



System i  
Securitatea  
EIM (Enterprise Identity Mapping)

*Versiunea 6 Ediția 1*







System i

Securitatea

EIM (Enterprise Identity Mapping)

*Versiunea 6 Ediția 1*

**Notă**

Înainte de a folosi aceste informații și produsul la care se referă, aveți grijă să citiți “Observații”, la pagina 125.

Această ediție se aplică la versiunea 6, ediția 1, modificarea 0 a produsului IBM i5/OS (număr produs 5761–SS1) și la toate edițiile și modificările ulterioare, până când este altfel indicat în noile ediții. Această versiune nu rulează pe toate modelele RISC și nici pe modelele CISC.

© Copyright International Business Machines Corporation 2002, 2008. Toate drepturile rezervate.

# Cuprins

## EIM (Enterprise Identity Mapping) . . . . 1

Ce este nou pentru V6R1 . . . . .	1
Fișierul PDF pentru EIM (Enterprise Identity Mapping) . . . . .	1
Privire generală asupra EIM . . . . .	2
Concepte EIM . . . . .	4
Controlerul de domeniu EIM . . . . .	5
Domeniul EIM . . . . .	6
Identificatorii EIM . . . . .	8
Definițiile de registru EIM . . . . .	11
Definițiile de registru de sistem . . . . .	13
Definițiile de registru de aplicații . . . . .	14
Definiții registru grup . . . . .	15
Asocierile EIM . . . . .	16
Informațiile de căutare . . . . .	16
Asocierile de identificator . . . . .	17
Asocierile de politică . . . . .	21
Asocierile de politică de domeniu implicite . . . . .	21
Asocierile de politică registru implicite . . . . .	23
Asocierile de politică de filtrare certificate . . . . .	24
Operațiile de căutare EIM . . . . .	27
Exemple de operații de căutare: Exemplu 1 . . . . .	29
Exemple de operații de căutare: Exemplu 2 . . . . .	30
Exemple de operații de căutare: Exemplu 3 . . . . .	32
Exemple de operații de căutare: Exemplu 4 . . . . .	34
Exemple de operații de căutare: Exemplu 5 . . . . .	35
Suportul pentru politica EIM și activarea . . . . .	37
Controlul accesului în EIM . . . . .	38
Grupul de control al accesului EIM: Autorizarea API . . . . .	41
Grupul de control acces EIM: Autorizarea operației EIM . . . . .	43
Concepte LDAP pentru EIM . . . . .	46
Numele distinctiv . . . . .	46
Numele distinctiv părinte . . . . .	47
Schema LDAP și alte considerente pentru EIM . . . . .	48
Concepte EIM pentru i5/OS . . . . .	49
Considerente pentru profilul utilizator i5/OS pentru EIM . . . . .	49
Auditarea i5/OS pentru EIM . . . . .	50
Aplicațiile permise EIM pentru i5/OS . . . . .	50
Scenarii: EIM (Enterprise Identity Mapping) . . . . .	51
Planificarea pentru EIM (Enterprise Identity Mapping) . . . . .	51
Planificarea EIM (Enterprise Identity Mapping) pentru eServer . . . . .	51
Cerințele de setare EIM (Mapare de identități în întreprindere) pentru eServer . . . . .	51
Identificarea rolurilor și calificărilor necesare . . . . .	53
Planificarea domeniului EIM . . . . .	55
Planificarea unui controler de domeniu EIM . . . . .	56
Dezvoltarea unui plan de numire definiții de registru EIM (Enterprise Identity Mapping) . . . . .	58
Dezvoltarea unui plan de mapare identități . . . . .	60
Planificarea asocierilor EIM . . . . .	60
Dezvoltarea unui plan de numire identificatori EIM . . . . .	63

Fișele de lucru pentru planificarea implementării EIM . . . . .	64
Planificarea pentru dezvoltarea aplicațiilor de mapare EIM (Enterprise Identity Mapping) . . . . .	66
Planificarea EIM (Enterprise Identity Mapping) pentru i5/OS . . . . .	67
Cerințe preliminare instalare EIM pentru i5/OS . . . . .	67
Instalarea opțiunilor Navigator System i necesare . . . . .	67
Considerațiile de salvare și recuperare pentru EIM . . . . .	68
Salvarea de rezervă și recuperarea datelor domeniului EIM . . . . .	68
Salvarea de rezervă și recuperarea informațiilor de configurare EIM . . . . .	69
Configurarea EIM (Enterprise Identity Mapping) . . . . .	69
Crearea și alăturarea la un domeniu local nou . . . . .	70
Finalizarea configurației EIM pentru domeniu . . . . .	74
Crearea și alăturarea la un nou domeniu la distanță . . . . .	75
Finalizarea configurației EIM pentru domeniu . . . . .	79
Alăturarea la un domeniu existent . . . . .	80
Finalizarea configurației EIM pentru domeniu . . . . .	84
Configurarea unei conexiuni securizate la controlerul de domeniu EIM . . . . .	85
Gestionarea EIM (Enterprise Identity Mapping) . . . . .	86
Gestionarea domeniilor EIM (Enterprise Identity Mapping) . . . . .	86
Adăugarea unui domeniu EIM la folderul Gestionare domeniu . . . . .	86
Conectarea la domeniul EIM . . . . .	86
Activarea asocierilor de politică pentru un domeniu . . . . .	87
Testarea mapărilor EIM . . . . .	88
Lucrul cu rezultatele testului și rezolvarea problemelor . . . . .	89
Înlăturarea unui domeniu EIM din folderul Gestionare domeniu . . . . .	90
Ștergerea unui domeniu EIM și a tuturor obiectelor de configurare . . . . .	90
Gestionarea definițiilor de registre EIM . . . . .	91
Adăugarea unei definiții de registru sistem . . . . .	91
Adăugarea unei definiții de registru aplicație . . . . .	91
Adăugarea unei definiții de registru grup . . . . .	92
Adăugarea unui alias la o definiție de registru . . . . .	92
Definirea tipului de registru de utilizatori privat în EIM . . . . .	93
Activarea suportului de căutare mapare și a utilizării asocierilor de politică pentru un registru destinație . . . . .	94
Ștergerea unei definiții de registru . . . . .	95
Înlăturarea unui alias din identificatorul de registru . . . . .	96
Adăugarea unui membru la o definiție de registru grup . . . . .	97
Gestionarea identificatorilor EIM . . . . .	97
Crearea unui identificator EIM . . . . .	97
Adăugarea unui alias la un identificator EIM . . . . .	98
Înlăturarea unui alias din identificatorul EIM . . . . .	99
Ștergerea unui identificator EIM . . . . .	99
Personalizarea vizualizării de identificatori EIM . . . . .	100
Gestionarea asocierilor EIM . . . . .	100

Crearea asocierilor EIM . . . . .	100	Afișarea tuturor asocierilor de politică pentru o definiție de registru . . . . .	112
Crearea unei asocieri de identificator EIM . . . . .	101	Ștergerea unei asocieri de identificator . . . . .	113
Crearea unei asocieri de politică . . . . .	102	Ștergerea unei asocieri de politică . . . . .	114
Adăugarea de informații de căutare la o identitate de utilizator destinație . . . . .	108	Gestionarea controlului de acces al utilizatorului EIM . . . . .	114
Adăugarea informațiilor de căutare la o identitate utilizator destinație într-o asociere identificator . . . . .	108	Gestionarea proprietăților de configurare EIM . . . . .	115
Adăugarea informațiilor de căutare la o identitate utilizator destinație dintr-o asociere politică. . . . .	109	Depanarea EIM (Enterprise Identity Mapping) . . . . .	116
Înlăturarea informațiilor de căutare de la o identitate utilizator destinație . . . . .	110	Depanarea problemelor conexiunii la controlerul de domeniu . . . . .	116
Înlăturarea informațiilor de căutare pentru o identitate utilizator destinație dintr-o asociere identificator. . . . .	110	Depanarea probleme generale legate de domeniu și de configurația EIM. . . . .	118
Afișarea tuturor asocierilor de identificator pentru un identificator EIM. . . . .	111	Depanarea problemelor de mapare EIM . . . . .	119
Afișarea tuturor asocierilor de politică pentru un domeniu . . . . .	112	API-urile EIM . . . . .	122
		Informații legate de EIM (Enterprise Identity Mapping) . . . . .	123
		<b>Anexa. Observații . . . . .</b>	<b>125</b>
		Mărci comerciale. . . . .	127
		Termenii și condițiile . . . . .	127

---

## EIM (Enterprise Identity Mapping)

EIM (Enterprise Identity Mapping) pentru platforma System i este implementarea i5/OS a unei infrastructuri IBM care permite administratorilor și dezvoltatorilor de aplicații să rezolve problemele de gestionare a registrelor de utilizatori multiple din întreprinderea lor.

Cele mai multe întreprinderi cu rețea se confruntă cu problema registrelor de utilizatori multiple, 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 transformă rapid într-o mare problemă administrativă care afectează utilizatorii, administratorii și dezvoltatorii de aplicații. EIM activează soluții de cost redus pentru gestionarea registrelor de utilizatori multiple și a identităților utilizatorilor în întreprinderea dumneavoastră.

EIM vă permite să creați un sistem de mapări de identitate, numite asocieri, între diferitele identități de utilizatori din diferitele registre de utilizatori și o persoană din întreprinderea dumneavoastră. De asemenea, EIM oferă un set comun de API-uri care pot fi folosite la mai multe platforme pentru dezvoltarea de aplicații care să folosească mapările de identitate pe care le-ați creat, pentru a găsi relațiile dintre identitățile de utilizatori. În plus, puteți utiliza EIM împreună cu serviciul de autentificare în rețea (NAS), implementarea i5/OS a lui Kerberos, pentru a furniza un mediu de semnare unică.

Puteți configura și gestiona EIM prin System i Navigator, interfața grafică de utilizator System i. Platforma System i utilizează EIM pentru a activa interfețele i5/OS pentru a autentifica utilizatorii prin mijloacele serviciului de autentificare în rețea. Aplicațiile, ca și i5/OS, pot accepta tichete EIM și să utilizeze EIM pentru a afla profilul utilizator care reprezintă aceeași persoană ca și cea reprezentată de tichetul Kerberos.

Pentru a afla mai multe despre cum funcționează EIM, despre conceptele EIM și despre cum puteți să folosiți EIM în întreprinderea dumneavoastră examinați următoarele:

---

### Ce este nou pentru V6R1

Citiți despre informații noi sau modificate semnificativ pentru colecția de subiect EIM (Enterprise Identity Mapping).



#### Funcțiile noi și îmbunătățite pentru EIM

- În ediții anterioare ale i5/OS EIM suporta numa i maparea la o identitate utilizator locală per sistem. În i5/OS V6R1 EIM suportă selectarea de la mapări multiple identitate utilizator pentru același sistem, utilizând adresa IP a sistemului destinație pentru a selecta corect maparea de identitate utilizator locală.

În plus, subiectul Semnare unică a fost actualizat și furnizează informații despre implementarea EIM ca parte a unui mediu de semnare unică pentru a descrește gestionarea parolei. Acest subiect furnizează un număr de scenarii detaliate de situații de semnare unică cu instrucțiuni de configurare detaliată pentru implementarea lor.

#### Cum să vedeți ce este nou sau modificat

Pentru a vă ajuta să vedeți unde s-au făcut modificări tehnice, această publicație folosește:

- Imaginea  pentru marcarea locului unde încep informațiile noi sau cele modificate.
- Imaginea  pentru marcarea locului unde se termină informațiile noi sau cele modificate.

Pentru a afla alte informații despre ce este nou sau schimbat în această ediție, vedeți Memo către utilizatori.

---

### Fișierul PDF pentru EIM (Enterprise Identity Mapping)

Puteți vizualiza și tipări un fișier PDF cu aceste informații.

Pentru a vizualiza sau descărca versiunea PDF a acestui document, selectați **Maparea identității în întreprindere** (aproximativ 1820 KB).

Puteți vizualiza sau descărca aceste PDF-uri înrudite ca subiect:


- Network authentication services (cam 1398 KB) conține informații despre cum să configurați serviciul de autentificare în rețea în conjunctură cu EIM pentru a crea un mediu de semnare unică.
- IBM Tivoli Directory Server for i5/OS (LDAP) (cam 1700 KB) conține informații despre cum să configurați serverul LDAP, pe care îl puteți utiliza ca un controler de domeniu EIM, împreună cu informațiile despre configurarea avansată LDAP.

## Salvarea fișierelor PDF

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

1. Faceți clic dreapta pe legătura la PDF din acest browser.
2. Faceți clic pe opțiunea care salvează local PDF-ul.
3. Navigați către directorul unde vreți să salvați PDF-ul.
4. Faceți clic pe **Save**.

## Descărcarea programului Adobe Reader

Vă trebuie Adobe Reader instalat pe sistemul dumneavoastră pentru a vizualiza sau tipări aceste PDF-uri. Puteți descărca o copie gratis de la situl Web Adobe ([www.adobe.com/products/acrobat/readstep.html](http://www.adobe.com/products/acrobat/readstep.html)) .

---

## Privire generală asupra EIM

EIM (Enterprise Identity Mapping) vă poate ajuta să rezolvați probleme care survin când încercați să gestionați mai mult de un registru de utilizatori.

Mediile de rețea actuale sunt construite din grupuri complexe de sisteme și de aplicații, având ca efect necesitatea gestionării mai multor registre de utilizatori. Confruntarea cu registre de utilizatori multiple crește rapid într-o mare problemă de administrare care afectează utilizatorii, administratorii și dezvoltatorii de aplicații. Drept urmare, multe companii se luptă să gestioneze în siguranță autentificarea și autorizarea pentru sisteme și aplicații. EIM permite administratorilor și dezvoltatorilor de aplicații să rezolve această problemă mai ușor și cu un cost redus, față de posibilitățile anterioare.

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

## Problema gestionării registrelor de utilizatori multiple

Mulți administratori gestionează rețele care includ sisteme și servere diferite, fiecare cu o modalitate unică de gestionare a utilizatorilor prin intermediul a variate registre de utilizatori. În aceste rețele complexe, administratorii sunt responsabili pentru gestionarea identităților și parolilor fiecărui utilizator în cadrul mai multor sisteme. Suplimentar, adesea administratorii trebuie să sincronizeze aceste identități și parole, iar utilizatorii sunt împovărați cu memorarea mai multor identități și parole și cu păstrarea lor sincronizate. Regia pentru utilizator și pentru administrator este excesivă în acest mediu. În consecință, administratorii petrec un timp prețios pentru depanarea încercărilor de logare nereușite și resetând parole uitate în loc să gestioneze activitatea.

Problema gestionării registrelor de utilizatori multiple afectează de asemenea dezvoltatorii de aplicații care doresc să furnizeze aplicații pe mai multe niveluri sau eterogene. Acești dezvoltatori înțeleg că clienții au date importante de afaceri răspândite pe mai multe tipuri de sisteme diferite, iar fiecare sistem procesează propriile registre de utilizator. Ca urmare, dezvoltatorii trebuie să creeze registre de utilizatori proprietare și semantica de securitate asociate pentru aplicațiile lor. Deși aceasta rezolvă problema pentru dezvoltatorul de aplicații, aceasta sporește regia pentru utilizatori și administratori.



## Abordările actuale

Sunt disponibile mai multe abordări curente ale industriei pentru rezolvarea problemei gestionării de registre de utilizatori multiple, dar toate acestea furnizează soluții incomplete. De exemplu, LDAP (Lightweight Directory Access Protocol) furnizează o soluție de registru de utilizatori distribuit. Totuși, utilizarea LDAP (sau a altor soluții populare precum Microsoft Passport) înseamnă că administratorii trebuie în continuare să gestioneze un alt registru de utilizatori și semanticile de securitate sau trebuie să înlocuiască aplicațiile existente care sunt construite să folosească registre.

Utilizând acest tip de soluție, administratorii trebuie să gestioneze mecanisme de securitate multiple pentru resurse individuale, de aceea crescând regia administrativă și măbind potențial posibilitatea expunerilor de securitate. Atunci când mai multe mecanisme suportă o singură resursă, probabilitatea de modificare a autorizării printr-un mecanism și 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 interfețe, dar i se permite accesul prin intermediul uneia sau mai multor interfețe diferite.

După terminarea acestei munci, administratorii își dau seama că nu au rezolvat complet problema. În general, întreprinderile au investit prea mulți bani în registrele de utilizatori curente și în semanticile de securitate asociate acestora pentru a face practică utilizarea acestui tip de soluție. Crearea unui alt registru de utilizatori și a semanticilor de securitate asociate rezolvă problema pentru furnizorul de aplicații, dar nu și problemele pentru utilizatori și administratori.

O altă soluție posibilă este să utilizați abordarea de semnare unică. Sunt disponibile mai multe produse care permit administratorilor să gestioneze fișiere care conțin toate identitățile și parolele utilizator. Totuși, această abordare are câteva slăbiciuni:

- Se adresează doar unei probleme cu care se confruntă utilizatorii. Deși permite utilizatorilor să se înregistreze pe mai multe sisteme prin furnizarea unei singure identități și 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 fișiere sunt stocate parole în text clar sau decriptabile. Parolele nu trebuie să fie stocate niciodată în fișiere în text clar sau să fie accesibile oricui, inclusiv administratorilor.
- Nu rezolvă problemele dezvoltatorilor de aplicații de la o a treia parte care furnizează aplicații eterogene, pe mai multe niveluri. Aceștia trebuie să furnizeze în continuare registre de utilizatori proprietare pentru aplicațiile lor.

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

## Abordarea EIM

EIM oferă o nouă abordare pentru soluțiile de construire ieftine pentru a gestiona mai ușor mai multe registre de utilizatori și identități de utilizatori într-un mediu de aplicații eterogen, cu mai multe niveluri (tier). EIM este o arhitectură pentru descrierea relațiilor dintre indivizi sau entități (cum ar fi serverele de fișiere și cele de tipărire) într-o întreprindere și multe identități care-i reprezintă într-o întreprindere. În plus, EIM furnizează un set de API-uri care permit aplicațiilor pună întrebări despre aceste relații.

De exemplu, fiind dată identitatea utilizator a unei persoane dintr-un registru de utilizatori, puteți determina ce identitate utilizator dintr-un alt registru de utilizatori reprezintă aceeași persoană. Dacă utilizatorul s-a autentificat cu o identitate utilizator și puteți mapa această identitate utilizator într-un alt registru de utilizatori, utilizatorul nu mai are nevoie să furnizeze acreditări pentru a se autentifica din nou. Cunoașteți cine este utilizatorul și trebuie să cunoașteți doar ce identitate utilizator îl reprezintă pe acel utilizator într-un alt registru de utilizatori. De aceea, EIM furnizează o funcție de mapare de identități generalizată pentru întreprindere.

EIM permite mapări unul la mai mulți (cu alte cuvinte, un singur utilizator cu mai mult de o identitate utilizator într-un singur registru de utilizatori). Dar, nu este nevoie ca administratorii să aibă mapări individuale specifice pentru toate identitățile utilizator dintr-un registru de utilizatori. EIM permite de asemenea mapări multe-la-unul (în alte cuvinte, mai mulți utilizatori mapați la o singură identitate de utilizator într-un singur registru de utilizatori).

Posibilitatea de mapare între identitățile utilizatorului din registre utilizator diferite furnizează numeroase avantaje. În principal, înseamnă că aplicațiile pot avea flexibilitatea utilizării unui singur registru utilizator pentru autentificare în timp ce utilizează un registru de utilizatori cu totul diferit pentru autorizare. De exemplu, un administrator ar putea mapa o identitate utilizator Windows într-un registru Kerberos la un profil utilizator i5/OS într-un registru de utilizatori diferit pentru a accesa resursele i5/OS la care profilul utilizator i5/OS este autorizat.

EIM este o arhitectură deschisă pe care administratorii o pot utiliza pentru a reprezenta relații de mapare a identităților pentru orice registru. Nu necesită copierea datelor existente într-un nou depozit și încercarea de a le ține sincronizate. Singurele date noi pe care le introduce EIM sunt informațiile despre relații. EIM memorează aceste date într-un director LDAP, care oferă flexibilitatea gestionării datelor într-un singur loc și având copii (replici) acolo unde este folosită informația. În final, EIM furnizează întreprinderilor și dezvoltatorilor de aplicații flexibilitatea de a lucra ușor într-o gamă largă de medii cu un cost mai scăzut decât cel care ar fi posibil fără acest suport.

EIM, utilizat în conjuncție cu serviciul de autentificare în rețea, implementarea i5/OS a Kerberos, furnizează o soluție semnare unică. Se pot scrie aplicații care folosesc API-uri GSS și EIM pentru a accepta tichete Kerberos și pentru a le mapa la alte identități de utilizator asociate dintr-un alt registru de utilizatori. Asocierea dintre identitățile de utilizator care oferă această mapare de identități poate fi realizată prin crearea de asocieri de identificatori care asociază indirect identitatea unui utilizator cu a altuia printr-un identificator EIM sau prin crearea asocierilor politică care asociază direct o identitate de utilizator într-un grup cu o singură identitate de utilizator specifică.

Utilizarea mapării identităților necesită ca administratorii să realizeze următoarele:

1. Configurarea în rețea a unui domeniu EIM. Puteți utiliza vrăjitorul de configurare EIM pentru a crea un controler de domeniu pentru domeniu și să configurați accesul la domeniu. Când folosiți vrăjitorul puteți alege să creați un nou domeniu EIM și să creați un controler de domeniu pe sistemul local sau pe un sistem de la distanță. Sau, dacă există deja un domeniu EIM, puteți alege să participați într-un domeniu EIM existent.
2. Determinarea utilizatorilor definiți serverului de director care găzduiește controlerul de domeniu EIM care au permisiunea de a gestiona sau accesa informațiile specifice într-un domeniu EIM și atribuirea lor la grupurile de control acces EIM corespunzătoare.
3. Crearea de definiții registru EIM pentru acele registre de utilizatori care vor participa într-un domeniu EIM. Deși puteți defini orice registru de utilizatori la un domeniu EIM, trebuie să definiți registre de utilizatori pentru acele aplicații și sisteme de operare care sunt activate EIM.
4. Bazat pe nevoile dumneavoastră de implementare EIM, determinați care din următoarele operații să le realizați pentru a termina configurarea EIM:
  - Creați identificatori EIM pentru fiecare utilizator din domeniu și creați asocieri identificator pentru ei.
  - Creați asocieri de politică.
  - Creați o combinație a acestora.

