selezionato determina le altre informazioni che devono essere fornite per completare la finestra di dialogo come segue:
   • Se si seleziona **DN e parola d'ordine**, fornire le seguenti informazioni:
     - Nel campo **DN**, immettere il DN LDAP che identifica l'utente di OS/400 da utilizzare quando si contatta l'unità di controllo del dominio EIM.
     - Nel campo **Parola d'ordine**, immettere la parola d'ordine dell'utente.
     - Nel campo **Conferma parola d'ordine**, immettere di nuovo la parola d'ordine.
   • Se si seleziona **Principal Kerberos e parola d'ordine**, fornire le seguenti informazioni:
     - Nel campo **Principal**, inserire il nome del principal Kerberos che identifica l'utente di OS/400 da utilizzare quando si contatta l'unità di controllo del dominio EIM.

- Nel campo **Dominio**, inserire il nome del dominio Kerberos del principal.
- Nel campo **Parola d'ordine**, immettere la parola d'ordine dell'utente.
- Nel campo **Conferma parola d'ordine**, immettere di nuovo la parola d'ordine. 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 viene rappresentato nel file keytab come jsmith@ordept.myco.com.

• Se si seleziona **File keytab e principal Kerberos**, fornire le seguenti informazioni:
- Nel campo **File Keytab**, immettere il nome del file keytab sul server iSeries che identifica l'utente di OS/400 da utilizzare quando si contatta l'unità di controllo del dominio EIM. Oppure, è possibile fare clic su **Sfoglia** per selezionare il file keytab.
- Nel campo **Principal**, inserire il nome del principal Kerberos da utilizzare per identificare l'utente.
- Nel campo **Dominio**, inserire il nome del dominio Kerberos del principal.

• Fare clic su **Verifica collegamento** per verificare il collegamento dell'utente di sistema appena creato.
• Fare clic su **Avanti**.

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

Una volta terminato il wizard, è terminata anche la configurazione di base di EIM. Tuttavia, è necessario completare queste attività per finalizzare la configurazione di EIM per questo server:

1. Aggiunta del dominio collegato alla cartella Gestione dominio EIM.
2. Aggiunta di registri EIM al dominio EIM per i server e le applicazioni non iSeries che si desidera facciano parte del dominio EIM.
3. Creazione di identificativi EIM nel dominio per ogni entità o utente univoco per i sistemi che fanno parte del dominio EIM.
4. Creazione di associazioni tra diverse identità utente della persona o entità e questi identificativi EIM.

Inoltre, per abilitare un ambiente a collegamento singolo, è necessario configurare il servizio di autenticazione di rete per il server iSeries.

Gestione EIM

Una volta configurato EIM sul proprio server iSeries, per gestire le informazioni e il proprio dominio EIM, possono essere eseguite molte attività. Gli argomenti riportati di seguito trattano specifiche attività utilizzate per gestire EIM sul proprio server iSeries e all'interno della società nella rete.

Gestione domini EIM
Gestione delle informazioni EIM presenti nel dominio EIM e delle proprietà relative a quest'ultimo.

Gestione associazioni
Conservazione delle associazioni delle identità utente agli identificativi EIM per tutti gli utenti all'interno della società.

Gestione identificativi EIM
Conservazione degli identificativi EIM associati agli utenti nella società.

Gestione autorizzazioni utente EIM
Mantenimento della sicurezza delle informazioni EIM tramite la gestione delle autorizzazioni EIM per controllare le operazioni e le funzioni EIM che possono essere eseguite dagli utenti.

Gestione registri utenti
Gestione dei registri utenti aggiunti al proprio dominio EIM.

Gestione domini EIM

E' possibile utilizzare iSeries Navigator per gestire tutti i propri domini EIM. Per gestire un qualsiasi dominio EIM, il dominio deve essere elencato oppure deve essere aggiunto alla cartella Gestione dominio nella cartella Rete in iSeries Navigator. Una volta creato e configurato un nuovo dominio EIM, è necessario aggiungerlo alla cartella Gestione dominio per gestire le informazioni presenti nel dominio.

