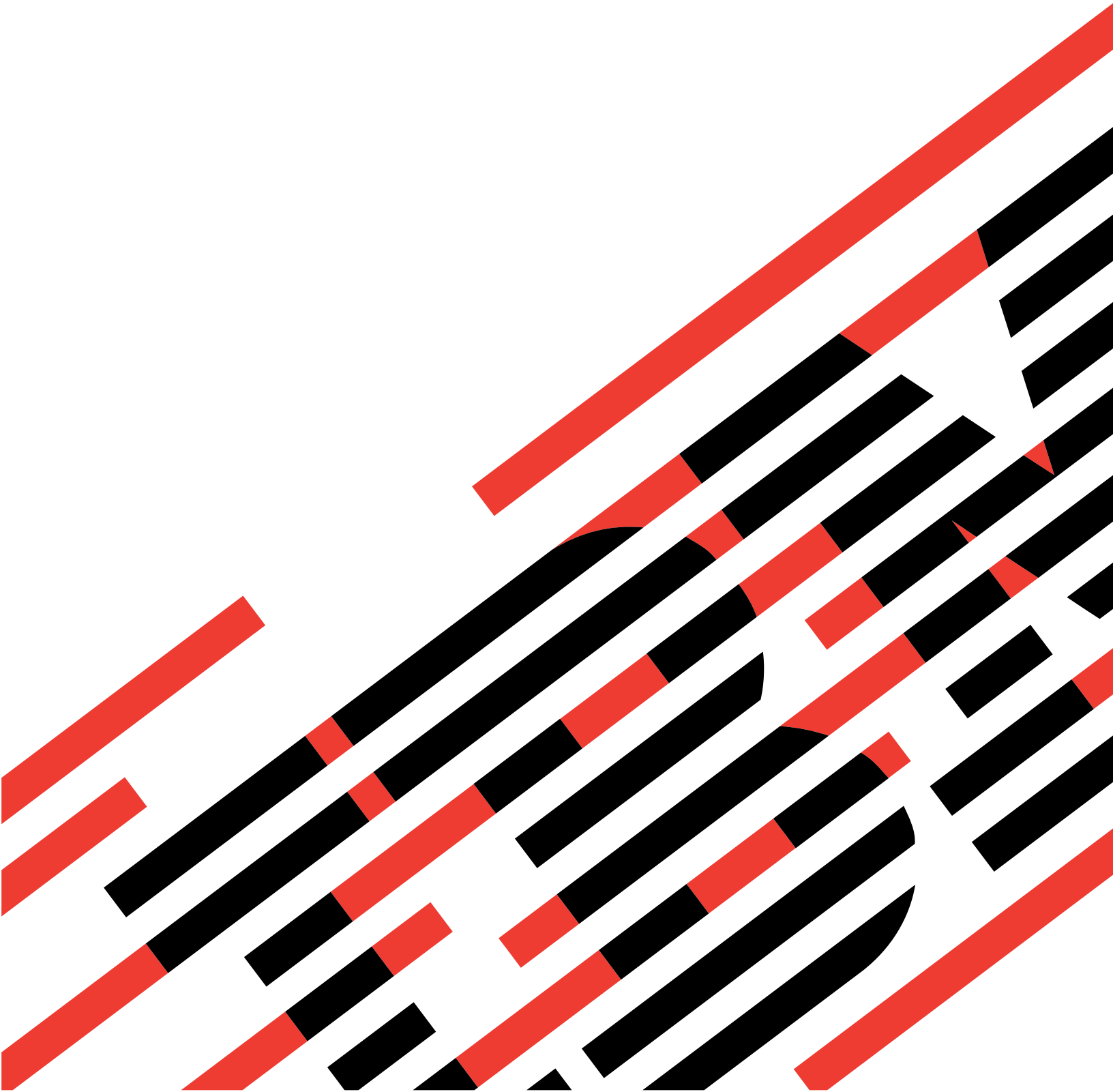
IBM

eserver

iSeries

Enterprise Identity Mapping



IBM

@server

iSeries

Enterprise Identity Mapping

© Copyright International Business Machines Corporation 1998, 2002. Toate drepturile rezervate.

Cuprins

© Copyright IBM Corp. 1998, 2002

Maparea identităţilor din întreprindere (EIM)

Cele mai multe întreprinderi cu reţea se confruntă cu problema înregistrării multiple a utilizatorilor, care necesită ca fiecare persoană sau identitate din cadrul întreprinderii să aibă o identitate de utilizator pentru fiecare registru. Nevoia de mai multe registre de utilizatori se dezvoltă rapid într-o mare problemă administrativă care afectează utilizatorii, administratorii şi dezvoltatorii de aplicaţii. Maparea identităţilor din întreprindere (EIM) oferă soluţii necostisitoare pentru gestiunea uşoară a mai multor registre de utilizatori şi identităţi de utilizatori din întreprinderea dumneavoastră.

EIM este un mecanism pentru maparea (asocierea) unei persoane sau a unei entităţi cu identităţile utilizator corespunzătoare în diferite registre pentru întreprindere. EIM furnizează API-uri pentru crearea şi gestionarea acestor relaţii de mapare a identităţilor, cât şi API-uri pe care aplicaţiile să le utilizeze pentru interogarea acestor informaţii. În plus, OS/400(R) utilizează capabilităţile EIM şi Kerberos pentru a furniza un mediu cu înregistrare unică.

Navigatorul iSeries, Interfaţa utilizator grafică a iSeries, furnizează vrăjitori pentru a configura şi gestiona EIM. În plus, administratorii pot gestiona relaţiile EIM pentru profilurile utilizator prin intermediul Navigatorului iSeries.

Serverul iSeries(TM) utilizează EIM pentru a da posibilitatea interfeţelor OS/400 să autentifice utilizatorii prin intermediu serviciului de autentificare în reţea. Aplicaţiile, cât şi OS/400, pot accepta tichete Kerberos şi utiliza EIM pentru a găsi profilul de utilizator care reprezintă aceeaşi persoană pe care o reprezintă tichetul Kerberos.

Subiectele următoare furnizează informaţii specifice despre EIM:

Tipărirea acestui subiect
Tipăriţi un PDF al acestui subiect EIM şi al altor subiecte înrudite.

Privire generală asupra Mapării identităţilor din întreprindere
Învăţaţi despre problemele pe care EIM vă poate ajuta să le rezolvaţi, despre abordările curente ale industriei ale acestor probleme şi de ce abordarea EIM este o soluţie mai bună.

Concepte EIM
Învăţaţi despre conceptele EIM pe care trebuie să le înţelegeţi pentru a implementa cu succes EIM.

Concepte LDAP pentru EIM
Învăţaţi despre conceptele LDAP (Lightweight Directory Access Protocol) de care trebuie să le înţelegeţi pentru a implementa cu succes EIM.

Posibilitatea de înregistrare unică
Citiţi despre avantajele pe care le furnizează EIM pentru simplificarea înregistrării utilizatorului.

Planificarea EIM
Vă asiguraţi că aveţi configurate toate serviciile şi aplicaţiile necesare înainte de a configura EIM.

Configurarea EIM
Utilizaţi Vrăjitorul de configurare a Mapării identităţilor din întreprindere (apoi referit ca vrăjitorul Configurare EIM) pentru a porni EIM.

Gestionarea EIM
Gestionaţi proprietăţile EIM, domeniile EIM, registrele utilizator, autorizările utilizator EIM şi altele.

API-uri pentru EIM
Utilizaţi API-urile EIM în aplicaţiile şi în reţeaua dumneavoastră.

© Copyright IBM Corp. 1998, 2002

Depanarea EIM
Găsiţi soluţii pentru problemele şi erorile obişnuite care se pot produce când utilizaţi EIM în reţeaua dumneavoastră.

Informaţii înrudite pentru EIM
Legătură la informaţii înrudite pentru EIM.

Tipăriţi acest subiect

Pentru a vizualiza sau pentru a descărca versiunea PDF, selectaţi Maparea identităţilor din întreprindere

(aproximativ 390 KB sau 50 de pagini).

Alte informaţii

Puteţi vizualiza şi descărca aceste subiecte înrudite:

- Servicii de autentificare în reţea (aproximativ 199 KB sau 60 de pagini) conţine informaţii despre cum se realizează configurarea serviciului de autentificare în reţea împreună cu EIM pentru a crea un mediu cu înregistrare unică.
- Servicii de director (LDAP) (aproximativ 323 KB sau66 de pagini) conţine informaţii despre cum se realizează configurarea serverului LDAP, pe care îl puteţi utiliza ca un controler de domeniu EIM, împreună cu informaţii despre configurarea avansată a LDAP.

Salvarea fişierelor PDF

Pentru a salva un PDF pe staţia dumneavoastră pentru a-l vizualiza sau tipări:

1. Deschideţi PDF-ul în browserul dumneavoastră (faceţi clic pe legătura de mai sus).
2. În meniu browserului dumneavoastră, faceţi clic pe **Fişier (File)**.
3. Faceţi clic pe **Salvare ca... (Save as...)**
4. Navigaţi către directorul în care doriţi să salvaţi PDF-ul.
5. Faceţi clic pe **Salvare (Save)**.

Descărcarea programului de vizualizare Adobe Acrobat Reader

Dacă aveţi nevoie de Adobe Acrobat Reader pentru a vizualiza sau pentru a tipări aceste PDF-uri, puteţi descărca o copie de pe situl Web Adobe (www.adobe.com/prodindex/acrobat/readstep.html)

.

Maparea identităţilor din întreprindere

Mediile de reţea actuale sunt construite din grupuri complexe de sisteme şi de aplicaţii, având ca efect necesitatea gestionării mai multor registre utilizator. Confruntarea cu registre utilizator multiple creşte rapid într-o mare problemă de administrare care afectează utilizatorii, administratorii şi dezvoltatorii de aplicaţii. Drept urmare, multe companii se luptă să gestioneze sigur autentificarea şi autorizarea pentru sisteme şi aplicaţii. Maparea identităţilor din întreprindere (EIM) este o tehnologie de infrastructură IBM

care permite administratorilor şi dezvoltatorilor de aplicaţii să abordeze această problemă mult mai uşor şi mai puţin costisitor decât era posibil înainte.

Informaţiile care urmează descriu aceste probleme, trec în revistă abordările curente ale industriei şi explică de ce este mai bună abordarea EIM.

Problema gestionării registrelor utilizator multiple

Mulţi administratori gestionează reţele care includ sisteme şi servere diferite, fiecare cu o modalitate unică de gestionare a utilizatorilor prin intermediul a variate registre utilizator. În aceste reţele complexe, administratorii sunt responsabili pentru gestionarea identităţilor şi parolelor fiecărui utilizator în cadrul mai multor sisteme. Suplimentar, adesea administratorii trebuie să sincronizeze aceste identităţi şi parole iar utilizatorii sunt împovăraţi cu amintirea a multiple identităţi şi parole şi cu păstrarea sincronizării acestora. Regia pentru utilizator şi pentru administrator este excesivă în acest mediu. Ca urmare, administratorii pierd adesea timp preţios cu depanarea încercărilor de înregistrare eşuate şi cu resetarea parolelor uitate, în locul gestionării întreprinderii.

Problema gestionării registrelor utilizator multiple afectează de asemenea dezvoltatorii de aplicaţii care doresc să furnizeze aplicaţii pe mai multe niveluri sau eterogene. Aceşti dezvoltatori înţeleg că clienţii au date importante de afaceri răspândite pe mai multe tipuri de sisteme diferite, cu fiecare sistem procesând propriile registre utilizator. Ca urmare, dezvoltatorii trebuie să creeze registre utilizator proprietare şi semantica de securitate asociate pentru aplicaţiile lor. Deşi aceasta rezolvă problema pentru dezvoltatorul de aplicaţii, aceasta sporeşte regia pentru utilizatori şi administratori.

Abordările curente

Sunt disponibile mai multe abordări curente ale industriei pentru rezolvarea problemei gestionării de registre utilizator multiple, dar toate dintre acestea furnizează soluţii incomplete. De exemplu, LDAP (Lightweight Directory Access Protocol) furnizează o soluţie de registru utilizator distribuit. Totuşi, utilizând LDAP (sau alte soluţii populare ca Microsoft Passport) înseamnă că administratorii trebuie să mai gestioneze încă un registru utilizator şi semanticile de securitate sau trebuie să înlocuiască aplicaţiile existente care sunt construite pentru a utiliza acele registre utilizator.

Utilizând acest tip de soluţie, administratorii trebuie să gestioneze mecanisme de securitate multiple pentru resurse individuale, de aceea crescând regia administrativă şi mărind potenţial posibilitatea expunerilor de securitate. Atunci când mai multe mecanisme suportă o singură resursă, probabilitatea de modificare a autorizării printr-un mecanism şi omiterea modificării autorizării pentru unul sau mai multe dintre celelalte mecanisme este mult mai mare. De exemplu, o expunere de securitate se poate produce atunci când unui utilizator i se interzice corespunzător accesul prin intermediul unei interfeţe, dar i se permite accesul prin intermediul uneia sau mai multor interfeţe.

După terminarea acestei sarcini, administratorii îşi dau seama că nu au rezolvat complet problema. În general, întreprinderile au investit prea mulţi bani în registrele utilizator curente şi în semanticile de securitate asociate acestora pentru a face practică utilizarea acestui tip de soluţie. Crearea unui alt registru utilizator şi a semanticilor de securitate asociate rezolvă problema pentru furnizorul de aplicaţii, dar nu şi problemele pentru utilizatori şi administratori.

O altă soluţie posibilă este utilizarea unei abordării cu înregistrare unică. Sunt disponibile mai multe produse care permit administratorilor să gestioneze fişiere care conţin toate identităţile şi parolele utilizator. Totuşi, această abordare are câteva slăbiciuni:

- Se adresează doar unei probleme cu care se confruntă utilizatorii. Deşi permite utilizatorilor să se înregistreze pe mai multe sisteme prin furnizarea unei singure identităţi şi parole, nu elimină nevoia ca utilizatorul să aibă parole pe alte, sau nevoia de gestionare a acestor parole.
- Aceasta introduce o problemă nouă prin crearea unei expuneri de securitate deoarece în aceste fişiere sunt stocate parole în text clar sau decriptabile. Parolele nu trebuie să fie stocate niciodată în fişiere în text clar sau să fie accesibile oricui, inclusiv administratorilor.

- Nu rezolvă problemele dezvoltatorilor de aplicaţii de la o a treia parte care furnizează aplicaţii eterogene, pe mai multe niveluri. Aceştia trebuie să furnizeze în continuare registre utilizator proprietare pentru aplicaţiile lor.

În ciuda acestor slăbiciuni, unele întreprinderi au ales să adopte acest abordări deoarece acestea furnizează unele uşurări pentru problemele cu registrele utilizator multiple.

Abordarea EIM

EIM furnizează o abordare nouă pentru a oferi posibilitatea unor soluţii necostisitoare pentru a gestiona uşor registrele utilizator multiple şi identităţile dintr-o întreprindere. EIM este o arhitectură pentru descrierea relaţiilor dintre persoane sau entităţi (ca servere de fişiere şi server de imprimare) din întreprindere şi numeroasele identităţi care le reprezintă pe acestea în cadrul întreprinderii. În plus, EIM furnizează un set de API-uri care permit aplicaţiilor pună întrebări despre aceste relaţii.

De exemplu, fiind dată identitatea utilizator a unei persoane dintr-un registru utilizator, puteţi determina ce identitate utilizator dintr-un alt registru utilizator reprezintă aceiaşi persoană. Dacă utilizatorul s-a autentificat cu o identitate utilizator şi puteţi mapa această identitate utilizator într-un alt registru utilizator, utilizatorul nu mai are nevoie să furnizeze acreditări pentru a se autentifica din nou. Cunoaşteţi cine este utilizatorul şi trebuie să cunoaşteţi doar ce identitate utilizator îl reprezintă pe acel utilizator într-un alt registru utilizator. De aceea, EIM furnizează o funcţie de mapare de identităţi generalizată pentru întreprindere.

Posibilitatea de mapare între identităţile utilizatorului din registre utilizator diferite furnizează numeroase avantaje. În principal, înseamnă că aplicaţiile pot avea flexibilitatea utilizării unui singur registru utilizator pentru autentificare în timp ce utilizează un registru utilizator cu totul diferit pentru autorizare. De exemplu, un administrator poate mapa o identitate SAP (sau şi mai bine, SAP poate face singur maparea) pentru a accesa resursele SAP.

Utilizarea mapării identităţilor necesită ca administratorii să realizeze următoarele:

1. Crearea identificatorilor EIM care reprezintă persoane sau entităţi din întreprinderea lor.
2. Crearea definiţiilor de registru EIM care descriu registrele utilizator existente în întreprinderea lor.
3. Definirea relaţiei dintre identităţile utilizator din acele registre şi identificatorii EIM pe care i-au creat.

Nu sunt necesare modificări de cod pentru registrele utilizator existente. Administratorul nu trebuie să aibă mapări pentru toate identităţile dintru registru utilizator. EIM permite mapări unul la mai mulţi (cu alte cuvinte, un singur utilizator cu mai mult de o identitate utilizator într-un singur registru utilizator). EIM permite de asemenea mapări mai mulţi la unul (cu alte cuvinte, mai mulţi utilizatori partajând un singur utilizator). Un administrator poate reprezenta în EIM orice registru utilizator de orice tip.

EIM este o arhitectură deschisă pe care administratorii o pot utiliza pentru a reprezenta relaţii de mapare a identităţilor pentru orice registru. Nu necesită copierea datelor existente într-un nou depozit şi încercarea de a le ţine sincronizate. Singurele date noi pe care le introduce EIM sunt informaţiile despre relaţii. Administratorii gestionează aceste date într-un director LDAP, ceea ce furnizează flexibilitatea gestionării datelor într-un singur loc şi realizarea de replici oriunde este utilizată informaţia. În final, EIM furnizează întreprinderilor şi dezvoltatorilor de aplicaţii flexibilitatea de a lucra uşor într-o gamă largă de medii cu un cost mai scăzut decât cel care ar fi posibil fără acest suport.

Concepte EIM

O înţelegere conceptuală a modului în care lucrează EIM (Enterprise Identity Mapping - Mapare identitate în întreprindere) este necesară pentru a înţelege complet modul în care puteţi folosi EIM în întreprinderea dumneavoastră. Deşi configurarea şi implementarea API-urilor EIM pot fi diferite pe platforme de servere diferite, conceptele EIM sunt aceleaşi pe platformele IBM

.