#### Informații înrudite

Privire generală semnare unică

---

## Concepte EIM

Este necesară o înțelegere conceptuală a modului în care lucrează EIM pentru a înțelege complet modul în care puteți folosi EIM în întreprinderea dumneavoastră. Deși configurarea și implementarea API-urilor EIM pot diferi între platforme server, conceptele EIM sunt obișnuite de-a lungul platformelor IBM eServer.

Figura 1 furnizează un exemplu de implementare EIM într-o întreprindere. Trei servere se comportă ca niște clienți EIM și conțin aplicații EIM-activate care cer date EIM utilizând operații de căutare EIM **5**. Controlerul domeniu **1** stochează informații despre domeniul EIM **2**, care include un identificator EIM **3**, asocieri **4** între acești identificatori EIM și identități utilizator și definiții registru EIM **5**.

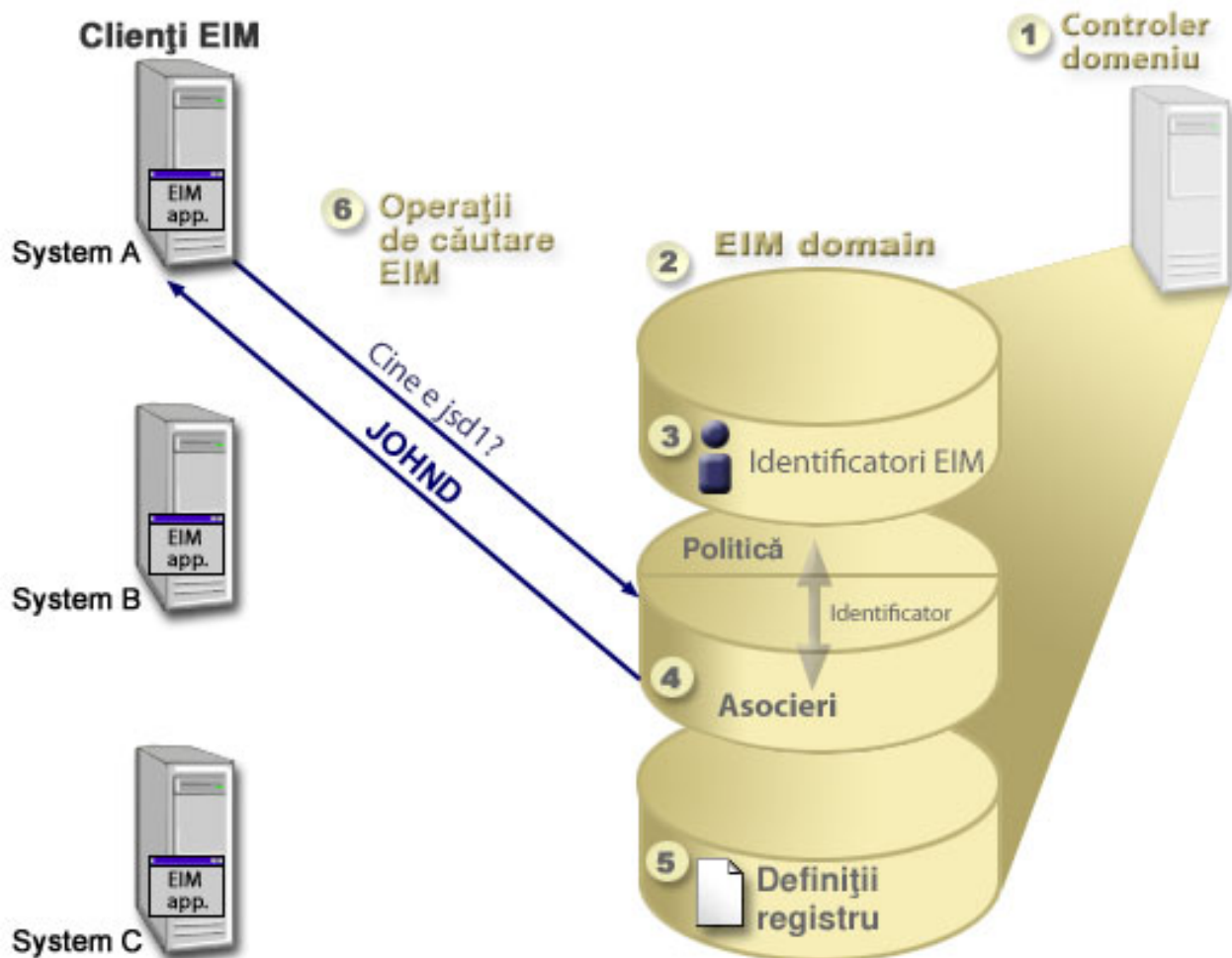


Figura 1. Un exemplu de implementare EIM

Revedeți următoarele informații pentru a afla mai multe despre aceste concepte EIM eServer:

#### Concepte înrudite

“Concepte LDAP pentru EIM” la pagina 46

EIM utilizează un server LDAP ca un controler de domeniu pentru a memora date EIM. De aceea trebuie să înțelegeți ceva concepte LDAP care se leagă de configurarea și folosirea EIM în întreprinderea dumneavoastră. De exemplu, puteți folosi un nume distinctiv LDAP ca identitate utilizator pentru a configura EIM și pentru a vă autentifica la controlerul de domeniu EIM.

“Concepte EIM pentru i5/OS” la pagina 49

Puteți implementa EIM pe orice platformă IBM eServer. Totuși, când implementați EIM pe un model System i, ar trebui să aveți grijă de unele informații care sunt specifice la implementarea System i.

## Controlerul de domeniu EIM

Un controler de domeniu EIM este un server LDAP (Lightweight Directory Access Protocol) care este configurat pentru a gestiona unul sau mai multe domenii EIM. Un domeniu EIM conține toate identificatoarele EIM, asocierile EIM și registrele de utilizatori care sunt definite în acest domeniu. Sistemele (clienți EIM) participă în domeniul EIM prin utilizarea datelor de domeniu pentru operații de căutare EIM.

Actualmente, puteți configura IBM Tivoli Directory Server for i5/OS pe unele platforme IBM eServer să se comporte 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-uri EIM pentru a contacta un controler de domeniu EIM de realizat. Locația

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

**Notă:** Dacă intenționați să configurați un server de director pe un sistem la distanță, serverul de director trebuie să asigure suport EIM. EIM necesită ca un server de director care suportă LDAP (Lightweight Directory Access Protocol) Versiunea 3 să găzduiască controlerul de domeniu. Suplimentar, produsul server de director trebuie să fie configurat să accepte schema EIM. IBM Tivoli Directory Server for i5/OS furnizează acest suport.

#### Concepte înrudite

“Operațiile de căutare EIM” la pagina 27

O aplicație sau un sistem de operare utilizează un API EIM pentru a realiza o operație de căutare pentru ca aplicația sau sistemul de operare poate mapa de la o identitate utilizator într-un registru la altă identitate utilizator în alt registru. O operație de căutare EIM este un proces prin care o aplicație sau un sistem de operare găsește o identitate de utilizator asociată necunoscută dintr-un anumit registru destinație prin furnizarea unor informații cunoscute și de încredere.

“Schema LDAP și alte considerente pentru EIM” la pagina 48

Utilizați aceste informații pentru a afla ce este cerut pentru ca serverul de director să funcționeze cu EIM (Enterprise Identity Mapping).

## Domeniul EIM

Un domeniu EIM (Enterprise Identity Mapping) este un director în care un server LDAP (Lightweight Directory Access Protocol) care conține date EIM pentru o întreprindere.

Un domeniu EIM este colecția tuturor identificatorilor EIM, asocierilor EIM și registrelor de utilizator definite în acel domeniu, precum și controlul accesului la date. Sistemele (clienții EIM) participă la domeniu prin utilizarea datelor domeniului pentru operații de căutare EIM.

Un domeniu EIM este diferit de un registru de utilizatori. Un registru de utilizatori definește un set de identități ale utilizatorului cunoscute și de încredere pentru o instanță particulară a unui sistem de operare sau a unei aplicații. Un registru de utilizatori conține de asemenea informațiile necesare pentru a-l autentifica pe utilizatorul identității. În plus, un registru de utilizatori conține de obicei alte atribute, cum ar fi preferințele utilizatorului, privilegiile de sistem sau informațiile personale pentru acea identitate.

Spre deosebire de registru, un domeniu EIM se *referă* la identitățile de utilizator care sunt definite în registrele de utilizator. Un domeniu EIM conține informații despre *relațiile* dintre identitățile din diferite registre de utilizatori (nume utilizator, tip registru și instanță registru) și persoanele sau identitățile adevărate pe care le reprezintă aceste identități.

Figura 2 prezintă datele care sunt memorate în cadrul domeniului EIM. Aceste date includ identificatorii EIM, definițiile de registre EIM și asocierile EIM. Datele EIM definesc relațiile dintre identitățile utilizator persoanele sau entitățile pe care le reprezintă aceste identități într-o întreprindere.

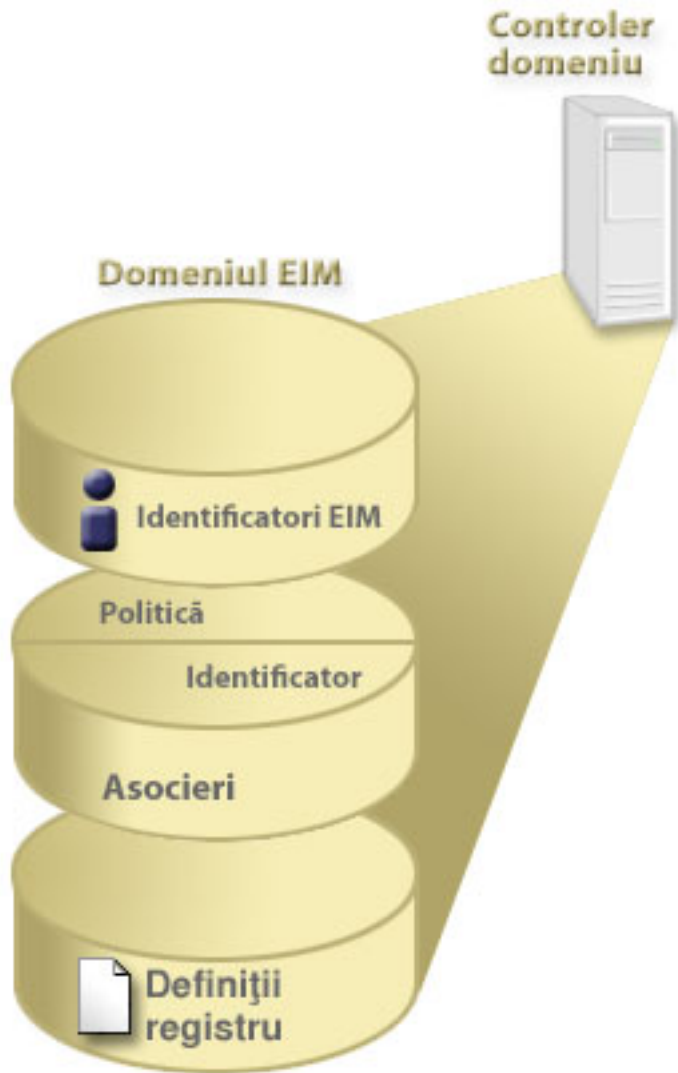


Figura 2. Domeniul EIM și datele care sunt stocate în cadrul domeniului

Datele EIM includ:

#### **Definiții pentru registrul EIM**

Fiecare definiție pentru registrul EIM pe care o creați reprezintă un registru de utilizatori real (și identitatea utilizator pe care o conține) care există pe un sistem din întreprindere. O dată ce definiți un numit registru de utilizatori în EIM, acel registru de utilizatori poate participa la domeniul EIM. Puteți crea două tipuri de definiții; un tip se referă la registrele de utilizator de sistem, iar celălalt la registrele de utilizator de aplicație.

#### **Identificatori EIM**

Fiecare identificator EIM pe care-l creați reprezintă în mod unic o persoană sau o intrare (ca serverul de tipărire sau un server de fișiere) dintr-o întreprindere. Puteți crea un identificator EIM atunci când doriți să aveți mapări unu-la-unu între identitățile de utilizator aparținând persoanei sau entității căreia îi corespunde identificatorul EIM.

#### **Asocieri EIM**

Asocierile EIM pe care le creați reprezintă relații dintre identități utilizator. Dacă definiți asocieri, clienții EIM pot utiliza API-urile EIM pentru a realiza cu succes operații de căutare EIM. Aceste operații de căutare EIM cercetează un domeniu EIM pentru a găsi asocieri definite. Există două tipuri diferite de asocieri pe care le puteți crea:

### Asocieri identificator

Asocierile identificator vă permit să definiți o relație unu-la-unu între identități utilizator definite pentru un individ. Fiecare asociere de identificator EIM pe care o creați reprezintă o relație unică, specifică între un identificator EIM și o identitate de utilizator asociată din întreprindere. Asocierile de identificator asigură informațiile care leagă un identificator EIM de o anumită identitate de utilizator într-un anumit registru de utilizatori și vă permit să creați mapări de identitate unu-la-unu pentru un utilizator. Asocierile de identități sunt în mod deosebit utile când indivizii au identități de utilizator cu autorizări speciale și alte privilegii pe care doriți să le controlați în mod special creând o mapare unu-la-unu între identitățile lor de utilizator.

### Asocieri de politică

Asocierile de politică vă permit să definiți o relație între un grup de identități utilizator din unul sau mai multe registre de utilizatori și o identitate utilizator individuală într-un alt registru de utilizatori. Fiecare asociere de politică EIM pe care o creați are ca rezultat o mapare mulți-la-unu între grupul sursă de identități de utilizator dintr-un registru de utilizatori și o singură identitate de utilizator destinație. În mod obișnuit, creați o asociere de politică pentru a mapa un grup de utilizatori care cer toți același nivel de autorizare la o singură identitate utilizator cu acel nivel de autorizare.

### Concepte înrudite

“Definițiile de registru EIM” la pagina 11

O definiție registru EIM (Enterprise Identity Mapping) este o intrare în EIM pe care o creați pentru a reprezenta un registru de utilizatori real, care există pe un sistem în întreprindere. Un registru de utilizatori funcționează asemănător unui director care conține o listă a identităților utilizator valide pentru un anumit sistem sau pentru o anumită aplicație.

“Identificatorii EIM”

Un identificator EIM (Enterprise Identity Mapping) reprezintă o persoană sau entitate într-o întreprindere. O rețea obișnuită este alcătuită din diferite platforme hardware și aplicații și registrele de utilizatori asociate acestora. Majoritatea platformelor și multe dintre aplicații utilizează registre de utilizatori specifice platformei sau specifice aplicației. Aceste registre de utilizatori conțin toate informațiile de identificare a utilizatorilor pentru utilizatorii care lucrează cu aceste server sau aplicații.

“Operațiile de căutare EIM” la pagina 27

O aplicație sau un sistem de operare utilizează un API EIM pentru a realiza o operație de căutare pentru ca aplicația sau sistemul de operare poate mapa de la o identitate utilizator într-un registru la altă identitate utilizator în alt registru. O operație de căutare EIM este un proces prin care o aplicație sau un sistem de operare găsește o identitate de utilizator asociată necunoscută dintr-un anumit registru destinație prin furnizarea unor informații cunoscute și de încredere.

## Identificatorii EIM

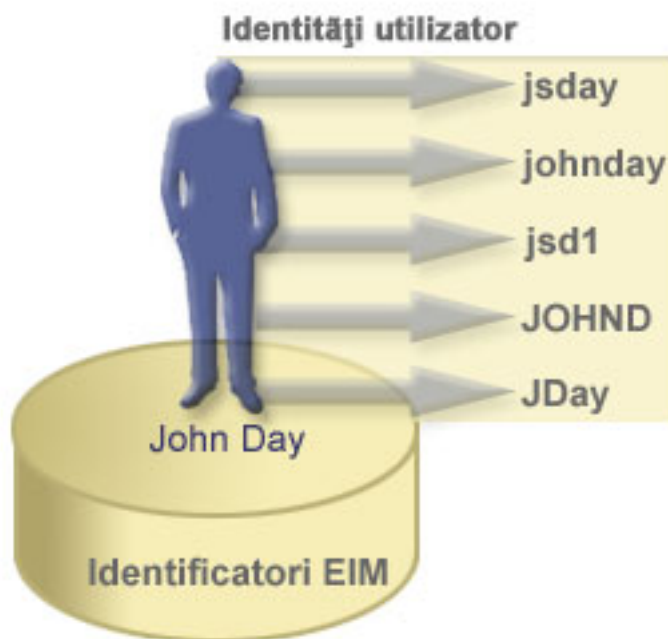
Un identificator EIM (Enterprise Identity Mapping) reprezintă o persoană sau entitate într-o întreprindere. O rețea obișnuită este alcătuită din diferite platforme hardware și aplicații și registrele de utilizatori asociate acestora. Majoritatea platformelor și multe dintre aplicații utilizează registre de utilizatori specifice platformei sau specifice aplicației. Aceste registre de utilizatori conțin toate informațiile de identificare a utilizatorilor pentru utilizatorii care lucrează cu aceste server sau aplicații.

Puteți folosi EIM pentru a crea identificatori EIM unici pentru persoane sau entități din întreprinderea dumneavoastră. Puteți crea apoi asocieri de identificatori (mapări de identitate unu-la-unu), între identificatorul EIM și diversele identități ale persoanei sau entității pe care o reprezintă identificatorul EIM. Acest proces face mai ușoară construirea aplicațiilor cu mai multe niveluri, eterogene. De asemenea, devine mai ușoară construirea și folosirea uneltelor care simplifică administrarea pe care o implică gestionarea fiecărei identități de utilizator pe care o persoană sau o entitate o are în întreprindere.

### Identificatorul EIM care reprezintă o persoană

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

**Figura 3:** Relația dintre identificatorul EIM pentru *John Day* și diferitele sale identități de utilizator

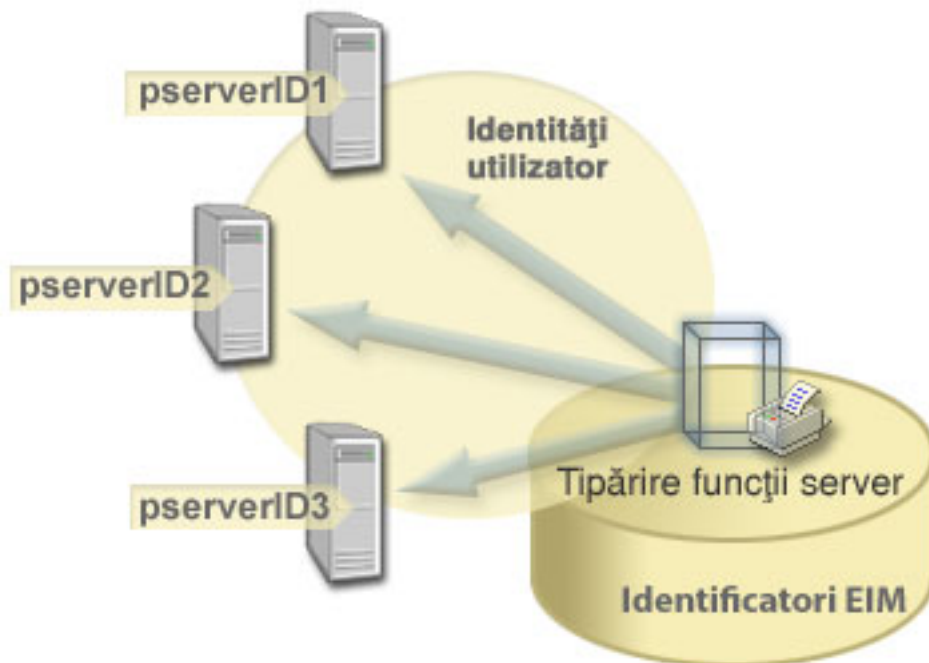


În EIM, puteți crea asocieri care definesc relațiile dintre identificatorul lui *John Day* și fiecare dintre diferitele identități de utilizator pentru *John Day*. Creând asocierile pentru a defini aceste relații, puteți scrie aplicații care utilizează API-urile EIM pentru a căuta o identitate de utilizator necesară și necunoscută, pe baza unei identități de utilizator cunoscute.

### Identificatorul EIM care reprezintă o entitate

Pe lângă reprezentarea utilizatorilor, identificatorii EIM pot reprezenta entități din cadrul întreprinderii dumneavoastră, așa cum ilustrează Figura 4. De exemplu, funcția de server de tipărire dintr-o întreprindere rulează adesea pe mai multe sisteme. În Figura 4, funcția de server de tipărire din întreprindere rulează pe trei sisteme diferite, sub trei identități de utilizator diferite, pserverID1, pserverID2 și pserverID3.

**Figura 4:** Relația dintre identificatorul EIM care reprezintă funcția de server de tipărire și diferitele identități de utilizator pentru acea funcție



Cu EIM, puteți crea un singur identificator care să reprezinte funcția de server de tipărire din cadrul întregii întreprinderi. Așa cum se vede în exemplu, identificatorul EIM Funcție server de tipărire reprezintă entitatea funcției propriu-zise de server de tipărire din întreprindere. Sunt create asocieri pentru a defini relațiile dintre identificatorul EIM (Funcție server de tipărire) și fiecare identitățile folosite pentru funcție (pserverID1, pserverID2 și pserverID3). Aceste asocieri permit dezvoltatorilor de aplicații să utilizeze operațiile de căutare EIM pentru a găsi o anumită funcție server de tipărire. Furnizorii de aplicații pot scrie apoi aplicații distribuite care gestionează mai ușor funcția server de imprimare din cadrul întreprinderii.