E' possibile utilizzare un qualsiasi collegamento iSeries per gestire un dominio EIM che si trova in una qualsiasi ubicazione nella stessa rete. L'iSeries collegato ad iSeries Navigator non deve fare parte di un dominio per gestire tale dominio.

Per gestire i propri domini EIM, è possibile completare le attività riportate di seguito:

- Aggiunta di un dominio a Gestione dominio
- Collegamento ad un dominio
- Cancellazione di un dominio
- Eliminazione di un dominio da Gestione dominio

Aggiunta di un dominio a Gestione dominio

Per aggiungere un dominio, è necessario disporre dell'autorizzazione speciale *SECADM. Per aggiungere un dominio EIM esistente a Gestione dominio, completare i passi riportati di seguito.

1. Espandere **Rete —> EIM (Enterprise Identity Mapping)**.
2. Fare clic con il tastino destro del mouse su **Gestione dominio** e selezionare **Aggiungi dominio...**.
3. Specificare le informazioni necessarie sul dominio e sul collegamento.
4. Fare clic su **OK** per aggiungere il dominio.

Collegamento ad un dominio

Se attualmente non si è collegati al dominio EIM in cui si desidera operare, è necessario innanzitutto collegarsi al dominio. E' possibile collegarsi ad un dominio EIM anche se il proprio server iSeries non è attualmente configurato per far parte di questo dominio.

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

1. Espandere **Rete —> EIM (Enterprise Identity Mapping) —> Gestione dominio**.
2. Selezionare il dominio a cui si desidera collegarsi. Se il dominio con cui si desidera operare non è elencato, è necessario consultare Aggiunta di un dominio EIM a Gestione dominio.
3. Fare clic con il tastino destro del mouse sul dominio EIM a cui si desidera collegarsi e selezionare **Collega...**.
4. Specificare il tipo di utente e le informazioni utente necessarie da utilizzare per collegarsi all'unità di controllo del dominio EIM.
5. Fare clic su **OK**.

Cancellazione di un dominio

Per completare questa attività, è necessario disporre dell'autorizzazione di amministratore LDAP o amministratore EIM. Prima di cancellare un dominio EIM, è necessario innanzitutto eliminare tutti i registri e tutte le informazioni sull'identificativo EIM dal dominio.

Per cancellare un dominio EIM, completare i passi riportati di seguito.

1. Espandere **Rete —> EIM (Enterprise Identity Mapping) —> Gestione dominio**.
2. Eliminare tutti i registri utenti dal dominio EIM.
3. Cancellare tutti gli identificativi EIM dal dominio EIM.
4. Fare clic con il tastino destro del mouse sul dominio che si desidera cancellare e selezionare **Cancella...**.
5. Fare clic su **Sì** sulla finestra di dialogo **Conferma cancellazione**.

Eliminazione di un dominio da Gestione dominio
Nel momento in cui non è necessario, è possibile eliminare un dominio EIM dalla cartella Gestione dominio una volta terminato con le modifiche.

Per eliminare un dominio, completare i passi riportati di seguito:

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

Gestione associazioni
Una associazione definisce una relazione tra un identificativo EIM e una identità utente all'interno di un registro. Ad esempio, è possibile creare un'associazione tra un profilo utente OS/400 o un principal Kerberos e un identificativo EIM. Questa associazione può essere poi utilizzata per determinare quale identificativo EIM corrisponde ad un profilo utente iSeries o ad un principal Kerberos locale.

Conservare le associazioni delle identità utente agli identificativi EIM appropriati costituisce la chiave per semplificare le attività amministrative necessarie per tenere traccia di quali utenti dispongono di account su diversi sistemi nella rete.

La gestione di queste associazioni consente inoltre di trarre vantaggio dall'abilitazione di un collegamento singolo sulla rete. Quando si implementa una rete a collegamento singolo sicuro, è necessario tenere aggiornate le associazioni.