Figura 1 furnizează un exemplu de implementare EIM într-o întreprindere. Trei servere sunt clienţi EIM şi conţin aplicaţii bazate pe EIM care cer date EIM folosind operaţii de căutare

6

. Controlerul de domeniu

1

conţine informaţii despre domeniul EIM

2

, care includ un identificator EIM

3

, asocieri

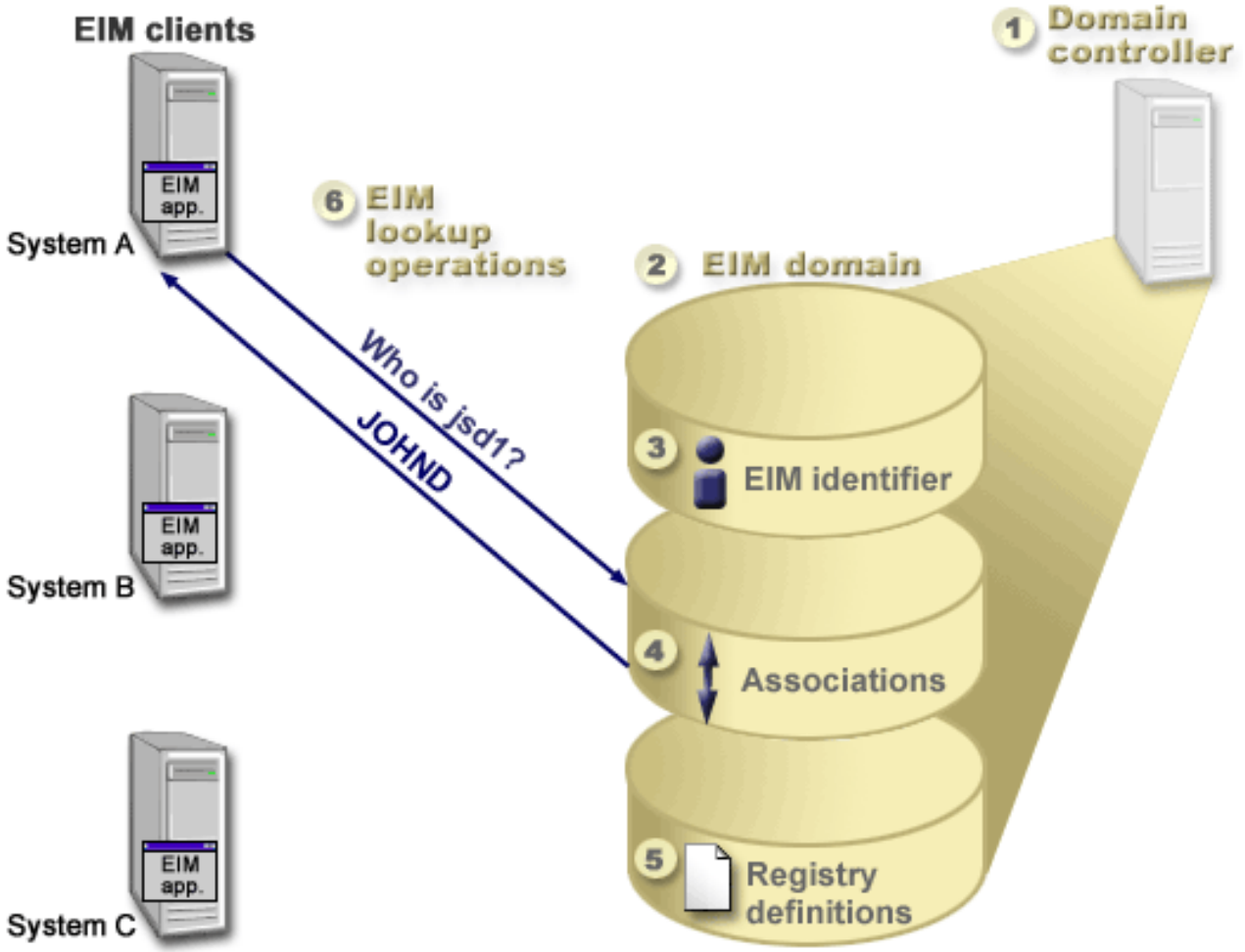
4

între aceşti identificatori EIM şi definiţii de regiştri EIM

5

.

Figura 1: Un exemplu de implementare EIM



Revedeţi informaţiile următoare pentru a învăţa mai multe despre conceptele EIM:

- Controler de domeniu EIM
- Domeniu EIM
- Identificator EIM
- Definiţii de regiştri EIM
- Asocieri EIM
- Operaţii de căutare EIM
- Autorizări EIM

Controlerul de domeniu EIM

Controlerul de domeniu EIM este un server LDAP (Lightweight Directory Access Protocol) care este configurat pentru a gestiona cel puţin un domeniu EIM. Un *domeniu EIM* este un director LDAP care constă din toţi identificatorii EIM, toate asocierile EIM şi din toate registrele utilizator care sunt definite în acest domeniu. Sistemele (clienţi EIM) participă în domeniul EIM prin utilizarea datelor de domeniu pentru operaţii de căutare EIM. În întreprindere trebuie să existe minim un controler de domeniu.

Curent, puteţi configura unele platforme IBM

pentru a se comporta ca un controler de domeniu EIM. Orice sistem care suportă API-urile EIM poate participa ca un client în domeniu. Aceste sisteme client utilizează API-urile EIM pentru a contacta controlerul de domeniu EIM pentru a efectua operaţii de căutare EIM.

Locaţia clientului EIM determină dacă controlerul de domeniu EIM este un sistem local sau la distanţă. Controlerul de domeniu este *local* dacă clientul EIM rulează pe acelaşi sistem cu controlerul de domeniu. Controlerul de domeniu este *la distanţă* dacă clientul EIM rulează pe un sistem separat de cel al controlerului de domeniu.

Domeniul EIM

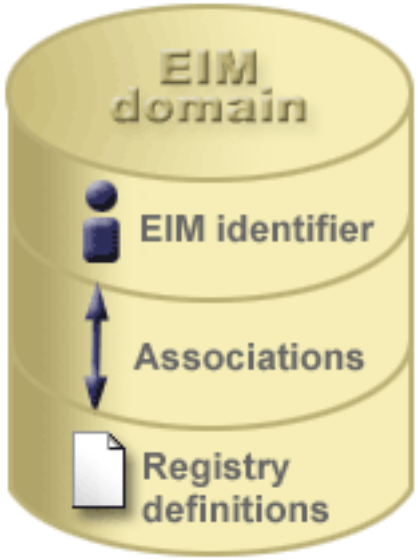
Un *domeniu EIM* este un director în cadrul unui server LDAP (Lightweight Directory Access Protocol) care conţine datele EIM pentru o întreprindere. Un domeniu EIM este colecţia tuturor identificatorilor EIM, asocierilor EIM şi a registrelor utilizator care sunt definite în domeniu. Sistemele (clienţi EIM) participă în domeniu prin utilizarea datelor de domeniu pentru operaţii de căutare EIM.

Un domeniu EIM este diferit de un registru utilizator. Un registru utilizator defineşte un set de identităţi utilizator cunoscute şi crezute de o instanţă particulară a unui sistem de operare sau a unei aplicaţii. U n registru utilizator conţine de asemenea informaţiile necesare pentru autentificarea utilizatorului identităţii. Suplimentar, un registru utilizator conţine de obicei alte atribute cum ar fi preferinţele utilizator, privilegiile sistem sau informaţii personale pentru acea identitate.

În contrast, un domeniu EIM se *referă* la identităţile utilizator care sunt definite în registrele utilizator. Un domeniu EIM conţine informaţii despre *relaţiile* dintre identităţile din diferite registre utilizator (nume utilizator, tip registru şi instanţă registru) şi persoanele sau identităţile adevărate pe care le reprezintă aceste identităţi. Deoarece EIM urmăreşte doar informaţiile despre relaţii, nu există nimic de sincronizat între registrele utilizator şi EIM.

Figura 2 prezintă datele care sunt memorate în cadrul domeniul EIM. Aceste date includ identificatorii EIM, definiţiile de registre EIM şi asocierile EIM. Datele EIM definesc relaţiile dintre identităţile utilizator persoanele sau entităţile pe care le reprezintă aceste identităţi într-o întreprindere.

Figura 2: Domeniul EIM şi datele care sunt memorate în cadrul domeniului



Datele EIM includ:

- **Identificatorii EIM.** Fiecare identificator EIM pe care îl creţi reprezintă o persoană sau o entitate (ca un server de imprimante sau un server de fişiere) din cadrul unei întreprinderi. Vedeţi Identificatori EIM pentru informaţii suplimentare.
- **Definiţii registre EIM.** Fiecare registru EIM pe care îl creţi reprezintă un registru utilizator real (şi informaţiile de identitate utilizator pe care le conţine) care există în cadrul unui sistem din întreprindere. Odată ce definiţi un numit registru utilizator în EIM, acel registru utilizator poate participa în domeniul EIM. Vedeţi Definiţii de registru EIM pentru informaţii suplimentare.
- **Asocieri EIM.** Fiecare asociere EIM pe care o creaţi reprezintă relaţia dintre un identificator EIM şi o identitate asociată în cadrul întreprinderii. Creaţi asocieri pentru identităţile din registrele utilizator care participă la domeniul EIM. Asocierile furnizează informaţiile care leagă identificatorul EIM de o anumită identitate utilizator dintr-un anumit registru utilizator. Ca urmare, este necesar ca asocierile să fie definite astfel încât clienţii EIM să poată utiliza API-urile EIM pentru a efectua cu succes operaţii de căutare EIM. Aceste operaţii de căutare EIM caută într-un domeniu EIM asocierile definite între identificatorii EIM şi identităţile utilizator din registrele utilizator recunoscute. Vedeţi Operaţii de căutare EIM pentru informaţii suplimentare.

Odată ce aţi creat identificatorii EIM, definiţiile de registre şi asocierile, puteţi începe să utilizaţi EIM pentru a organiza şi lucra mai uşor cu identităţile din cadrul întreprinderii dumneavoastră.

Identificatorul EIM

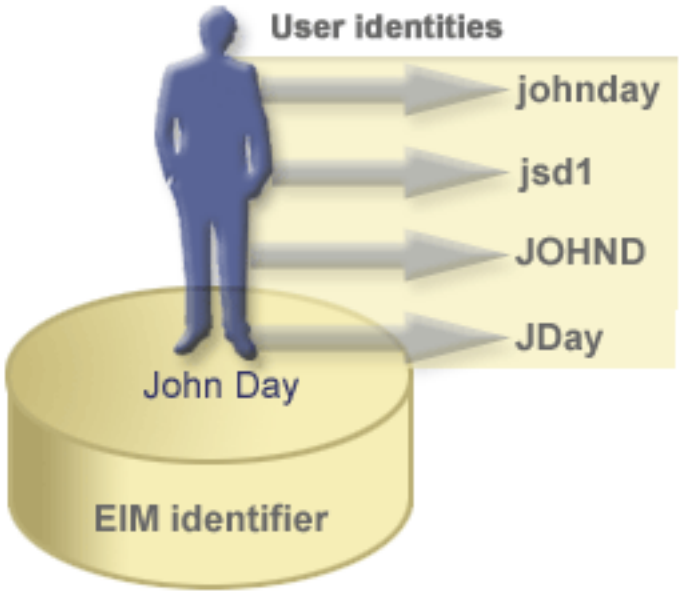
Un *identificator EIM* reprezintă o persoană sau o entitate din între prindere. O reţea obişnuită este alcătuită din diferite platforme hardware şi aplicaţii şi registrele utilizator asociate acestora. Majoritatea platformelor şi multe dintre aplicaţii utilizează registre utilizator specifice platformei sau specifice aplicaţiei. Aceste registre utilizator conţin toate informaţiile de identificare a utilizatorilor pentru utilizatorii care lucrează cu aceste server sau aplicaţii.

Atunci când creaţi un identificator EIM şi îl asociaţi cu diferitele identităţi utilizator pentru o persoană sau pentru o entitate, devine mai uşoară construirea de aplicaţii eterogene, pe mai multe niveluri, de exemplu, un mediu cu înregistrare unică. Atunci când creaţi un identificator EIM şi asocieri, devine de asemenea mai uşor să construiţi şi să utilizaţi unelte care simplifică administrarea implicată în gestionarea fiecărei identităţi utilizator pe care o are o persoană sau o entitate din cadrul întreprinderii.

Identificatorul EIM care reprezintă o persoană

Figura 3 prezintă un exemplu de identificator EIM care reprezintă o persoană numită *John Day* şi diferitele sale identităţi utilizator dintr-o întreprindere. În acest exemplu, persoana *John Day* are patru identităţi utilizator în patru registre utilizator diferite: johnday, jsd1, JOHND şi JDay.

Figura 3: Relaţiile dintre identificatorii EIM pentru *John Day* diferitele sale identităţi utilizator

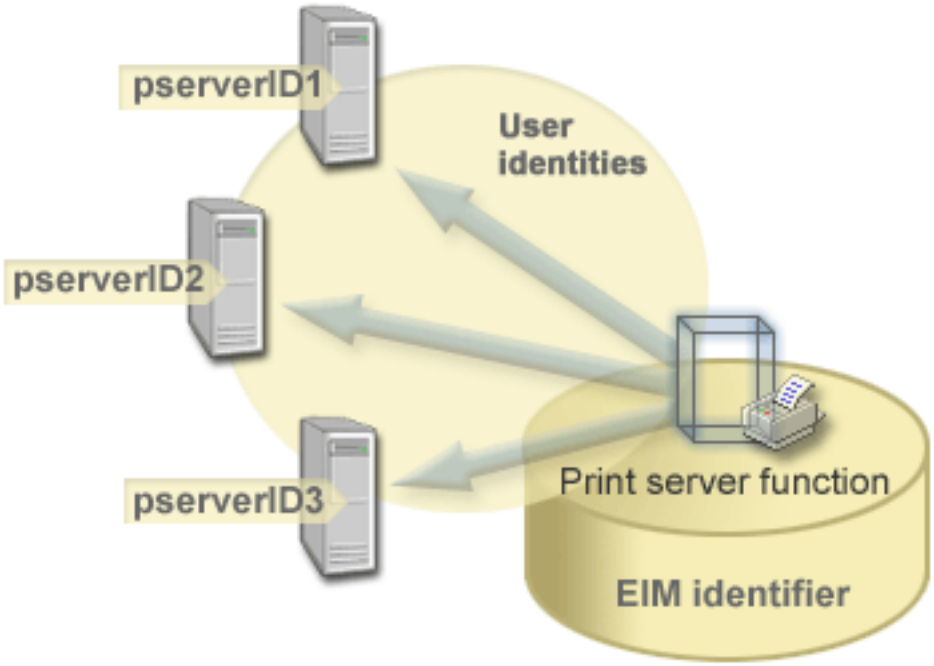


În EIM, puteţi crea asocieri care definesc relaţiile dintre identificatorul lui John Day şi fiecare dintre diferitele identităţi utilizator pentru *John Day*. Prin crearea acestor asocieri pentru a defini acest relaţii, dumneavoastră sau alte persoane puteţi acrie aplicaţii care utilizează API-urile EIM pentru căutarea unei identităţi utilizator necesară, dar necunoscută, pe baza unei identităţi utilizator cunoscute.

Identificatorul EIM care reprezintă o entitate

În plus faţă de reprezentarea utilizatorilor, identificatorii EIM pot reprezenta entităţi din cadrul întreprinderii dumneavoastră aşa cu ilustrează Figura 4. De exemplu, funcţia de server de imprimante dintr-o întreprindere rulează adesea pe mai multe sisteme. În Figura 4, funcţia de server de imprimante din întreprindere rulează pe trei sisteme diferite sub trei identităţi utilizator diferite, pserverID1, pserverID2 şi pserverID3.

Figura 4: Relaţia dintre identificatorul EIM care reprezintă funcţia de server de imprimante şi diferitele identităţi utilizator pentru acea funcţie



Cu EIM, puteţi crea un singur identificator care reprezintă funcţia de server de imprimante din cadrul întregii întreprinderi. În acest exemplu, identificatorul EIM funcţie server imprimante reprezintă entitatea reală cu funcţia de server de imprimante din întreprindere. Asocierile sunt create pentru a defini relaţiile dintre identificatorul EIM (funcţie server imprimante) şi fiecare dintre identităţile utilizator pentru această funcţie pserverID1, pserverID2 şi pserverID3). Aceste asocieri permit dezvoltatorilor de aplicaţii să utilizeze operaţiile de căutare EIM pentru a găsi o anumită funcţie server de imprimare. Furnizorii de aplicaţii pot scrie apoi aplicaţii distribuite care gestionează mai uşor funcţia server de imprimare din cadrul întreprinderii.

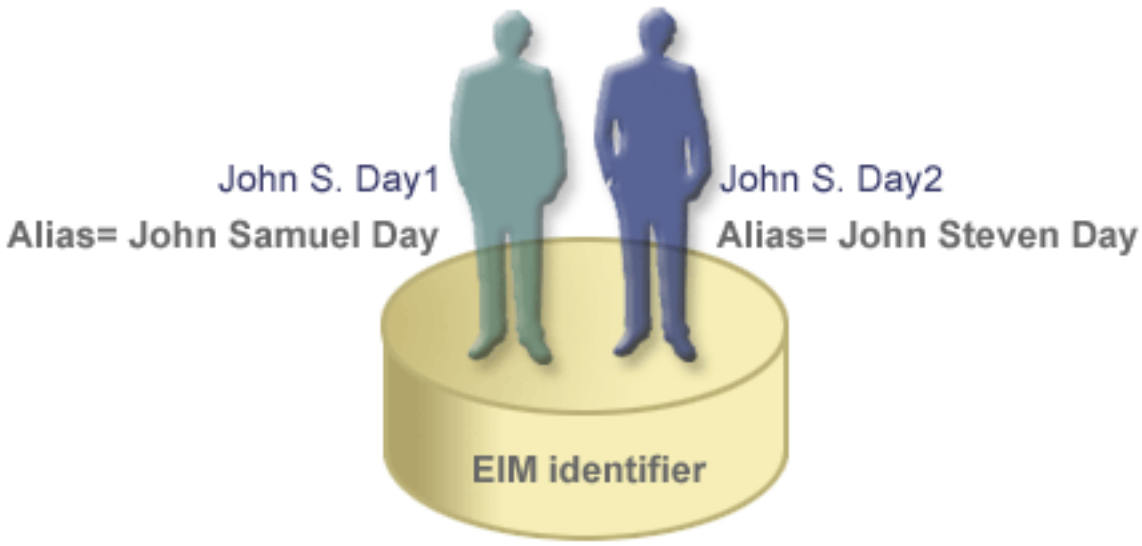
Identificatori EIM şi crearea de alias-uri

Puteţi crea de asemenea alias-uri pentru identificatorii EIM. Alias-urile pot ajuta la localizarea unui anumit identificator EIM la efectuarea unei operaţii de căutare EIM. De exemplu, alias-urile pot fi utile în situaţiile în care numele legal al cuiva este diferit de numele cu care este cunoscută acea persoană.

Numele de i9dentificatori EIM trebuie să fie unice în cadrul unui domeniu EIM. Alias-urile pot ajuta în situaţiile de adresare unde utilizarea de nume de identificatori unice poate fi dificilă. De exemplu, persoane diferite din cadrul unei întreprinderi pot împărţi acelaşi nume, ceea ce poate fi confuz dacă utilizaţi numele proprii ca identificatori EIM.

Figura 5 ilustrează un exemplu în care o întreprindere are doi utilizatori care se numesc *John S. Day*. Administratorul EIM a creat doi identificatori EIM diferiţi pentru a face distincţia între aceştia: John S. Day1 şi John S. Day2. Totuşi, care dintre *John S. Day* este reprezentat prin fiecare dintre aceşti identificatori nu este imediat aparent.

Figura 5: Alias-uri pentru doi identificatori EIM pe baza aceluiaşi nume propriu *John S. Day*



Prin utilizarea de alias-uri, administratorul EIM poate furniza informaţii suplimentare despre persoana pentru fiecare identificator EIM. Aceste informaţii pot fi de asemenea utilizate într-o operaţie de căutare EIM pentru a face diferenţa între utilizatorii pe care îi reprezintă identificatorul. De exemplu, alias-ul pentru John S. Day1 poate fi John Samuel Day iar alias-ul pentru John S. Day2 poate fi John Steven Day.

Fiecare identificator EIM poate avea mai multe alias-uri pentru a identifica pe care dintre *John S. Day* îl reprezintă identificatorul EIM. Administratorul EIM poate adăuga un alt alias pentru fiecare dintre identificatorii EIM pentru cei două persoane pentru a le distinge mai bine între ale. De exemplu, alias-urile suplimentare pot conţine numărul de angajat, numărul departamentului, profesia fiecărui utilizator sau un alt atribut distinctiv.

Definiţii de registre EIM

O *definiţie de registru EIM* reprezintă un registru utilizator real care există pe un sistem din carul întreprinderii. Un registru utilizator funcţionează asemănător unui director care conţine o listă a identităţilor utilizator valide pentru un anumit sistem sau pentru o anumită aplicaţie. Un registru utilizator de bază conţine identităţile utilizator şi parolele acestora. Un exemplu de registru utilizator este registrul z/OS Security Server Resource Access Control Facility (RACF(R)). Registrele utilizator pot de asemenea conţine alte informaţii. De exemplu, un director LDAP (Lightweight Directory Access Protocol) conţine nume distinctive de asociere, parole şi controale de acces la datele care sunt stocate în LDAP. Alte exemple de registre utilizator uzuale sunt un centru de distribuţie de chei Kerberos (KDC) şi registrul de profiluri utilizator OS/400.