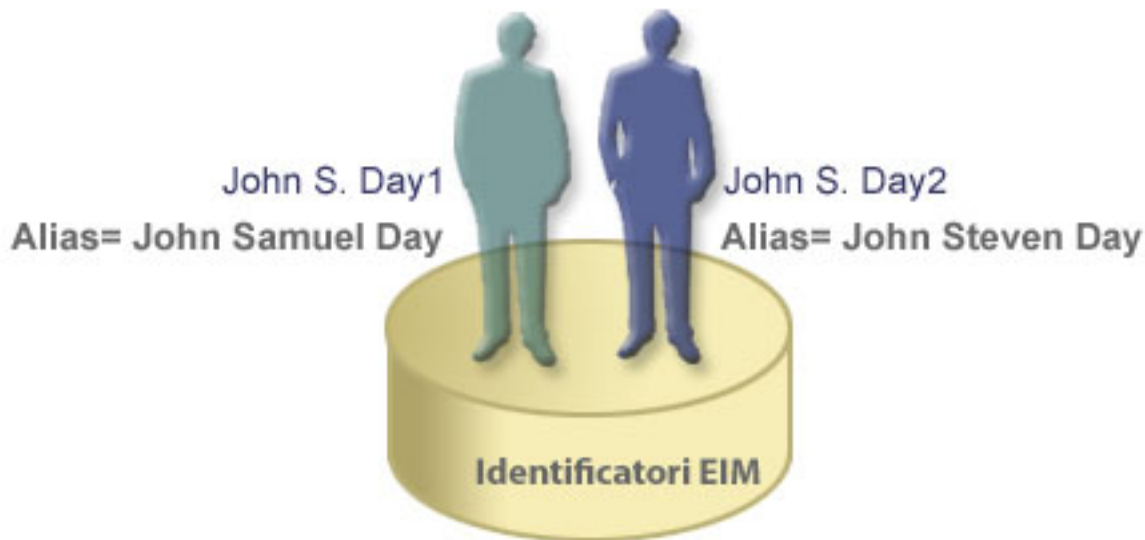
## Identificatorii EIM și crearea de aliasuri

Numele de identificatori EIM trebuie să fie unice în cadrul unui domeniu EIM. Aliasurile pot ajuta în situațiile în care utilizarea unor nume de identificatori unice poate fi dificilă. Un exemplu privind utilitatea aliasului de identificator EIM îl reprezintă situațiile în care numele adevărat al unei persoane este diferit de numele după care este cunoscută. De exemplu, două persoane diferite din cadrul unei întreprinderi pot avea același nume și aceasta poate crea confuzie dacă utilizați 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 diferiți pentru a face distincția între aceștia: *John S. Day1* și *John S. Day2*. Însă nu este evident care persoană *John S. Day* este reprezentată de fiecare dintre acești identificatori.

**Figura 5:** Aliasuri pentru doi identificatori EIM bazați pe un nume propriu comun, *John S. Day*





Prin utilizarea de aliasuri, administratorul EIM poate furniza informații suplimentare despre persoană pentru fiecare identificator EIM. Fiecare identificator EIM poate avea mai multe aliasuri pentru a identifica pe care *John S. Day* îl reprezintă. De exemplu, aliasurile suplimentare pot conține numărul de angajat, numărul departamentului, profesia fiecărui utilizator sau un alt atribut distinctiv. În acest exemplu, un alias pentru John S. Day1 poate fi John Samuel Day, iar un alias pentru John S. Day2 poate fi John Steven Day.

Puteți folosi informațiile aliasului pentru a localiza un anumit identificator EIM. De exemplu, o aplicație care utilizează EIM poate specifica un alias pe care îl folosește pentru a găsi identificatorul EIM corespunzător. Un administrator poate adăuga acest alias unui identificator EIM, astfel că aplicația poate folosi aliasul în locul numelui unic de identificare pentru operațiile EIM. O aplicație poate specifica aceste informații atunci când folosește API-ul Get EIM Target Identities from the Identifier (`eimGetTargetFromIdentifier()`) pentru a realiza o operație de căutare EIM ca să găsească identitatea de utilizator de care are nevoie.

#### Concepte înrudite

“Domeniul EIM” la pagina 6

Un domeniu EIM (Enterprise Identity Mapping) este un director în care un server LDAP (Lightweight Directory Access Protocol) care conține date EIM pentru o întreprindere.

## Definițiile de registru EIM

O definiție registru EIM (Enterprise Identity Mapping) este o intrare în EIM pe care o creați pentru a reprezenta un registru de utilizatori real, care există pe un sistem în întreprindere. Un registru de utilizatori funcționează asemănător unui director care conține o listă a identităților utilizator valide pentru un anumit sistem sau pentru o anumită aplicație.

Un registru de utilizatori de bază conține identitățile utilizator și parolele acestora. Un exemplu de registru de utilizatori este registrul z/OS Security Server RACF (Resource Access Control Facility). Registrele de utilizatori pot de asemenea conține alte informații. De exemplu, un director LDAP (Lightweight Directory Access Protocol) conține nume distinctive de asociere, parole și controale de acces la datele care sunt stocate în LDAP. Alte exemple de registre de utilizatori obișnuiți sunt principalii dintr-o regiune Kerberos sau identitățile utilizator din domeniul Windows Active Directory și registrul de profiluri utilizator i5/OS.

Puteți defini de asemenea registre de utilizatori care exista în cadrul altor registre de utilizatori. Unele aplicații utilizează un subset al identităților utilizator în cadrul unei singure instanțe a unui registru de utilizatori. De exemplu, registrul z/OS Security Server (RACF) poate conține registrele de utilizatori specifici care sunt un subset de utilizatori din tot registrul de utilizatori RACF.

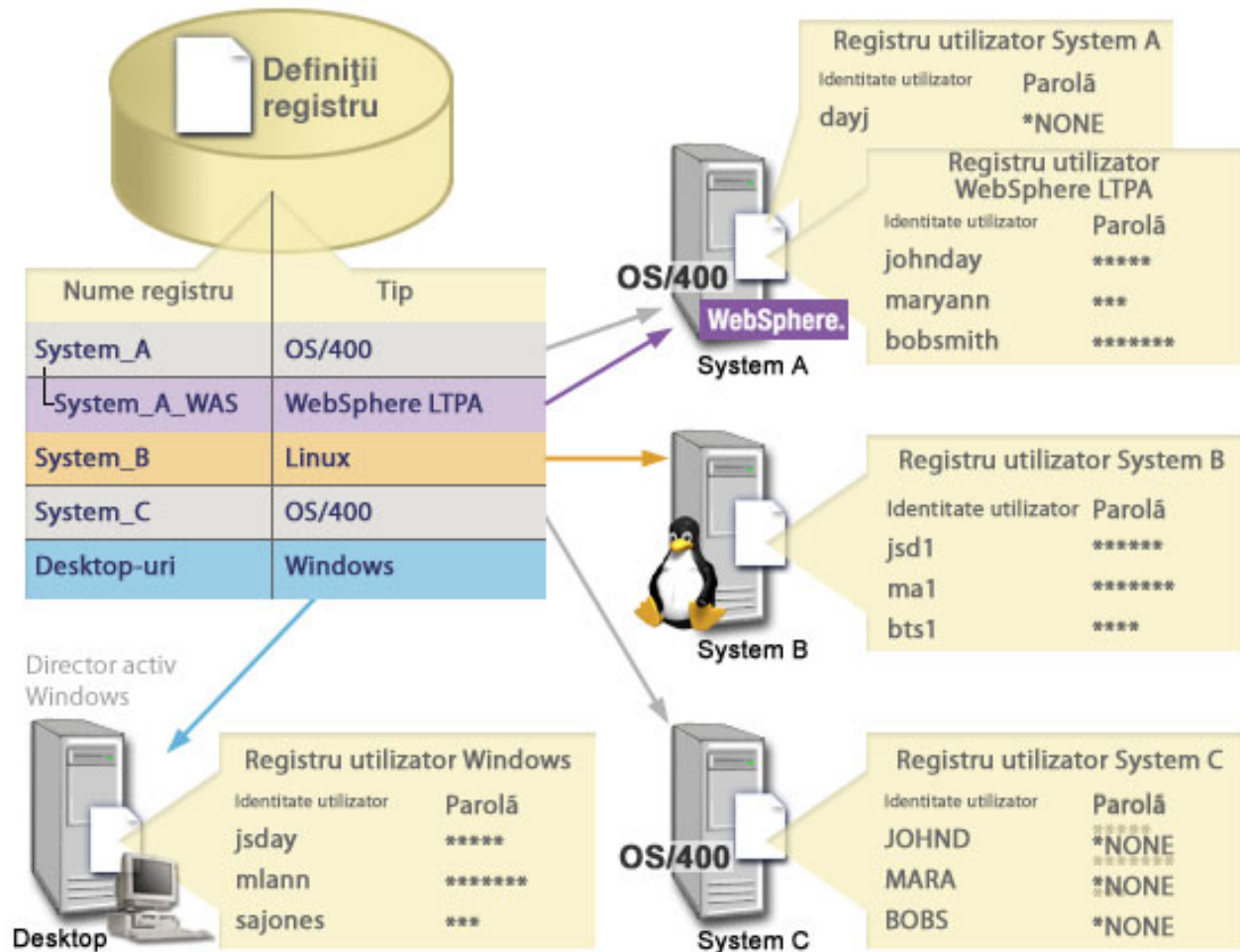
Definițiile de registru EIM furnizează informații cu privire la acele registre de utilizatori dintr-o întreprindere. Administratorul definește aceste registre pentru EIM prin furnizarea informațiilor următoare:

- Un nume unic, arbitrar, de registru EIM. Fiecare definiție pentru registru reprezintă o instanță specifică a unui registru de utilizatori. Ca urmare, ar trebui să alegeți un nume de definiție de registru EIM care să vă ajute să identificați instanța particulară a registrului de utilizatori. De exemplu, ați putea alege numele de gazdă TCP/IP pentru un registru de utilizatori al unui sistem sau numele de gazdă combinat cu numele aplicației pentru un registru de utilizatori de aplicație. Puteți folosi orice combinație de caractere alfanumerice, majuscule sau litere mici și spații pentru a crea nume de definiții registru EIM unice.
- Tipul registrului de utilizatori. Există un număr de tipuri de registre de utilizatori predefinite pe care EIM le furnizează pentru a acoperi majoritatea registrelor de utilizatori ale sistemelor de operare. Acestea includ:
  - AIX
  - Domino - nume lung
  - Domino - nume scurt
  - Kerberos
  - Kerberos - sensibil la majuscule
  - LDAP
  - LDAP - nume scurt
  - Linux
  - Novell Directory Server
  - Altul
  - Altul - sensibil la majuscule
  - i5/OS (sau OS/400)
  - Tivoli Access Manager
  - RACF
  - Windows - local
  - Domeniu Windows (Kerberos) (Acest tip este sensibil la majuscule.)
  - X.509

Deși tipurile de definiții de registre predefinite acoperă majoritatea registrelor de utilizatori ale sistemelor de operare, puteți dori să creați o definiție de registru pentru care EIM nu include un tip un tip de registru predefinit. În această situație aveți două opțiuni. Puteți, fie să folosiți o definiție de registru care se potrivește cu caracteristicile registrului dumneavoastră de utilizatori sau puteți defini un tip de registru de utilizatori privat. De exemplu în figura 6, administratorul a urmat procesul cerut și a definit tipul de registru sa WebSphere LTPA pentru definiția registru aplicație System\_A\_WAS.

În Figura 6, administratorul a creat definiții pentru registrul sistem EIM pentru registrele de utilizatori care reprezintă System A, System B, System C și un Windows Active Directory care conține principalii Kerberos ai utilizatorilor cu care utilizatorii se înregistrează pe stațiile de lucru desktop. În plus, administratorul a creat o definiție pentru registrul aplicație pentru WebSphere (R) LTPA (Lightweight Third-Party Authentication), care rulează pe System A. Numele definiției registrului pe care îl folosește administratorul ajută la identificarea apariției specifice a tipului de registru de utilizatori. De exemplu, o adresă IP sau un nume de gazdă este adesea suficient pentru multe tipuri de registre de utilizatori. În acest exemplu, administratorul folosește System\_A\_WAS ca nume definiție pentru registrul de aplicație pentru a identifica această instanță specifică a aplicației WebSphere LTPA. El a specificat de asemenea că registrul sistem părinte pentru definiția registrului aplicație este registrul System\_A.

**Figura 6:** Definițiile de registru EIM pentru cinci registre de utilizatori într-o întreprindere



**Notă:** Pentru a reduce în continuare nevoia de parole utilizator, administratorul din Figura 6 setează parolele profilului utilizator i5/OS pe System A și pe System C la \*NONE. Administratorul în acest caz configurează un mediu de semnare unică și singura aplicație cu care utilizatorii săi lucrează sunt aplicații EIM-activate ca Navigator System i. În consecință, administratorul vrea să înlăture parolele din profilurile lor utilizator i5/OS astfel încât ambii utilizatori și el să aibă mai puține parole de gestionat.

### Concepte înrudite

“Domeniul EIM” la pagina 6

Un domeniu EIM (Enterprise Identity Mapping) este un director în care un server LDAP (Lightweight Directory Access Protocol) care conține date EIM pentru o întreprindere.

“Definirea tipului de registru de utilizatori privat în EIM” la pagina 93

Când creați o definiție registru EIM (Enterprise Identity Mapping) puteți specifica unul din numerele de tipuri de registru de utilizatori predefinite pentru a reprezenta un registru de utilizatori actual care există pe un sistem din întreprindere.

### Definițiile de registru de sistem

O definiție pentru registru sistem este o intrare pe care o creați în EIM (Enterprise Identity Mapping) pentru a reprezenta și descrie un registru utilizator distinct într-o stație de lucru sau într-un server.

Puteți crea o definiție de registru sistem EIM pentru un registru de utilizatori când registru în întreprindere are următoarele trăsături:

- Registrul este furnizat de un sistem de operare, ca AIX, i5/OS sau de un produs de gestiune securitate ca z/OS Facilitate de accesare resursă(RACF).

- Registrul conține identități utilizator care sunt unice unei aplicații specifice, precum Lotus Notes.
- Registrul conține identități utilizator distribuite, cum ar fi principalii Kerberos sau numele distinctive Lightweight Directory Access Protocol (LDAP).

Operațiile de căutare EIM se realizează corect indiferent dacă un administrator EIM definește un registru fie ca sistem, fie ca aplicație. Totuși, definițiile de registru separate permit ca datele de mapare să fie gestionate pe baza de aplicație. Responsabilitatea gestionării mapărilor specific aplicației poate fi alocată unui administrator pentru un registru specific.

### Operații înrudite

“Adăugarea unei definiții de registru aplicație” la pagina 91

Pentru a crea o definiție registru de aplicație, trebuie să fiți conectat la domeniul EIM (Enterprise Identity Mapping) în care vreți să lucrați și trebuie să aveți control acces EIM.

## Definițiile de registru de aplicații

O definiție pentru registrul aplicație este o intrare în EIM (Enterprise Identity Mapping) pe care o creați să descrie și să reprezinte un subset de identități utilizator care sunt definite într-un registru sistem. Aceste identități utilizator partajează un set comun de atribute sau caracteristici care le permit să utilizeze o anumită aplicație sau un set de aplicații.

Definițiile registru de aplicații reprezintă registrele de utilizatori care există în alte registre de utilizatori. De exemplu, registrul z/OS Security Server (RACF) poate conține registrele de utilizatori specifici care sunt un subset de utilizatori din tot registrul de utilizatori RACF. Din cauza acestei relații, trebuie să specificați numele registrului sistemului părinte pentru fiecare definiție pentru registrul de aplicație pe care o creați.

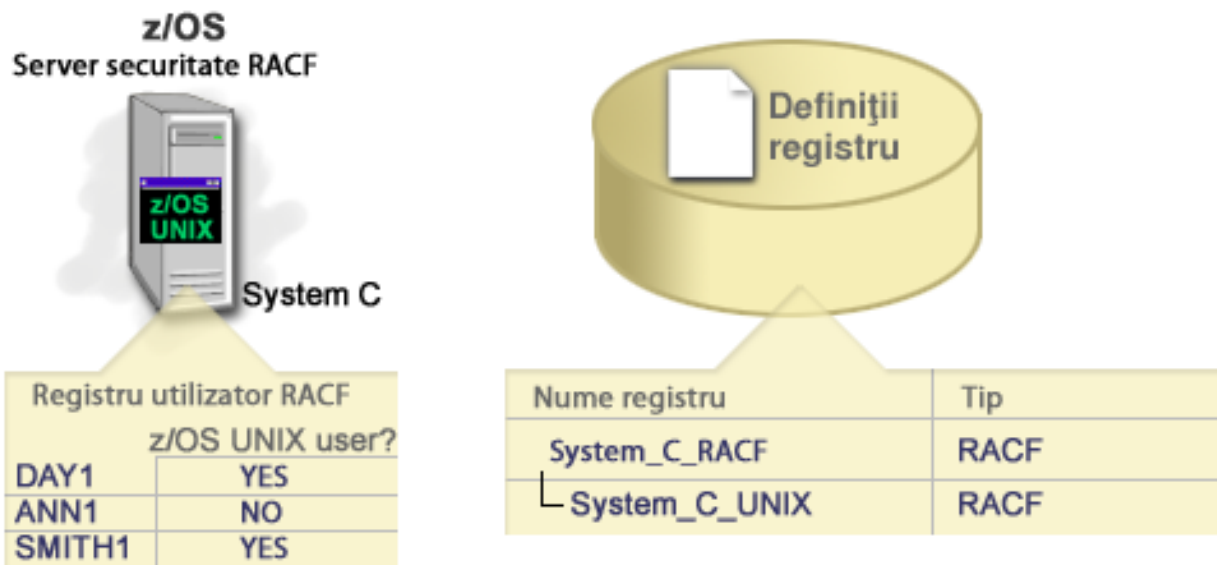
Puteți crea o definiție pentru registrul de aplicație EIM pentru un registru de utilizatori când identitățile utilizatorilor din registru au următoarele caracteristici:

- Identitățile utilizator pentru o aplicație nu sunt memorate într-un registru de utilizatori specific unei aplicații.
- Identitățile utilizator pentru o aplicație sunt memorate într-un registru de utilizatori pentru alte aplicații.

Operațiile de căutare EIM funcționează corect indiferent dacă un administrator EIM creează o aplicație sau o definiție pentru registrul sistem pentru un registru de utilizatori. Totuși, definițiile de registru separate permit ca datele de mapare să fie gestionate pe baza de aplicație. Responsabilitatea gestionării mapărilor specific aplicației poate fi alocată unui administrator pentru un registru specific.

De exemplu, Figura 7 arată cum a creat un administrator EIM o definiție pentru registrul sistem care reprezintă un registru z/OS Security Server RACF. Administratorul a creat de asemenea o definiție pentru registrul aplicație care să reprezinte identitățile utilizator din registrul RACF care utilizează z/OS<sup>(TM)</sup> UNIX System Services (z/OS UNIX). System C conține un registru de utilizatori RACF care conține informații pentru identitățile utilizator, DAY1, ANN1 și SMITH1. Două din aceste identități de utilizatori (DAY1 și SMITH1) accesează z/OS UNIX pe System C. Aceste identități utilizator sunt de fapt utilizatori RACF cu atribute unice care-i identifică ca utilizatori z/OS UNIX. În definiția registrului EIM, administratorul a definit System\_C\_RACF pentru a reprezenta registrul general RACF. Administratorul a definit de asemenea System\_C\_UNIX pentru a reprezenta identitățile utilizator care au atribute z/OS UNIX.

**Figura 7:** Definițiile de registru EIM pentru registrul de utilizatori RACF și pentru utilizatorii z/OS UNIX



## Definiții registru grup

Gruparea logică a definițiilor registrului vă permite să reduceți cantitatea de lucru pe care trebuie să o realizați pentru a configura maparea EIM. Puteți gestiona o definiție pentru registrul grup într-un mod similar cu modul în care gestionați o definiție pentru registrul individual.

Toți membrii definiției pentru registrul grup conțin cel puțin o identitate utilizator comun în care doriți să creați o asociere de sursă sau destinație. Grupând membrii împreună puteți crea doar o singură asociere, în locul mai multor asocieri, la definiția pentru registrul grup și la identitatea utilizatorului

De exemplu, John Day se înregistrează pe sistemul său primar cu identitatea utilizator de jday și utilizează aceeași identitate utilizator JOHND, pe sisteme multiple. De aceea, registrul de utilizatori pentru fiecare sistem conține identitatea utilizator JOHND. În mod obișnuit, John Day creează o asociere de destinație separată de identificatorul EIM John Day pentru fiecare dintre registrele de utilizatori individuale care conțin JOHND. Pentru a reduce cantitatea de lucru pe care trebuie să o realizeze ca să configureze maparea EIM, el poate crea o definiție pentru registrul grup cu toate registrele de utilizatori care păstrează identitatea de utilizator JOHND ca membri ai grupului. El poate apoi să creeze o singură asociere de destinație din identificatorul EIM John Day în definiția pentru registrul grup decât asocieri de destinație multiple din identificatorul EIM John Day la fiecare definiție pentru registrul individual. Această unică asociere de destinație la definiția pentru registrul grup permite identității utilizatorului John Day de jday să mapeze la identitatea utilizatorului JOHND.

Citiți următoarele informații despre definițiile pentru registrul de grup

- Toți membrii (definițiilor pentru registrul individual) ai definițiilor pentru registrul grup trebuie să aibă aceeași sensibilitate la majuscule.
- Toți membrii (definițiilor pentru registrul individual) ai definițiilor pentru registrul grup trebuie să fie definiți în domeniul EIM înainte să-i puteți adăuga la o definiție pentru registrul grup.
- O definiție registru poate fi membră a mai multor grupuri, dar ar trebui să evitați să specificați un registru de utilizatori individual ca membru al mai multor definiții registru grup, deoarece operația de căutare ar putea să returneze rezultate ambigue. Definiția de registru grup nu poate fi un membru al altei definiții de registru grup.