Possono essere creati tre tipi di associazioni: origine, destinazione e amministrativa. Per creare o conservare le associazioni tra identità utente e identificativi EIM appropriati, è possibile eseguire una delle attività riportate di seguito:

- Creazione di un'associazione
- Cancellazione di un'associazione

Creazione di un'associazione
Per abilitare un ambiente a collegamento singolo, è necessario creare associazioni tra diversi identificativi utente di una persona o entità e un singolo identificativo EIM relativo a tale persona o entità. E' possibile creare tre tipi di associazione: destinazione, origine e amministrativa.

Per creare un'associazione origine o amministrativa, è necessario disporre dell'autorizzazione di amministratore identificativi o di amministratore EIM. Per creare un'associazione di destinazione, è necessario disporre dell'autorizzazione di amministratore registri per tutti i registri, amministratore registri per il registro specificato o amministratore EIM.

Per creare un'associazione per un identificativo EIM, completare i passi riportati di seguito:

1. Espandere **Rete —> EIM (Enterprise Identity Mapping) —> Gestione dominio**.
2. E' necessario essere collegati al dominio EIM in cui si desidera operare.
   - Se il dominio EIM da gestire non è elencato nella cartella Gestione dominio, consultare Aggiunta di un dominio EIM a Gestione dominio.
   - Se attualmente non si è collegati al dominio EIM in cui si desidera operare, consultare Collegamento all'unità di controllo del dominio EIM.
3. Espandere il dominio EIM a cui si è ora collegati.
4. Fare clic su **Identificativi** per visualizzare la lista degli identificativi EIM.
5. Fare clic con il tastino destro del mouse sull'identificativo EIM appropriato e selezionare **Proprietà...**.
6. Fare clic sul separatore **Associazioni**.
7. Fare clic su **Aggiungi...** per visualizzare la finestra di dialogo **Aggiungi associazione**.

8. Fare clic su **Aiuto** se si necessita di ulteriori informazioni per completare i campi.
9. Una volta specificate le informazioni richieste, fare clic su **OK**.

Cancellazione di un'associazione
Per cancellare un'associazione origine o amministrativa, è necessario disporre dell'autorizzazione di amministratore identificativi o dell'autorizzazione di amministratore EIM. Per cancellare un'associazione di destinazione, è necessario disporre dell'autorizzazione di amministratore per i registri selezionati (incluso il registro che si desidera gestire), dell'autorizzazione di amministratore registri o dell'autorizzazione di amministratore EIM.

Per cancellare un'associazione, completare i passi riportati di seguito.

1. Espandere **Rete —> EIM (Enterprise Identity Mapping) —> Gestione dominio**.
2. E' necessario essere collegati al dominio EIM in cui si desidera operare:
   - Se il dominio EIM che si desidera gestire non è elencato in Gestione dominio, consultare Aggiunta di un dominio EIM a Gestione dominio.
   - Se attualmente non si è collegati al dominio EIM in cui si desidera operare, consultare Collegamento ad un dominio EIM.
3. Espandere il dominio EIM a cui si è ora collegati.
4. Fare clic su **Identificativi**.
5. Fare clic con il tastino destro del mouse sull'identificativo EIM desiderato e selezionare **Proprietà...** .
6. Fare clic sul separatore **Associazioni** per visualizzare le associazioni correnti relative all'identificativo EIM.
7. Selezionare l'associazione che si desidera eliminare.
8. Fare clic su **Elimina** per eliminare le associazioni.
9. Fare clic su **OK**.

Gestione identificativi EIM
La conservazione degli identificativi EIM che rappresentano gli utenti è fondamentale per la sicurezza. Gli utenti di una società cambiano spesso, alcuni vengono assunti, altri licenziati e altri ancora vengono spostati da un reparto ad un altro. Insieme a queste modifiche si presenta la necessità di tracciare gli account degli utenti e il relativo accesso ai sistemi all'interno della rete. La creazione degli identificativi EIM e la relativa associazione alle identità di ogni utente rende più semplice l'attività di traccia.

Abilitazione di un collegamento singolo rende più semplice l'attività per gli utenti anche quando vengono spostati in un altro reparto all'interno della società. Devono essere modificati anche le necessità di accesso al sistema e gli spazi di sicurezza. L'abilitazione di un collegamento singolo elimina la necessità, per questi utenti, di ricordare i nuovi nomi utente e parole d'ordine per i nuovi sistemi.