Definiţiile de registru EIM furnizează informaţii cu privire la acele registre utilizator dintr-o întreprindere. Administratorul defineşte aceste registre pentru EIM prin furnizarea informaţiilor următoare:

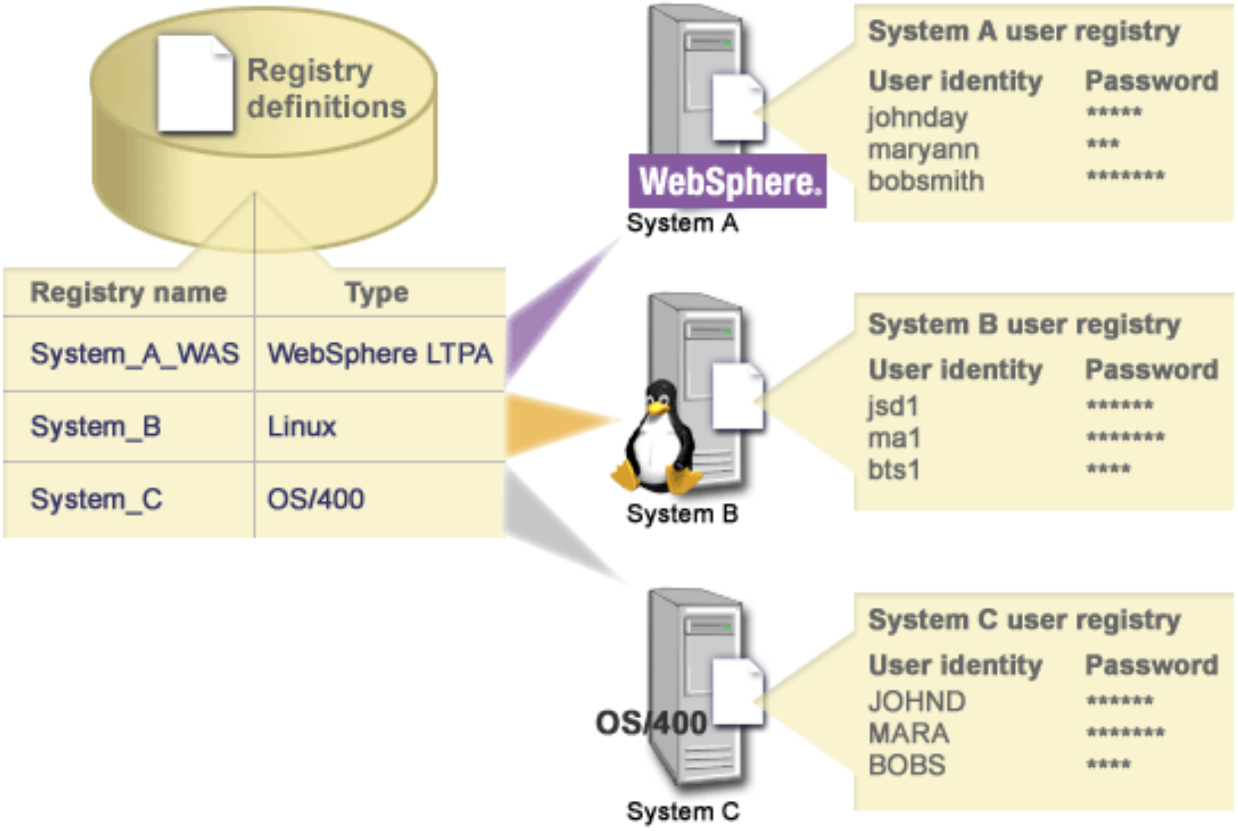
- Un nume de registru EIM unic, arbitrar
- Tipul registrului utilizator

Fiecare definiţie de registru reprezintă o anumită instanţă a unui registru utilizator. Ca urmare, ar trebui să alegeţi un nume de definiţie de registru EIM care să vă ajute să identificaţi instanţa particulară a registrului utilizator. De exemplu, aţi putea alege numele de gazdă TCP/IP pentru un registru utilizator al unui sistem sau numele de gazdă combinat cu numele aplicaţiei pentru un registru utilizator de aplicaţie. Puteţi utiliza orice combinaţie de caractere alfanumerice, litere mari amestecate cu litere mici şi spaţii pentru a crea nume unice de definiţii de registru utilizator.

În Figura 6, administratorul a creat definiţii de registru EIM pentru registrele utilizator reprezentând sistemul A, sistemul B şi sistemul C. De exemplu, sistemul A conţine un registru utilizator pentru WebSphere

Lightweight Third-Party Authentication (LTPA). Numele definiţiei de registru pe care îl utilizează administratorul ajută la identificarea anumitei apariţii a tipului de registru utilizator. De exemplu, o adresă IP sau un nume de gazdă este adesea suficient pentru multe tipuri de registre utilizator. În acest exemplu, administratorul identifică instanţa registrului utilizator specifică prin utilizarea System_A_WAS ca numele definiţiei de registru. În plus faţă de nume, administratorul furnizează de asemenea tipul registrului ca WebSphere LTPA.

Figura 6: Definiţii de registre EIM pentru trei registre utilizator dintr-o întreprindere



Puteţi defini de asemenea registre utilizator care exista în cadrul altor registre utilizator. De exemplu, registrul Security Server (RACF) al z/OS poate conţine anumite registre utilizator care sunt un subset al utilizatorilor din cadrul întregului registru utilizator RACF. Pentru un exemplu mai detaliat despre cum funcţionează aceasta, vedeţi Definiţii de registru aplicaţie şi sistem.

Definiţii de registru EIM şi asocieri

De asemenea puteţi crea alias-uri pentru definiţiile de registru EIM. Puteţi utiliza tipuri de alis-uri predefinite sau vă puteţi defini propriile alias-uri pentru a le utiliza. Tipurile de alias-uri predefinite includ:

- nume de gazdă DNS (Domain Name System)
- domeniu Kerberos
- Nume distinctiv (DN) iniţial
- Nume distinctiv (DN) rădăcină
- adresă TCP/IP
- nume de gazdă DNS LDAP

Acest suport pentru alias-uri permite programatorilor să scrie aplicaţii fără să cunoască de la început numele arbitrar al registrului EIM ales de către administratorul care instalează aplicaţia. Documentaţia aplicaţiei poate furniza administratorului EIM numele de alias pe care îl utilizează aplicaţia. Utilizând această informaţie, administratorul EIM poate atribui acest nume de alias definiţiei registrului EIM care reprezintă registrul utilizator real pe care administratorul doreşte ca aplicaţia să îl utilizeze.

Atunci când administratorul adaugă alias-ul la definiţia registrului EIM, aplicaţia poate efectua o căutare de alias pentru a găsi numele registrului EIM la iniţializare. Căutarea de alias permite aplicaţiei să determine numele registrului sau registrelor EIM pe care să le utilizeze ca intrare pentru API-urile care efectuează operaţii de căutare EIM.

Definiţii de registru aplicaţie sau sistem

Unele aplicaţii utilizează un subset al identităţilor utilizator în cadrul unei singure instanţe a unui registru utilizator. EIM permite administratorilor să modeleze acest scenariu prin furnizarea a două tipuri de definiţii de registru EIM: sistem şi aplicaţie.

O **definiţie de registru sistem** reprezintă un registru distinct în cadrul unei staţii de lucru sau server. Puteţi crea o definiţie de registru sistem atunci când registrul din întreprindere are unele dintre caracteristicile următoare:

- Registrul este furnizat de către un sistem de operare, cum ar fi AIX(R), OS/400(R) sau de către un produs de gestiune a securităţii cum ar fi z/OS Security Server Resource Access Control Facility (RACF(R)).
- Registrul conţine identităţile utilizator care sunt unice pentru o anumită aplicaţie, cum ar fi Lotus Notes(R).
- Registrul conţine identităţi utilizator distribuite, cum ar fi principalii Kerberos sau numele distinctive Lightweight Directory Access Protocol (LDAP).

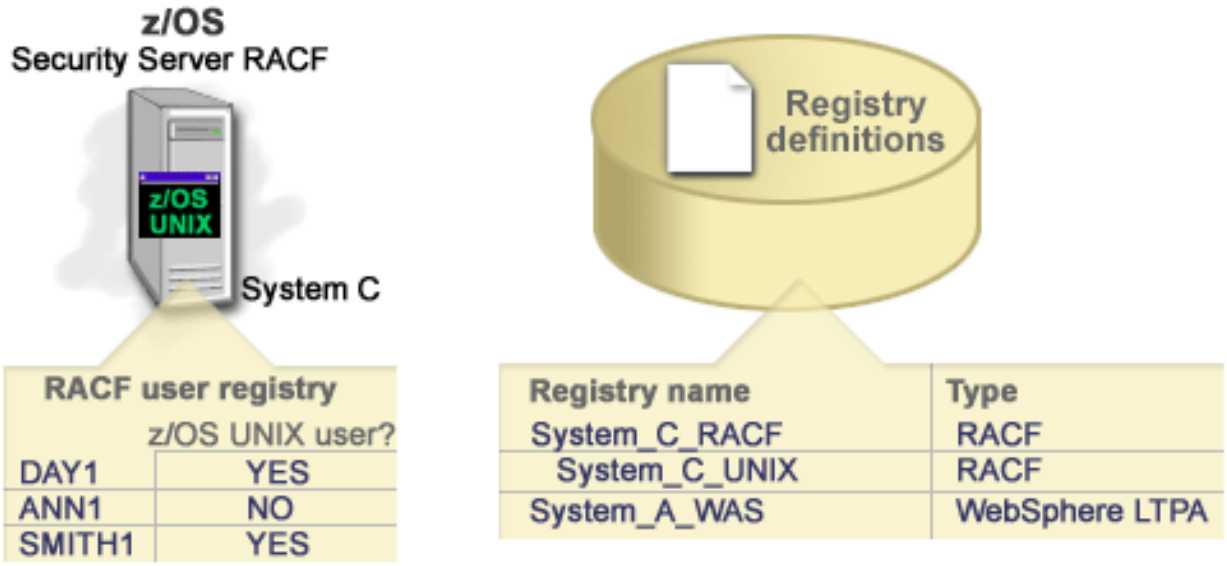
O **definiţie de registru aplicaţie** reprezintă un subset al identităţilor utilizator care sunt definite într-un registru sistem. Aceste identităţi utilizator partajează un set comun de atribute sau caracteristici care le permit să utilizeze o anumită aplicaţie sau un set de aplicaţii. Puteţi crea o definiţie de registru aplicaţie atunci când identităţile utilizator au următoarele caracteristici:

- Identităţile utilizator pentru aplicaţie sau pentru setul de aplicaţii nu sunt memorate într-un registru utilizator specific aplicaţiei sau setului de aplicaţii.
- Identităţile utilizator pentru aplicaţie sau pentru setul de aplicaţii nu sunt memorate într-un registru sistem care conţine identităţi utilizator pentru alte aplicaţii.

Operaţiile de căutare EIM se realizează corect indiferent dacă un administrator EIM defineşte un registru fie ca sistem, fie ca aplicaţie. Totuşi, definiţiile de registru separate permit ca datele de mapare să fie gestionate pe baza de aplicaţie. Responsabilitatea gestionării mapărilor specific aplicaţiei poate fi alocată unui administrator pentru un registru specific.

De exemplu, Figura 7 prezintă cum a creat un administrator EIM o definiţie de registru sistem pentru a reprezenta un registru RACF z/OS Security Server. Administratorul a creat de asemenea o definiţie de registru aplicaţie pentru a reprezenta identităţile utilizator din cadrul registrului RACF care utilizează UNIX System Services (z/OS UNIX)z/OS. Sistemul C conţine un registru utilizator RACF care conţine informaţii pentru trei identităţi utilizator, DAY1, ANN1 şi SMITH1. Două dintre aceste identităţi utilizator (DAY1 şi SMITH1) accesează UNIX z/OS de pe sistemul C. Aceste identităţi utilizator sunt în realitate utilizatori RACF cu atribute unice care în identifică pe aceştia ca utilizatori UNIX z/OS. Cu definiţiile de registre EIM, administratorul EIM a definit System_C_RACF pentru a reprezenta întregul registru utilizator RACF. Administratorul a definit de asemenea System_C_UNIX pentru a reprezenta identităţile utilizator care au atribute UNIX z/OS.

Figura 7: Definiţii registru EIM pentru registrul utilizator RACF şi pentru utilizatorii UNIX z/OS



Asocieri EIM

O *asociere EIM* este o relaţie între un identificator EIM care reprezintă o anumită persoană şi o singură identitate de utilizator dintr-un registru utilizator care reprezintă de asemenea acea persoană. Atunci când creaţi asocieri între un identificator EIM şi toate identităţile unei persoane sau entităţi, furnizaţi o înţelegere singulară, completă a modului în care acea persoană sau entitate foloseşte resursele din întreprindere. EIM furnizează API-uri care permit aplicaţiilor să găsească identitatea unui utilizator necunoscut într-un registru utilizator specific (destinaţie) prin furnizarea unei identităţi de utilizator cunoscute în alte registre utilizator (sursă). Acest proces se numeşte *mapare identitate*.

Înainte de a crea o asociere, trebuie să creaţi mai întâi identificatorul EIM corespunzător şi definiţia de registru EIM corespunzătoare pentru registrul utilizator care conţine identitatea utilizatorului asociat. O asociere defineşte o relaţie între un identificator EIM şi o identitate de utilizator prin folosirea următoarelor informaţii:

- Nume de identificator EIM
- Nume de identitate utilizator
- Nume de definiţie registru EIM
- Tip de asociere

Un administrator poate creat tipuri diferite de asocieri între un identificator EIM şi un utilizator pe baza modului în care este folosită identitatea utilizatorului. Identităţile utilizatorului pot fi folosite pentru autentificare, autorizare sau ambele.

Autentificarea este procesul de verificare a faptului că o entitate sau persoană care furnizează o identitate de utilizator are dreptul de a-şi asuma acea identitate. Verificarea este realizată deseori prin forţarea acelei persoane care lansează identitatea utilizatorului de a furniza informaţii secrete asociate cu identitatea utilizatorului, cum ar fi o parolă.

Autorizarea este procedeul de asigurare a faptului că o identitate de utilizator autentificată corect poate efectua doar funcţii sau poate accesa resurse pentru care identitatea a primit privilegii. În trecut, aproape toate aplicaţiile erau forţate să folosească identităţile utilizatorilor într-un singur registru utilizator atât pentru autentificare cât şi pentru autorizare. Prin folosirea operaţiilor de căutare EIM, aplicaţiile pot folosi acum

identităţile utilizatorilor dintr-un registru utilizator pentru autentificare în timp ce se folosesc identităţi de utilizator dintr-un registru utilizator diferit pentru autorizare.

În EIM, există trei tipuri de asocieri pe care le poate defini un administrator între un identificator EIM şi o identitate utilizator. Aceste tipuri sunt sursă, destinaţie şi administrativ.

Asociere sursă

Atunci când o identitate utilizator este folosită pentru *autentificare*, acea identitate utilizator ar trebui să aibă o asociere sursă cu un identificator EIM. O asociere sursă permite identităţii utilizatorului să fie folosită ca sursă într-o operaţie de căutare EIM pentru a găsi o identitate de utilizator diferită care este asociată cu acelaşi identificator EIM. Dacă o identitate utilizator doar cu o asociere sursă este folosită ca identitate destinaţie într-o operaţie de căutare EIM, nu este returnată nici o identitate utilizator asociată.

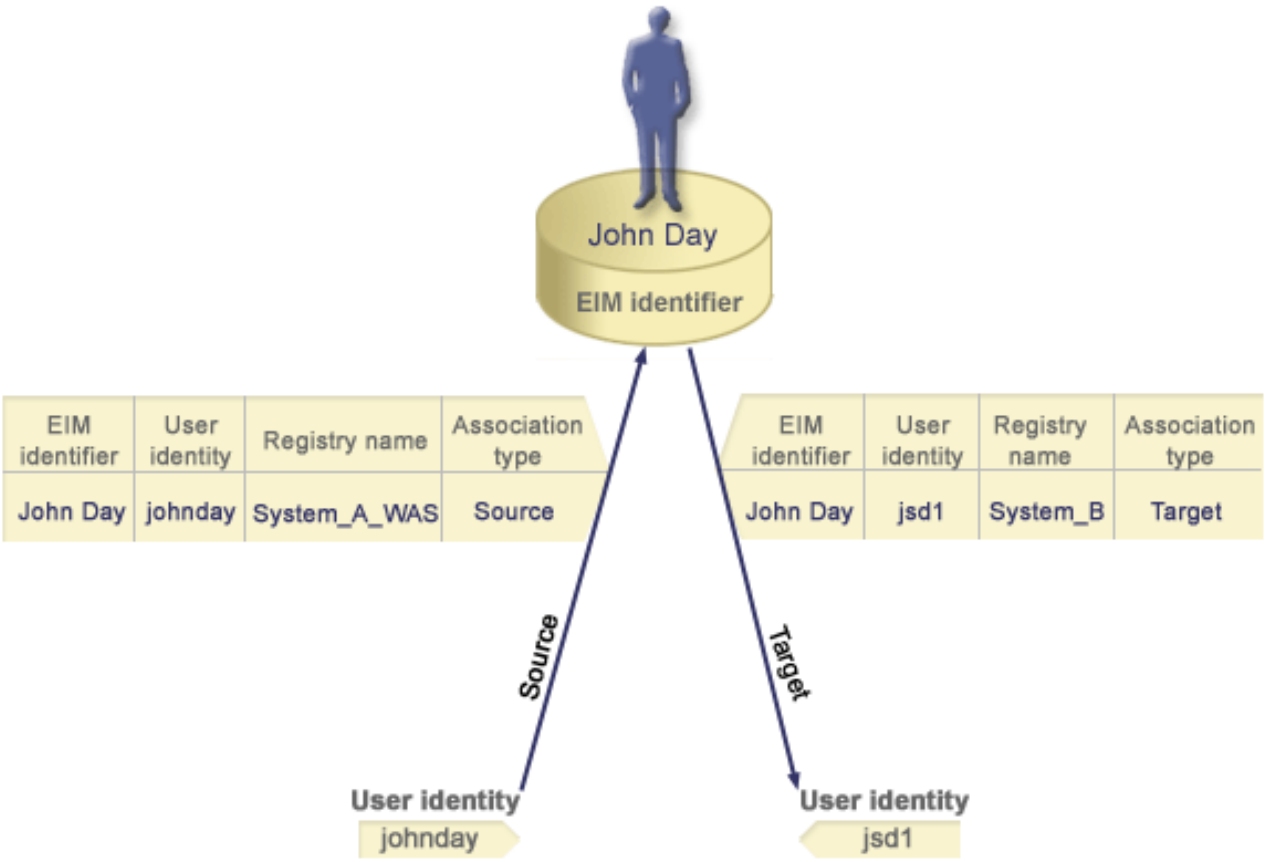
Asociere destinaţie

Atunci când o identitate utilizator este folosită pentru mai degrabă pentru *autorizare* decât pentru autentificare, acea identitate utilizator ar trebui să aibă o asociere destinaţie cu un identificator EIM. O asociere destinaţie permite identităţii utilizator să fie returnată ca rezultat al unei operaţii de căutare EIM. Dacă o identitate utilizator doar cu o asociere destinaţie este folosită ca identitate sursă într-o operaţie de căutare EIM, nu este returnată nici o identitate de utilizator asociată.

Este posibil să fie nevoie să fie create atât asociere destinaţie cât şi sursă pentru o singură identitate utilizator. Aceasta este necesar atunci când o persoană foloseşte un singur sistem atât ca client cât şi ca server sau pentru persoane care sunt administratori. De exemplu, un utilizator se autentifică în mod normal pe o platformă Windows şi rulează aplicaţii care accesează un server AIX. Din cauza responsabilităţilor slujbei utilizatorului, acesta trebuie să se log-eze uneori direct la serverul AIX. În această situaţie ar trebuie să creaţi atât o asociere sursă cât şi una destinaţie între identitatea de utilizator pe AIX şi identificatorul EIM al persoanei. Identităţile utilizator care reprezintă utilizatori finali au nevoie în mod normal doar de o asociere destinaţie.

Figura 6 arată un exemplu de asociere sursă şi destinaţie. În acest exemplu, administratorul a creat două asocieri pentru identificatorul EIM John Day pentru a defini relaţia între acest identificator şi două identităţi utilizator asociate. Administratorul a creat o asociere sursă pentru johnday, identitatea utilizator WebSphere Lightweight Third-Party Authentication (LTPA) din registrul utilizator System_A_WAS. Administratorul a creat de asemenea o asociere destinaţie pentru jsd1, profilul de utilizator OS/400 din registrul utilizator System B. Aceste asocieri furnizează pentru aplicaţii o metodă de a obţine o identitate de utilizator necunoscut (destinaţia, jsd1) pe baza unei identităţi de utilizator cunoscute (sursa, johnday) ca parte a unei operaţii de căutare EIM.