### Concepte înrudite

“Exemple de operații de căutare: Exemplul 5” la pagina 35

Utilizați acest exemplu pentru a afla despre operațiile de căutare care returnează rezultate ambigue care implică definiții pentru registrul grup.

## Asocierile EIM

O asociere EIM (Enterprise Identity Mapping) este o intrare pe care o creați într-un domeniu EIM pentru a defini o relație între identități utilizator în diferite registre de utilizatori. În funcție de tipul de asociere pe care îl creați, relația este directă sau indirectă.

Puteți crea unul dintre două tipuri de asocieri EIM: asocieri de identificator și asocieri de politică. Puteți folosi asocierile de politică în locul sau în combinație cu asocierile de identificator. Modul în care folosiți asocierile depinde de planul general de implementare EIM.

Pentru a afla mai multe despre lucrul cu asocierile, consultați următoarele informații:

### Informațiile de căutare

Cu EIM (Enterprise Identity Mapping) puteți utiliza date opționale numite informații de căutare pentru a identifica mai de parte o identitate utilizator destinație. Această identitate utilizator destinație poate fi specificată fie într-o asociere de identificator, fie într-o asociere de politică.

Informațiile de căutare reprezintă un șir de caractere unic pe care-l poate folosi, fie API-ul EIM `eimGetTargetFromSource`, fie API-ul EMI `eimGetTargetFromIdentifier` în timpul unei operație de căutare mapare pentru o căutare mai fină pentru identitatea utilizatorului destinație care este obiectul operației. Datele pe care le specificați pentru informațiile de căutare corespund cu parametrul de informații suplimentare utilizatori al registrului pentru aceste API-uri EMI.

Informațiile de căutare sunt necesare doar când o operație de căutare mapare poate întoarce mai mult de o identitate de utilizator destinație. O operație de căutare mapări poate întoarce mai multe identități de utilizator destinație când există una sau mai multe din situațiile următoare:

- Un identificator EIM are mai multe asocieri destinație individuale la același registru destinație.
- Mai mult de un identificator EIM are aceeași identitate utilizator specificată într-o asociere sursă și fiecare din acești identificatori EIM are o asociere destinație la același registru destinație, deși identitatea utilizator specificată pentru fiecare asociere destinație poate fi diferită.
- Mai mult de o asociere politică domeniu implicită specifică același registru destinație.
- Mai mult de o asociere politică registru implicită specifică același registru sursă și același registru destinație.
- Mai mult de o asociere politică filtru certificate specifică aceleași registru sursă X.509, filtru de certificate și registru destinație.

**Notă:** O operație de căutare mapare returnează mai mult de o identitate utilizator destinație poate crea probleme pentru aplicațiile permise EIM, inclusiv aplicațiile și produsele iOS, care nu sunt proiectate să trateze aceste rezultate ambigue. Totuși, aplicațiile de bază iOS ca System i Access pentru Windows nu pot utiliza informații de căutare pentru a distinge printre identități utilizator destinație returnate de o operație de căutare. În consecință, ați putea considera redefinirea asocierilor pentru domeniu pentru a vă asigura că o operație de căutare de mapare poate returna o singură identitate utilizator destinație pentru a se asigura că aplicațiile iOS de bază pot realiza operații de căutare și mapare de identități cu succes.

Puteți folosi informațiile de căutare pentru a evita situațiile în care este posibil pentru operațiile de căutare mapări să întoarcă mai mult de o identitate utilizator destinație. Pentru a împiedica operațiile de căutare mapări să întoarcă mai multe identități utilizator destinație, trebuie să definiți, în fiecare asociere, informații de căutare unice pentru fiecare identitate de utilizator destinație. Aceste informații de căutare trebuie furnizate operației de căutare mapări pentru a vă asigura că operația întoarce o identitate unică de utilizator destinație. Altfel, aplicațiile care se bazează pe EIM s-ar putea să nu poată determina identitatea destinație exactă de folosit.

De exemplu, aveți un identificator EIM numit **John Day** care are două profiluri utilizator pe System A. Unul din aceste profiluri utilizator este **JDUSER** pe System A și altul este **JDSECADM**, care are autorizarea specială de administrator cu securitatea. Există două asocieri destinație pentru identificatorul John Day. Una dintre aceste asocieri destinație este pentru identitatea utilizator **JDUSER** în registrul destinație din **System\_A** și are informații de căutare **autorizare**

utilizator specificate pentru JDUSER. Cealaltă asociere destinație este pentru identitatea utilizator JDSECADM în registrul destinație din System\_A și are informații de căutare responsabil cu securitatea specificate pentru JDSECADM.

Dacă o operație de căutare mapări nu specifică nici o informație de căutare, operația de căutare întoarce amândouă identitățile JDUSER și JDSECADM. Dacă o operație de căutare mapări specifică o informație de căutare autorizare utilizator, operația de căutare întoarce numai identitatea utilizator JDUSER. Dacă o operație de căutare mapări specifică o informație de căutare responsabil cu securitatea, operația de căutare întoarce numai identitatea utilizator JDSECADM.

**Notă:** Dacă ștergeți ultima asociere destinație pentru o identitate utilizator (fie că este o asociere identificator, fie că este o asociere de politică), identitatea utilizator destinație și toată informația de căutare este ștearsă și din domeniu.

Deoarece puteți utiliza asocierile de politică certificat și alte asocieri într-o varietate de moduri de suprapunere, ar trebui să aveți o înțelegere solidă atât a suportului politicii de mapare EIM și despre cum lucrează informațiile de căutare înainte de a crea și utiliza asocierile de politică certificat.

### Concepte înrudite

“Suportul pentru politica EIM și activarea” la pagina 37

Suportul politicii de mapare EIM (Enterprise Identity Mapping) vă permite să folosiți asocieri de politică precum și asocieri identificator specifice într-un domeniu EIM. Puteți folosi asocierile de politică în locul sau în combinație cu asocierile identificator.

“Operațiile de căutare EIM” la pagina 27

O aplicație sau un sistem de operare utilizează un API EIM pentru a realiza o operație de căutare pentru ca aplicația sau sistemul de operare poate mapa de la o identitate utilizator într-un registru la altă identitate utilizator în alt registru. O operație de căutare EIM este un proces prin care o aplicație sau un sistem de operare găsește o identitate de utilizator asociată necunoscută dintr-un anumit registru destinație prin furnizarea unor informații cunoscute și de încredere.

“Asocierile de politică de domeniu implicite” la pagina 21

O asociere de politică domeniu implicită este un tip de asociere de politică pe care îl puteți folosi pentru a crea mapări multe-la-unu între identități utilizator.

“Asocierile de politică registru implicite” la pagina 23

O asociere de politică registru implicită este un tip de asociere de politică pe care îl puteți folosi pentru a crea mapări multe-la-unu între identități utilizator.

## Asocierile de identificator

Un identificator EIM reprezintă o persoană sau entitate specifică din întreprindere. O asociere identificator EIM descrie o relație între un identificator EIM și o singură identitate utilizator dintr-un registru de utilizatori care reprezintă de asemenea acea persoană. Atunci când creați asocieri între un identificator EIM și toate identitățile unei persoane sau entități, furnizați o înțelegere singulară, completă a modului în care acea persoană sau entitate folosește resursele din întreprindere.

Identitățile 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-și asuma acea identitate. Verificarea este realizată deseori prin forțarea acelei persoane care lansează identitatea utilizatorului de a furniza informații 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 funcții sau poate accesa resurse pentru care identitatea a primit privilegii. În trecut, aproape toate aplicațiile erau forțate să folosească identitățile dintr-un singur registru de utilizatori atât pentru autentificare cât și pentru autorizare. Folosind operațiile de căutare EIM, acum aplicațiile pot folosi identitățile dintr-un registru de utilizatori pentru autentificare în timp ce folosesc identități utilizator asociate dintr-un registru diferit pentru autorizare.

Identificatorul EIM furnizează o asociere indirectă între acele identități utilizator, care permite aplicațiilor să găsească o identitate utilizator diferită pentru un identificator EIM pe baza unei identități utilizator cunoscute. EIM furnizează

API-uri care permit aplicațiilor să găsească identitatea unui utilizator necunoscut într-un registru de utilizatori specific (destinație) prin furnizarea unei identități de utilizator cunoscute în alte registre de utilizatori (sursă). Acest proces se numește mapare a identității.

În EIM, un administrator poate defini trei tipuri diferite de asocieri pentru a descrie relația între un identificator EIM și o identitate utilizator. Asocierile identificator pot fi de oricare din tipurile: sursă, destinație sau administrative. Tipul asociației pe care îl creați este bazat pe modul în care e folosită identitatea utilizator. De exemplu, dacă creați o asociație sursă și destinație pentru acele identități utilizator care vreți să participe în operațiile de căutare mapare. Tipic, dacă o identitate utilizator e folosită pentru autentificare, creați o asociație sursă pentru ea. Puteți crea asociații sursă pentru acele identități utilizator care sunt folosite pentru autentificare.

Înainte să puteți crea o asociație identificator, mai întâi trebuie să creați identificatorul EIM corespunzător și definiția registrului EIM corespunzătoare pentru registrul de utilizatori care conține identitatea utilizator asociată. O asociere definește o relație între un identificator EIM și o identitate de utilizator prin folosirea următoarelor informații:

- Numele identificatorului EIM
- Numele identității utilizatorului
- Numele definiției pentru registrul EIM
- Tipul de asociere
- Opțional: informații de căutare pentru a identifica mai departe identitatea utilizator destinație într-o asociație destinație.

## Asocierea sursă

O asociere sursă permite identității utilizatorului să fie folosită ca sursă într-o operație de căutare EIM pentru a găsi o identitate de utilizator diferită care este asociată cu același identificator EIM.

Atunci când o identitate utilizator este folosită pentru *autentificare*, acea identitate utilizator ar trebui să aibă o asociere sursă cu un identificator EIM. De exemplu, ați putea crea o asociere sursă pentru un principal Kerberos deoarece această formă de identitate utilizator este folosită pentru autentificare. Pentru a asigura operații de căutare mapare EIM cu succes pentru identificatori EIM, asocierile sursă și destinație trebuie să fie folosite împreună pentru un singur identificator EIM.

## Asocierea destinație

O asociere destinație permite identității utilizator să fie returnată ca rezultat al unei operații de căutare EIM. Identitățile utilizator care reprezintă utilizatori finali au nevoie în mod normal doar de o asociere destinație.

Atunci când o identitate utilizator este folosită pentru mai degrabă pentru *autorizare* decât pentru autentificare, acea identitate utilizator ar trebui să aibă o asociere destinație cu un identificator EIM. De exemplu, ați putea crea o asociere destinație pentru profilul utilizator i5/OS deoarece acest formular de identitate utilizator determină ce resurse și privilegii are utilizatorul pe platforma specifică System i. Pentru a asigura operații de căutare mapare EIM cu succes pentru identificatori EIM, asocierile sursă și destinație trebuie să fie folosite împreună pentru un singur identificator EIM.

## Relația dintre asocierea sursă și cea destinație

Pentru a asigura operații de căutare mapare cu succes, trebuie să creați cel puțin o asociere sursă și una sau mai multe asocieri destinație pentru un singur identificator EIM. Tipic, creați o asociere destinație pentru fiecare identitate utilizator dintr-un registru de utilizatori pe care persoana o poate folosi pentru autorizare pe sistemul sau aplicația pentru care registrul de utilizatori corespunde.

De exemplu, utilizatorii din întreprinderea dumneavoastră se loghează și autentifică normal la ecranele Windows și accesează o platformă System i pentru a realiza un număr de taskuri. Utilizatorii se loghează la ecranele lor utilizând un

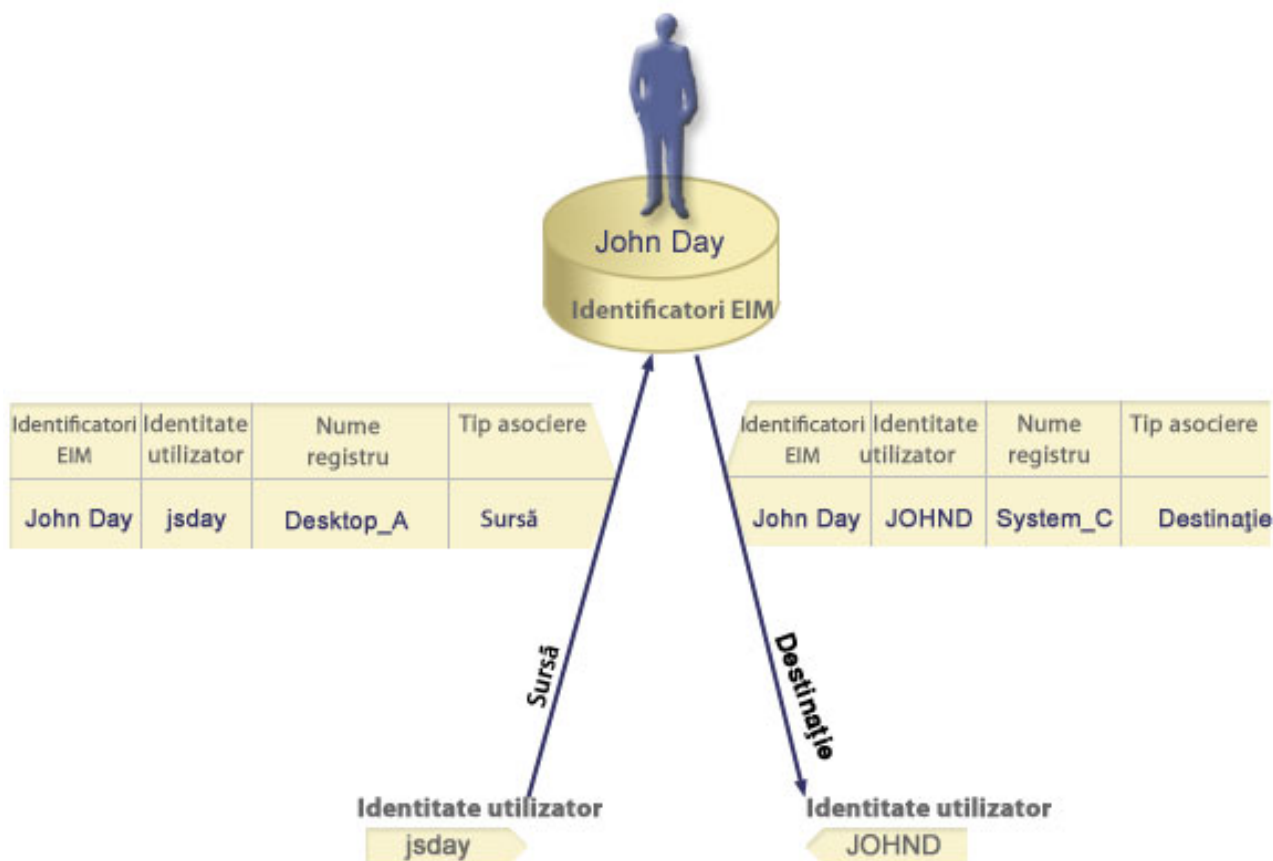


Kerberos principal și logare la platformă System i folosind un profil utilizat i5/OS. Doriți să creați un mediu semnare unică în care utilizatorii se autentifică la ecranele lor folosind Kerberos principal și nu mai trebuie să se autentifice manual la platforma System i.

Pentru a atinge acest scop, creați o asociație sursă pentru principalul Kerberos pentru fiecare utilizator și profilul său EIM. Apoi creați o asocieră de destinație pentru profilul utilizator i5/OS pentru fiecare utilizator și pentru identificatorul EIM al aceluși utilizator. Această configurație asigură că i5/OS poate realiza o operație de căutare mapare pentru a determina profilul utilizator corect necesar pentru un utilizator care accesează platforma System i după ce s-a conectat la desktop-ul lui. i5/OS permite apoi accesul utilizatorului la resursele de pe server bazat pe profilul utilizator corespunzător fără să ceară utilizatorului să se autentifice manual în server.

Figura 6 ilustrează alt exemplu în care un administrator EIM creează două asocieri, o asocieră sursă și una destinație pentru identificatorul EIM John Day pentru a defini relația dintre identificatorul său și două identități utilizator asociate. Administratorul creează o asocieră sursă pentru jsday, un principal Kerberos din registrul de utilizatori Desktops. Administratorul creează de asemenea o asocieră de destinație pentru JOHND, profilul utilizator i5/OS din registrul de utilizatori System\_C. Aceste asocieri furnizează un mijloc pentru aplicații de a obține o identitate utilizator necunoscută (destinația, JOHND) pe baza unei identități utilizator cunoscute (sursa, jsday) ca parte a unei operații de căutare EIM.

**Figura 6:** Asocierile EIM sursă și destinație pentru identificatorul EIM John Day



Pentru a extinde exemplul, presupuneți că administratorul EIM realizează că John Day utilizează același profil utilizator i5/OS, jsd1, pe cinci sisteme diferite. În această situație, administratorul trebuie să creeze șase asocieri pentru identificatorul EIM John Day pentru a defini relația dintre acest identificator și o identitate utilizator asociată în cinci registre de utilizatori: o asocieră de sursă pentru johnday, un principal Kerberos în registrul de utilizatori Desktop\_A și cinci asocieri de destinație pentru jsd1, profilul utilizator i5/OS din cele cinci registre de utilizatori: System\_B,

System\_C, System\_D, System\_E și System\_F. Pentru a reduce cantitatea de lucru care trebuie efectuată pentru a configura maparea EIM, administratorul EIM creează o definiție pentru registrul grup. Membrii definiției de registrul grup includ numele de definiții pentru registrul grup System\_B, System\_C, System\_D, System\_E și System\_F. Gruparea membrilor permite administratorului să creeze o singură asociere destinație la definiția pentru registrul grup și la identitatea utilizatorului, decât mai multe asocieri la numele de definiții registrul individual. Asocierile sursă și destinație furnizează un mijloc pentru ca aplicațiile să obțină o identitate utilizator necunoscută (destinația, jsd1) în cinci registre de utilizatori reprezentate ca membrii definiției pentru registrul grup bazată pe o identitate utilizator cunoscută (sursa, johnday) ca parte a unei operații de căutare EIM.

Pentru unii utilizatori, poate fi necesară crearea atât a unei asocieri sursă, cât și a uneia destinație pentru aceeași identitate utilizator. Aceasta este necesar atunci când o persoană folosește un singur sistem atât ca client cât și ca server sau pentru persoane care sunt administratori.

**Notă:** Identitățile utilizator care reprezintă utilizatori tipici necesită tipic doar o asociere destinație.

Pentru unii utilizatori, poate fi necesară crearea atât a unei asocieri sursă, cât și a uneia destinație pentru aceeași identitate utilizator. Aceasta este necesar atunci când o persoană folosește un singur sistem atât ca client cât și ca server sau pentru persoane care sunt administratori.

De exemplu, un administrator utilizează funcția Administrare centrală în Navigator System i pentru a gestiona un sistem central și mai multe sisteme punct final. Administratorul realizează diverse funcții și aceste funcții pot avea originea pe sistemul central sau pe un sistem punct final. În această situație veți crea atât o asociere sursă cât și una destinație pentru fiecare din identitățile utilizatorului pe fiecare sistem. Asta asigură că, indiferent de sistemul pe care administratorul îl folosește pentru a da originea accesului la unul din celelalte sisteme, identitatea utilizator folosită pentru a da originea accesului la celălalt sistem poate fi mapată pe identitatea utilizator corespunzătoare pentru sistemul următor pe care îl accesează administratorul.

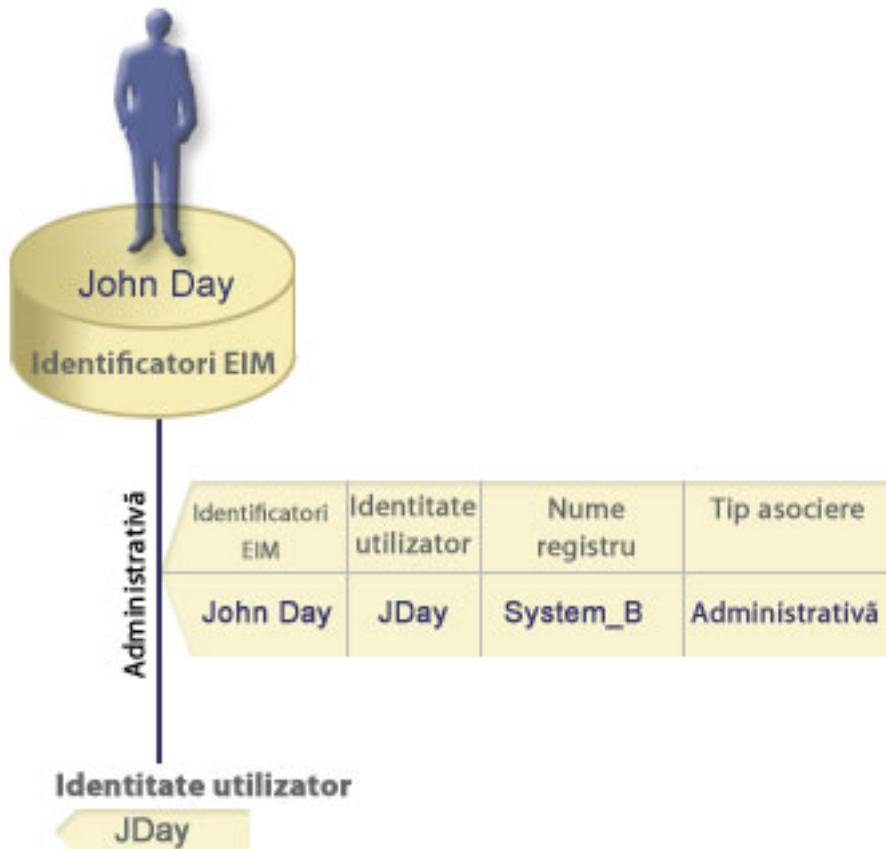
## Asocierea administrativă

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

Din cauza naturii speciale a asocierilor administrative, acest tip de asociere nu poate participa în operații de căutare mapare EIM. În consecință, o operație de căutare EIM care furnizează o identitate utilizator sursă cu o asociere administrativă nu returnează nici un rezultat. Similar, o identitate utilizator cu o asociere administrativă nu este întoarsă niciodată ca rezultat al unei operații de căutare EIM.