La gestione degli identificativi EIM degli utenti di una società riguarda molte attività che potrebbero diventare una routine. E' possibile utilizzare le attività riportate di seguito per gestire gli identificativi EIM nella propria rete e domini:

- Creazione di un identificativo EIM
- Aggiunta di un alias ad un identificativo EIM
- Cancellazione di un identificativo EIM

Per informazioni sulla gestione delle associazioni, consultare l'argomento Gestione associazioni.

Creazione di un identificativo EIM
Per creare un identificativo EIM, è necessario disporre dell'autorizzazione di amministratore identificativi o dell'autorizzazione di amministratore EIM.

Per creare un identificativo EIM per una persona o un'entità, completare i passi riportati di seguito:

1. Espandere **Rete —> EIM (Enterprise Identity Mapping) —> Gestione dominio**.
2. E' necessario essere collegati al dominio EIM in cui si desidera operare:
   - Se il dominio EIM che si desidera gestire non è elencato in **Gestione dominio**, consultare Aggiunta di un dominio a Gestione dominio.
   - Se attualmente non si è collegati al dominio EIM in cui si desidera operare, consultare Collegamento ad un dominio.
3. Espandere il dominio EIM a cui si è ora collegati.
4. Fare clic con il tastino destro del mouse su **Identificativi** e selezionare **Nuovo identificativo...**.
5. Fare clic su **Aiuto** se si necessita di ulteriori informazioni su uno qualsiasi dei campi.
6. Una volta specificate le informazioni richieste, fare clic su **OK**.

Aggiunta di un alias ad un identificativo EIM

E' possibile creare un alias per fornire ulteriori informazioni distinte per un identificativo EIM. L'alias può essere poi utilizzato per distinguere un identificativo EIM da un altro. 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.

Per aggiungere un alias ad un identificativo, è necessario disporre dell'autorizzazione di amministratore identificativi o dell'autorizzazione di amministratore EIM.

Per aggiungere un alias ad un identificativo EIM, completare i passi riportati di seguito.

1. Espandere **Rete —> EIM (Enterprise Identity Mapping) —> Gestione dominio**.
2. E' necessario essere collegati al dominio EIM in cui si desidera operare:
   - Se il dominio EIM che si desidera gestire non è elencato in Gestione dominio, consultare Aggiunta di un dominio EIM a Gestione dominio.
   - Se attualmente non si è collegati al dominio EIM in cui si desidera operare, consultare Collegamento all'unità di controllo del dominio EIM.
3. Espandere il dominio EIM a cui si desidera collegarsi.
4. Fare clic con il tastino destro del mouse sull'identificativo EIM desiderato e selezionare **Proprietà**. Se non esistono identificativi EIM, consultare Creazione di un identificativo EIM.
5. Specificare il nome dell'alias che si desidera aggiungere a questo identificativo EIM e fare clic su **Aggiungi**.
6. Fare clic su **OK** per salvare le modifiche.

Cancellazione di un identificativo EIM

Per cancellare un identificativo EIM, è necessario disporre dell'autorizzazione di amministratore EIM.

Per cancellare un identificativo EIM, completare i passi riportati di seguito:

1. Espandere **Rete —> EIM (Enterprise Identity Mapping) —> Gestione dominio**.
2. E' necessario essere collegati al dominio EIM in cui si desidera operare:
   - Se il dominio EIM che si desidera gestire non è elencato in Gestione dominio, consultare Aggiunta di un dominio EIM a Gestione dominio.
   - Se attualmente non si è collegati al dominio EIM in cui si desidera operare, consultare Collegamento all'unità di controllo del dominio EIM.
3. Espandere il dominio EIM a cui si è ora collegati.
4. Fare clic su **Identificativi**.
5. Selezionare uno o più identificativi EIM da cancellare.
6. Fare clic con il tastino destro del mouse sugli identificativi EIM selezionati e selezionare **Cancella**.
7. Fare clic su **Sì** sulla finestra di dialogo **Conferma cancellazione** per eliminare gli identificativi EIM selezionati.