Figura 6: Asocieri destinaţie şi sursă EIM pentru identificatorul EIM John Day



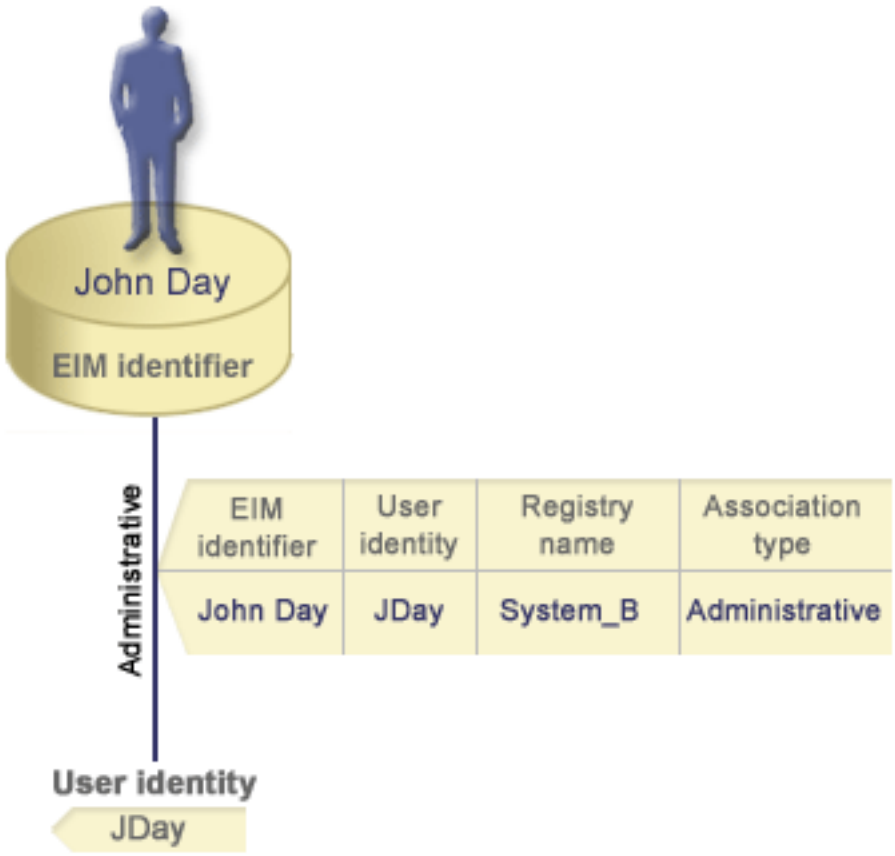
Asociere administrativă

O asociere administrativă pentru un identificator EIM este folosită de obicei pentru a arăta că persoana sau entitatea reprezentată de către identificatorul EIM deţine o identitate utilizator care necesită consideraţii speciale pentru un anumit sistem. Acest tip de asociere poate fi folosit, de exemplu, cu regiştri utilizator foarte sensibili.

Datorită naturii unei asocieri administrative, o operaţie de căutare EIM care furnizează o identitate utilizator sursă cu o asociere administrativă nu întoarce rezultate. Similar, o identitate utilizator cu o asociere administrativă nu este întoarsă niciodată ca rezultat al unei operaţii de căutare EIM.

Figura 7 arată un exemplu de asociere administrativă. În acest exemplu, John Day are o identitate utilizator pe Sistemul A şi o altă identitate utilizator pe Sistemul B, care este un sistem securizat. Administratorul de sistem doreşte să se asigure că utilizatorii se autentifică pe sistemul B folosind doar registrul utilizator local al sistemului. Administratorul nu doreşte să permită unei aplicaţii să autentifice pe John Day pe sistem prin folosirea unor mecanisme de autentificare străine. Prin folosirea asocierii administrative pentru identitate utilizator JDay pe Sistemul B, administratorul EIM poate vedea că John Day deţine un cont pe Sistemul B, dar EIM nu întoarce informaţii despre identitatea JDay în operaţiile de căutare EIM. Chiar dacă aplicaţiile există pe acest sistem care foloseşte operaţiuni de căutare EIM, nu pot găsi identităţi utilizator care au asocieri administrative.

Figura 7: Asocierea administrativă EIM pentru identificatorul EIM John Day



Operaţiile de căutare EIM

O *operaţie de căutare EIM* este un proces prin care o aplicaţie sau un sistem de operare găseşte o identitate utilizator asociată necunoscută într-un anumit registru destinaţie prin furnizarea unor informaţii cunoscute şi de încredere. Aplicaţiile care utilizează API-urile EIM pot efectua aceste operaţii de căutare EIM de informaţii doar dacă aceste informaţii sunt memorate în domeniul EIM. O aplicaţie poate efectua unul dintre cele două tipuri de operaţii de căutare EIM în funcţie de tipul informaţiilor pe care le furnizează aplicaţia ca sursă a operaţiei de căutare EIM: o identitate utilizator sau un identificator EIM.

Atunci când o aplicaţie furnizează *o identitate utilizator ca sursă*, aplicaţia trebuie să furnizeze de asemenea numele definiţiei de registru EIM pentru identitatea utilizator sursă şi numele definiţiei de registru EIM care este destinaţia operaţiei de căutare EIM. Pentru a fi utilizată ca sursă a unei operaţii de căutare EIM, o identitate utilizator trebuie să aibă definită o asociere sursă.

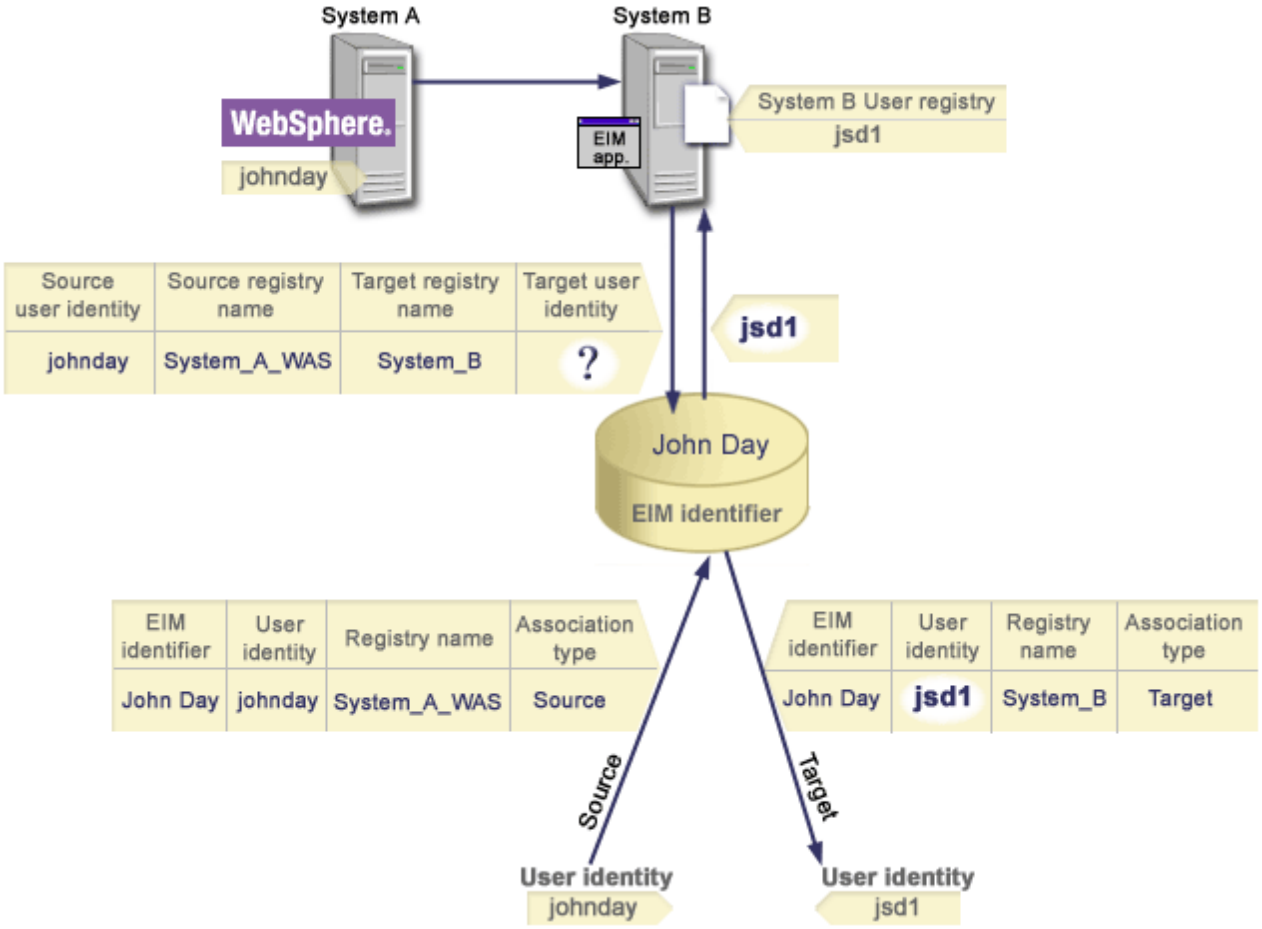
Atunci când o aplicaţie furnizează *un identificator EIM ca sursă* a operaţiei de căutare EIM, aplicaţia trebuie să furnizeze de asemenea numele definiţiei de registru EIM care este destinaţia operaţiei de căutare EIM. Pentru ca o identitate utilizator să fie returnată ca destinaţie a oricărui tip de operaţie de căutare EIM, identitatea utilizator trebuie să aibă definită o asociere destinaţie.

Informaţiile furnizate sunt transmise controlerului de domeniu EIM unde sunt stocate toate informaţiile EIM, iar operaţia de căutare EIM caută asocierea sursă care se potriveşte cu informaţiile furnizate. Pe baza identificatorului EIM (furnizat API-ului sau determinat din informaţiile despre asocierea sursă), operaţia de căutare EIM caută apoi o asociere destinaţie pentru acel identificator care se potriveşte cu numele definiţiei de registru EIM destinaţie.

În Figura 10, identitatea utilizator johnday se autentifică către Serverul de aplicaţii Websphere utilizând LPTA (Lightweight Third-Party Authentication) de pe sistemul A. Serverul de aplicaţii Websphere de pe sistemul A

apelează un program nativ de pe sistemul B pentru a accesa date de pe sistemul B. Programul nativ utilizează un API EIM pentru a efectua o operaţia de căutare EIM pe baza identităţii utilizator de pe sistemul A ca sursă a operaţiei. Aplicaţia furnizează următoarele informaţii pentru a efectua operaţia: johnday ca identitatea utilizator sursă, System_A_WAS ca numele definiţiei de registru EIM sursă şi System_B ca numele definiţiei de registru EIM destinaţie. Aceste informaţii sursă sunt transmise controlerului de domeniu EIM, iar operaţia de căutare EIM găseşte o asociere sursă care se potriveşte cu aceste informaţii. Utilizând numele identificatorului EIM, operaţia de căutare EIM caută o asociere destinaţie pentru identificatorul John Day care se potriveşte cu numele definiţiei de registru EIM destinaţie pentru System_B. Atunci când se găseşte asocierea destinaţie care se potriveşte, operaţia de căutare EIM întoarce către aplicaţie identitatea utilizator jsd1.

Figura 10: Operaţie de căutare EIM pe baza identităţii utilizator cunoscute johnday



Autorizări EIM

Autorizările EIM permit unui utilizator să efectueze anumite operaţii administrative sau operaţii de căutare EIM. Doar utilizatorii cu autorizarea de administrator EIM pot acorda sau revoca autorizări pentru alţi utilizatori. Autorizările EIM sunt acordate doar identităţilor utilizator care sunt cunoscute controlerului de domeniu EIM.

În continuare sunt prezentate descrieri succinte ale funcţiilor pe care le poate efectua fiecare grup de autorizări EIM:

- **Administrator LDAP (Lightweight Directory Access Protocol).** Această autorizare permite utilizatorului să configureze un domeniu EIM nou. Un utilizator cu această autorizare poate efectua funcţiile următoare:

  - Crearea unui domeniu
  - Ştergerea unui domeniu
  - Crearea şi eliminarea de identificatori EIM
  - Crearea şi înlăturarea unei definiţii de registru EIM
  - Crearea şi înlăturarea de asocieri sursă, destinaţie şi administrative
  - Efectuarea de operaţii de căutare EIM
  - Extragerea de asocieri, identificatori EIM şi de definiţii de registru EIM
  - Adăugarea, înlăturarea şi listarea informaţiilor despre autorizarea EIM
- **Administrator EIM.** Această autorizare permite utilizatorului să gestioneze toate datele EIM din cadrul acelui domeniu EIM. Un utilizator cu această autorizare poate efectua funcţiile următoare:
  - Ştergerea unui domeniu
  - Crearea şi eliminarea de identificatori EIM
  - Crearea şi înlăturarea unei definiţii de registru EIM
  - Crearea şi înlăturarea de asocieri sursă, destinaţie şi administrative
  - Efectuarea de operaţii de căutare EIM
  - Extragerea de asocieri, identificatori EIM şi de definiţii de registru EIM
  - Adăugarea, înlăturarea şi listarea informaţiilor despre autorizarea EIM
- **Administrator identificatori EIM** Această autorizare permite utilizatorului să adauge şi să modifice identificatori EIM şi să gestioneze asocieri sursă şi administrative. Un utilizator cu această autorizare poate efectua funcţiile următoare:
  - Crearea unui identificator EIM
  - Adăugarea şi eliminarea de asocieri sursă
  - Adăugarea şi eliminarea de asocieri administrative
  - Efectuarea de operaţii de căutare EIM
  - Extragerea de asocieri, identificatori EIM şi de definiţii de registru EIM
- **Căutare mapări EIM.** Această autorizare permite utilizatorului să coordoneze operaţii de căutare EIM. Un utilizator cu această autorizare poate efectua funcţiile următoare:
  - Efectuarea de operaţii de căutare EIM
  - Extragerea de asocieri, identificatori EIM şi de definiţii de registru EIM
- **Administrator registre EIM.** Această autorizare permite utilizatorului să gestioneze toate definiţiile de registru EIM. Un utilizator cu această autorizare poate efectua funcţiile următoare:
  - Adăugarea şi eliminarea de asocieri destinaţie
  - Efectuarea de operaţii de căutare EIM
  - Extragerea de asocieri, identificatori EIM şi de definiţii de registru EIM
- **Administrator registru EIM X.** Această autorizare permite utilizatorului să gestioneze o anumită definiţie de registru EIM. Această autorizare permite unui utilizat să:
  - Adauge şi să înlăture asocieri destinaţie pentru definiţia de registru EIM
  - Să efectueze de operaţii de căutare EIM
  - Să extragă asocieri, identificatori EIM şi de definiţii de registru EIM

Fiecare dintre tabelele următoare sunt organizate după operaţia EIM pe care o efectuează API-ul. Fiecare tabel prezintă fiecare API EIM, diferitele autorizări EIM şi accesul pe care au fiecare dintre aceste autorizări la anumite funcţii EIM.

Tabelul 1: Gestionarea de domenii

API EIM	Administrator LDAP	Administrator EIM	Administrator identificatori EIM	Căutare mapări EIM	Administrator registre EIM	Administrator registru EIM X
eimChangeDomain	X	X	-	-	-	-
eimCreateDomain	X	-	-	-	-	-
eimDeleteDomain	X	X	-	-	-	-
eimListDomains	X	X	-	-	-	-

Tabelul 2: Gestionarea identificatorilor

API EIM	Administrator LDAP	Administrator EIM	Administrator identificatori EIM	Căutare mapări EIM	Administrator registre EIM	Administrator registru EIM X
eimAddIdentifier	X	X	X	-	-	-
eimChangeIdentifier	X	X	X	-	-	-
eimListIdentifiers	X	X	X	X	X	X
eimRemoveIdentifier	X	X	-	-	-	-

Table 3: Gestionarea registrelor

API EIM	Administrator LDAP	Administrator EIM	Administrator identificatori EIM	Căutare mapări EIM	Administrator registre EIM	Administrator registru EIM X
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	-	-	-	-

Tabelul 4: Gestionarea asocierilor

Pentru API-urile eimAddAssociation() şi eimRemoveAssociation() sunt patru parametri care determină tipul de asociaţie care este adăugată sau eliminată. Autorizările pentru aceste API-uri diferă în funcţie de tipul de asociere specificat în aceşti parametri. În tabelul următor, tipul asocierilor este inclus pentru fiecare dintre aceste API-uri.

API EIM	Administrator LDAP	Administrator EIM	Administrator identificatori EIM	Căutare mapări EIM	Administrator registre EIM	Administrator registru EIM X
eimAddAssociation (administrative)	X	X	X	-	-	-
eimAddAssociation (sursă)	X	X	X	-	-	-
eimAddAssociation (sursă şi dest.)	X	X	X	-	X	X
eimAddAssociation (dest.)	X	X	-	-	X	X
eimListAssociations	X	X	X	X	X	X
eimRemoveAssociation (administrativ)	X	X	X	-	-	-
eimRemoveAssociation (sursă)	X	X	X	-	-	-
eimRemoveAssociation (sursă şi dest.)	X	X	X	-	X	X
eimRemoveAssociation (dest.)	X	X	-	-	X	X

Table 5: Gestionarea mapărilor

API EIM	Administrator LDAP	Administrator EIM	Administrator identificatori EIM	Căutare mapări EIM	Administrator registre EIM	Administrator registru EIM X
eimGetAssociatedIdentifier	X	X	X	X	X	X
eimGetTargetFromIdentifier	X	X	X	X	X	X
eimGetTargetFromSource	X	X	X	X	X	X

Table 6: Gestionarea accesului

API EIM	Administrator LDAP	Administrator EIM	Administrator identificatori EIM	Căutare mapări EIM	Administrator registre EIM	Administrator registru EIM X
eimAddAccess	X	X	-	-	-	-
eimListAccess	X	X	-	-	-	-
eimListUserAccess	X	X	-	-	-	-
eimQueryAccess	X	X	-	-	-	-
eimRemoveAccess	X	X	-	-	-	-

Concepte LDAP pentru EIM

Maparea identităţilor din întreprindere (EIM) utilizează un server LDAP (Lightweight Directory Access Protocol) ca controler de domeniu EIM pentru a stoca datele EIM. Puteţi utiliza numele distinctive LDAP când configuraţi EIM pentru serverul dumneavoastră iSeries şi ca o modalitate de autentificare cu controlerul de domeniu EIM.

Pentru a utiliza numele distinctive LDAP când configuraţi şi administraţi EIM, trebuie să înţelegeţi următoarele concepte LDAP:

- Nume distinctiv LDAP
- Nume distinctiv părinte LDAP

Nume distinctiv LDAP

Un nume distinctiv (DN) LDAP este o intrare LDAP (Lightweight Directory Access Protocol) care identifică şi descrie un utilizator autorizat pentru un server LDAP. Utilizaţi vrăjitorul Configurare EIM pentru a configura serverul LDAP să memoreze informaţiile de domeniu EIM. Puteţi utiliza numele distinctive LDAP ca o modalitate de a accesa şi extrage aceste date EIM pentru ca serverul dumneavoastră iSeries să poată participa într-un mediu de înregistrare unică.

Numele distinctive constau din însuşi numele intrării, cât şi din numele, in ordine de jos in sus, obiectelor de deasupra sa din directorul LDAP. Un exemplu de nume distinctiv LDAP complet ar putea fi cn=Tim Jones, o=IBM, c=US. Fiecare intrare are cel puţin un atribut care este utilizat pentru a denumi intrarea. Acest atribut de denumire este numit nume distinctiv relativ (RDN) al intrării. Intrarea de deasupra unui anumit RDN este denumită nume distinctiv părinte al său. În acest exemplu, cn=Tim Jones denumeşte intrarea, deci este RDN-ul. o=IBM, c=US este DN-ul părinte pentru cn=Tim Jones.Vedeţi Nume distinctiv părinte LDAP pentru a învăţa mai multe despre cum le utilizează EIM pe acestea.