Figura 7 arată un exemplu de asociere administrativă. În acest exemplu, un angajat numit John Day are o identitate utilizator John\_Day pe System A și o identitate utilizator JDay pe System B, care e un sistem cu securitate înaltă. Administratorul de sistem dorește să se asigure că utilizatorii se autentifică pe System B folosind doar registrul de utilizatori local al sistemului. Administratorul nu vrea să-i permită unei aplicații să-l autentifice pe John Day pentru sistem folosind un alt mecanism de autentificare. Prin folosirea asocierii administrative pentru identitate utilizator JDay pe System B, administratorul EIM poate vedea că John Day deține un cont pe System B, dar EIM nu întoarce informații despre identitatea JDay în operațiile de căutare EIM. Chiar dacă aplicațiile există pe acest sistem care folosește operațiuni de căutare EIM, nu pot găsi identități utilizator care au asocieri administrative.

**Figura 7:** Asociere EIM administrativă pentru identificatorul EIM John Day



## Asocierile de politică

Politica de mapare EIM (Enterprise Identity Mapping) permite unui administrator EIM să creeze și să utilizeze asocieri de politică pentru a defini o relație între identități utilizator multipli într-unul sau mai multe registre de utilizatori și o identitate utilizator într-un alt registru de utilizatori.

Asocierile de politică folosesc suport pentru politica de mapare EIM pentru a crea mapări multe-la-una între identități utilizator fără a invoca un identificator EIM. Puteți folosi asocierile de politică în locul sau în combinație cu asocierile identificator care furnizează mapări unu-la-unu între un identificator EIM și o singură identitate utilizator.

O asociere de politică afectează doar acele identități utilizator pentru care nu există asocieri EIM individuale. Când există asocieri identificator specifice între un identificator EIM și identitățile utilizator, atunci identitatea utilizator destinație din asocierea identificator este returnată aplicației care realizează operația de căutare, chiar și când există o asociere de politică și e activată folosirea asocierilor de politică.

Puteți crea trei tipuri diferite de asocieri de politică:

### Concepte înrudite

“Operațiile de căutare EIM” la pagina 27

O aplicație sau un sistem de operare utilizează un API EIM pentru a realiza o operație de căutare pentru ca aplicația sau sistemul de operare poate mapa de la o identitate utilizator într-un registru la altă identitate utilizator în alt registru. O operație de căutare EIM este un proces prin care o aplicație sau un sistem de operare găsește o identitate de utilizator asociată necunoscută dintr-un anumit registru destinație prin furnizarea unor informații cunoscute și de încredere.

**Asocierile de politică de domeniu implicite:**

O asociere de politică domeniu implicită este un tip de asociere de politică pe care îl puteți folosi pentru a crea mapări multe-la-unu între identități utilizator.

Puteți folosi o asociere de politică domeniu implicită pentru a mapa un set sursă de identități utilizator multiple (în acest caz, toți utilizatorii din domeniu) pe o singură identitate utilizator destinație într-un registru de utilizatori destinație specificat. Într-o asociere de politică domeniu implicită, toți utilizatorii din domeniu sunt sursa asocierii de politică și sunt mapați pe un singur registru destinație și identitate utilizator destinație.

Pentru a folosi o asociere de politică domeniu implicită, trebuie să activați căutări mapare folosind asocieri de politică pentru domeniu. Trebuie de asemenea să activați căutări mapare pentru registrul de utilizatori destinație al asocierii de politică. Când configurați această activare, registrele de utilizatori din asocierea de politică pot participa în operații de căutare mapare.

Asocierea de politică domeniu implicită are efect când o operație de căutare mapare nu e satisfăcută de asocierea identificatorului, asocierea de politică de filtrare a certificatelor sau asocierea implicită de politică registru pentru registrul destinație. Rezultatul este că certificatele utilizator din domeniu sunt mapate la singura identitate utilizator destinație așa cum a fost specificată de asociația de politică domeniu implicită.

De exemplu, creați o asociere de politică domeniu implicită cu o identitate utilizator destinație `John_Day` în registrul destinație `Registry_xyz` și nu ați creat nici o asociere de identificator sau alte asocieri de politică care mapează la această identitate utilizator. Așadar, când `Registry_xyz` e specificat ca registru destinație în operații de căutare, asocierea de politică domeniu implicită asigură că identitatea utilizator destinație `John_Day` este returnată pentru toate identitățile utilizator din domeniu care nu au nici o altă asociere definită pentru ele.

Specificați aceste două lucruri pentru a defini o asociere de politică domeniu implicită:

- **Registru destinație.** Registrul destinație pe care îl specificați este numele unui registru EIM (Enterprise Identity Mapping) care conține identitatea utilizator la care sunt mapate toate identitățile utilizator din domeniu.
- **Utilizator destinație.** Utilizatorul destinație este numele identității utilizator care e returnată ca destinația unei operații de căutare mapare EIM pe baza acestei asocieri de politică.

Puteți defini o asociere de politică domeniu implicită pentru fiecare registru din domeniu. Dacă două sau mai multe asocieri de politică a domeniului se referă la același registru destinație, trebuie să definiți informații de căutare unice pentru fiecare dintre aceste asocieri de politică pentru a vă asigura că operațiile de căutare mapare se pot distinge între ele. Altfel, operațiile de căutare mapare pot returna identități utilizator destinație multiple. Ca răspuns la aceste rezultate ambigue, aplicațiile care se bazează pe EIM s-ar putea să nu fie capabile să determine identitatea utilizator destinație exactă care va fi folosită.

Deoarece puteți utiliza asocierile de politică într-o varietate de căi de suprapunere, ar trebui să aveți o înțelegere bună a suportului politicii de mapare EIM și căutarea operațiilor de lucru înainte de a crea și utiliza asocierile de politică.

**Notă:** Ați putea dori să creați o asociere de politică a domeniului implicit cu o identitate utilizator destinație care există într-o definiție pentru registrul grup. Toți utilizatorii din domeniu sunt sursa asocierii de politică și sunt mapați la o identitate utilizator destinație într-o definiție pentru registrul grup. Identitatea utilizatorului pe care o definiți în asocierea de politică al domeniului implicit există în membrii definiției pentru registrul grup.

De exemplu, John Day utilizează același profil utilizator `i5/OS, John_Day`, pe cinci sisteme diferite: System B, System C, System D, System E și System F. Pentru a reduce cantitatea de muncă pe care trebuie să o facă pentru a configura maparea EIM, administratorul EIM creează o definiție pentru registrul grup numită `Group_1`. Membrii definiției pentru registrul grup includ numele definițiilor pentru registrul grup `System_B, System_C, System_D, System_E` și `System_F`. Gruparea membrilor permite administratorului să creeze o singură asociere a destinației la definiția pentru registrul grup și la identitatea utilizatorului, decât mai multe asocieri la definițiile pentru registrele individuale.

Administratorul EIM creează o asociere de politică cu o identitate utilizator destinație a `John_Day` în registrul destinație `Group_1`. În acest caz, nu se aplică alte asocieri de identificator specific sau asocieri de politică. Prin

urmare, când `Group_1` este specificat ca registru destinație în operații de căutare, politica asigură că identitatea utilizator destinație pentru `John_Day` este returnată pentru toate identitățile din domeniu care nu au asocieri de identificatori specifici pentru ei.

### Concepte înrudite

“Informațiile de căutare” la pagina 16

Cu EIM (Enterprise Identity Mapping) puteți utiliza date opționale numite informații de căutare pentru a identifica mai de parte o identitate utilizator destinație. Această identitate utilizator destinație poate fi specificată fie într-o asociere de identificator, fie într-o asociere de politică.

“Suportul pentru politica EIM și activarea” la pagina 37

Suportul politicii de mapare EIM (Enterprise Identity Mapping) vă permite să folosiți asocieri de politică precum și asocieri identificator specifice într-un domeniu EIM. Puteți folosi asocierile de politică în locul sau în combinație cu asocierile identificator.

### Asocierile de politică registru implicite:

O asociere de politică registru implicită este un tip de asociere de politică pe care îl puteți folosi pentru a crea mapări multe-la-unu între identități utilizator.

Puteți folosi o asociere de politică registru implicită pentru a mapa un set sursă de identități utilizator multiple (în acest caz, cele dintr-un singur registru) pe o singură identitate utilizator destinație într-un registru de utilizatori destinație specificat. Într-o asociere de politică registru implicită, toți utilizatorii dintr-un singur registru sunt sursa asocierii de politică și sunt mapați pe un singur registru destinație și utilizator destinație.

Pentru a folosi asocieri de politică registru implicite, trebuie să activați căutări de mapare folosind asocieri de politică pentru domeniu. Trebuie de asemenea să activați căutări mapare pentru registrul sursă și să activați căutările mapare și utilizarea asocierilor de politică pentru registrul de utilizatori destinație al asocierii. Când configurați această activare, registrele de utilizatori din asocierea de politică pot participa în operații de căutare mapare.

Asocierea de politică registru implicită are efect când o operație de căutare mapare nu e satisfăcută de asocierile identificatorului, asocierile de politică de filtrare a certificatelor sau asocieri implicite de politică registru pentru registrul destinație. Rezultatul este că certificatele utilizator din registrul sursă sunt mapate la singura identitate utilizator destinație așa cum a fost specificată de asociația de politică registru implicită.

De exemplu, creați o asociere de politică registru implicită care are un registru sursă `my_realm.com`, care sunt principali într-o regiune Kerberos specifică. Pentru această asociere de politică, specificați de asemenea o identitate utilizator destinație de `general_user1` în registrul destinație `i5/OS_system_reg`, care este un profil utilizator specific într-un registru de utilizatori `i5/OS`. În acest caz, nu ați creat nici o asociere de identificatori sau alte asocieri de politică care să se aplice oricărei identități utilizator din registrul sursă. Prin urmare, când `i5/OS_system_reg` este specificat ca registru destinație și `my_realm.com` este specificat ca registrul sursă în operații de căutare, asocierea de politică registru implicit asigură că identitatea utilizatorului destinație a `general_user1` este returnată pentru toate identitățile utilizator în `my_realm.com` care nu au nici o asociere de identificator specific sau nici o asociere de politică filtru de certificat definită pentru ele.

Specificați aceste trei lucruri pentru a defini o asociere de politică registru implicită:

- **Registru sursă.** Aceasta este definiția registrului pe care vreți ca asocierea să-l folosească ca sursă a mapării. Toate identitățile utilizator din acest registru de utilizatori sursă vor fi mapate la utilizatorul destinație specificat al asocierii de politică.
- **Registru destinație.** Registrul destinație pe care îl specificați este numele unei definiții de registru EIM (Enterprise Identity Mapping). Registrul destinație trebuie să conțină identitatea utilizator destinație la care vor fi mapate toate identitățile utilizator din registrul sursă.
- **Utilizator destinație.** Utilizatorul destinație este numele identității utilizator care e returnată ca destinația unei operații de căutare mapare EIM pe baza acestei asocieri de politică.

Puteți defini mai mult de o asociere de politică registru implicită. Dacă două sau mai multe asocieri de politică cu același registru sursă se referă la același registru destinație, trebuie să definiți informații de căutare unice pentru fiecare

din asocierile de politică pentru a asigura că operațiile de căutare mapare se pot distinge între ele. Altfel, operațiile de căutare mapare pot returna identități utilizator destinație multiple. Ca răspuns la aceste rezultate ambigue, aplicațiile care se bazează pe EIM s-ar putea să nu fie capabile să determine identitatea destinație exactă care va fi folosită.

Deoarece puteți utiliza asocierile de politică într-o varietate de moduri de suprapunere, înainte să creați și să utilizați asocierile de politică, ar trebui să aveți o înțelegere bună despre suportul de politică de mapare EIM și cum funcționează operațiile de căutare.

**Notă:** Ați putea dori să creați o asociere de politică a registrului implicit cu o identitate utilizator destinație care există într-o definiție pentru registrul grup. Toți utilizatorii din registrul de utilizatori sursă sunt sursa asocierii de politică și sunt mapați la o identitate utilizator destinație într-o definiție pentru registrul grup. Identitatea utilizator pe care o definiți în asocierea de politică implicită există printre membrii definiției pentru registrul grup.

De exemplu, John Day utilizează același profil utilizator i5/OS, `John_Day`, pe cinci sisteme diferite: `System_B`, `System_C`, `System_D`, `System_E` și `System_F`. Pentru a reduce cantitatea de muncă pe care trebuie să o facă pentru a configura maparea EIM, administratorul EIM creează o definiție pentru registrul grup numită `Group_1`. Membrii definiției pentru registrul grup includ numele definiției pentru registrele `System_B`, `System_C`, `System_D`, `System_E` și `System_F`. Gruparea membrilor permite administratorului să creeze o singură asociere a destinației la definiția pentru registrul grup și la identitatea utilizatorului, decât mai multe asocieri la definițiile registru individuale.

Administratorul EIM creează o asociere de politică registru implicit care are un registru sursă de `my_realm.com`, care sunt principali într-o regiune Kerberos specifică. Pentru această asociere de politică, el specifică de asemenea o identitate utilizator destinație de `John_Day` în registrul destinație `Group_1`. În acest caz, nici o altă asociere de identificator sau asocieri de politică nu se aplică. Prin urmare, când `Group_1` este specificat ca registru destinație și `my_realm.com` este specificat ca registru sursă în operații de căutare, asocierea de politică registru implicit asigură că identitatea utilizatorului destinație de `John_Day` este returnată pentru toate identitățile utilizator în `my_realm.com` care nu au nici o asociere de identificator specific în ele.

### Concepte înrudite

“Informațiile de căutare” la pagina 16

Cu EIM (Enterprise Identity Mapping) puteți utiliza date opționale numite informații de căutare pentru a identifica mai de parte o identitate utilizator destinație. Această identitate utilizator destinație poate fi specificată fie într-o asociere de identificator, fie într-o asociere de politică.

“Suportul pentru politica EIM și activarea” la pagina 37

Suportul politicii de mapare EIM (Enterprise Identity Mapping) vă permite să folosiți asocieri de politică precum și asocieri identificator specifice într-un domeniu EIM. Puteți folosi asocierile de politică în locul sau în combinație cu asocierile identificator.

### Asocierile de politică de filtrare certificate:

O asociație de politică de filtrare certificate este un tip de asociere de politică pe care o puteți folosi pentru a crea mapări multe-la-una între identități utilizator. Puteți folosi o asociere de politică de filtrare certificate pentru a mapa un set sursă de certificate la o singură identitate utilizator într-un registru de utilizatori destinație specificat.

Într-o asociere de politică de filtrare certificate, specificați un set de certificate într-un singur registru X.509 ca sursă a asocierii. Aceste certificate sunt mapate pe un singur registru destinație și utilizator destinație pe care îi specificați. Spre deosebire de o asociere de politică registre implicite în care toți utilizatorii dintr-un singur registru sunt sursa asocierii, domeniul unei asocieri de politică de filtrare certificate este mai flexibil. Puteți specifica un subset de certificate în registru ca sursă. Filtrul de certificat pe care îl specificați pentru asocierea de politică este ceea ce își determină scopul.

**Notă:** Când vreți să mapați toate certificatele într-un registru de utilizatori X.509 la o singură identitate utilizator destinație, creați și folosiți o asociere de politică implicită a registrelor.

Pentru a folosi asocieri de politică de filtrare certificate, trebuie să activați căutări mapare folosind asocieri de politică pentru domeniu. Trebuie de asemenea să activați căutări mapare pentru registrul sursă și la utilizarea asocierilor de politică pentru registrul de utilizatori destinație al asocierii. Când configurați această activare, registrele de utilizatori din asocierea de politică pot participa în operații de căutare mapare.

Când un certificat digital este identitatea utilizator sursă într-o operație de căutare mapare EIM (după ce aplicația de cerere utilizează API-ul EMI `eimFormatUserIdentity()` pentru a formata numele identității utilizatorului), EIM verifică mai întâi să vadă dacă există o asociere între un identificator EIM și identitatea utilizatorului specificat. Dacă nu există nici una, EIM compară apoi informația DN din certificat cu informația DN sau DN parțial specificată în filtrul pentru asocierea de politică. Dacă informația DN din certificat satisface criteriile filtrului, EIM returnează identitatea utilizator destinație pe care a specificat-o asocierea de politică. Rezultatul este că certificatele din registrul X.509 sursă care satisfac criteriile filtrului de certificat sunt mapate la singura identitate utilizator destinație așa cum a fost specificată de asociația de politică de filtrare.

De exemplu, creați o asociere de politică de filtrare care are un registru sursă de `certificates.x509`. Acest registru conține certificatele pentru toți angajații companiei, inclusiv toți pe care managerii din departamentul de resurse umane îi utilizează pentru a accesa unele pagini interne web private și alte resurse pe care le accesează prin modelul System i. Pentru această asociere politică, specificați de asemenea o identitate utilizator destinație a `hr_managers` în registrul destinație `system_abc` care este un profil utilizator specific într-un registru de utilizatori i5/OS. Pentru a vă asigura că doar certificatele care aparțin managerilor resurselor umane sunt acoperite de această asociere de politică, specificați un filtru de certificate cu un SDN (subject distinguished name) de `ou=hrmgr,o=myco.com,c=us`.

În acest caz, nu ați creat nici o asociere de identificatori sau alte asocieri de politică de filtrare certificate care să se aplice oricărei identități utilizator din registrul sursă. Așadar, când `system_abc` e specificat ca registru destinație și `certificates.x509` e specificat ca registru sursă în operații de căutare, asocierea de politică de filtrare certificate asigură că identitatea utilizator destinație `hr_managers` este returnată pentru toate certificatele din registrul `certificates.x509` care se potrivesc filtrului specificat și care nu au nici o asociere de identificator specific definită pentru ele.

Specificați următoarele informații pentru a defini o asociere de politică de filtrare certificate:

- **Registru sursă.** Definiția registrului sursă pe care o specificați trebuie să fie un registru de utilizatori tip X.509. Politica de filtrare certificate creează o asociere între identități utilizator în acest registru de utilizatori X.509 și o singură identitate utilizator destinație specifică. Asocierea se aplică doar acelor identități utilizator din registru care îndeplinesc criteriile filtrului de certificate pe care îl specificați pentru această politică.
- **Filtru certificate.** Un filtru de certificat definește un set de attribute certificat utilizator similare. Asocierea de politică filtrare de certificate mapează orice certificate cu aceste attribute definite în registrul de utilizatori X.509 pe o identitate utilizator destinație specifică. Specificați filtrul pe baza unei combinații între SDN (Subject distinguished name) și IDN (Issuer distinguished name) care se potrivește cu certificatele pe care vreți să le folosiți ca sursă a mapării. Filtrul de certificate pe care îl specificați pentru politică trebuie să existe deja în domeniul EIM.
- **Registru destinație.** Definiția registrului destinație pe care îl specificați este registrul de utilizatori care conține identitatea utilizator pentru care vreți să mapați certificatele care se potrivesc cu filtrul certificatului.
- **Utilizator destinație.** Utilizatorul destinație este numele identității utilizator care e returnată ca destinația unei operații de căutare mapare EIM pe baza acestei asocieri de politică.

Pentru că puteți utiliza asocierea de politică certificat și alte asocieri într-o varietate de moduri de suprapunere, ar trebui să aveți o înțelegere bună atât a suportului politicii de mapare EIM și cum să căutați operații de lucru înainte de a crea și utiliza asocieri de politică certificat.

**Notă:** Ați putea dori să creați o asociere de politică filtru de certificate cu o identitate utilizator care există într-o definiție pentru registru. Utilizatorii din registrul sursă care îndeplinesc criteriile specificate de filtrul de certificate sunt sursa asocierii politice și sunt mapate la o identitate utilizator destinație într-o definiție grup registru. Identitatea utilizatorului pe care o definiți în asocierea de politică filtru de certificat există în membrii definiției pentru registrul grup.

De exemplu, John Day utilizează același profil utilizator i5/OS, `John_Day`, pe cinci sisteme diferite: System B, System C, System D, System E și System F. Pentru a reduce cantitatea de muncă pe care trebuie să o facă pentru

a configura maparea EIM, administratorul EIM creează o definiție pentru registrul grup. Membrii definiției pentru registrul grup includ numele definițiilor registrelor pentru **System\_B**, **System\_C**, **System\_D**, **System\_E** și **System\_F**. Gruparea membrilor permite administratorului să creeze o singură asociere a destinației la definiția registru grup și la identitatea utilizatorului, decât mai multe asocieri la definițiile registru individuale.

Administratorul EIM creează o asociere pentru politica filtrului certificatului unde definește un subset de certificate cu un singur registru X.509 ca sursă a asocierii politice. El specifică o identitate utilizator destinație al **John\_Day** în registrul destinație **Group\_1**. În acest caz, nici o altă asociere identificator specifică sau alte asocieri pentru politica filtrului certificatului nu se aplică. Prin urmare, când **Group\_1** este specificat ca registru destinație în operații de căutare, toate certificatele din registrul X.509 sursă care îndeplinesc criteriul filtrului certificatului sunt mapate la o identitate utilizator destinație specifică.

#### *Filtrele de certificate:*

Un filtru de certificate definește un set de atribute cu nume distinctiv similare pentru un grup de certificate utilizator într-un registru de utilizatori sursă X.509. Puteți folosi filtrul de certificate ca baza unei asocieri de politică de filtrare certificate.