Gestione autorizzazioni utente EIM

EIM definisce varie autorizzazioni EIM necessarie per eseguire diverse operazioni all'interno del dominio. Ciò include le funzioni di gestione del dominio come la creazione degli identificativi, l'elenco dei registri e l'esecuzione delle operazioni di ricerca delle corrispondenze. Solo gli utenti con autorizzazione di amministratore EIM possono concedere o revocare le autorizzazioni degli altri utenti.

Consultare Autorizzazioni EIM per brevi definizioni di ogni gruppo di autorizzazioni e dettagli sull'accesso specifico a determinate funzioni EIM che viene fornito da queste autorizzazioni.

Per modificare le autorizzazioni EIM per un utente, seguire i passi riportati di seguito:

1. In iSeries Navigator, espandere **Rete —> EIM (Enterprise Identity Mapping) —> Gestione dominio**.
2. Espandere il dominio EIM in cui si desidera operare. Se attualmente non si è collegati a questo dominio, verrà effettuata una richiesta di collegamento. Assicurarsi di essere collegati al dominio con un'autorizzazione utente che disponga dell'autorizzazione di amministratore EIM.
3. Fare clic con il tastino destro del mouse sul dominio EIM e selezionare **Autorizzazione...**.
4. Sulla finestra di dialogo **Modifica autorizzazione EIM**, specificare l'utente per il quale si stanno modificando le autorizzazioni EIM.
5. Fare clic su **OK**.
6. Sulla finestra di dialogo **Modifica autorizzazione EIM**, apportare le modifiche necessarie alle autorizzazioni dell'utente.
7. Una volta terminato, fare clic su **OK** per salvare le modifiche alle autorizzazioni.

Gestione registri utenti

Prima di poter creare associazioni tra identità presenti nei registri utenti e gli appropriati identificativi EIM, è necessario innanzitutto definire il registro utenti nel dominio EIM:

Le attività riportate di seguito fanno parte della gestione dei registri utenti all'interno di un dominio EIM.

- Aggiunta di un registro utenti
- Aggiunta di un alias ad un registro utenti
- Definizione di un tipo di registro utenti privato in EIM
- Eliminazione di un registro utenti
- Eliminazione di un alias da un registro utenti

Aggiunta di un registro utenti

Per aggiungere un registro utenti, è necessario disporre dell'autorizzazione di amministratore EIM. Per dettagli su questa autorizzazione e sugli elementi cui può accedere un utente che ne dispone, consultare Autorizzazioni EIM.

Per aggiungere un registro utenti ad un dominio EIM, completare i passi riportati di seguito.

1. Espandere **Rete —> EIM (Enterprise Identity Mapping) —> Gestione dominio**.
2. Collegarsi al dominio EIM con un utente che disponga dell'autorizzazione di amministratore EIM.
   - Se il dominio EIM da gestire non è elencato nella cartella Gestione dominio, consultare Aggiunta di un dominio EIM a Gestione dominio.
   - Se attualmente non si è collegati al dominio EIM in cui si desidera operare, consultare Collegamento all'unità di controllo del dominio EIM.
3. Espandere il dominio EIM a cui si è ora collegati.
4. Fare clic con il tastino destro del mouse su **Registri utenti** e selezionare **Aggiungi registro...**.
5. Specificare le informazioni richieste sul registro utenti. E' possibile specificare anche le informazioni alias del registro.
6. Fare clic su **OK** per salvare le informazioni e aggiungere il registro utenti al dominio EIM.

Aggiunta di un alias ad un registro utenti

L'utente, o lo sviluppatore dell'applicazione, potrebbe voler creare un alias per fornire informazioni distinte aggiuntive relative ad un registro utenti. L'alias può essere poi utilizzato per distinguere un registro utenti da un altro. Ad esempio, gli amministratori e gli sviluppatori di applicazioni utilizzano un alias su un registro utenti per comunicare quali registri EIM devono essere utilizzati da un'applicazione. Per informazioni sull'utilizzo degli alias con i registri utenti, vedere Definizioni di registro EIM.