Deoarece EIM utilizează serverul LDAP pentru a memora datele EIM, puteţi utiliza numele distinctive LDAP ca un mijloc de autentificare pentru controlerul de domeniu EIM. De asemenea, puteţi utiliza numele distinctive LDAP la configurarea EIM pentru serverul dumneavoastră iSeries. De exemplu, puteţi utiliza numele distinctive LDAP când:

- Configuraţi serverul LDAP pentru a se comporta ca controler de domeniu EIM. Realizaţi aceasta prin crearea şi utilizarea numelui distinctiv LDAP care identifică administratorul LDAP pentru serverul LDAP. Dacă serverul LDAP nu a fost configurat ulterior, puteţi configura serverul LDAP când utilizaţi vrăjitorul Configurare EIM pentru a crea şi a uni un domeniu nou.
- Utilizaţi vrăjitorul Configurare EIM pentru a selecta tipul identităţii utilizatorului pe care trebuie să îl utilizeze vrăjitorul pentru a se conecta la controlerul de domeniu EIM. Numele distinctiv este unul dintre tipurile de utilizatori pe care le puteţi selecta. Numele distinctiv LDAP trebuie să reprezinte un utilizator care este autorizat pentru a crea obiecte în spaţiul de nume local al serverului LDAP.
- Utilizaţi vrăjitorul Configurare EIM pentru a selecta tipul utilizatorului care să efectueze operaţii EIM în numele funcţiilor sistemului de operare. Aceste operaţii includ căutări de mapări şi asocieri de ştergere la ştergerea unui profil de utilizator OS/400 local. Numele distinctiv este unul dintre tipurile de utilizatori pe care le puteţi selecta.
- Vă conectaţi la controlerul de domeniu pentru a efectua administrarea EIM, de exemplu, pentru a gestiona registrele şi identificatorii şi pentru a efectua operaţii de căutare de mapări.

Pentru a învăţa mai multe despre numele distinctive şi despre cum le utilizează LDAP, vedeţi Bazele LDAP.

Nume distinctiv părinte LDAP

Un nume distinctiv (DN) părinte LDAP este o intrare în spaţiul de nume al unui server de directoare LDAP (Lightweight Directory Access Protocol). Intrările serverului LDAP sunt aranjate intr-o structură ierarhică ce poate reflecta graniţele politice, geografice, organizaţionale sau de domeniu. Un nume distinctiv este considerat un DN părinte atunci când DN-ul este la nivelul cel mai înalt al spaţiului de nume al serverului LDAP.

Un exemplu de nume distinctiv LDAP complet ar putea fi cn=Tim Jones, o=IBM, c=US. Fiecare intrare are cel puţin un atribut care este utilizat pentru a denumi intrarea. Acest atribut de denumire este numit nume distinctiv relativ (RDN) al intrării. Intrarea de deasupra unui anumit RDN este denumită nume distinctiv părinte al său. În acest exemplu, cn=Tim Jones denumeşte intrarea, deci este RDN-ul. o=IBM, c=US este DN-ul părinte pentru cn=Tim Jones.

Deoarece EIM utilizează serverul LDAP pentru a memora datele EIM, puteţi utiliza numele distinctive LDAP ca un mijloc de autentificare pentru controlerul de domeniu EIM. De asemenea, puteţi utiliza numele distinctive LDAP şi numele distinctive părinte la configurarea EIM pentru serverul dumneavoastră iSeries. De exemplu, când utilizaţi vrăjitorul Configurare EIM pentru a crea şi pentru a uni un domeniu nou, puteţi alege să specificaţi un DN părinte pentru domeniul pe care îl creţi. Prin utilizarea unui DN părinte, puteţi specifica unde trebuie să se afle datele EIM pentru domeniu în spaţiul de nume LDAP local. Când nu specificaţi un DN părinte, datele EIM se află în sufixul propriu în spaţiul de nume.

Pentru a învăţa mai multe despre numele distinctive şi despre cum sunt utilizate acestea, vedeţi Bazele LDAP.

Posibilitatea de înregistrare unică prin intermediul EIM

EIM furnizează un mecanism necostisitor pentru posibilitatea de înregistrare unică în cadrul unei întreprinderi. Implementarea OS/400 a EIM şi Kerberos furnizează un mediu pe mai multe nivele, de înregistrare unică eterogenă adevărat. Beneficiile pentru utilizatori, pentru administratori şi pentru dezvoltatorii de aplicaţii atunci când este disponibil în întreprindere un mediu cu înregistrare unică sunt următoarele:

Beneficii pentru utilizatori
Într-un mediu cu înregistrare unică, autentificarea se produce de fiecare dată când utilizatorii încearcă să acceseze un sistem nou; totuşi, aceştia nu vor fi interogaţi pentru parole. EIM reduce necesitatea ca utilizatorii să ţină evidenţa şi să gestioneze mai multe nume de utilizator şi parole pentru a acces alte sisteme din reţea. De îndată ce un utilizator este autentificat în reţea, utilizatorul poate accesa servicii şi aplicaţii din cadrul întreprinderii fără necesitatea mai multor parole pentru aceste sisteme diferite.

Beneficii pentru administratori
Pentru un administrator, înregistrarea unică simplifică gestionarea pe ansamblu a securităţii unei întreprinderi. Fără înregistrarea unică, utilizatorii şi aplicaţiile pot stoca temporar parole pentru alte sisteme, ceea ce poate compromite securitatea întregii reţele. Administratorii cheltuiesc timp şi bani pe soluţii pentru a diminua aceste riscuri de securitate. Identificarea unică reduce regia de administrare pentru gestionarea autentificării în timp ce menţine sigură întreaga reţea. Suplimentar, identificarea unică reduce costurile administrative pentru resetarea parolelor uitate.

Beneficii pentru dezvoltatorii de aplicaţii
Pentru dezvoltatorii de aplicaţii care trebuie să ruleze în reţele eterogene, EIM furnizează infrastructura pentru a dezvolta aplicaţii care lucrează pe mai multe platforme. Prin utilizarea API-urilor EIM, programatorii pot scrie aplicaţii care utilizează registrul utilizator existent cel mai potrivit pentru autentificare în timp ce se utilizează un registru utilizator diferit pentru autorizare. Dezvoltatorii de aplicaţii nu trebuie să suporte registre utilizator specifice unei platforme în cadrul aplicaţiei pe care o creează deoarece EIM furnizează infrastructura pentru crearea de aplicaţii care mapează identităţile utilizatorului din cadrul acelor registre într-un singur registru utilizator. În plus, EIM permite programatorilor să întreţină aceste aplicaţii fără să modifice semantica de securitate asociată, iar securitatea la nivel de aplicaţie reduce semnificativ costul implementării aplicaţiilor pe mai multe niveluri, pe platforme diferite.

Posibilitatea iSeries de înregistrare unică
Pentru a activa un mediu de înregistrare unică, IBM utilizează două tehnologii care lucrează împreună: EIM şi serviciul de autentificare în reţea, care este implementarea IBM a Kerberos şi a API-urilor GSS. Prin configurarea acestor două tehnologii, un administrator poate activa un mediu de înregistrare unică. Windows 2000, XP, AIX şi zSeries utilizează protocolul Kerberos pentru a autentifica utilizatorii în reţea. Kerberos implică utilizarea unui centru de distribuţie de chei bazat pe reţea, sigur, care autentifică principalii(utilizatorii Kerberos) în reţea. Un utilizator primeşte un tichet Kerberos de la un centru de distribuţie de chei, centralizat. Acest tichet autentifică utilizatorul pentru un alt serviciu dintr-o întreprindere. Un tichet poate fi trecut de la un utilizator la un serviciu care accepta tichete. Serviciul care accepta un tichet îl utilizează pe

acesta pentru a determina cine pretinde utilizatorul că este (în cadrul registrului de utilizatori şi domeniului Kerberos) şi că aceştia sunt de fapt cine pretind că sunt.

În timp ce serviciul de autentificare în reţea permite unui server iSeries să participe într-un domeniu Kerberos, EIM furnizează un mecanism pentru asocierea acestor principali Kerberos unui singur identificator EIM care reprezintă acel utilizator în cadrul întregii întreprinderi. Alte identităţi ale utilizatorului, cum este un nume de utilizator OS/400, pot fi asociate, de asemenea, cu acest identificator EIM. Pe baza acestor asocieri, EIM furnizează un mecanism pentru OS/400 şi pentru aplicaţii de a determina ce profil de utilizator OS/400 reprezintă persoana sau entitatea reprezentată de principalul Kerberos. Vă puteţi gândi la informaţiile din EIM ca la un arbore cu un identificator EIM ca rădăcină, iar lista de identităţi utilizator asociată cu identificatorul EIM ca ramuri.

Utilizând figura de mai jos ca un exemplu, imaginaţi-vă că un utilizator, cum este John Smith, se înregistrează în reţea prin intermediul PC-ului său Windows şi accesează o instanţă a OS/400 pentru a accesa aplicaţii care suportă Kerberos. John nu este interogat pentru numele său de utilizator OS/400. Aceste aplicaţii pot căuta asocierea cu identificatorul EIM al lui John pentru a găsi numele de utilizator OS/400. John Smith nu mai are nevoie de o parolă în profilul său de utilizator OS/400 deoarece profilul de utilizator nu este utilizat pentru autentificare; acesta este utilizat doar pentru autorizare.

Figura 1. Mediu cu înregistrare unică

Subiectul, Scenariu: Activarea înregistrării unice, furnizează un exemplu despre cum configurează un administrator serviciul de autentificare în reţea şi EIM pentru a activa un mediu cu înregistrare unică.

Aplicaţiile următoare pot fi accesate prin înregistrarea unică:

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

Planificarea EIM

Tehnologiile şi serviciile pe care EIM le înglobează în serverul iSeries sunt multiple. Înainte de a configura EIM pe serverul dumneavoastră, trebuie să decideţi funcţionalitatea pe care doriţi să o implementaţi utilizând EIM şi facilităţile de înregistrare unică.

Înainte de a implementa EIM, trebuie să fi decis cerinţele de securitate de bază pentru reţeaua dumneavoastră şi să fi implementat aceste măsuri de securitate. EIM furnizează administratorilor şi utilizatorilor o modalitate mai uşoară de gestiune a identităţilor în cadrul întreprinderii.Când se utilizează împreună cu serviciul de autentificare în reţea, EIM furnizează capacităţile de înregistrare unică pentru întreprinderea dumneavoastră.

Următoarea foaie de lucru pentru planificare identifică serviciile pe care trebuie să le instalaţi înainte de a configura EIM.

Foaie de lucru pentru planificare	**Răspunsuri**
Aveţi versiunea OS/400 V5R2 (5722-SS1) sau mai recentă?	
Este instalat Cryptographic Access Provider (5722-AC3) pe serverele dumneavoastră iSeries?	
Este instalat Acces iSeries pentru Windows (5722-XE1) pe PC-urile corespunzătoare din reţeaua dumneavoastră (PC-urile utilizate pentru a lucra cu serverele iSeries) şi pe serverele dumneavoastră iSeries?	
Este instalată subcomponenta Reţea a Navigatorului iSeries pe toate PC-urile din reţea şi pe sistemele iSeries?	
Dacă este configurat curent un server LDAP şi doriţi să îl utilizaţi ca controlerul de domeniu EIM, cunoaşteţi numele distinctiv (DN) şi parola administratorului LDAP?	
Dacă este configurat curent un server LDAP, acesta poate fi oprit temporar? (Aceasta lucru va fi necesar pentru a efectua procesul de configurare EIM.)	
Aveţi autorizările speciale *SECADM, *ALLOBJ şi *IOSYSCFG?	
Aţi aplicat cele mai recente corecţii temporare de program (PTF-uri)?	

Dacă planificaţi să utilizaţi Kerberos pentru a autentifica utilizatorii, trebuie să configuraţi de asemenea serviciul de autentificare în reţea. Vedeţi Planificarea serviciului de autentificare în reţea pentru o foaie de lucru completă pentru planificarea serviciului de autentificare în reţea.

Dacă configuraţi serviciul de autentificare în reţea şi EIM pentru a activa înregistrarea unică, vedeţi Scenariu: Activarea identificării unice care prezintă o companie configurată pentru ambele dintre aceste produse.

Instalarea opţiunilor necesare pentru Navigatorul iSeries

Pentru a activa un mediu cu înregistrare unică utilizând EIM şi serviciul de autentificare în reţea, trebuie să instalaţi ambele opţiuni Reţea şi Securitate ale Navigatorului iSeries. EIM se află în cadrul opţiunii Reţea, iar serviciul de autentificare în reţea se află în cadrul opţiunii Securitate. Dacă nu planificaţi să utilizaţi serviciul de autentificare în reţea în reţeaua dumneavoastră, nu aveţi nevoie să instalaţi opţiunea Securitate a Navigatorului iSeries.

Pentru a instala opţiunea Reţea a Navigatorului iSeries sau pentru a verifica dacă aveţi această opţiune instalată curent, asiguraţi-vă că Acces iSeries pentru Windows este instalat pe PC-ul pe care îl utilizaţi pentru a lucra cu serverul iSeries.

Pentru a instala opţiunea Reţea:

1. Faceţi clic pe **Start —> Programe —> IBM Acces iSeries pentru Windows —> Setare selectivă**.
2. Urmaţi instrucţiunile din dialog. În dialogul **Selectare componente**, expandaţi **Navigator iSeries** şi apoi selectaţi opţiunea **Reţea**.
   Dacă planificaţi să utilizaţi serviciul de autentificare în reţea, trebuie să selectaţi, de asemenea, opţiunea **Securitate**.
3. Continuaţi până la terminarea Setării selective.

Configurarea serviciului de autentificare în reţea

Serviciul de autentificare în reţea vă dă posibilitatea să utilizaţi autentificarea Kerberos pe serverul dumneavoastră iSeries. Acest serviciu nu este o cerinţă preliminară pentru utilizarea EIM pe serverul dumneavoastră; totuşi, sunt multe avantaje ale utilizării autentificării Kerberos pentru securitatea reţelei dumneavoastră.

Serviciul de autentificare în reţea, când este utilizat împreună cu EIM, vă furnizează mijloacele de a activa un mediu cu înregistrare unică. Un mediu cu înregistrare unică este avantajos pentru utilizatori şi pentru administratori. Utilizatorii au nume de utilizator şi parole mai puţine şi administratorii au mai puţine informaţii de urmărit pentru fiecare utilizator. Deoarece posibilitatea de înregistrare unică ajută de asemenea la traversarea diferenţelor dintre platforme multiple şi sisteme diferite care pot exista în reţeaua dumneavoastră, costurile dezvoltării de aplicaţii şi de administrare generală pot fi reduse.

Dacă nu aveţi serviciul de autentificare în reţea configurat curent pe serverul dumneavoastră iSeries sau pe toate serverele din reţeaua dumneavoastră, vedeţi Planificarea serviciului de autentificare în reţea pentru informaţii de planificare pentru a vă ajuta să porniţi la drum. Dacă sunteţi familiarizat cu serviciul de autentificare în reţea, vedeţi Configurarea serviciului de autentificare în reţea pentru a porni procesul de configurare.

Configurarea EIM

Pentru a activa un mediu de logare singulară pe mai multe platforme fără a fi nevoie de a modifica politicile de securitate de la bază, trebuie să configuraţi EIM precum şi serviciul de autentificare în reţea. Totuşi, configurarea şi utilizarea serviciului de autentificare în reţea nu este o cerinţă preliminară sau o necesitate pentru configurarea şi folosirea EIM.

Pentru a începe procesul de configurare EIM pentru ca serverul iSeries să facă parte dintr-un mediu cu logare singulară, folosiţi vrăjitorul Configurare EIM. În funcţie de necesităţile dumneavoastră de configurare, puteţi folosi vrăjitorul fie pentru a uni un domeniu existent, fie pentru a crea şi uni un nou domeniu.

Vrăjitorul de configurare EIM vă permite să efectuaţi cu uşurinţă o configurare de bază a EIM. De exemplu, dacă nu aveţi configurat deja un server LDAP sau dacă nu aţi configurat serviciul de autentificare în reţea, vrăjitorul de configurare EIM vă permite să efectuaţi aceste task-uri.

După ce folosiţi vrăjitorul pentru a efectua configurare de bază EIM, trebuie să efectuaţi anumiţi paşi de configurare suplimentari înainte de a putea folosi un mediu cu logare singulară. Consultaţi Scenariu: Activare logare singulară pentru un exemplu care arată modul în care o companie fictivă a configurat un mediu de logare singulară folosind servicul de autentificare în reţea şi EIM.

Înainte de a folosi vrăjitorul de configurare EIM, ar trebui să fi efectuat toţi paşii de planificare pentru a determina exact modul în care veţi folosi atât EIM cât şi serviciul de autentificare în reţea pentru a activa mediul de logare singulară. Din momentul în care planificarea este terminată, puteţi folosi vrăjitorul pentru a configura EIM pentru serverul dumneavoastră iSeries într-unul din două moduri: crearea de domenii noi sau unirea domeniilor existente. Subiectele următoare furnizează instrucţiuni pentru configurarea EIM:

Crearea şi unirea unui domeniu nou
Alegeţi acest task pentru a crea un domeniu EIM pentru reţeaua dumneavoastră şi pentru a configura serverul iSeries pentru a participa în acesta. Vrăjitorul creează noul domeniu şi configurează serverul LDAP local pentru a fi controlerul de domeniu pentru noul domeniu. De asemenea, dacă Kerberos nu este configurat în mod curent pe serverul iSeries, vrăjitorul vă invită să lansaţi vrăjitorul de configurare serviciu de autentificare în reţea. După ce aţi efectuat acest task, puteţi configura alte servere iSeries pentru a participa în acest domeniu. Pentru a configura alte servere pentru a participa în domeniu, conectaţi-vă la fiecare din ele şi folosiţi vrăjitorul de configurare EIM pentru a configura un server pentru a se alătura unui domeniu EIM existent.

Unirea unui domeniu existent
După ce aţi folosit vrăjitorul de configurare EIM pentru a configura un controler de domeniu şi un domeniu EIM, alegeţi acest task pentru a configura alte servere iSeries pentru a participa în domeniu. Trebuie să efectuaţi acest task pentru fiecare server iSeries din reţea care va folosi EIM. După ce terminaţi cu vrăjitorul, trebuie să furnizaţi informaţii despre domeniul ce se uneşte, incluzând informaţii despre conexiune (cum ar fi numărul portului şi dacă să se folosească Transport Layer Security (TLS)/Secure Sockets Layer (SSL) la controlerul de domeniu EIM. Dacă Kerberos nu este configurat în mod curent pe serverul iSeries, vrăjitorul vă va invita să lansaţi vrăjitorul de configurare serviciu de autentificare în reţea.

Modul de accesare al vrăjitorului de configurare EIM

Petru a accesa vrăjitorul de configurare EIM, urmaţi aceşti paşi :

1. Porniţi iSeries Navigator.
2. Logaţi-vă la serverul iSeries pentru care doriţi să configuraţi EIM.
   Dacă configuraţi EIM pe mai mult decât un server iSeries, începeţi cu cel pe care doriţi să configuraţi controlerul de domeniu pentru EIM.
3. Expandaţi **Reţea —> Mapare identitate în întreprindere**.
4. Faceţi clic dreapta **Configurare** şi selectaţi **Configurare...** pentru a lansa vrăjitorul de configurare EIM.
5. Selectaţi fie **Unire domeniu existent**, fie **Creare şi unire a unui domeniu nou**.

După ce aţi terminat de folosit vrăjitorul de configurare EIM pentru a crea controlerul de domeniu şi pentru a configura serverul dumneavoastră iSeries pentru a participa în domeniu, trebuie să efectuaţi aceste taskuri pentru a finaliza configurarea EIM:

1. Adăugare regiştri EIM la domeniul EIM pentru servere non-iSeries şi aplicaţii care doriţi să participe în domeniul EIM.
2. Creare identificatori EIM în domeniu pentru fiecare utilizator sau entitate pentru sistemele ce participă în domeniul EIM.
3. Creare de asocieri între diferitele identităţi de utilizator ale unei persoane sau entităţi la identificatorii EIM.

Crearea şi unirea unui domeniu nou

Puteţi folosi vrăjitorul de configurare EIM pentru a configura serverul LDAP pe serverul iSeries pentru a fi controlerul de domeniu pentru un domeniu nou. Dacă este necesar, vrăjitorul de configurare EIM se asigură că furnizaţi informaţii pentru configurarea de bază a serverului LDAP.