Filtrul de certificate într-o asociere de politică determină care certificate din registrul sursă X.509 specificat să fie mapate la utilizatorul destinație specificat. Acele certificate care au informațiile DN subiect și DN emitent care satisfac criteriile filtrelor sunt mapate la utilizatorul destinație specificat în timpul operațiilor de căutare mapare EIM (Enterprise Identity Mapping).

De exemplu, creați un filtru de certificate cu un SDN (subject distinguished name) de **o=ibm,c=us**. Toate certificatele cu aceste DN-uri ca parte a informațiilor lor SDN îndeplinesc criteriile filtrului, cum ar fi un certificat cu SDN-ul **cn=JohnDay,ou=LegalDept,o=ibm,c=us**. Dacă există mai mult de un filtru de certificate pentru care certificatul îndeplinește criteriile, valoarea celui mai specific filtru cu care se potrivește cel mai mult un certificat este folosită. De exemplu, aveți un filtru de certificate cu un SDN de **o=ibm,c=us** și alt filtru de certificate cu SDN **ou=LegalDept,o=ibm,c=us**. Dacă aveți un certificat în registrul sursă X.509 cu un SDN de **cn=JohnDay,ou=LegalDept,o=ibm,c=us**, atunci al doilea, sau filtrul de certificate mai specific este folosit. Dacă aveți un certificat în registrul sursă X.509 cu un SDN de **cn=SharonJones,o=ibm,c=us**, atunci filtrul de certificate cel mai puțin specific este folosit deoarece certificatul îndeplinește criteriile sale mai îndeaproape.

Puteți specifica una sau ambele din următoarele pentru a defini un filtru de certificate:

- SDN (Subject distinguished name). DN-ul întreg sau parțial pe care îl specificați pentru filtru trebuie să corespundă porțiunii de DN subiect al certificatului digital, care desemnează proprietarul certificatului. Puteți furniza întregul și DN subiect sau puteți furniza unul sau mai multe DN-uri parțiale care ar putea cuprinde SDN-ul complet.
- IDN (Issuer distinguished name). DN-ul întreg sau parțial pe care îl specificați pentru filtru trebuie să corespundă porțiunii de DN emitent al certificatului digital, care desemnează Autoritatea de certificare care a emis certificatul. Puteți furniza întregul și DN emitent sau puteți furniza unul sau mai multe DN-uri parțiale care ar putea cuprinde IDN-ul complet.

Sunt mai multe metode pe care le puteți utiliza pentru a crea un filtru de certificate, inclusiv utilizarea API-ului Format filtru de politică EIM (`eimFormatPolicyFilter`) API pentru a genera filtrele de certificate utilizând un certificat ca șablon pentru a crea DN-urile necesare în formatul și ordinea corectă SDN și IDN.

#### **Concepte înrudite**

“Numele distinctiv” la pagina 46

Un DN (distinguished name) este o intrare LDAP care identifică și descrie în mod unic o intrare într-un server (LDAP) director. Utilizați vrăjitorul Configurare EIM (Enterprise Identity Mapping) pentru a configura serverele de director să memoreze informațiile domeniului EIM. Deoarece EIM folosește serverul de director pentru a memora datele EIM, puteți folosi numele distinctiv ca un mijloc de autentificare la controlerul de domeniu EIM.

#### **Informații înrudite**

API Format EIM Filtru poliță (`eimFormatPolicyFilter`)



## Operațiile de căutare EIM

O aplicație sau un sistem de operare utilizează un API EIM pentru a realiza o operație de căutare pentru ca aplicația sau sistemul de operare poate mapa de la o identitate utilizator într-un registru la altă identitate utilizator în alt registru. O operație de căutare EIM este un proces prin care o aplicație sau un sistem de operare găsește o identitate de utilizator asociată necunoscută dintr-un anumit registru destinație prin furnizarea unor informații cunoscute și de încredere.

Aplicațiile care utilizează API-urile EIM pot efectua aceste operații de căutare EIM de informații doar dacă aceste informații sunt memorate în domeniul EIM. O aplicație poate efectua unul dintre cele două tipuri de operații de căutare EIM în funcție de tipul informațiilor pe care le furnizează aplicația ca sursă a operației de căutare EIM: o identitate utilizator sau un identificator EIM.

Când aplicațiile sau sistemele de operare folosesc API-ul `eimGetTargetFromSource()` pentru a obține o identitate utilizator destinație pentru un registru destinație dat, trebuie să furnizeze o *identitate utilizator ca sursă* pentru operația de căutare. Ca să fie folosită ca sursă pentru o operație de căutare EIM, o identitate utilizator trebuie să aibă o asociere sursă identificator definită pentru ea sau să fie acoperită de o asociere politică. Când o aplicație sau un sistem de operare folosește acest API, aplicația sau sistemul de operare trebuie să furnizeze trei informații:

- O identitate utilizator ca sursă sau punct de plecare pentru operație.
- Numele definiției registru EIM pentru identitatea utilizator sursă.
- Numele definiției registru EIM care este destinația operației de căutare EIM. Această definiție pentru registru descrie registrul de utilizatori care conține identitatea utilizatorului pe care aplicația o caută.

Când aplicațiile sau sistemele de operare folosesc API-ul `eimGetTargetFromIdentifier()` pentru a obține o identitate utilizator pentru un registru destinație dat, trebuie să furnizeze un *identificator EIM ca sursă* pentru operația de căutare EIM. Când o aplicație folosește acest API, aplicația sau trebuie să furnizeze două informații:

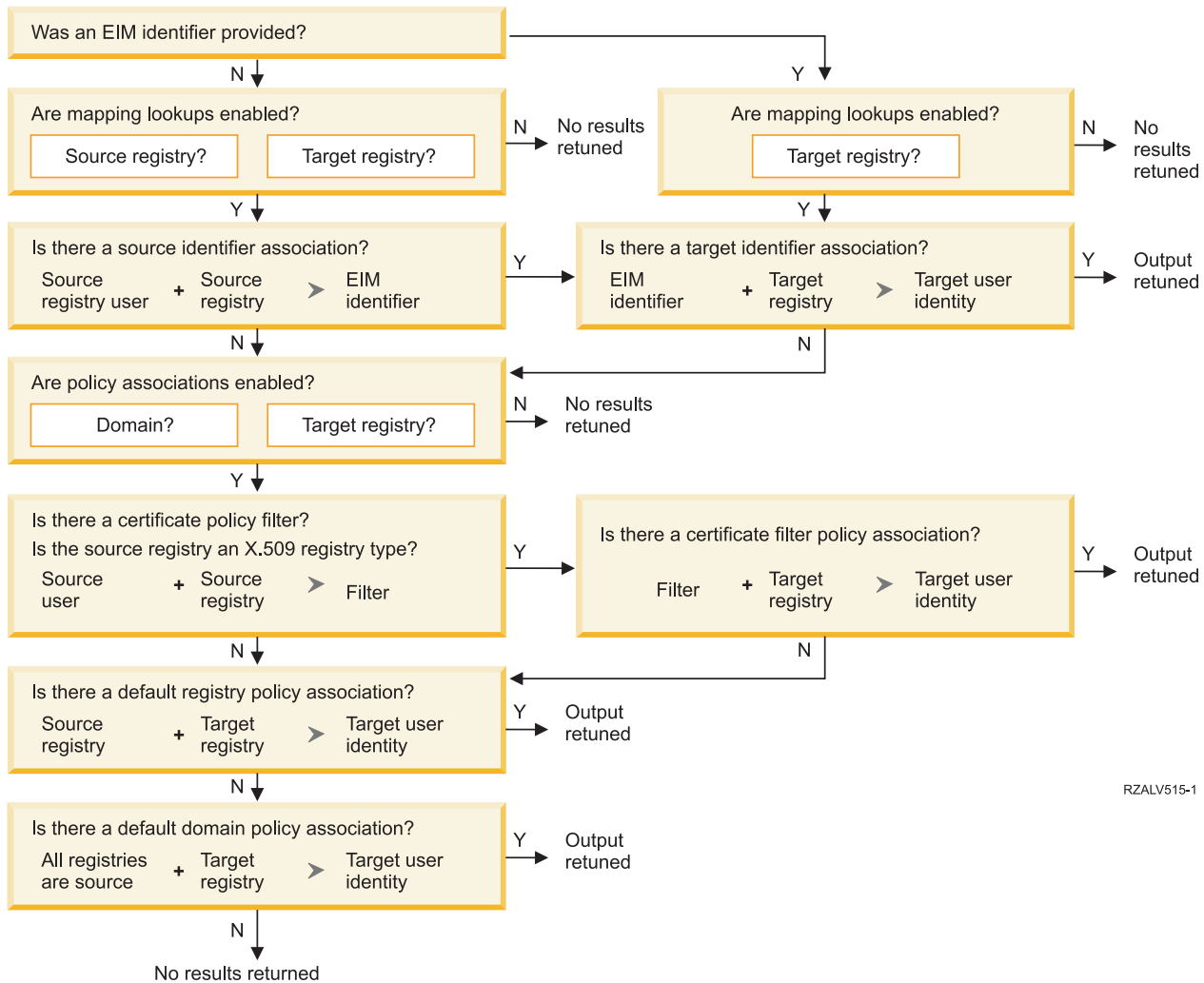
- Un identificator EIM ca sursă sau punct de plecare pentru operație.
- Numele definiției registru EIM care este destinația operației de căutare EIM. Această definiție pentru registru descrie registrul de utilizatori care conține identitatea utilizatorului pe care aplicația o caută.

Pentru ca o identitate utilizator să fie returnată ca destinație a oricărui tip de operație de căutare EIM, identitatea utilizator trebuie să aibă definită o asociere destinație. Această asociere destinație poate fi sub forma unei asocieri identificator sau unei asocieri politică.

Informația livrată este trecută către EIM și operația de căutare EIM o caută și întoarce orice identitate utilizator destinație, căutarea datelor EIM făcându-se în ordinea următoare, după cum se vede și în figura 10:

1. Asociere destinație identificator pentru un identificator EIM. Identificatorul EIM este identificat în una din următoarele feluri: este furnizat de API-ul `eimGetTargetFromIdentifier()`. Sau identificatorul EIM este determinat din informația livrată de API-ul `eimGetTargetFromSource()`.
2. Asociere politică filtrare certificate.
3. Asociere politică registru implicită.
4. Asociere politică domeniu implicită.

**Figura 10:** Diagrama fluxului procesului general al operației de căutare EIM



RZALV515-1

**Notă:** În următorul flux, operațiile de căutare verifică mai întâi definiția pentru registrul individual, precum registrul sursă specificat sau registrul destinație. Dacă operațiile de căutare eșuează în găsirea unei mapări utilizând definiția pentru registrul individual, determină dacă definiția pentru registrul individual este un membru al definiției pentru registrul grup. Dacă este un membru al unei definiții pentru registrul grup, operația de căutare verifică definiția pentru registrul de grup pentru a satisface cererea de căutare mapare.

Operația de căutare se desfășoară după următorul algoritm:

1. Operația de căutare verifică dacă sunt activate căutările de mapări. Operația de căutare determină dacă sunt activate căutările de mapări pentru registrul sursă specificat, pentru registrul destinație specificat sau pentru amândouă. Dacă nu sunt activate căutările de mapare pentru unul sau amândouă registrele, atunci operația de căutare se oprește fără să întoarcă o identitate de utilizator destinație.
2. Operația de căutare verifică dacă există asocieri de identificatori care se potrivesc criteriului de căutare. Dacă a fost furnizat un identificator EIM, operația de căutare folosește numele identificatorului EIM specificat. Altfel, operația de căutare verifică dacă există o asociere sursă identificator anume care se potrivește cu identitatea de utilizator sursă specificată și cu registrul sursă. Dacă există una, operația de căutare o folosește pentru a determina numele identificatorului EIM corespunzător. Apoi, operația de căutare folosește numele identificatorului EIM pentru a căuta pentru o asociere destinație identificator pentru identificatorul EIM care se potrivește cu numele specificat al definiției de registru EIM destinație. Dacă există o asociere destinație identificator care se potrivește, operația de căutare întoarce identitatea utilizatorului destinație definită în asocierea destinație.
3. Operația de căutare verifică dacă este activată folosirea asocierilor de politică. Operația de căutare verifică dacă domeniul este activat ca să permită căutările de mapări folosind asocierile de politică. Operația de căutare verifică

de asemenea dacă registrul destinație este activat să folosească asocierile de politică. Dacă domeniul nu este activat pentru asocierile de politică sau dacă registrul nu este activat pentru asocierile de politică, atunci operația de căutare se oprește fără să întoarcă o identitate utilizator destinație.

4. Operația de căutare verifică pentru asocierile de politică filtrare certificate. Operația de căutare verifică dacă registrul sursă este de tipul X.509. Dacă este un tip de registru X.509, operația de căutare verifică dacă există o asociere politică de filtrare certificate care se potrivește cu numele de definiții registru sursă și destinație. Operația de căutare verifică dacă sunt certificate în registrul sursă X.509 care satisfac criteriul specificat în asocierea de politică filtrare certificate. Dacă există o asociere politică care se potrivește și există certificate care satisfac criteriul de filtrare certificate, operația de căutare întoarce identitatea de utilizator destinație corespunzătoare pentru acea asociere de politică.
5. Operația de căutare verifică asocierile de politică registru implicite. Operația de căutare verifică dacă există o asociere politică care se potrivește cu numele definițiilor registru sursă și destinație. Dacă există o asociere politică care se potrivește operația de căutare întoarce identitatea de utilizator destinație corespunzătoare pentru acea asociere de politică.
6. Operația de căutare verifică asocierile de politică domeniu implicite. Operația de căutare verifică dacă există o asociere politică domeniu implicită definită pentru definiția registru destinație. Dacă există o asociere politică care se potrivește operația de căutare întoarce identitatea de utilizator destinație asociată pentru acea asociere de politică.
7. Operația de căutare nu a putut întoarce nici un rezultat

Pentru a afla mai multe despre operațiile de căutare EIM (Enterprise Identity Mapping) vizualizați următoarele exemple:

#### **Concepte înrudite**

“Domeniul EIM” la pagina 6

Un domeniu EIM (Enterprise Identity Mapping) este un director în care un server LDAP (Lightweight Directory Access Protocol) care conține date EIM pentru o întreprindere.

“Asocierile de politică” la pagina 21

Politica de mapare EIM (Enterprise Identity Mapping) permite unui administrator EIM să creeze și să utilizeze asocieri de politică pentru a defini o relație între identități utilizator multipli într-unul sau mai multe registre de utilizatori și o identitate utilizator într-un alt registru de utilizatori.

“Controlerul de domeniu EIM” la pagina 5

Un controler de domeniu EIM este un server LDAP (Lightweight Directory Access Protocol) care este configurat pentru a gestiona unul sau mai multe domenii EIM. Un domeniu EIM conține toate identificatoarele EIM, asocierile EIM și registrele de utilizatori care sunt definite în acest domeniu. Sistemele (clienți EIM) participă în domeniul EIM prin utilizarea datelor de domeniu pentru operații de căutare EIM.

“Informațiile de căutare” la pagina 16

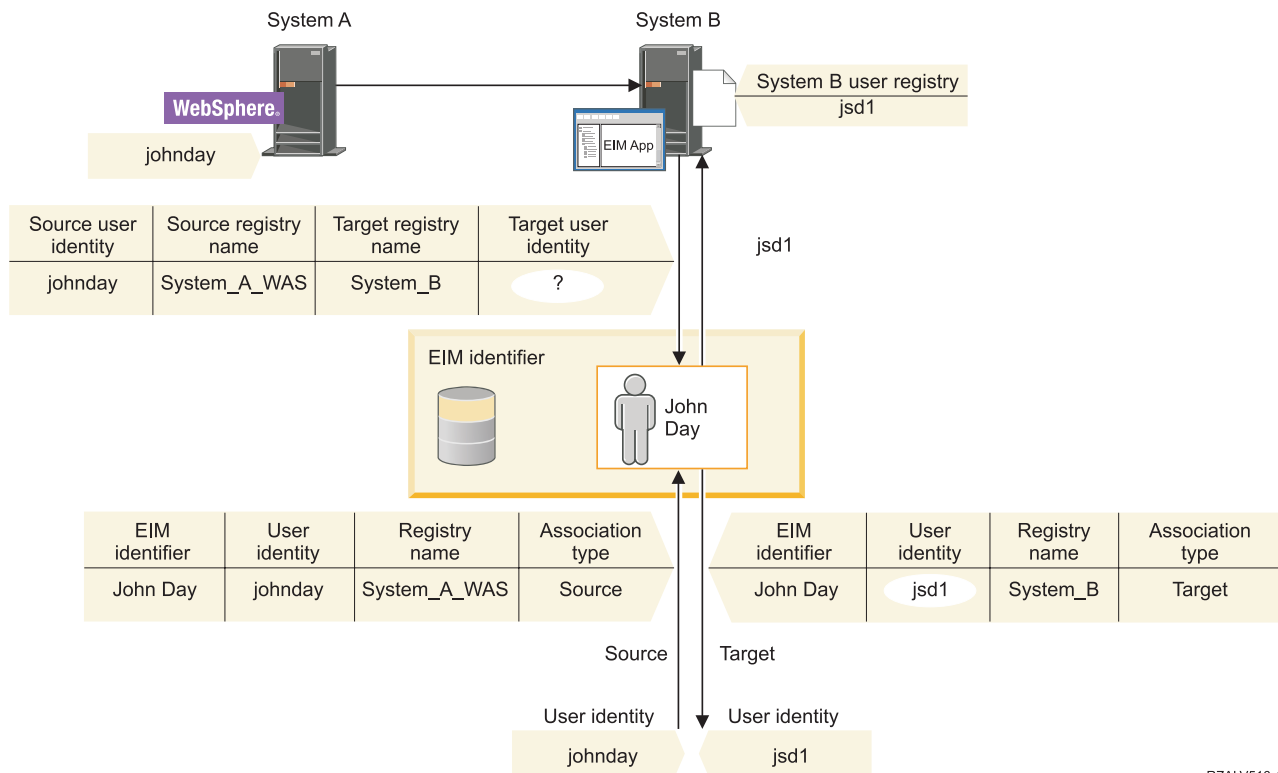
Cu EIM (Enterprise Identity Mapping) puteți utiliza date opționale numite informații de căutare pentru a identifica mai de parte o identitate utilizator destinație. Această identitate utilizator destinație poate fi specificată fie într-o asociere de identificator, fie într-o asociere de politică.

### **Exemple de operații de căutare: Exemplu 1**

Utilizați acest exemplu pentru a afla cum lucrează fluxul de căutare pentru o operație de căutare care returnează o identitate utilizator destinație dintr-o asociere de identitate specifică bazată pe identitatea utilizator cunoscută.

În figura 11, identitatea utilizatorului johnday se autentifică la WebSphere Application Server folosind LPTA (Lightweight Third-Party Authentication) pe System A. WebSphere Application Server pe System A apelează un program integrat pe System B pentru a accesa date pe System B. Programul integrat utilizează API EIM (Enterprise Identity Mapping) pentru a realiza o operație de căutare EIM bazată pe identitatea utilizator de pe System A ca sursă a operației. Aplicația furnizează următoarele informații pentru a efectua operația: johnday ca identitatea utilizator sursă, System\_A\_WAS ca numele definiției de registru EIM sursă și System\_B ca numele definiției de registru EIM destinație. Această informație sursă este trecută la EIM și operația de căutare EIM găsește o asociere de sursă identificator care se potrivește cu informația. Folosind numele identificatorului EIM John Day, operația de căutare EIM caută o asociere destinație a identificatorului pentru acest identificator care se potrivește cu numele definiției registrului EIM destinație pentru System\_B. Când este găsită asocierea destinație potrivită, operația de căutare EIM întoarce aplicației identitatea utilizator jsd1.

**Figura 11:** Operația de căutare EIM întoarce o identitate de utilizator destinație de la asocierile de identificator specifice bazat pe identitatea de utilizator cunoscută johnday



RZALV516-1

## Exemple de operații de căutare: Exemplu 2

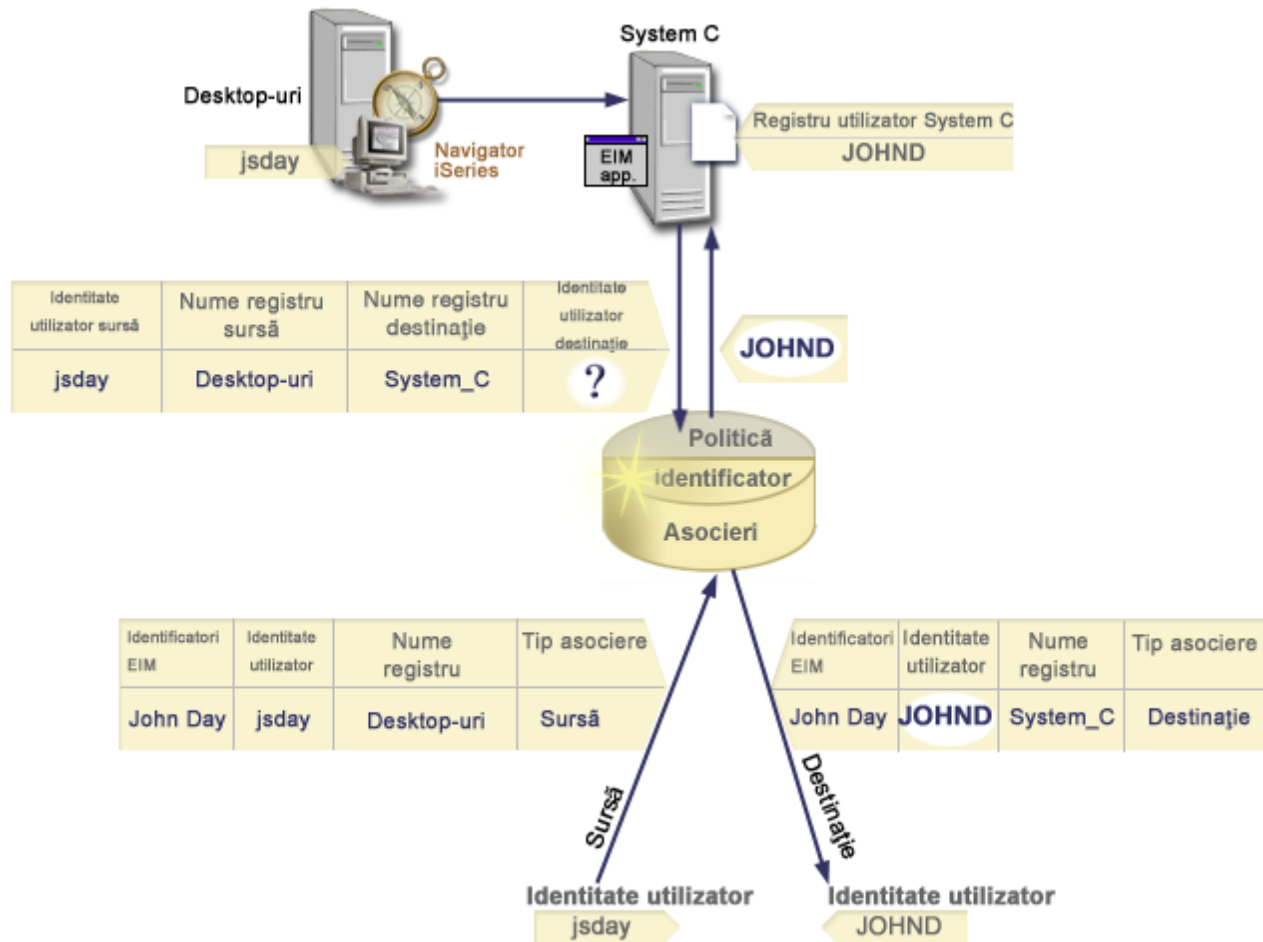
Utilizați acest exemplu pentru a afla cum lucrează fluxul de căutare pentru o operație de căutare care returnează o identitate utilizator destinație dintr-o asociere de identificator specifică bazată pe identitatea principalul Kerberos cunoscut.