Per aggiungere un alias ad un registro utenti, è necessario utilizzare una delle seguenti autorizzazioni: amministratore EIM, amministratore registri per tutti i registri oppure amministratore registri per il registro specifico per cui si sta eseguendo questa attività.

Per aggiungere un alias ad un registro utenti all'interno di un dominio EIM, completare i passi riportati di seguito:

1. Espandere **Rete —> EIM (Enterprise Identity Mapping) —> Gestione dominio**.
2. E' necessario essere collegati al dominio EIM in cui si desidera operare:
   - Se il dominio EIM da gestire non è elencato nella cartella Gestione dominio, consultare Aggiunta di un dominio EIM a Gestione dominio.
   - Se attualmente non si è collegati al dominio EIM in cui si desidera operare, consultare Collegamento all'unità di controllo del dominio EIM.
3. Espandere il dominio EIM a cui si è ora collegati.
4. Fare clic su **Registri utenti** per visualizzare la lista dei registri all'interno del dominio.
5. Fare clic con il tastino destro del mouse sul registro utenti a cui si sta aggiungendo un alias e selezionare **Proprietà...**.
6. Fare clic sul separatore **Alias** sulla finestra di dialogo **Proprietà**.
7. Specificare il nome e il tipo di alias che si desidera aggiungere. E' possibile specificare un tipo di alias che non è presente nella lista dei tipi.
8. Fare clic su **Aggiungi**.
9. Fare clic su **OK** per salvare le modifiche.

Definizione di un tipo di registro utenti privato in EIM

Per definire un tipo di registro privato che EIM non riconosce come valore predefinito, 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'identificativo oggetto (OID) per OS/400 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.`. E' 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). E' possibile trovare una pagina informativa con i collegamenti ad un modulo di domanda sul sito web ANSI all'indirizzo http://web.ansi.org/public/services/reg_org.html

  . 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. E' necessario attendere circa due settimane prima di ricevere l'identificativo OID di partenza assegnato dall'ANSI. Quest'ultimo assegnerà un numero (NEWNUM), creando un nuovo identificativo OID di partenza: 2.16.840.1.NEWNUM.
- Nella maggior parte dei paesi o regioni, l'associazione degli standard nazionale conserva un registro di OID. Per quanto riguarda ANSI, gli identificativi di partenza vengono generalmente 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.iso.ch/addresse/membodies.html

  . Le informazioni includono l'indirizzo postale e l'indirizzo di posta elettronica. In molti casi, viene specificato anche un indirizzo web.
- Un altro possibile punto di partenza potrebbe essere il Registro internazionale degli schemi NSAP DCC ISO. NSAP sta per Network Service Access Point e viene utilizzato in diversi standard internazionali. E' possibile reperire il registro per gli schemi all'indirizzo http://www.fei.org.uk sotto l'intestazione ISO DCC NSAP

  . Attualmente il sito web contiene informazioni sui contatti per 13 autorità di denominazione, alcune delle quali assegnano anche gli OID.
- 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) così 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, vedere http://csrc.nist.gov/csor/

  .

Per ulteriori informazioni sugli OID per le normative di certificazione, vedere http://csrc.nist.gov/csor/pkireg.htm

.

Eliminazione di un registro utenti

Eliminando un registro utenti da un dominio EIM, verranno perse le associazioni agli identificativi EIM per le identità utente presenti nel registro. Aggiungendo di nuovo il registro utenti nel dominio EIM dopo la cancellazione, non verranno ripristinate le relazioni di associazione.

Per eliminare un registro utenti, è necessario disporre dell'autorizzazione di amministratore EIM.

Per eliminare un registro utenti, completare i passi riportati di seguito:

1. Espandere **Rete —> EIM (Enterprise Identity Mapping) —> Gestione dominio**.
2. E' necessario essere collegati al dominio EIM in cui si desidera operare.
   - Se il dominio EIM da gestire non è elencato nella cartella Gestione dominio, consultare Aggiunta di un dominio EIM a Gestione dominio.
   - Se attualmente non si è collegati al dominio EIM in cui si desidera operare, consultare Collegamento all'unità di controllo del dominio EIM.
3. Espandere il dominio EIM a cui si è ora collegati.
4. Fare clic su **Registri utenti** per visualizzare la lista dei registri utenti presenti nel dominio.
5. Fare clic con il tastino destro del mouse sul registro utenti che si desidera eliminare e selezionare **Cancella...**.
6. Fare clic su **Sì** sulla finestra di dialogo **Conferma** per cancellare il registro utenti.