De asemenea, dacă Kerberos nu este configurat în mod curent pe serverul iSeries, vrăjitorul vă invită să lansaţi vrăjitorul de configurare a serviciului de autentificare în reţea. Atunci când efectuaţi acest vrăjitor, este configurat un domeniu EIM nou, sistemul dumneavoastră iSeries este configurat pentru a se uni la la noul domeniu şi registrele utilizator pe care le-aţi specificat sunt adăugate la domeniu.

Pentru a folosi acest vrăjitor pentru efectuarea acestui task, trebuie să aveţi autorizările speciale Security Administrator (*SECADM), All Object (*ALLOBJ) şi System Configuration (*IOSYSCFG).

Pentru a porni şi folosi vrăjitorul de configurare EIM pentru crearea şi unirea unui domeniu EIM nou, efectuaţi aceşti paşi din iSeries Navigator:

Notă: Acest vrăjitor vă configurează de asemenea serverul LDAP local ca noul controler de domeniu.

1. Expandaţi **Reţea** —> **Mapare identitate în întreprindere**. .
2. Faceţi clic dreapta **Configurare** şi selectaţi **Configurare...** pentru a lansa vrăjitorul de configurare EIM.
3. Pe pagina de **Bun venit** a vrăjitorului, selectaţi **Creare şi unire a unui domeniu nou** şi apoi apăsaţi **Următor**.
4. Dacă serviciul de autentificare în reţea nu este configurat în mod curent pe serverul iSeries, este afişat dialogul **Configurarea serviciilor de autentificare în reţea** . Acest dialog vă invită să selectaţi dacă să configuraţi serviciul de autentificare în reţea. Dacă selectaţi **Da**, se lansează vrăjitorul de configurare a serviciului de autentificare în reţea. După ce efectuaţi configurarea serviciului de autentificare în reţea, continuă vrăjitorul de configurare EIM.
5. Dacă serverul LDAP nu este configurat, apare dialogul **Configurarea Directory Server**. Furnizaţi informaţiile următoare în dialog pentru a configura serverul LDAP local.
   - În câmpul **Port**, acceptaţi numărul de port implicit **389**sau introduceţi un număr de port diferit pentru folosirea comunicaţiilor EIM nesigure cu directory server.
   - În câmpul **Nume distinctiv**, introduceţi numele distinctiv (distinguished name - DN) LDAP care identifică administratorul LDAP pentru serverul LDAP. Vrăjitorul de configurare EIM creează acest DN de administrator LDAP şi îl foloseşte pentru a configura serverul LDAP drept controler de domeniu pentru domeniul pe care îl creaţi.
   - În câmpul **Parolă**, introduceţi parola pentru administratorul LDAP.
   - În câmpul **Confirmare parolă**, reintroduceţi parola.
   - Faceţi clic pe **Următor**.
6. În dialogul **Specificaţi controlerul de domeniu**, furnizaţi informaţiile următoare:
   - În câmpul **Domeniu**, specificaţi numele domeniului EIM pe care doriţi să-l creaţi. Acceptaţi numele implicit al **EIM** sau folosiţi orice şir de caractere care vă convin. Totuşi, nu puteţi folosi caractere speciale cum ar fi = + < > , # ; \ şi *.
   - În câmpul **Descriere**, introduceţi un text de descriere a domeniului.
   - Faceţi clic pe **Următor**.
7. În dialogul **Specificaţi DN-ul părintelui domeniului**, selectaţi dacă să specificaţi un DN părinte pentru domeniul pe care îl creaţi. Prin specificarea unui părinte DN, puteţi specifica unde să se afle datele EIM spaţiu de nume al serverului LDAP pentru domeniu. Atunci când nu specificaţi un părinte DN, datele EIM se află în propriul sufix din spaţiul de nume. Dacă selectaţi **Da**, folosiţi caseta listă pentru a selecta sufixul LDAP de folosire ca DN părinte sau introduceţi text pentru a crea şi numi un nou DN părinte. Nu este necesar să specificaţi un DN părinte pentru noul domeniu.
8. În dialogul **Specificaţi utilizatorul pentru conexiune**, selectaţi un **tip de utilizator** pentru conexiune. Puteţi selecta unul din următoarele tipuri de utilizatori: Nume distinctiv şi parolă, Keytab Kerberos şi

principal sau Principal Kerberos şi parolă. Cele două tipuri de utilizatori Kerberos sunt disponibile doar dacă este configurat serviciul de autentificare în reţea pentru sistemul iSeries local. Tipul de utilizator pe care îl selectaţi determină celelalte informaţii pe care trebuie să le furnizaţi pentru a efectua dialogul care urmează:

- Dacă aţi selectat **Nume distinctiv şi parolă**, furnizaţi următoarele informaţii:
  - În câmpul **Nume distinctiv**, introduceţi numele distinctiv LDAP (DN) c are identifică utilizatorul care este autorizat să creeze obiecte în spaţiul de nume local al serverului LDAP. Dacă aţi folosit acest vrăjitor pentru a configura serverul LDAP într-un pas anterior, ar trebuie să introduceţi numele distinctiv al administratorului LDAP pe care l-aţi creat în acel pas.
  - În câmpul **Parolă**, introduceţi parola pentru utilizator.
  - În câmpul **Confirmare parolă**, reintroduceţi parola.
- Dacă aţi selectat **Keytab Kerberos şi principal**, furnizaţi următoarele informaţii :
  - În câmpul **Fişier keytab**, introduceţi numele fişierului keytab de pe serverul iSeries care identifică utilizatorul care este autorizat să creeze obiecte în spaţiul de nume local al serverului LDAP. Sau puteţi apăsa **Răsfoire** pentru a selecta fişierul keytab.
  - În câmpul **Principal**, introduceţi numele principal-ului Kerberos de folosit pentru a identifica utilizatorul.
  - În câmpul **Regiune**, introduceţi numele regiunii pentru principal. Numele principalului şi al regiunii ce identifică în mod unic utilizatorii Kerberos din fişierul keytab. De exemplu, principalul jsmith din regiunea ordept.myco.com este reprezentat în fişierul keytab ca jsmith@ordept.myco.com.
- Dacă selectaţi **Principal Kerberos şi parolă**, furnizaţi informaţiile următoare:
  - În câmpul **Principal**, introduceţi numele principalului Kerberos care identifică utilizatorul care este autorizat să creeze obiecte în spaţiul de nume local al serverului LDAP.
  - În câmpul **Regiune**, introduceţi numele regiunii Kerberos pentru principal.
  - În câmpul **Parolă**, introduceţi parola pentru utilizator.
  - În câmpul **Confirmare parolă**, reintroduceţi parola.Numele principalului şi al regiunii ce identifică în mod unic utilizatorii Kerberos din fişierul keytab. De exemplu, principalul jsmith din regiunea ordept.myco.com este reprezentat în fişierul keytab ca jsmith@ordept.myco.com.
- Apăsaţi **Verificare conexiune** pentru a testa informaţiile de configurare utilizator pentru conexiunea la controlerul de domeniu.
- Faceţi clic pe **Următor**.

9. În dialogul **Informaţii registru**, selectaţi tipul regiştrilor utilizator pe care doriţi să-i adăugaţi în domeniul EIM. Selectaţi unul sau ambii din aceşti tipuri de regiştri utilizator:
   - Selectaţi **OS400** pentru a adăuga un registru utilizator care reprezintă registrul local la domeniul EIM. În câmpul furnizat, introduceţi numele registrului de creat în domeniu. Numele registrului EIM este un şir arbitrar care reprezintă tipul registrului şi instanţa specifică a acelui registru.
   - Selectaţi **Kerberos** pentru a adăuga un registru de utilizator Kerberos la domeniul EIM. În câmpul furnizat, introduceţi numele registrului de creat în domeniu şi selectaţi **Identităţile de utilizator Kerberos sunt sensibile la majuscule**, dacă este necesar.
   - Faceţi clic pe **Următor**.
10. În dialogul **Specificaţi utilizatorul de sistem EIM**, selectaţi tipul de utilizator care doriţi să fie folosit de sistem atunci când se efectuează operaţii EIM în numele funcţiilor sistemului de operare. Aceste operaţii includ căutări de mapare şi ştergerea asocierilor atunci când se şterge un profil de utilizator OS/400 local. Puteţi selecta unul din următoarele tipuri de utilizatori: Nume distinctiv şi parolă, Fişier keytab Kerberos şi principal sau Principal Kerberos ş i parolă. Tipul de utilizator pe care îl selectaţi determină celelalte informaţii pe care trebuie să le furnizaţi pentru a efectua dialogul care urmează:

Notă: Utilizatorul pe care îl specificaţi trebuie să aibă privilegii de efectuare a căutărilor de mapare şi administrare de registre pentru rgistrul utilizator local. Dacă utilizatorul specificat nu are aceste privilegii, atunci anumite funcţii ale sistemului de operare legate de logarea singulară şi ştergerea profilelor de utilizator ar putea eşua.

11. Dacă aţi selectat **Nume distinctiv şi parolă**, furnizaţi următoarele informaţii:
    - În câmpul **Nume distinctiv**, introduceţi numele distinctiv LDAP care identifică utilizatorul pentru OS/400 de folosit atunci când se contactează controlerul de domeniu EIM.
    - În câmpul **Parolă**, introduceţi parola pentru utilizator.
    - În câmpul **Confirmare parolă**, reintroduceţi parola.
12. Dacă selectaţi **Principal Kerberos şi parolă**, furnizaţi informaţiile următoare:
    - În câmpul **Principal**, introduceţi principalul Kerberos care identifică utilizatorul pentru OS/400 de folosit atunci când se contactează controlerul de domeniu EIM.
    - În câmpul **Regiune**, introduceţi numele regiunii Kerberos pentru principal.
    - În câmpul **Parolă**, introduceţi parola pentru utilizator.
    - În câmpul **Confirmare parolă**, reintroduceţi parola. Numele principalului şi al regiunii ce identifică în mod unic utilizatorii Kerberos din fişierul keytab. De exemplu, principalul jsmith din regiunea ordept.myco.com este reprezentat în fişierul keytab ca jsmith@ordept.myco.com.
13. Dacă aţi selectat **Keytab Kerberos şi principal**, furnizaţi următoarele informaţii :
    - În câmpul **Fişier keytab**, introduceţi numele fişierului keytab de pe serverul iSeries care identifică utilizatorul pentru OS/400 de folosit atunci când se contactează controlerul de domeniu EIM. Sau puteţi apăsa **Răsfoire** pentru a selecta fişierul keytab.
    - În câmpul **Principal**, introduceţi numele principal-ului Kerberos de folosit pentru a identifica utilizatorul.
    - În câmpul **Regiune**, introduceţi numele regiunii pentru principal. Numele principalului şi al regiunii ce identifică în mod unic utilizatorii Kerberos din fişierul keytab. De exemplu, principalul jsmith din regiunea ordept.myco.com este reprezentat în fişierul keytab ca jsmith@ordept.myco.com.
14. Apăsaţi **Verificare conexiune** pentru a testa conexiunea la controlerul de domeniu pentru utilizatorul de sistem pe care l-aţi creat.
15. Faceţi clic pe **Următor**.
16. În panoul **Rezumat**, revizualizaţi informaţiile de configurare pe care le-aţi furnizat. Dacă toate informaţiile sunt corecte, apăsaţi **Terminare**.

Atunci când vrăjitorul se termină, aţi terminat configurarea de bază a EIM. Totuşi, trebuie să efectuaţi aceste taskuri pentru a termina configurarea EIM pentru acest server.

1. Adăugarea unui domeniu pe care l-aţi creat la folderul Gestiunea domeniului.
2. Adăugarea regiştrilor EIM la domeniul EIM pentru alte servere şi aplicaţii care doriţi să participe în domeniul EIM.
3. Crearea identificatorilor EIM în domeniu pentru fiecare utilizator unic sau entitate pentru sisteme ce participă în domeniul EIM.
4. Crearea asocierilor între diferite identităţi utilizator ale unei persoane sau entităţi şi aceşti identificatori EIM.

În plus, poate doriţi să folosiţi Secure Sockets Layer (SSL) sau Transport Layer Security (TLS) pentru configurarea unei conexiuni sigure la controlerul de domeniu.

Configurarea unei conexiuni sigure la controlerul de domeniu EIM

După ce utilizaţi vrăjitorul pentru a crea şi uni un domeniu nou, este posibil să doriţi să utilizaţi SSL (Secure Sockets Layer) sau TLS (Transport Layer Security Protocol) pentru a stabili o conexiune sigură la controlerul de domeniu EIM. Pentru a configura SSL sau TLS pentru EIM, trebuie să must efectuaţi aceste operaţii:

1. Activaţi SSL pentru controlerul de domeniu server LDAP.
2. Utilizaţi DCM (Digital Certificate Manager - Manager de certificate digitale) pentru a crea certificatul de care are nevoie serverul LDAP pentru a-l utiliza pentru SSL.
3. Utilizaţi DCM pentru a atribui certificatul serverului LDAP.

4. Actualizaţi proprietăţile de Configurare EIM pentru a specifica că serverul iSeries utilizează o conexiune SSL.
5. Actualizaţi proprietăţile de Domeniu EIM pentru fiecare domeniu EIM pentru a specifica faptul că EIM utilizează o conexiune SSL când se gestionează domeniul prin intermediul Navigatorului iSeries.

Unirea unui domeniu existent

Puteţi folosi vrăjitorul de configurare EIM pentru a uni un domeniu EIM existent. Folosiţi această opţiune din vrăjitorul de configurare EIM atunci când au fost deja configurate un domeniu EIM şi un controler de domeniu în reţea. Pe măsură ce lucraţi cu vrăjitorul trebuie să furnizaţi informaţii despre domeniu, incluzând informaţii de conexiune la controlerul de domeniu EIM. Vrăjitorul memorează aceste informaţii pe serverul iSeries şi apoi le foloseşte pentru a se conecta la controlerul de domeniu EIM. Vrăjitorul creează de asemenea un registru utilizator EIM reprezentând profilul utilizator OS/400 pe acest server iSeries.

Pentru a folosi acest vrăjitor pentru efectuarea acestui task, trebuie să aveţi autorizările speciale Security Administrator (*SECADM) şi All Object (*ALLOBJ).

Pentru a porni şi folosi vrăjitorul de configurare EIM pentru unirea unui domeniu EIM existent, efectuaţi aceşti paşi folosind iSeries Navigator:

1. Expandaţi **Reţea —> Mapare identitate în întreprindere**.
2. Faceţi clic dreapta **Configurare** şi selectaţi **Configurare...** pentru a lansa vrăjitorul de configurare EIM. Atunci când vrăjitorul porneşte, furnizaţi informaţiile următoare pe măsură ce treceţi prin dialoguri.
3. În dialogul **Bun venit** al vrăjitorului, selectaţi **Unirea unui domeniu existent** şi apăsaţi **Următor**.
4. Dacă serviciul de autentificare în reţea nu este configurat în mod curent pe serverul iSeries, este afişat dialogul **Configurarea serviciilor de autentificare în reţea** . Acest dialog vă invită să selectaţi dacă să configuraţi serviciul de autentificare în reţea. Dacă selectaţi **Da**, se lansează vrăjitorul de configurare a serviciului de autentificare în reţea. După ce efectuaţi configurarea serviciului de autentificare în reţea, continuă vrăjitorul de configurare EIM.
5. La apariţia dialogului **Specificaţi controlerul de domeniu**, furnizaţi informaţiile următoare:
   - În câmpul **Nume controler de domeniu**, specificaţi numele sistemului care este controlerul de domeniu pentru domeniul EIM la care vreţi să se unească serverul iSeries.
   - Apăsaţi **Folosire Secure Sockets Layer (SSL)** dacă doriţi ca extragerea de informaţii EIM de la controlerul de domeniu să folosească SSL pentru a proteja transmisia datelor EIM.
   - Apăsaţi **Verificare conexiune** pentru a testa informaţiile de configurare ale controlerului de domeniu.

Notă: Dacă aţi specificat utilizarea SSL şi primiţi un mesaj de eroare, mesajul poate indica faptul că serverul LDAP nu a fost configurat să folosească SSL.

   - Faceţi clic pe **Următor**.
6. În dialogul **Specificaţi utilizator pentru conexiune**, selectaţi **tip de utilizator** pentru conexiune. Puteţi selecta unul din următoarele tipuri de utilizatori: Nume distinctiv şi parolă, Fişier keytab Kerberos şi principal sau Principal Kerberos şi parolă. Cele două tipuri de utilizatori Kerberos sunt disponibile doar dacă este configurat serviciul de autentificare în reţea pentru sistemul iSeries local. Tipul de utilizator pe care îl selectaţi determină celelalte informaţii pe care trebuie să le furnizaţi pentru a efectua dialogul care urmează:
   - Dacă aţi selectat **Nume distinctiv şi parolă**, furnizaţi următoarele informaţii:
     - — În câmpul **Nume distinctiv**, introduceţi numele distinctiv LDAP (DN) c are identifică utilizatorul care este autorizat să creeze obiecte în spaţiul de nume local al serverului LDAP.
     - — În câmpul **Parolă**, introduceţi parola pentru utilizator.
     - — În câmpul **Confirmare parolă**, reintroduceţi parola.
   - Dacă aţi selectat **Keytab Kerberos şi principal**, furnizaţi următoarele informaţii :

- În câmpul **Fişier keytab**, introduceţi numele fişierului keytab de pe serverul iSeries care identifică utilizatorul care este autorizat să creeze obiecte în spaţiul de nume local al serverului LDAP. Sau puteţi apăsa **Răsfoire** pentru a selecta fişierul keytab.
- În câmpul **Principal**, introduceţi numele principal-ului Kerberos de folosit pentru a identifica utilizatorul.
- În câmpul **Regiune**, introduceţi numele regiunii pentru principal. Numele principalului şi al regiunii ce identifică în mod unic utilizatorii Kerberos din fişierul keytab. De exemplu, principalul jsmith din regiunea ordept.myco.com este reprezentat în fişierul keytab ca jsmith@ordept.myco.com.

• Dacă selectaţi **Principal Kerberos şi parolă**, furnizaţi informaţiile următoare:
- În câmpul **Principal**, introduceţi numele principalului Kerberos care identifică utilizatorul care este autorizat să creeze obiecte în spaţiul de nume local al serverului LDAP.
- În câmpul **Regiune**, introduceţi numele regiunii Kerberos pentru principal.
- În câmpul **Parolă**, introduceţi parola pentru utilizator.
- În câmpul **Confirmare parolă**, reintroduceţi parola. Numele principalului şi al regiunii ce identifică în mod unic utilizatorii Kerberos din fişierul keytab. De exemplu, principalul jsmith din regiunea ordept.myco.com este reprezentat în fişierul keytab ca jsmith@ordept.myco.com.

• Apăsaţi **Verificare conexiune** pentru a testa informaţiile de configurare utilizator pentru conexiunea la controlerul de domeniu.
• Faceţi clic pe **Următor**.

7. În pagina **Specificaţi domeniul**, selectaţi numele domeniului pe care do riţi să-l uniţi şi apăsaţi **Următor**.
8. În pagina **Informaţii registru**, selectaţi tipul regiştrilor utilizator pe care doriţi să-i adăugaţi în domeniul EIM. Selectaţi unul sau ambii din aceşti tipuri de regiştri utilizator:
   • Selectaţi **OS400** pentru a adăuga un registru utilizator care reprezintă registrul local la domeniul EIM. În câmpul furnizat, introduceţi numele registrului de creat în domeniu. Numele registrului EIM este un şir arbitrar care reprezintă tipul registrului şi instanţa specifică a acelui registru.
   • Selectaţi **Kerberos** pentru a adăuga un registru de utilizator Kerberos la domeniul EIM. În câmpul furnizat, introduceţi numele registrului de creat în domeniu şi selectaţi **Identităţile de utilizator Kerberos sunt sensibile la majuscule**, dacă este necesar. Puteţi accepta valoarea implicită; numele de registru Kerberos este acelaşi cu numele regiunii. Prin folosirea aceluiaşi nume pentru numele de registru Kerberos şi pentru numele regiunii, puteţi mări performanţele în extragerea de informaţii din registru. Pentru informaţii suplimentare despre modul în care pot fi definiţi regiştrii utilizator într-un EIM, consultaţi definiţii de regiştri EIM.
   • Faceţi clic pe **Următor**.
9. În dialogul **Specificaţi utilizatorul de sistem EIM**, selectaţi tipul de utilizator care doriţi să fie folosit de sistem atunci când se efectuează operaţii EIM în numele funcţiilor sistemului de operare. Aceste operaţii includ căutări de mapare şi ştergerea asocierilor atunci când se şterge un profil de utilizator OS/400 local. Puteţi selecta unul din următoarele tipuri de utiliza tori: Nume distinctiv şi parolă, Fişier keytab Kerberos şi principal sau Principal Kerberos şi parolă. Tipul de utilizator pe care îl selectaţi determină celelalte informaţii pe care trebuie să le furnizaţi pentru a efectua dialogul care urmează:
   • Dacă aţi selectat **Nume distinctiv şi parolă**, furnizaţi următoarele informaţii:
     - În câmpul **Nume distinctiv**, introduceţi numele distinctiv LDAP care identifică utilizatorul pentru OS/400 de folosit atunci când se contactează controlerul de domeniu EIM.
     - În câmpul **Parolă**, introduceţi parola pentru utilizator.
     - În câmpul **Confirmare parolă**, reintroduceţi parola.
   • Dacă selectaţi **Principal Kerberos şi parolă**, furnizaţi informaţiile următoare:
     - În câmpul **Principal**, introduceţi principalul Kerberos care identifică utilizatorul pentru OS/400 de folosit atunci când se contactează controlerul de domeniu EIM.
     - În câmpul **Regiune**, introduceţi numele regiunii Kerberos pentru principal.
     - În câmpul **Parolă**, introduceţi parola pentru utilizator.