În Figura 12, un administrator vrea să mapeze un utilizator Windows într-un registru Windows Active Directory la un profil utilizator i5/OS. Kerberos este metoda de autentificare pe care o folosește Windows și numele registrului Windows Active Directory așa cum l-a definit în EIM ca **Desktops**. Identitatea utilizatorului pe care administratorul dorește să o mapeze este un principal Kerberos numit **jsday**. Numele registrului i5/OS așa cum l-a definit administratorul în EIM este **System\_C** și identitatea utilizator la care administratorul vrea să mapeze este un profil utilizator numit **JOHND**.

Administratorul creează un identificator EIM numit **John Day**. Apoi el adaugă două asocieri la acest identificator EIM:

- O asociere sursă pentru principalul Kerberos numită **jsday** în registrul **Desktops**.
- O asociere destinație pentru profilul utilizator i5/OS numit **JOHND** în registrul **System\_C**.

**Figura 12:** Operația de căutare EIM întoarce o identitate de utilizator destinație de la asocierile de identificator specifice bazat pe principalul Kerberos cunoscut **jsday**



Această configurare permite o operație de căutare mapare pentru a mapa din principalul Kerberos în profilul utilizator i5/OS după cum urmează:

Registru și identitate utilizator sursă	---	Identificatori EIM	---	Identitate utilizator destinație
jsday în registrul Desktops	---	John Day	---	JOHND (în registrul System_C)

Operația de căutare se desfășoară după următorul algoritm:

1. Utilizatorul jsday se loghează și se autentifică la Windows prin intermediul principalului său Kerberos în registrul Windows Active Directory: Desktops.
2. Utilizatorul deschide Navigator System i pentru a accesa date pe System\_C.
3. i5/OS utilizează un API EIM pentru a realiza o operație de căutare EIM cu o identitate utilizator sursă de jsday, un registru sursă de Desktops și un registru destinație de System\_C.
4. Operația de căutare EIM verifică dacă căutările de mapări sunt activate pe registrul sursă Desktops și registrul destinație System\_C. Ele sunt activate.
5. Operația de căutare verifică dacă există o asociere sursă identificator specifică care se potrivește cu identitatea de utilizator sursă furnizată, jsday, într-un registru sursă Desktops.
6. Operația de căutare folosește asocierea sursă identificator potrivită pentru a determina numele identificatorului EIM corespunzător, care este John Day.

7. Operația de căutare folosește numele identificatorului EIM pentru a căuta pentru o asociere destinație identificator pentru identificatorul EIM care se potrivește cu numele specificat al definiției de registru EIM destinație System\_C.
8. Există o asemenea asociere destinație identificator și operația de căutare întoarce identitatea utilizator destinație JOHND, așa cum este definită în asocierea destinație.
9. Cu operația de căutare finalizată, Navigator System i începe să ruleze sub profilul utilizator JOHND. Autorizarea utilizatorului de a accesa resurse și de a realiza acțiuni Navigator System i este determinată de autorizarea definită pentru profilul utilizator JOHND mai degrabă decât autorizarea definită pentru identitatea utilizatorului jsday.

### Exemple de operații de căutare: Exemplu 3

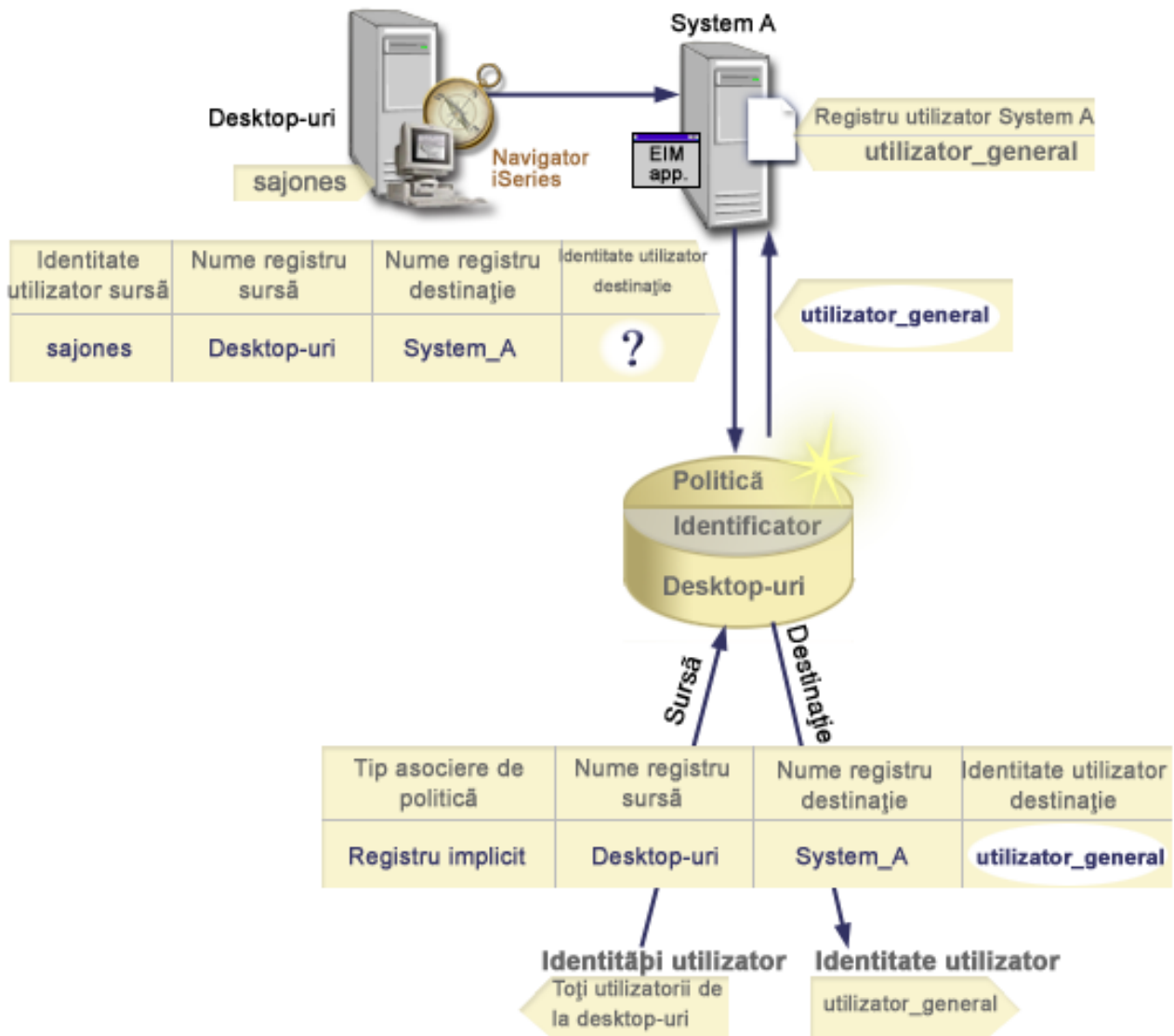
Utilizați acest exemplu pentru a afla cum lucrează fluxul de căutare pentru o operație de căutare care returnează o identitate utilizator destinație dintr-o asociere de politică registru implicit.

În Figura 13, un administrator vrea să mapeze toți utilizatorii stație de lucru din registrul Windows Active Directory la un singur profil utilizator i5/OS numit utilizator\_general într-un i5/OS registru pe care l-a numit System\_A în EIM (Enterprise Identity Mapping). Kerberos este metoda de autentificare pe care o folosește Windows și numele registrului Windows Active Directory așa cum l-a definit în EIM ca Desktops. Una din identitățile utilizator pe care administratorul dorește să o mapeze este un principal Kerberos numit sajones.

Administratorul creează o asociere politică registru implicită cu următoarele informații:

- Un registru sursă Desktops.
- Un registru destinație System\_A.
- Un identificator utilizator destinație utilizator\_general.

**Figura 13:** O operație de căutare întoarce o identitate utilizator destinație dintr-o asociere politică registru implicită.



Această configurare permite o operație de căutare mapare pentru a mapa toți principalii Kerberos în registrul Desktops incluzând principalul sajones, în profilul utilizator i5/OS numit utilizator\_general după cum urmează:

Registru și identitate utilizator sursă	---	Asociere de politică registru implicit	---	Identitate utilizator destinație
sajones în registrul Desktops	---	Asociere de politică registru implicit	---	utilizator_general (în registrul System_A)

Operația de căutare se desfășoară după următorul algoritm:

1. Utilizatorul sajones se înregistrează și se autentifică la desktop-ul său Windows prin principalul său Kerberos din registrul Desktops.
2. Utilizatorul deschide Navigator System i pentru a accesa date pe System A.
3. i5/OS utilizează un API EIM pentru a realiza o operație de căutare EIM cu o identitate utilizator sursă de sajones, un registru sursă de Desktops și un registru destinație de System\_A.
4. Operația de căutare EIM verifică dacă căutărilor de mapări sunt activate pe registrul sursă Desktops și registrul destinație System\_A. Ele sunt activate.

5. Operația de căutare verifică dacă există o asociere sursă identificator specifică care se potrivește cu identitatea de utilizator sursă furnizată, **sajones**, într-un registru sursă **Desktops**. Nu găsește o asociere de identificator potrivită.
6. Operația de căutare verifică de asemenea dacă domeniul este activat să folosească asocierile de politică. Este activat.
7. Operația de căutare verifică de asemenea dacă registrul destinație (**System\_A**) este activat să folosească asocierile de politică. Este activat.
8. Operația de căutare verifică dacă registrul sursă (**Desktops**) este un registru X.509. Nu este.
9. Operația de căutare verifică dacă există o asociere politică de registru implicită care se potrivește cu numele de definiție pentru registrul sursă **Desktops**) și cu numele definiției registru destinație (**System\_A**).
10. Operația de căutare determină dacă există una și întoarce **utilizator\_general** ca identitate de utilizator destinație.

Uneori operația de căutare EIM întoarce rezultate ambigue. Aceasta se poate întâmpla, de exemplu, când mai mult de o identitate utilizator destinație se potrivește criteriului operației de căutare specificat. Unele aplicații permise EIM, inclusiv aplicațiile și produsele i5/OS nu sunt proiectate să trateze aceste rezultate ambigue și ar putea eșua sau da rezultate neașteptate. S-ar putea să fie nevoie să acționați pentru a rezolva această situație. De exemplu, s-ar putea să fie nevoie să modificați configurația EIM sau să definiți informații de căutare pentru fiecare identitate de utilizator destinație pentru a preveni potrivirea mai multor identități utilizator destinație. De asemenea, puteți testa o mapare pentru a determina dacă schimbările făcute funcționează așa cum vă așteptați.

### Exemple de operații de căutare: Exemplul 4

Utilizați acest exemplu pentru a afla cum lucrează fluxul de căutare pentru o operație de căutare care returnează o identitate utilizator destinație într-un registru de utilizatori care este un membru unei definiții pentru registrul grup.

Un administrator vrea să mapeze un utilizator Windows la un profil utilizator i5/OS. Kerberos este metoda autentificată pe care o utilizează Windows și numele registrului așa cum l-a definit administratorul în EIM (Enterprise Identity Mapping) este **Desktop\_A**. Identitatea utilizatorului din administratorul dorește să mapeze este un principal Kerberos numit **jday**. Numele definiției pentru registrul i5/OS așa cum l-a definit administratorul în EIM este **Group\_1** și identitatea utilizator la administratorul dorește să mapeze este un profil utilizator numit **JOHND** care există în trei registre individuale: **System\_B**, **System\_C** și **System\_D**. Fiecare registru individual este un membru al definiției pentru registrul grup **Group\_1**.

Administratorul creează un identificator EIM numit John Day. Apoi el adaugă două asocieri la acest identificator EIM:

- O asociere sursă pentru principalul Kerberos numită **jday** în registrul **Desktop\_A**.
- O asociere destinație pentru profilul utilizator i5/OS numit **JOHND** în registrul **Group\_1**.

Această configurare permite o operație de căutare mapare pentru a mapa din principalul Kerberos în profilul utilizator i5/OS după cum urmează:

Registru și identitate utilizator sursă	--->	Identificator EIM	--->	Identitate utilizator destinație
jday în registrul Desktop_A	--->	John Day	--->	JOHND (în definiția pentru registrul grup Group_1)

Operația de căutare se desfășoară după următorul algoritm:

1. Utilizatorul (**jday**) se înregistrează și se autentifică în Windows pe **Desktop\_A**
2. Utilizatorul deschide Navigator System i pentru a accesa date pe **System\_B**.
3. i5/OS utilizează un API EIM pentru a realiza o operație de căutare EIM cu o identitate utilizator sursă de **jday**, un registru sursă de **Desktop\_A** și un registru destinație de **System\_B**.
4. Operația de căutare EIM verifică dacă căutărilor de mapare sunt permise pentru registrul sursă (**Desktop\_A**) și pentru registrul destinație (**System\_B**).



5. Operația de căutare verifică pentru o asociere de sursă specifică individuală care se potrivește identitatea de utilizator sursă livrată de jday într-un registru sursă Desktop\_A.
6. Operația de căutare utilizează asocierea de sursă potrivită pentru a determina numele identificatorului EIM corespunzător, care este John Day.
7. Operația de căutare utilizează numele identificatorului EIM pentru a căuta o asociere de destinație individuală pentru identificatorul EIM care se potrivește cu numele definiției pentru registrul EIM destinație specificat, de System\_B. (Nu există.)
8. Operațiile de căutare verifică să vadă dacă registrul sursă (Desktop\_A) este membru al vreunei definiții pentru registrul grup. (Nu este.)
9. Operația de căutare verifică să vadă dacă registrul destinație (System\_B) este membru al vreunei definiții pentru registrul grup. Este un membru al definiției pentru registrul grup Group\_1.
10. Operația de căutare utilizează numele identificatorului EIM pentru a căuta o asociere de destinație individuală pentru identificatorul EIM care se potrivește cu numele definiției pentru registrul EIM destinație specificat, de Group\_1.
11. Există astfel de asociere de destinație individuală iar operația de căutare returnează identitatea utilizatorului destinație de JOHND ca definit în asocierea de destinație.

**Notă:** În unele cazuri, operația de căutare EIM returnează rezultate ambigue apoi mai mult o identitate utilizator destinație se potrivește criteriilor specificate operației de căutare. Deoarece EIM nu poate returna o singură identitate utilizator destinație, aplicațiile EIM-activate, inclusiv aplicațiile și produsele 5/OS, care nu sunt proiectate să manevreze aceste rezultate ambigue ar putea eșua sau da rezultate neașteptate. S-ar putea să fie nevoie să acționați pentru a rezolva această situație. De exemplu, s-ar putea să fie nevoie să modificați configurația EIM sau să definiți informații de căutare pentru fiecare identitate de utilizator destinație pentru a preveni potrivirea mai multor identități utilizator destinație. Puteți testa o mapare să determine dacă modificările pe care le-ați făcut merg așa cum se așteaptă.

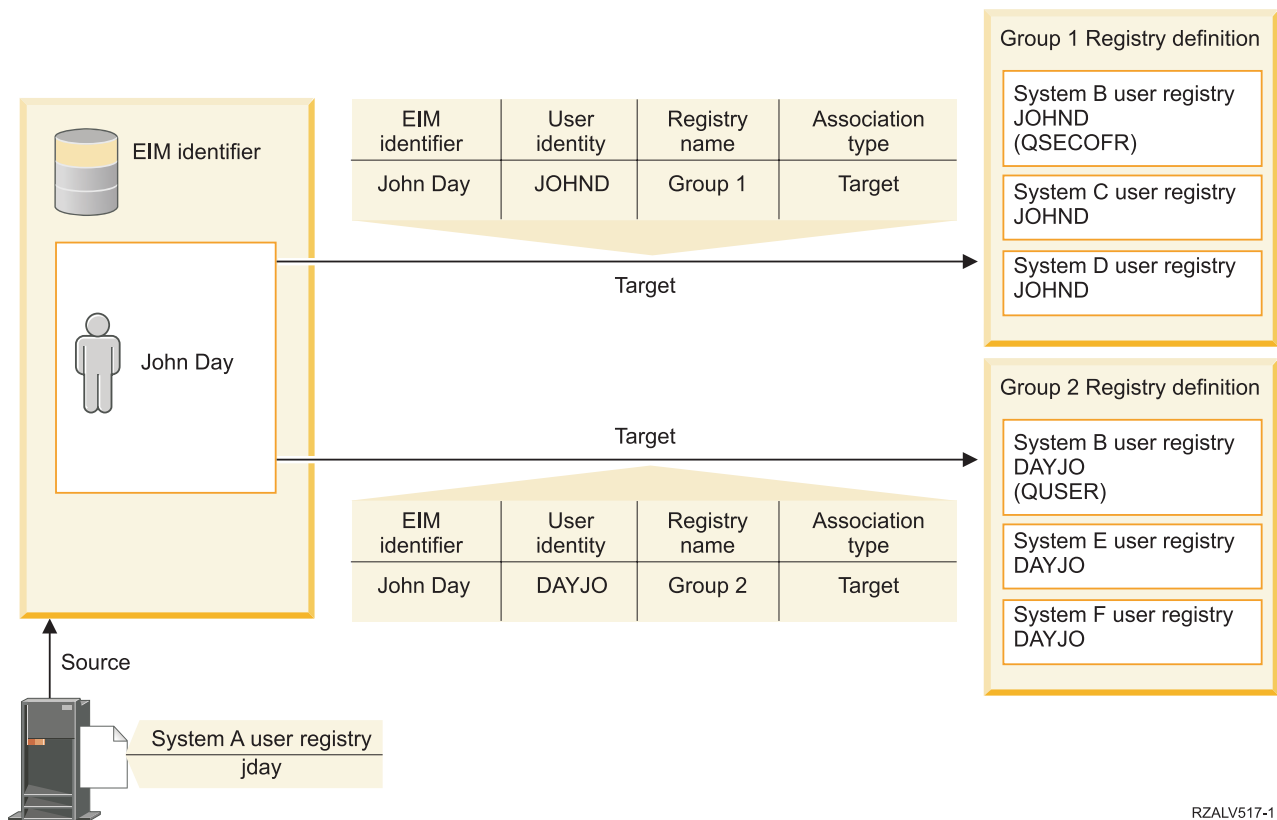
## Exemple de operații de căutare: Exemplul 5

Utilizați acest exemplu pentru a afla despre operațiile de căutare care returnează rezultate ambigue care implică definiții pentru registrul grup.

În unele cazuri o operație de căutare mapare returnează rezultate ambigue când mai mult de o identitate utilizator destinație se potrivește cu criteriul de căutare specificat. Pentru că o situație cu rezultate ambigue ar putea cauza ca aplicațiile care utilizează EIM să eșueze sau să dea rezultate neașteptate, trebuie să acționați pentru a împiedica sau rezolva situația.

În particular, fiți conștienți că operațiile de căutare pot returna rezultate ambigue când specificați o definiție pentru registrul de utilizatori ca un membru al mai mult de o definiție pentru registrul grup. Dacă o definiție pentru registru de utilizatori individuală este un membru al mai multor definiții pentru registrul grup și creați asocieri de identificator EIM individuali sau asocieri de politică care utilizează o definiție pentru registrul grup ca registru sursă sau ca registru destinație, operațiile de căutare ar putea returna rezultate ambigue. De exemplu, ați putea utiliza două identități utilizator diferite pentru două tipuri diferite de task-uri de sistem pe care le realizați: realizați task-uri ca administrator de securitate care necesită o identitate utilizator cu autorizarea QSECOFR și realizați task-uri utilizator tipice care necesită o identitate utilizator cu autorizarea QUSER. Dacă ambele identități utilizator ale dumneavoastră se află în registrul de utilizatori care este un membru a două definiții pentru registru grup diferite și creați asocieri de identificator destinație ambelor identități utilizator destinație, operațiile de căutare găsesc ambele identități utilizator destinație și returnează în consecință rezultate ambigue.