Eliminazione di un alias da un registro utenti

Per eliminare un alias da un registro utenti, è necessario disporre dell'autorizzazione di amministratore registri e dell'autorizzazione di amministratore per i registri selezionati (incluso il registro che si desidera gestire) oppure dell'autorizzazione di amministratore EIM.

Per eliminare un alias da un registro utenti all'interno di un dominio EIM, completare i passi riportati di seguito:

1. Espandere **Rete —> EIM (Enterprise Identity Mapping) —> Gestione dominio**.
2. E' necessario essere collegati al dominio EIM in cui si desidera operare:
   - Se il dominio EIM da gestire non è elencato nella cartella Gestione dominio, consultare Aggiunta di un dominio EIM a Gestione dominio.
   - Se attualmente non si è collegati al dominio EIM in cui si desidera operare, consultare Collegamento all'unità di controllo del dominio EIM.
3. Espandere il dominio EIM a cui si è ora collegati.
4. Fare clic su **Registri utenti** per visualizzare la lista dei registri all'interno del dominio.
5. Fare clic con il tastino destro del mouse sul registro utenti per il quale si desidera eliminare un alias e selezionare **Proprietà**.
6. Fare clic sul separatore **Alias** sulla finestra di dialogo **Proprietà**.
7. Selezionare l'alias che si desidera eliminare e fare clic su **Elimina**.
8. Fare clic su **OK** per salvare le modifiche.

API relative a EIM

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. E' 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 interrogazione.

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

Per informazioni dettagliate ed una lista completa delle API relative ad EIM disponibili per il server iSeries, consultare l'argomento API relative a EIM (Enterprise Identity Mapping).

Risoluzione dei problemi di EIM

EIM è composto da più tecnologie e da molte applicazioni e funzioni. Poiché è possibile intraprendere più percorsi per la risoluzione di problemi, gli argomenti riportati di seguito contengono informazioni e istruzioni dettagliate su come risolvere i problemi o correggere alcuni degli errori comuni che potrebbero verificarsi, ad esempio:

- Impossibile collegarsi all'unità di controllo del dominio
- La visualizzazione della lista degli identificativi EIM richiede del tempo
- Il wizard Configurazione EIM si blocca durante l'elaborazione finale
- Il gestore EIM non è più valido
- Autenticazione Kerberos e messaggi di diagnostica

Impossibile collegarsi all'unità di controllo del dominio

Quando si tenta il collegamento all'unità di controllo del dominio, è possibile che diversi fattori contribuiscano a creare problemi di connessione. Controllare le voci riportate di seguito per un aiuto nella ricerca della causa del problema:

- Verificare che le informazioni specificate per le voci riportate di seguito siano corrette:
  - Nome dell'unità di controllo del dominio
  - Porta specificata
  - ID utente e parola d'ordine
- Verificare che l'unità di controllo del dominio sia attiva. Se l'unità di controllo del dominio è un server iSeries, è possibile utilizzare iSeries Navigator e seguire i passi riportati di seguito:

1. Espandere **Rete —> Server —> TCP/IP**.
2. Verificare che lo stato di Server indirizzari sia **Avviato**. Se il server è arrestato, fare clic con il tastino destro del mouse su **Server indirizzari** e selezionare **Avvia...**

Una volta che l'unità di controllo del dominio è attiva, tentare di nuovo il collegamento al dominio.

1. Espandere **Rete —> EIM (Enterprise Identity Mapping) —> Gestione dominio**.
2. Selezionare il dominio a cui si desidera collegarsi. Se non vengono elencati domini EIM oppure se il dominio EIM che si desidera gestire non è elencato nella cartella Gestione dominio, sarà necessario aggiungere un dominio EIM a Gestione dominio.
3. Fare clic con il tastino destro del mouse sul dominio EIM a cui si desidera collegarsi e selezionare **Collega...**.
4. Specificare il tipo di utente e le informazioni utente necessarie da utilizzare per collegarsi all'unità di controllo del dominio EIM.
5. Fare clic su **OK**.