- În câmpul **Confirmare parolă**, reintroduceţi parola. Numele principalului şi al regiunii ce identifică în mod unic utilizatorii Kerberos din fişierul keytab. De exemplu, principalul jsmith din regiunea ordept.myco.com este reprezentat în fişierul keytab ca jsmith@ordept.myco.com.

• Dacă aţi selectat **Keytab Kerberos şi principal**, furnizaţi următoarele informaţii :
  - În câmpul **Fişier keytab**, introduceţi numele fişierului keytab de pe serverul iSeries care identifică utilizatorul pentru OS/400 de folosit atunci când se contactează controlerul de domeniu EIM. Sau puteţi apăsa **Răsfoire** pentru a selecta fişierul keytab.
  - În câmpul **Principal**, introduceţi numele principal-ului Kerberos de folosit pentru a identifica utilizatorul.
  - În câmpul **Regiune**, introduceţi numele regiunii pentru principal.
• Apăsaţi **Verificare conexiune** pentru a testa conexiunea pentru utilizatorul sistem pe care l-aţi creat.
• Faceţi clic pe **Următor**.

10. În panoul **Rezumat**, revizualizaţi informaţiile de configurare pe care le-aţi furnizat. Dacă toate informaţiile sunt corecte, apăsaţi **Terminare**.

Atunci când vrăjitorul se termină, aţi terminat configurarea de bază a EIM. Totuşi, trebuie să efectuaţi aceste taskuri pentru a termina configurarea EIM pentru acest server.

1. Adăugarea unui domeniu pe care l-aţi unit la folderul Gestiunea domeniului EIM.
2. Adăugare regiştri EIM la domeniul EIM pentru servere non-iSeries şi aplicaţii care doriţi să participe în domeniul EIM.
3. Crearea identificatorilor EIM în domeniu pentru fiecare utilizator unic sau entitate pentru sisteme ce participă în domeniul EIM.
4. Crearea asocierilor între diferite identităţi utilizator ale unei persoane sau entităţi şi aceşti identificatori EIM.

De asemenea, pentru a activa un mediu de logare singulară, trebuie să configuraţi serviciul de autentificare în reţea pentru serverul iSeries.

Gestionarea EIM

După ce aţi configurat EIM pe serverul dumneavoastră iSeries, există multe taskuri pe care le puteţi efectua pentru a gestiona domeniul şi informaţiile EIM. Subiectele următoare discută taskurile specifice folosite pentru a gestiona EIM pe serverul dumneavoastră iSeries şi în reţeaua întreprinderii.

Gestionarea domeniilor EIM
Lucrul cu informaţiile EIM conţinute în domeniul dumneavoastră EIM şi în proprietăţile domeniului EIM.

Gestionarea asocierilor
Întreţinerea asocierilor identităţilor utilizatorilor la identificatorii EIM pentru toţi utilizatorii din întreprindere.

Gestionarea identificatorilor EIM
Întreţinerea identificatorilor EIM asociaţi cu utilizatorii în întreprindere.

Gestionarea autorizărilor de utilizatori EIM
Întreţinerea securităţii informaţiilor EIM prin lucrul cu autorizările EIM pentru a controla funcţiile şi operaţiile EIM pe care le pot efectua utilizatorii.

Gestionarea regiştrilor utilizator
Lucrul cu regiştrii utilizator pe care le-aţi adăugat la domeniul dumneavoastră EIM.

Gestiunea domeniilor EIM

Puteţi folosi iSeries Navigator pentru a gestiona toate domeniile EIM. Pentru a gestiona orice domeniu EIM, domeniul trebuie să fie listat în sau trebuie adăugat în folderul Gestiunea domeniului din folderul Reţea din iSeries Navigator. După ce aţi creat şi configurat un domeniu EIM nou, trebuie să îl adăugaţi în folderul Gestiunea domeniului pentru a gestiona informaţiile din domeniu.

Puteţi folosi orie conexiune iSeries pentru a gestiona un domeniu EIM care se află oriunde în aceeaşi reţea. iSeries care este conectat la iSeries Navigator nu trebuie să fie în domeniu pentru a gestiona acel domeniu.

Puteţi efectua task-urile următoare pentru a gestiona domeniile EIM:

- Adăugarea unui domeniu la gestiunea domeniului
- Conectarea la un domeniu
- Ştergerea unui domeniu
- Înlăturarea unui domeniu din gestiunea domeniului

Adăugarea unui domeniu la gestiunea domeniului

Pentru a adăuga un domeniu, trebuie să aveţi autorizarea specială *SECADM. Pentru a adăuga un domeniu EIM existent la gestiunea domeniului, urmaţi aceşti paşi.

1. Expandaţi **Reţea —> Mapare identitate în întreprindere**.
2. Faceţi clic dreapta **Gestiunea domeniului** şi selectaţi **Adăugare domeniu...**.
3. Specificaţi domeniul cerut şi informaţiile de conexiune.
4. Apăsaţi **OK** pentru a adăuga domeniul.

Conectarea la un domeniu

Dacă nu sunteţi conectat în mod curent la un domeniu EIM cu care doriţi să lucraţi, trebuie să vă conectaţi mai întâi la domeniu. Vă puteţi conecta la un domeniu EIM chiar dacă serverul dumneavoastră iSeries nu este configurat în mod curent pentru a participa la acest domeniu.

Pentru a vă conecta la un domeniu EIM, efectuaţi paşii următori:

1. Expandaţi **Reţea —> Mapare identitate în întreprindere —> Gestiunea domeniului**.
2. Selectaţi domeniul la care doriţi să vă conectaţi. Dacă domeniul cu care doriţi să lucraţi nu este listat, trebuie să Adăugaţi un domeniu EIM la gestiunea domeniului.
3. Efectuaţi clic-dreapta pe domeniul EIM la care doriţi să vă conectaţi şi selectaţi **Conectare...**.
4. Specificaţi tipul utilizatorului şi informaţiile de utilizator necesare care ar trebui folosite pentru a vă conecta la controlerul de domeniu EIM.
5. Selectaţi **OK**.

Ştergerea unui domeniu

Pentru a efectua acest task, trebuie să aveţi fie autorizarea de administrator LDAP, fie autorizarea de administrator EIM. Înainte de ştergerea unui domeniu EIM, trebuie să ştergeţi mai întâi toţi regiştrii şi informaţiile de identificare EIM din domeniu.

Pentru a şterge un domeniu EIM, efectuaţi paşii următori.

1. Expandaţi **Reţea —> Mapare identitate în întreprindere —> Gestiunea domeniului**.
2. Înlăturaţi toţi regiştrii utilizator din domeniul EIM.
3. Ştergeţi toţi identificatorii EIM din domeniul EIM.
4. Efectuaţi clic dreapta pe domeniul pe care doriţi să îl ştergeţi şi selectaţi **Ştergere...**.
5. Apăsaţi **Da** în dialogul **Confirmare de ştergere**.

Înlăturarea unui domeniu din Gestiunea domeniului

Deşi nu este necesar, puteţi înlătura un domeniu EIM din folderul Gestiunea domeniului atunci când aţi terminat de efectuat modificări.

Pentru a înlătura un domeniu, efectuaţi paşii următori:

1. Expandaţi **Reţea —> Mapare identitate în întreprindere**.
2. Faceţi clic dreapta **Gestiunea domeniului** şi selectaţi **Înlăturare domeniu...**.
3. Selectaţi domeniul EIM pe care doriţi să-l ştergeţi din gestiunea domeniului.
4. Apăsaţi **OK** pentru a înlătura domeniul.

Gestionarea asocierilor

O asociere defineşte o relaţie între un identificator EIM şi o identitate utilizator dintr-un registru. De exemplu, puteţi crea o asociere între un profil de utilizator OS/400 sau un utilizator-director Kerberos şi un identificator EIM. Această asociere poate fi folosită apoi pentru a determina ce identificator EIM corespunde la profilul utilizator iSeries local sau la utilizatorul-director Kerberos.

Întreţinerea asocierilor identităţilor utilizatorilor cu identificatorii EIM corespunzători este cheia simplificării taskurilor administrative necesare pentru a gestiona utilizatorii care au conturi pe diferite sisteme din reţea.

Gestionarea acestor asocieri vă permite de asemenea să beneficiaţi de avantajele activării logării unice în reţeaua dumneavoastră. Trebuie să păstraţi asocierile actualizate atunci când implementaţi o reţea cu logare singulară.

Există trei tipuri de asocieri pe care le puteţi crea: sursă, destinaţie şi administrative. Pentru a crea sau menţine asocieri între identităţile utilizatorilor la identificatorii EIM corespunzători, puteţi efectua una din următoarele taskuri:

- Crearea unei asocieri
- Ştergerea unei asocieri

Crearea unei asocieri

Pentru a activa mediul de logare singulară trebuie să creaţi asocieri între diferitele identităţi utilizator ale unei persoane sau entităţi la un singur identificator EIM pentru acea persoană sau identitate. Puteţi crea trei tipuri de asocieri: destinaţie, sursă şi administrativă.

Pentru a crea o asociere administrativă sau sursă, trebuie să aveţi autorizare de identificare administrator sau autorizare de administrator EIM. Pentru a crea o asociere destinaţie, trebuie să aveţi administrare registru pentru toţi regiştrii, administrare registru pentru un anumit registru sau autorizare de administrator EIM.

Pentru a crea o asociere pentru un identificator EIM, urmaţi aceşti paşi:

1. Expandaţi **Reţea —> Mapare identitate în întreprindere —> Gestiunea domeniului**.
2. Trebuie sa fiti conectat la domeniul EIM in care doriţi să lucraţi:
   - Dacă domeniul EIM cu care doriţi să lucraţi nu este listat în folderul Gestiunea Domeniului, consultaţi Adăugarea unui domeniu EIM la gestiunea domeniului.
   - Dacă nu sunteţi conectat în mod curent la domeniul EIM în care doriţi să lucraţi, consultaţi Conectarea la controlerul de domeniu EIM.
3. Expandaţi domeniul EIM la care sunteţi conectat acum.
4. Apăsaţi **Identificatori** pentru a afişa o listă a identificatorilor EIM.
5. Faceţi clic dreapta pe identificatorul EIM corespunzător şi selectaţi **Proprietăţi...** .
6. Apăsaţi fişa **Asocieri**.
7. Apăsaţi **Adăugare...** pentru a afişa dialogul **Adăugare asociere**.
8. Apăsaţi **Ajutor** dacă aveţi nevoie de mai multe informaţii pentru a completa câmpurile.
9. Atunci când aţi specificat informaţiile necesare, apăsaţi **OK**.

Ştergerea unei asociaţii
Pentru a şterge o asociere administrativă sau sursă, trebuie să aveţi autorizare de identificare administrator sau autorizare de administrator EIM. Pentru a şterge o asociere destinaţie, trebuie să aveţi autorizare de administrator pentru regiştrii selectaţi (incluzând registrul cu care doriţi să lucraţi), autorizare de administrator registru sau autorizare de administrator EIM.

Pentru a şterge o asociere, urmaţi paşii următori.

1. Expandaţi **Reţea —> Mapare identitate în întreprindere —> Gestiunea domeniului**.
2. Trebuie sa fiţi conectat la domeniul EIM in care doriţi să lucraţi:
   - Dacă domeniul EIM cu care doriţi să lucraţi nu este listat în Gestiunea Domeniului, consultaţi Adăugarea unui domeniu EIM la gestiunea domeniului.
   - Dacă nu sunteţi conectat în mod curent la domeniul EIM în care doriţi să lucraţi, consultaţi Conectarea la un domeniu EIM.
3. Expandaţi domeniul EIM la care sunteţi conectat acum.
4. Apăsaţi **Identificatori**.
5. Faceţi clic dreapta pe identificatorul EIM pe care îl doriţi şi selectaţi **Proprietăţi...** .
6. Apăsaţi fişa **Asocieri** pentru a afişa asocierile curente pentru identificatorul EIM.
7. Selectaţi asocierea pe care doriţi să o înlăturaţi.
8. Apăsaţi **Înlăturare** pentru a înlătura asocierile.
9. Selectaţi **OK**.

Gestionarea identificatorilor EIM
Întreţinerea identificatorilor EIM care reprezintă utilizatorii din reţeaua dumneavoastră este crucială pentru securitate. Utilizatorii din întreprindere se schimbă tot timpul, unii vin, alţii pleacă şi alţii se mută între diferite zone din întreprindere. Împreună cu aceste schimbări apare şi necesitatea de a urmări conturile utilizatorilor şi accesul acestora la sistemele din reţea. Crearea identificatorilor EIM şi asocierea acestora cu identităţile utilizatorilor pentru fiecare utilizator face ca acest task de urmărire să fie mai uşor de realizat.

Activarea logării singulare face ca taskul de logare să fie mai uşor pentru utilizatori pe măsură ce se mută în alt departament sau zonă din întreprindere. Permisiunile lor de securitate şi nevoile de acces la sistem le pot schimba de asemenea. Activarea logării singulare elimină nevoia ca aceşti utilizatori să iţi amintească noile nume de utilizator şi parola pentru sistemele noi.

Gestionarea identificatorilor EIM pentru utilizatorii dumneavoastră din întreprindere implică mai multe taskuri ca pot fi de rutină. Puteţi folosi task-urile următoare pentru a gestiona identificatorii EIM din reţeaua şi domeniile dumneavoastră.

- Crearea unui identificator EIM
- Adăugarea unui alias la un identificator EIM
- Ştergerea unui identificator EIM

Pentru informaţii despre gestionarea asocierilor, consultaţi subiectul Gestionarea asocierilor.

Crearea unui identificator EIM
Pentru crea un identificator EIM, trebuie să aveţi fie autorizare de administrare identificator, fie autorizare de administrare EIM.

Pentru a crea un identificator EIM pentru o persoană sau o entitate, urmaţi aceşti paşi:

1. Expandaţi **Reţea —> Mapare identitate în întreprindere —> Gestiunea domeniului**.
2. Trebuie sa fiti conectat la domeniul EIM in care doriţi să lucraţi:
   - Dacă domeniul EIM cu care doriţi să lucraţi nu este listat în **Gestiunea domeniului**, consultaţi Adăugarea unui domeniu la Gestiunea domeniului.

- Dacă nu sunteţi conectat în mod curent la domeniul EIM în care doriţi să lucraţi, consultaţi Conectarea la un domeniu .

3. Expandaţi domeniul EIM la care sunteţi conectat acum.
4. Faceţi clic dreapta pe **Identificatori** şi selectaţi **Identificator nou...**.
5. Apăsaţi **Ajutor** dacă aveţi nevoie de informaţii suplimentare despre oricare din câmpuri.
6. Atunci când aţi specificat informaţiile necesare, apăsaţi **OK**.

Adăugarea unui alias la un identificator EIM

Este posibil să doriţi să creaţi un alias pentru a furniza informaţii de identificare suplimentare pentru un identificator EIM. Dumneavoastră sau alţii puteţi folosi aliasul pentru distinge un identificator EIM de un altul. De exemplu, daca aveţi doi utilizatori numiţi John J. Johnson, aţi putea crea un alias al lui John Joseph Johnson şi un alias al lui John Jeffrey Johnson pentru a face mai uşoară deosebirea între identităţile fiecărui utilizator.

Pentru adăuga un alias la un identificator, trebuie să aveţi fie autorizare de administrare identificator, fie autorizare de administrare EIM.

Pentru a adăuga un alias la un identificator EIM, efectuaţi aceşti paşi.

1. Expandaţi **Reţea —> Mapare identitate în întreprindere —> Gestiunea domeniului**.
2. Trebuie sa fiţi conectat la domeniul EIM in care doriţi să lucraţi:
   - Dacă domeniul EIM cu care doriţi să lucraţi nu este listat în folderul Gestiunea domeniului, consultaţi Adăugarea unui domeniu EIM la Gestiunea domeniului.
   - Dacă nu sunteţi conectat în mod curent la domeniul EIM în care doriţi să lucraţi, consultaţi Conectarea la controlerul de domeniu EIM.
3. Expandaţi domeniul EIM la care sunteţi conectat acum.
4. Faceţi clic dreapta pe identificatorul EIM pe care îl doriţi şi selectaţi **Proprietăţi...** .Dacă nu există identificatori EIM, consultaţi Crearea unui identificator EIM.
5. Specificaţi numele unui alias pe care doriţi să-l adăugaţi la acest identificator EIM şi apăsaţi **Adăugare**.
6. Apăsaţi **OK** pentru a salva modificările.

Ştergerea unui identificator EIM

Pentru a şterge un identificator EIM, trebuie să aveţi autorizarea de administrare EIM.

Pentru a şterge un identificator EIM, efectuaţi aceşti paşi:

1. Expandaţi **Reţea —> Mapare identitate în întreprindere —> Gestiunea domeniului**.
2. Trebuie sa fiţi conectat la domeniul EIM in care doriţi să lucraţi:
   - Dacă domeniul EIM cu care doriţi să lucraţi nu este listat în folderul Gestiunea domeniului, consultaţi Adăugarea unui domeniu EIM la Gestiunea domeniului.
   - Dacă nu sunteţi conectat în mod curent la domeniul EIM în care doriţi să lucraţi, consultaţi Conectarea la controlerul de domeniu EIM.
3. Expandaţi domeniul EIM la care sunteţi conectat acum.
4. Apăsaţi **Identificatori**.
5. Selectaţi unul sau mai mulţi identificatori EIM pentru ştergere.
6. Faceţi clic dreapta pe identificatorii EIM selectaţi şi selectaţi **Ştergere** .
7. Apăsaţi **Da** în dialogul **Confirmare de ştergere** pentru a şterge identificatorii EIM selectaţi.

Gestionarea autorizărilor de utilizator EIM

EIM defineşte diferite autorizări EIM care sunt necesare pentru a efectua diferite operaţii în domeniu. Aceasta include funcţii de gestiune a domeniului cum ar fi crearea identificatorilor şi efectuarea operaţiilor de căutare mapare. Doar utilizatorii cu autorizarea de administrare EIM au permisiunea de a acorda sau revoca autorizări pentru alţi utilizatori.

Consultaţi autorizări EIM pentru o scurtă descriere a fiecărui grup de autorizare şi pentru detalii despre accesul specific al acestor autorizări la anumite funcţii EIM.

Pentru a modifica autorizările EIM pentru un utilizator, urmaţi paşii următori:

1. În iSeries Navigator, expandaţi **Reţea —> Mapare identitate în întreprindere —> Gestiunea domeniului**.
2. Expandaţi domeniul EIM cu care doriţi să lucraţi. Dacă nu sunteţi conectat în mod curent la acest domeniu, sunteţi invitat să vă conectaţi. Asiguraţi-vă ca v-aţi conectat la domeniu cu o autorizare de utilizator care are autorizarea de administrator EIM.
3. Faceţi clic dreapta pe domeniul EIM şi selectaţi **Autorizare...** .
4. În dialogul **Editare autorizare EIM**, specificaţi utilizatorul pentru care modificaţi autorizările.
5. Selectaţi **OK**.
6. În dialogul **Editare autorizare EIM**, efectuaţi modificările necesare la autorizările pentru utilizator.
7. Atunci când aţi terminat, apăsaţi **OK** pentru a salva modificările.

Gestionarea regiştrilor utilizator

Înainte de a putea crea asocieri între identităţi conţinute în regiştrii utilizator şi identificatorii EIM corespunzători, trebuie să definiţi mai întâi registrul utilizator în domeniul EIM.

Taskurile următoare reprezintă o parte a gestionării regiştrilor utilizator din domeniul EIM.

- Adăugarea unui registru utilizator
- Adăugarea unui alias la un registru utilizator
- Definirea unui tip de registru de utilizator privat în EIM
- Înlăturarea unui registru utilizator
- Înlăturarea unui alias dintr-un registru utilizator

Adăugarea unui registru utilizator

Pentru a adăuga un registru utilizator, trebuie să aveţi autorizarea de administrare EIM. Pentru detalii despre această autorizare şi despre ce poate accesa un utilizator cu această autorizare, consultaţi autorizări EIM.

Pentru a adăuga un registru utilizator la un domeniu EIM, efectuaţi paşii următori.

1. Expandaţi **Reţea —> Mapare identitate în întreprindere —> Gestiunea domeniului**.
2. Conectaţi-vă la domeniul EIM cu un utilizator care are autorizare de administrator EIM.
   - Dacă domeniul EIM cu care doriţi să lucraţi nu este listat în folderul Gestiunea Domeniului, consultaţi Adăugarea unui domeniu EIM la gestiunea domeniului.
   - Dacă nu sunteţi conectat în mod curent la domeniul EIM în care doriţi să lucraţi, consultaţi Conectarea la controlerul de domeniu EIM.
3. Expandaţi domeniul EIM la care sunteţi conectat acum.
4. Faceţi clic dreapta **Regiştri utilizator** şi selectaţi **Adăugare registru...**.
5. Specificaţi informaţiile de registru utilizator necesare. Puteţi de asemenea să specificaţi informaţii de alias pentru registrul utilizator.
6. Apăsaţi **OK** pentru a salva informaţiile şi pentru a adăuga registrul utilizator la domeniul EIM.

Adăugarea unui alias la un registru utilizator

Este posibil ca dumneavoastră sau un dezvoltator de aplicaţii să doriţi să creaţi un alias pentru a furniza informaţii suplimentare de identificare pentru un registru utilizator. Dumneavoastră sau alţii puteţi apoi utiliza aliasul pentru a distinge un registru utilizator de un altul. De exemplu, dezvoltatorii de aplicaţii şi administratorii folosesc un alias pe un registru utilizator pentru a comunica ce regiştrii EIM ar trebui să folosească o aplicaţie. Pentru informaţii despre folosirea atribuirii de aliasuri la regiştrii utilizatori, consultaţi definiţii registru EIM.

Pentru a adăuga un alias la un registru utilizator, trebuie să folosiţi una din următoarele autorizări: administrator EIM, administrator de registru pentru toţi regiştrii sau administrator de registru pentru un anumit registru pentru care efectuaţi acest task.

Pentru a adăuga un alias la un registru utilizator dintr-un domeniu EIM, urmaţi aceşti paşi:

1. Expandaţi **Reţea —> Mapare identitate în întreprindere —> Gestiunea domeniului**.
2. Trebuie sa fiţi conectat la domeniul EIM in care doriţi să lucraţi:
   - Dacă domeniul EIM cu care doriţi să lucraţi nu este listat în folderul Gestiunea domeniului, consultaţi Adăugarea unui domeniu EIM la gestiunea domeniului.
   - Dacă nu sunteţi conectat în mod curent la domeniul EIM în care doriţi să lucraţi, consultaţi Conectarea la controlerul de domeniu EIM.
3. Expandaţi domeniul EIM la care sunteţi conectat acum.
4. Apăsaţi **Regiştri utilizator** pentru a afişa lista regiştrilor din domeniu.
5. Faceţi clic dreapta registrul utilizator la care adăugaţi un alias şi selectaţi **Proprietăţi...**.
6. Apăsaţi fişa **Alias** din dialogul **Proprietăţi**.
7. Specificaţi numele şi tipul aliasului pe are doriţi să îl adăugaţi. Puteţi specifica un tip de alias care nu este inclus în lista tipurilor.
8. Selectaţi **Adăugare**.
9. Apăsaţi **OK** pentru a salva modificările.

Definirea unui tip de registru de utilizator privat în EIM

Pentru a defini un tip de registru utilizator privat pe care EIM nu este predefinit să îl recunoască, trebuie să specificaţi tipul registrului în forma **IdentificatorObiect - normalizare**, unde **IdentificatorObiect** este un identificator de obiect în notaţie zecimală cu punct cum ar fi 1.2.3.4.5.6.7, şi **normalizare** este fie valoarea **caseExact**, fie valoarea **caseIgnore**. De exemplu, identificatorul de obiect (OID) pentru OS/400 este 1.3.18.0.2.33.2-caseIgnore.

Ar trebui să obţineţi orice OID-uri de care aveţi nevoie de la autorităţile de înregistrare OID corespunzătoare pentru a vă asigura că folosiţi şi creaţi OID-uri unice. OID-urile unice vă ajută să evitaţi conflictele potenţiale cu OID-urile create de către alte organizaţii sau aplicaţii.

Există două moduri de a obţine OID-uri.

- **Înregistraţi obiectele cu o autorizare.**
  Această metodă este o alegere bună atunci când aveţi nevoie de un număr mic de OID-uri fixe pentru a reprezenta informaţia. De exemplu, acele OID-uri ar putea să reprezinte politici certificate pentru utilizatorii din întreprinderea dumneavoastră.
- **Obţineţi o asignare arc de la o autorizare de înregistrare şi asignaţi propriile OID-uri după cum este necesar.**
  Această metodă, care este o asignare de interval de identificator obiect zecimal cu punct este o bună alegere dacă aveţi nevoie de un număr mare de OID-uri sau dacă este posibil ca asignările OID-ului să se schimbe. Asignarea arc constă din numerele de început în notaţie zecimală cu punct din care trebuie să bazaţi **IdentificatorObiect**. De exemplu, asignarea arc ar putea fi 1.2.3.4.5.. Aţi putea crea apoi OID-uri prin adăugarea la acest arc de bază. De exemplu, aţi putea crea OID-uri sub forma 1.2.3.4.5.x.x.x).

Puteţi învăţa mai multe despre înregistrare OID-urilor dumneavoastră cu o autorizare de înregistrare prin consultarea acestor resurse Internet:

- American National Standards Institute (ANSI) este autorizarea de înregistrare pentru Statele Unite pentru nume de organizaţii aflate sub incidenţa procesului de înregistrare globală stabilit de către ISO (International Standards Organization) şi ITU (International Telecommunication Union). Un document cu legături la un formular de aplicaţie se află pe site-ul Web al ANSI

http://web.ansi.org/public/services/reg_org.html

. Arc-ul OID al ANSI pentru organizaţii este 2.16.840.1. ANSI taxează pentru asignările arc OID. Durează aproximativ două săptămâni pentru a primi arc-ul OID asignat de la ANSI. ANSI va asigna un număr (NEWNUM), creând un nour arc OID: 2.16.840.1.NEWNUM.

- În cele mai multe ţări sau regiuni, asociaţie naţională de standarde întreţine un registru OID. LA fel ca şi arc-ul ANSI, acestea sunt arc-uri generale asignate cu OID-ul 2.16. Ar putea fi nevoie de anumite investigaţii pentru a găsi autoritatea OID pentru o anumită ţară sau regiune. Adresele pentru membrii ISO naţionali pot fi găsite la http://www.iso.ch/addresse/membodies.html

. Informaţiile includ adresa poştală şi adresă de poştă electronică. În cele mai multe cazuri, este specificat şi un site Web.

- Un alt punct posibil de pornire este International Register al schemelor ISO DCC NSAP. NSAP înseamnă Network Service Access Point şi este folosit în diferite standarde internaţionale. Registrul pentru scheme poate fi obţinut la http://www.fei.org.uk sub ISO DCC NSAP

. Site-ul Web conţine informaţii de contact pentru 13 autorităţi de denumire dintre care unele asignează şi OID-uri.

- Internet Assigned Numbers Authority (IANA) asignează numere de întreprindere private, care sunt OID-uri, în arc-ul 1.3.6.1.4.1. IANA a asignat arc-uri la peste 7500 de companii până acum. Pagina aplicaţiei se află la http://www.iana.org/cgi-bin/enterprise.pl

, sub Private Enterprise Numbers. De obicei, cu IANA, asignarea durează o săptămână. Un OID de la IANA este gratuit. IANA va asigna un număr (NEWNUM) astfel încât anoul arc OID va fi 1.3.6.1.4.1.NEWNUM.

- Guvernul Federal al Statelor Unite întreţine Computer Security Objects Registry (CSOR). CSOR este autoritatea de denumire pentru arc-ul 2.16.840.1.101.3 şi înregistrează în mod curent obiecte pentru etichete de securitate, algoritmi de criptografie şi politici certificate. OID-urile de politici certificate sunt definite în arc-ul 2.16.840.1.101.3.2.1. CSOR furnizează OID-uri la agenţiile Guvernului Federal al Statelor Unite. Pentru mai multe informaţii despre CSOR, consultaţi http://csrc.nist.gov/csor/

.

Pentru informaţii suplimentare despre OID-uri pentru politici certificate, consultaţi http://csrc.nist.gov/csor/pkireg.htm

.

Înlăturarea unui registru utilizator

Înlăturarea unui registru utilizator dintr-un domeniu EIM provoacă pierderea oricăror asocieri dintre identificatorii EIM cu identităţile utilizatorilor din registrul utilizator. Adăugarea unui registru utilizator înapoi în domeniul EIM după înlăturarea lui nu resetează relaţiile de asociere.

Pentru a înlătura un registru utilizator, trebuie să aveţi autorizare de administrare EIM.

Pentru a înlătura un registru utilizator, efectuaţi paşii următori:

1. Expandaţi **Reţea —> Mapare identitate în întreprindere —> Gestiunea domeniului**.
2. Trebuie sa fiţi conectat la domeniul EIM in care doriţi să lucraţi:
   - Dacă domeniul EIM cu care doriţi să lucraţi nu este listat în folderul Gestiunea domeniului, consultaţi Adăugarea unui domeniu EIM la gestiunea domeniului.
   - Dacă nu sunteţi conectat în mod curent la domeniul EIM în care doriţi să lucraţi, consultaţi Conectarea la controlerul de domeniu EIM.
3. Expandaţi domeniul EIM la care sunteţi conectat acum.
4. Apăsaţi **Regiştri utilizator** pentru a afişa lista regiştrilor utilizator din domeniu.
5. Efectuaţi clic dreapta pe registrul utilizator pe care doriţi să îl înlăturaţi şi selectaţi **Ştergere...**.
6. Apăsaţi **Da** în dialogul **Confirmare** pentru a şterge registrul utilizator.

Înlăturarea unui alias dintr-un registru utilizator

Pentru a înlătura un alias dintr-un registru utilizator, trebuie să aveţi autorizare de administrator pentru regiştri şi autorizare de administrator pentru regiştrii selectaţi (incluzând registrul cu care doriţi să lucraţi) sau autorizare de administrare EIM.

Pentru a înlătura un alias dintr-un registru utilizator dintr-un domeniu EIM, urmaţi aceşti paşi:

1. Expandaţi **Reţea —> Mapare identitate în întreprindere —> Gestiunea domeniului**.
2. Trebuie sa fiti conectat la domeniul EIM in care doriţi să lucraţi:
   - Dacă domeniul EIM cu care doriţi să lucraţi nu este listat în folderul Gestiunea domeniului, consultaţi Adăugarea unui domeniu EIM la gestiunea domeniului.
   - Dacă nu sunteţi conectat în mod curent la domeniul EIM în care doriţi să lucraţi, consultaţi Conectarea la controlerul de domeniu EIM.
3. Expandaţi domeniul EIM la care sunteţi conectat acum.
4. Apăsaţi **Regiştri utilizator** pentru a afişa lista regiştrilor din domeniu.
5. Faceţi clic dreapta registrul utilizator din care înlăturaţi un alias şi selectaţi **Proprietăţi...**.
6. Apăsaţi fişa **Alias** din dialogul **Proprietăţi**.
7. Selectaţi un alias pe care vreţi să-l înlăturaţi si apăsaţi **Înlăturare**.
8. Apăsaţi **OK** pentru a salva modificările.

API-uri pentru EIM

EIM are mai multe API-uri care pot fi folosite de către aplicaţii pentru a realiza operaţii EIM în numele aplicaţiei sau în numele unui utilizator de aplicaţie. Puteţi folosi aceste API-uri pentru a realiza operaţii de căutare mapare, diferite gestionări EIM şi funcţii de configurare precum şi modificări de informaţii şi capabilităţi de interogare.

API-urile EIM sunt grupate după categorii, după cum urmează:

- operaţii de manipulare şi conectare EIM
- administrare de domeniu EIM
- Operaţii registru
- Operaţii cu identificatori EIM
- Gestiunea asocierilor EIM
- Operaţii de căutare mapare EIM
- Gestiunea autorizărilor EIM

Aplicaţiile care folosesc aceste API-uri pentru a gestiona sau folosi informaţiile EIM dintr-un domeniu EIM urmăresc de obicei următorul model de programare:

1. Obţinere mâner EIM
2. Conectare la un domeniu EIM

3. Procesare normală a aplicaţiei.
4. Folosirea unei API pentru operaţie de căutare mapare identitate EIM sau administrare EIM
5. Procesare normală a aplicaţiei.
6. Înainte de terminare, distrugerea mânerului EIM

Pentru informaţii detaliate şi pentru o listă completă a API-urilor EIM disponibile pentru serverul iSeries, consultaţi subiectul API-uri EIM.

Depanarea EIM

EIM este alcătuit din multiple tehnologii şi din multe aplicaţii şi funcţii. Deoarece sunt multe căi care pot fi urmate pentru a depana problemele, următoarele subiecte conţin informaţii şi instrucţiuni detaliate despre modalităţile de depanare sau de reparare a unor erori obişnuite pe care le puteţi întâlni, cum ar fi:

- Nu se poate realiza conectarea la controlerul de domeniu
- Listarea identificatorilor EIM durează un timp îndelungat
- Vrăjitorul Configurare EIM se blochează în timpul terminării procesării
- Mânerul EIM nu mai este valid
- Mesajele de autentificare şi de diagnosticare Kerberos

Nu se poate realiza conectarea la controlerul de domeniu

La problemele de conectare când încercaţi să vă conectaţi la controlerul de domeniu pot contribui un număr de factori. Verificaţi elementele următoare pentru a găsi cauza problemei:

- Verificaţi că informaţiile specificate pentru elementele următoare sunt corecte:
  - Numele controlerului de domeniu
  - Porul specificat
  - ID-ul de utilizator şi parola
- Verificaţi că controlerul de domeniu este activ. Dacă controlerul de domeniu este un server iSeries, puteţi utiliza Navigatorul iSeries şi urma aceşti paşi:
  1. Expandaţi **Reţea —> Servere —> TCP/IP**.
  2. Verificaţi că Serverul de directoare are starea **Pornit**. Dacă serverul este oprit, faceţi clic dreapta pe **Serverul de directoare** şi selectaţi **Pornire...**

Odată ce controlerul de domeniu este pornit, încercaţi să vă reconectaţi la domeniu.

1. Expandaţi **Reţea —> Mapare identităţi întreprindere —> Gestionare domenii**.
2. Selectaţi domeniul la care doriţi să vă conectaţi. Dacă nu este listat nici un domeniu EIM sub folderul Gestionare domenii, trebuie să adăugaţi un domeniu EIM la gestionarea de domenii.
3. Faceţi clic dreapta pe domeniul EIM la care doriţi să vă conectaţi şi selectaţi **Conectare...**.
4. Specificaţi tipul de utilizator şi informaţiile despre utilizator necesare care trebuie utilizate pentru conectarea la controlerul de domeniu EIM.
5. Selectaţi **OK**.

Lista identificatorilor EIM necesită un timp îndelungat

Când deschideţi folderul Identificatori în Navigatorul iSeries, generarea listei de identificatori poate dura un timp îndelungat. Este posibil să doriţi să restrângeţi criteriul de căutare pentru afişarea listei de identităţi EIM dacă aveţi un număr mare de identităţi în domeniul dumneavoastră.

Pentru a personaliza vizualizarea pentru identităţile EIM, urmaţi aceşti paşi:

1. În Navigatorul iSeries, expandaţi **Reţea —> Mapare identităţi întreprindere —> Gestionare domeniu**.
2. Expandaţi domeniul din care doriţi să afişaţi identificatorii EIM.

3. Faceţi clic dreapta pe **Identificatori** şi selectaţi **Personalizare vizualizare —> Includere...**.
4. Specificaţi criteril de afişare pe care îl doriţi. Caracterul asterisc (*) poate fi utilizat drept caracter de înlocuire.
5. Apăsaţi OK.

Data următoare când faceţi clic pe **Identificatori**, identificatorii EIM afişaţi sunt doar cei care se potrivesc cu criteriul pe care l-aţi specificat. Dacă doriţi să vizualizaţi toţi identificatorii EIM, utilizaţi paşii de mai sus şi selectaţi **Toţo identificatorii** ca opţiune pentru vizualizarea personalizată.

Vrăjitorul Configurare EIM se blochează în timpul terminării procesării

Dacă vrăjitorul pare a fi blocat în timpul terminării procesării, este posibil ca vrăjitorul să aştepte pornirea controlerului de domeniu. Verificaţi că nu s-a produs nici o eroare în timpul pornirii serverului LDAP. Pentru serverele iSeries, verificaţi istoricul de job pentru jobul QDIRSRV din subsistemul QSYSWRK.

Pentru a verifica istoricul de job, urmaţi aceşti paşi:

1. În Navigatorul iSeries, expandaţi **Gestiune lucrări —> Subsisteme —> Qsyswrk**.
2. Faceţi clic dreapta pe **Qdirsrv** şi selectaţi **Istoric job**.

Mânerul EIM nu mai este valid

În timpul gestionării EIM prin intermediul Navigatorului iSeries, dacă utilizatorul recepţionează o eroare indicând că mânerul EIM nu mai este valid, a fost pierdută conexiunea cu controlerul de domeniu.

Pe ntru a realiza reconectarea la controlerul de domeniu, urmaţi aceşti paşi:

1. În Navigatorul iSeries, expandaţi **Reţea —> Mapare identităţi întreprindere —> Gestionare domeniu**.
2. Faceţi clic dreapta pe domeniul cu care doriţi să lucraţi şi selectaţi **Reconectare...**.
3. Specificaţi informaţiile de conexiune.
4. Selectaţi **OK**.

Mesaje de autentificare şi de diagnosticare Kerberos

Când utilizaţi protocolul Kerberos pentru autentificarea cu EIM, mesajul de diagnosticare CPD3E3F este scris în istoricul de job de fiecare dată când autentificarea sau operaţiile de mapare identitate eşuează. Mesajul de diagnostic conţine ambele coduri de stare major şi minor pentru a indica unde s-a produs problema. Erorile cele mai întâlnite sunt documentate în mesaj împreună cu modalitatea de recuperare.

Pentru a începe depanarea problemei, consultaţi informaţiile de ajutor asociate cu mesajul de diagnosticare.

Informaţii înrudite pentru EIM

Este posibil să doriţi să învăţaţi despre alte tehnologii care sunt înrudite cu EIM. Următoarele subiecte din Centrul de informare vă pot ajuta să înţelegeţi aceste tehnologii înrudite:

- **Serviciul de autentificare în reţea**
  Acest subiect furnizează informaţii despre configurarea serviciului de autentificare în reţea de pe iSeries. Serviciul de autentificare în reţea permite unui server iSeries să participe într-o reţea Kerberos existentă. Când se utilizează cu EIM, serviciul de autentificare în reţea furnizează înregistrarea unică pentru reţea.
- **Serviciile de director (LDAP)**
  Acest subiect furnizează informaţii de configurare şi conceptuale pentru Serviciile de director (LDAP). EIM utilizează serverul LDAP pentru a stoca datele EIM şi pentru a mapa asocierile.

Tipărit în S.U.A.