La visualizzazione della lista degli identificativi EIM richiede del tempo

Quando si apre la cartella Identificativi in iSeries Navigator, la creazione, e relativa visualizzazione, della lista degli identificativi richiede del tempo. E' possibile ridurre i criteri di ricerca per la visualizzazione di tale lista se nel proprio dominio sono presenti molti identificativi EIM.

Per personalizzare la visualizzazione degli identificativi EIM, seguire i passi riportati di seguito:

1. In iSeries Navigator, espandere **Rete —> EIM (Enterprise Identity Mapping) —> Gestione dominio**.
2. Espandere il dominio in cui si desidera visualizzare gli identificativi EIM.
3. Fare clic con il tastino destro del mouse su **Identificativi** e selezionare **Personalizzare questa vista —> Includere...**.
4. Specificare i criteri di visualizzazione desiderati. Come carattere jolly può essere utilizzato l'asterisco (*).
5. Fare clic su OK.

Alla prossima selezione di **Identificativi**, gli identificativi EIM visualizzati saranno solo quelli che corrisponderanno ai criteri specificati. Se si desidera visualizzare tutti gli identificativi EIM, utilizzare i passi riportati di sopra e selezionare **Tutti gli identificativi** come opzione di visualizzazione personalizzata.

Il wizard Configurazione EIM si blocca durante l'elaborazione finale

Se il wizard sembra bloccarsi durante l'elaborazione finale, è possibile che stia attendendo l'avvio dell'unità di controllo del dominio. Verificare che non si siano verificati errori durante l'avvio del server LDAP. Per i server iSeries, controllare la registrazione lavori del lavoro QDIRSRV nel sottosistema QSYSWRK.

Per controllare la registrazione lavori, seguire i passi riportati di seguito:

1. In iSeries Navigator, espandere **Gestione lavoro —> Sottosistemi —> Qsyswrk**.
2. Fare clic con il tastino destro del mouse su **Qdirsrv** e selezionare **Registrazione lavori**.

Il gestore EIM non è più valido

Mentre si sta gestendo EIM tramite iSeries Navigator, se l'utente riceve un errore indicante che il gestore EIM non è più valido, il collegamento all'unità di controllo del dominio verrà perso.

Per ricollegarsi all'unità di controllo del dominio, seguire i passi riportati di seguito:

1. In iSeries Navigator, espandere **Rete —> EIM (Enterprise Identity Mapping) —> Gestione dominio**.
2. Fare clic con il tastino destro del mouse sul dominio su cui si desidera operare e selezionare **Ricollega...**.

3. Specificare le informazioni sul collegamento.
4. Fare clic su **OK**.

Autenticazione Kerberos e messaggi di diagnostica

Quando si utilizza il protocollo Kerberos per l'autenticazione tramite EIM, nella registrazione lavori viene scritto il messaggio di diagnostica CPD3E3F ogniqualvolta 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.

Informazioni correlate relative a EIM

L'utente potrebbe voler apprendere ulteriori informazioni sulle tecnologie correlate a EIM. Gli argomenti dell'Information Center riportati di seguito possono essere di ausilio nella comprensione di tali tecnologie:

- **Servizio di autenticazione di rete**
  Questo argomento fornisce informazioni sulla configurazione del servizio di autenticazione di rete su iSeries. Il servizio di autenticazione di rete consente ad iSeries di far parte di una rete Kerberos esistente. Quando viene utilizzato con EIM, il servizio di autenticazione di rete fornisce un collegamento singolo per una rete.
- **Servizi indirizzario (LDAP)**
  Questo argomento fornisce le informazioni concettuali e di configurazione per i servizi indirizzario (LDAP). EIM utilizza il server LDAP per memorizzare i dati EIM e le associazioni di corrispondenza.

Printed in Denmark by IBM Danmark A/S