Următorul exemplu descrie cum poate surveni această problemă când specificați un registru de utilizatori individual ca membru a două definiții pentru registrul grup și specificați una din definițiile pentru registrul grup ca registrul destinație în două asocieri de identificator EIM individuale.



RZALV517-1

### Exemplu:

John Day are următoarele identități utilizator într-o definiție pentru registrul sistem numită registru de utilizatori System B:

- JOHND
- DAYJO

Registrul utilizator System B este un membru din următoarele definiții pentru registrul grup:

- Grup 1
- Grup 2

Identificatorul EIM John Day are două asocieri destinație cu următoarele specificări:

- Asocierea de destinație: Registrul destinație este Grup 1 care conține identitatea utilizator JOHND în registrul de utilizatori System B.
- Asocierea de destinație: Registrul destinație este Grup 2 care conține identitatea utilizatorului DAYJO în registrul de utilizatori System B .

În această situație, o operație de căutare mapare returnează rezultate ambigue pentru că mai mult de o identitate utilizator destinație se potrivește cu criteriul de căutare specificat; ambele identități utilizator (JOHND și DAYOJO) se potrivesc criteriului de căutare specificat.

Similar, operațiile de căutare mapare pot returna rezultate ambigue dacă creați două asocieri de politică (în loc de asocieri de identificatori EIM individuali) care utilizează definiții de registru grup ca registre destinație.

Pentru a împiedica operațiile de căutare să returneze rezultate ambigue care implică definiții pentru registrul grup, considerați următoarele indicații:

- Specificați un registru de utilizatori individual ca un membru a nu mai mult de o definiție pentru registrul grup.

- Fiți prudenți la crearea asocierilor de identificatori EIM individuali sau a asocierilor de politică care utilizează definiții pentru registre de grup ori ca registru sursă ori ca registru destinație. Verificați că definiția pentru registrul grup este un membru a nu mai mult de o definiție pentru registrul grup. Fiți conștienți de faptul că dacă un membru al definiției pentru registrul grup destinație este de asemenea un membru a unei alte definiții pentru registrul grup, operațiile de căutare pot returna rezultate ambigue.
- Dacă aveți o situație cu rezultate ambigue unde specificați o definiție pentru registru individual ca un membru al mai multor definiții de registre grup și creați o asociere de identificator individual sau o asociere de politică care utilizează una dintre aceste definiții de registru grup fie ca registru sursă, fie ca registru destinație, puteți defini informații de căutare unice pentru fiecare identitate utilizator destinație în fiecare asociere pentru a face căutarea mai fină.

Ați putea defini următoarele informații de căutare pentru fiecare utilizator destinație în exemplul despre John Day:

- Pentru JOHND: Definiți Administrator ca informații de căutare.
- Pentru DAYJO: Definiți Utilizator ca informații de căutare

Totuși, aplicațiile de bază i5/OS ca System i Access pentru Windows nu pot utiliza informațiile de căutare pentru a face distincție între identități utilizator destinație multiple returnate de o operație de căutare. În consecință, ați putea considera redefinirea asocierilor pentru domeniu pentru a vă asigura că o operație de căutare de mapare poate returna o singură identitate utilizator destinație pentru a se asigura că aplicațiile i5/OS de bază pot realiza operații de căutare și mapare de identități cu succes.

### Concepte înrudite

“Definiții registru grup” la pagina 15

Gruparea logică a definițiilor registrului vă permite să reduceți cantitatea de lucru pe care trebuie să o realizați pentru a configura maparea EIM. Puteți gestiona o definiție pentru registrul grup într-un mod similar cu modul în care gestionați o definiție pentru registrul individual.

## Suportul pentru politica EIM și activarea

Suportul politicii de mapare EIM (Enterprise Identity Mapping) vă permite să folosiți asocieri de politică precum și asocieri identificator specifice într-un domeniu EIM. Puteți folosi asocierile de politică în locul sau în combinație cu asocierile identificator.

Suportul politicii de mapare EIM furnizează un mijloc de activare și dezactivare a folosirii asocierilor de politică pentru întregul domeniu, precum și ca pentru fiecare registru de utilizatori destinație specific. EIM de asemenea vă permite să setați dacă un registru specific poate participa în operații de căutare mapare în general. În consecință, puteți folosi suportul politicii de mapare pentru a controla mai precis cum returnează rezultatele operațiile de căutare mapare.

Setarea implicită pentru un domeniu EIM este că căutărilor mapare care folosesc asocieri de politică sunt dezactivate pentru domeniu. Când utilizarea asocierilor de politică este dezactivată pentru domeniu, toate operațiile de căutare mapare pentru domeniu returnează rezultatele utilizând doar asociații identificator specifice între identități utilizator și identificatori EIM.

Setările implicită pentru fiecare registru individual sunt că participarea la căutare mapare este activată și utilizarea asocierilor de politică este dezactivată. Când activați utilizarea asocierilor de politică pentru un singur registru destinație, trebuie de asemenea să asigurați că această setare este activă pentru domeniu.

Puteți configura participarea de căutare mapare și folosirea asocierilor de politică pentru fiecare registru în una din cele trei căi:

- Operațiile de căutare mapare nu pot fi folosite deloc pentru registrul specificat. Cu alte cuvinte, o aplicație care realizează o operație de căutare mapare care implică registrul nu va reuși să returneze rezultate.
- Operațiile de căutare mapare pot folosi asocieri identificator specifice doar între identități utilizator și identificatori EIM. Căutărilor mapare sunt permise pentru registru, dar folosirea asocierilor de politică nu e permisă pentru registru.
- Operațiile de căutare mapare pot folosi asocieri identificator specifice când ele există și asocieri de politică când aceste nu există (toate setările sunt active).

## Concepte înrudite

“Informațiile de căutare” la pagina 16

Cu EIM (Enterprise Identity Mapping) puteți utiliza date opționale numite informații de căutare pentru a identifica mai de parte o identitate utilizator destinație. Această identitate utilizator destinație poate fi specificată fie într-o asociere de identificator, fie într-o asociere de politică.

“Asocierile de politică de domeniu implicite” la pagina 21

O asociere de politică domeniu implicite este un tip de asociere de politică pe care îl puteți folosi pentru a crea mapări multe-la-unu între identități utilizator.

“Asocierile de politică registru implicite” la pagina 23

O asociere de politică registru implicite este un tip de asociere de politică pe care îl puteți folosi pentru a crea mapări multe-la-unu între identități utilizator.

“Crearea unei asocieri de politică” la pagina 102

O asociere de politică furnizează un mod de a defini o relație dintre mai multe identități de utilizatori din unul sau mai multe registre și o identitate de utilizator unică în alt registru.

## Operații înrudite

“Activarea asocierilor de politică pentru un domeniu” la pagina 87

O asociere de politică furnizează un mijloc de creare mapări multe-la-una în situații unde asocierile între identitățile utilizator și identificatorul EIM (Enterprise Identity Mapping) nu există.

“Activarea suportului de căutare mapare și a utilizării asocierilor de politică pentru un registru destinație” la pagina 94

Suportul politică de mapare EIM (Enterprise Identity Mapping) vă permite să utilizați asocieri de politică ca un mijloc de creare mapări multe-la-unul în situații unde asocieri între identități utilizator și un identificator EIM nu există. Puteți folosi o asociere de politică pentru a mapa un set sursă de identități de utilizator (în loc de o singură identitate de utilizator) la o unică identitate destinație de utilizator dintr-un registru de utilizatori destinație, specificat.

## Controlul accesului în EIM

Un utilizator EIM (Enterprise Identity Mapping) este un utilizator care are control acces EIM bazat pe calitatea sa de membru într-un grup de utilizatori predefinit LDAP (Lightweight Directory Access Protocol) pentru un domeniu specific.

Specificând controlul de acces EIM pentru un utilizator adaugă acel utilizator la un grup de utilizatori specific LDAP pentru un domeniu particular. Fiecare grup LDAP are autorizarea să realizeze operații EIM administrative specifice acelui domeniu. Grupul de control al accesului determină ce operații administrative pot realiza utilizatorii EIM care îi aparțin și de ce tip, inclusiv operațiile de căutare.

**Notă:** Pentru a configura EIM, trebuie să dovediți că sunteți de încredere în contextul rețelei, nu pe un anumit sistem. Autorizarea pentru a configura EIM nu este bazată pe autorizarea profilului dumneavoastră utilizator i5/OS, ci pe autorizarea control acces EIM. EIM este o resursă rețea, nu o resursă pentru vreun sistem anume; în consecință, EIM nu recunoaște autorizările speciale specifice i5/OS precum \*ALLOBJ și \*SECADM pentru configurație. O dată ce s-a configurat EIM, totuși, autorizarea pentru a realiza task-uri poate fi bazată pe un număr de tipuri de utilizatori diferiți, inclusiv profilurile utilizator i5/OS. De exemplu, IBM Tivoli Directory Server for i5/OS tratează profilurile i5/OS cu autorizarea specială \*ALLOBJ și \*IOSYSCFG ca administratori director.

Doar utilizatorii cu control al accesului de administrator EIM pot să adauge utilizatori într-un grup de control al accesului EIM sau să modifice setările de control al accesului pentru alți utilizatori. Pentru ca un utilizator să poată deveni membru al unui grup de control al accesului EIM, el trebuie să aibă o intrare în serverul de director care are rolul de controler de domeniu EIM. De asemenea, numai anumite tipuri de utilizatori pot deveni membri ai unui grup de control al accesului EIM. Identitatea utilizator poate fi sub forma unui principal Kerberos, un nume distinctiv LDAP sau un profil utilizator i5/OS atâta timp cât identitatea utilizatorului este definită în serverul de director.

**Notă:** Pentru a fi disponibil în EIM tipul utilizator principal Kerberos, trebuie să fie configurat pe sistem serviciul de autentificare în rețea. Pentru a avea tipul profilului utilizator i5/OS disponibil în EIM, trebuie să configurați un sufix obiect de sistem pe serverul de director. Aceasta permite serverului de director să facă referință la obiectele de sistem i5/OS, precum profilurile utilizator i5/OS.

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

## **Administratorul LDAP (Lightweight Directory Access Protocol)**

Administratorul LDAP este un nume distinctiv (DN) special din director, care este administratorul întregului director. Astfel, administratorul LDAP are acces la toate funcțiile administrative EIM, precum și la întregul director. Un utilizator cu acest control al accesului poate executa următoarele funcții:

- Creare domeniu.
- Ștergere domeniu.
- Creare și înlăturare identicatori EIM.
- Creare și înlăturare definiții de registru EIM.
- Creare și înlăturare asocieri sursă, destinație și administrative.
- Creare și înlăturare asocieri de politică.
- Creare și înlăturare filtre de certificat.
- Activare și dezactivare utilizare asocieri de politică pentru un domeniu.
- Activare și dezactivare căutări mapare pentru un registru.
- Activare și dezactivare utilizare asocieri de politică pentru un registru.
- Realizare operații de căutare EIM.
- Extragere asocieri de identicator, asocieri de politică, filtre de certificat, identicatori EIM și definiții de registru EIM.
- Adăugare, înlăturare și listare informații privind controlul accesului EIM.
- Modificați și înlăturați informațiile de acreditări pentru un utilizator din registru.

## **Administratorul EIM**

Calitatea de membru al acestui grup de control al accesului permite utilizatorului să gestioneze toate datele EIM dintr-un domeniu EIM. Un utilizator cu acest control al accesului poate executa următoarele funcții:

- Ștergere domeniu.
- Creare și înlăturare identicatori EIM.
- Creare și înlăturare definiții de registru EIM.
- Creare și înlăturare asocieri sursă, destinație și administrative.
- Creare și înlăturare asocieri de politică.
- Creare și înlăturare filtre de certificat.
- Activare și dezactivare utilizare asocieri de politică pentru un domeniu.
- Activare și dezactivare căutări mapare pentru un registru.
- Activare și dezactivare utilizare asocieri de politică pentru un registru.
- Realizare operații de căutare EIM.
- Extragere asocieri de identicator, asocieri de politică, filtre de certificat, identicatori EIM și definiții de registru EIM.
- Adăugare, înlăturare și listare informații privind controlul accesului EIM.
- Modificați și înlăturați informațiile de acreditări pentru un utilizator din registru.

## Administratorul de identificatori

Calitatea de membru al acestui grup de control al accesului permite utilizatorului să adauge și să modifice identificatorii EIM și să gestioneze asocierile sursă și administrative. Un utilizator cu acest control al accesului poate executa următoarele funcții:

- Creare identificatori EIM.
- Adăugare și înlăturare asocieri.
- Adăugare și înlăturare asocieri administrative.
- Realizare operații de căutare EIM.
- Extragere asocieri de identificator, asocieri de politică, filtre de certificat, identificatori EIM și definiții de registru EIM.

## Operațiile de mapare EIM

Calitatea de membru al acestui grup de control al accesului permite utilizatorului să conducă operații de căutare mapare EIM. Un utilizator cu acest control al accesului poate executa următoarele funcții:

- Realizare operații de căutare EIM.
- Extragere asocieri de identificator, asocieri de politică, filtre de certificat, identificatori EIM și definiții de registru EIM.

## Administratorul de registre

Calitatea de membru al acestui grup de control al accesului permite utilizatorului să gestioneze toate definițiile de registru EIM. Un utilizator cu acest control al accesului poate executa următoarele funcții:

- Adăugare și înlăturare asocieri destinație.
- Creare și înlăturare asocieri de politică.
- Creare și înlăturare filtre de certificat.
- Activare și dezactivare căutări mapare pentru un registru.
- Activare și dezactivare utilizare asocieri de politică pentru un registru.
- Realizare operații de căutare EIM.
- Extragere asocieri de identificator, asocieri de politică, filtre de certificat, identificatori EIM și definiții de registru EIM.

## Administratorul pentru registrele selectate

Calitatea de membru al acestui grup de control al accesului permite utilizatorului să gestioneze informații EIM numai pentru o definiție specificată de registru de utilizatori (cum ar fi Registry\_X). De asemenea, apartenența la acest grup de control al accesului permite utilizatorului să înlătore asocieri destinație numai pentru o definiție specificată de registru de utilizatori. Pentru a beneficia integral de operațiile de căutare mapare și de asocierile de politică, un utilizator cu acest control al accesului trebuie să aibă și accesul de control **Operații de mapare EIM**. Acest control al accesului permite unui utilizator să execute următoarele funcții pentru definiții de registru autorizate specific:

- Creare, înlăturare și listare asocieri destinație numai pentru definițiile de registru EIM specificate.
- Adăugare și înlăturare asocieri de politică domeniu implicit.
- Adăugare și înlăturare asocieri de politică numai pentru definițiile de registru specificate.
- Adăugare filtre de certificat numai pentru definițiile de registru specificate.
- Activare și dezactivare căutări mapare numai pentru definițiile de registru specificate.
- Activare și dezactivare asocieri de politică numai pentru definițiile de registru specificate.
- Extragere identificatori EIM.
- Extragere asocieri de identificator și filtre de certificat numai pentru definițiile de registru specificate.
- Extragere informații definiție pentru registrul EIM numai pentru definițiile de registru specificate.

**Notă:** Dacă definiția registrului specificat este o definiție pentru registrul grup, un utilizator cu control de acces Administrator la registrele selectate are acces Administrator doar la grup, nu și la membrii grupului.

Un utilizator care are atât controlul de acces **Administrator pentru registre selectate**, cât și controlul de acces **Operații de căutare mapare EIM** are posibilitatea să execute următoarele funcții:

- Adăugare și înlăturare asocieri de politică numai pentru registrele specificate.
- Realizare operații de căutare EIM.
- Extragere toate asocierile de identificator, asocierile de politică, filtrele de certificat, identificadorii EIM și definițiile de registru EIM.

## Căutarea de acreditări

Acest grup de control acces permite utilizatorului să extragă informații acreditate, precum parole.

Dacă un utilizator cu acest control acces vrea să realizeze o operație EIM, utilizatorul trebuie să fie membru al grupului de control acces care furnizează autorizarea pentru operația EIM dorită. De exemplu, dacă un utilizator cu acest control acces dorește să extragă asocierea de destinație dintr-o asociere de sursă, utilizatorul are nevoie să fie membru în unul din următoarele grupuri de control acces:

- Administrator EIM
- Administrator de identificator
- Operații de căutare mapare EIM
- Administrator de registru

### Concepte înrudite

“Considerente pentru profilul utilizator i5/OS pentru EIM.” la pagina 49

Capacitatea de a realiza taskuri în EIM (Enterprise Identity Mapping) nu este bazată pe autoritatea profilului dumneavoastră de utilizator i5/OS, ci mai degrabă pe autoritatea dumneavoastră de control acces EIM.

“Identificarea rolurilor și calificărilor necesare” la pagina 53

EIM (Enterprise Identity Mapping) este proiectat astfel încât o singură persoană poate fi responsabilă ușor pentru configurare și administrare într-o organizație mică. Sau, într-o organizație mai mare, poate preferați să aveți un număr de indivizi diferiți care să trateze aceste responsabilități.

### Operații înrudite

“Gestionarea controlului de acces al utilizatorului EIM” la pagina 114

Un utilizator EIM (Enterprise Identity Mapping) este un utilizator care posedă control acces EIM bazat pe apartenența la grupuri utilizator predefinite LDAP (Lightweight Directory Access Protocol). Specificarea controlului de acces EIM pentru un utilizator îl adaugă pe acel utilizator la un grup de utilizatori LDAP specific.

## Grupul de control al accesului EIM: Autorizarea API

Informațiile afișează tabele care sunt organizate de operația EIM (Enterprise Identity Mapping) pe care o realizează API.

Fiecare din următoarele tabele afișează fiecare API EIM, diferitele grupuri control EIM și dacă grupul control de acces are autorizarea să realizeze funcția EIM.

*Tabela 1. Lucrul cu domenii*

API EIM	Administrator LDAP	Administrator EIM	Administrator identicatori	Căutare mapări EIM	Administrator registru	Administrator pentru registrul selectat
eimChangeDomain	X	X	-	-	-	-
eimCreateDomain	X	-	-	-	-	-
eimDeleteDomain	X	X	-	-	-	-
eimListDomains	X	X	-	-	-	-

Tabela 2. Lucrul cu identificatori

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	-	-	-	-
eimGetAssociated Identificatori	X	X	X	X	X	X

Tabela 3. Lucrul cu registre

API EIM	Administrator LDAP	Administrator EIM	Administrator identificatori EIM	Căutare mapări EIM	Administrator registre EIM	Administrator registru EIM X
eimAddApplication Registru	X	X	-	-	-	-
eimAddSystemRegistry	X	X	-	-	-	-
eimChangeRegistry	X	X	-	-	X	X
eimChange RegistryUser	X	X	-	-	X	X
eimChangeRegistryAlias	X	X	-	-	X	X
eimGetRegistry NameFromAlias	X	X	X	X	X	X
eimListRegistries	X	X	X	X	X	X
eimListRegistry Asocieri	X	X	X	X	X	X
eimListRegistryAliases	X	X	X	X	X	X
eimListRegistry Utilizatori	X	X	X	X	X	X
eimRemoveRegistry	X	X	-	-	-	-

Tabela 4. Lucrul cu asocieri identificator. Pentru API-urile eimAddAssociation() și eimRemoveAssociation() sunt patru parametri care determină tipul asocierii care este fie adăugată fie înlăturată. Autorizările pentru aceste API-uri diferă în funcție de tipul de asociere specificat în acești 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 (administrativ)	X	X	X	-	-	-
eimAddAssociation (sursă)	X	X	X	-	-	-
eimAddAssociation (sursă și destinație)	X	X	X	-	X	X
eimAddAssociation (destinație)	X	X	-	-	X	X
eimListAssociations	X	X	X	X	X	X
eimRemoveAssociation (administrativ)	X	X	X	-	-	-
eimRemoveAssociation (sursă)	X	X	X	-	-	-
eimRemoveAssociation (sursă și destinație)	X	X	X	-	X	X



*Tabela 4. Lucrul cu asocieri identificator (continuare).* Pentru API-urile eimAddAssociation() și eimRemoveAssociation() sunt patru parametri care determină tipul asocierii care este fie adăugată fie înlăturată. Autorizările pentru aceste API-uri diferă în funcție de tipul de asociere specificat în acești 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
eimRemoveAssociation (destinație)	X	X	-	-	X	X

*Tabela 5. Lucrul cu asocieri de politică*

API EIM	Administrator LDAP	Administrator EIM	Administrator identificatori EIM	Căutare mapări EIM	Administrator registre EIM	Administrator registru EIM X
eimAddPolicyAssociation	X	X	-	-	X	X
eimAddPolicyFilter	X	X	-	-	X	X
eimListPolicyFilters	X	X	X	X	X	X
eimRemove PolicyAssociation	X	X			X	X
eimRemovePolicyFilter	-	-	-	-	-	

*Tabela 6. Lucrul cu mapări*

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

*Tabela 7. Lucrul cu accesul*

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	-	-	-	-

## Grupul de control acces EIM: Autorizarea operației EIM

Aceste informații afișează un tabel care explică relațiile dintre grupurile control de acces EIM și operațiile EIM pe care le pot realiza.

Deși administratorul LDAP nu este menționat în tabelă, acest nivel de control al accesului este necesar pentru a crea un nou domeniu EIM. De asemenea, administratorul LDAP are același control al accesului ca administratorul EIM, dar acesta nu are automat controlul de acces al administratorului LDAP.

*Tabela 8. Tabela 1: Grupuri de control acces EIM*

Task EIM	Administrator EIM	Administrator identificator	Operații de căutare mapare EIM	Administrator registru	Administrator pentru registrul selectat	Căutare acreditată
Creare domeniu	-	-	-	-	-	

Tabela 8. Tabela 1: Grupuri de control acces EIM (continuare)

Task EIM	Administrator EIM	Administrator identificator	Operații de căutare mapare EIM	Administrator registru	Administrator pentru registrul selectat	Căutare acreditată
Ștergere domeniu	X	-	-	-	-	
Modificare domeniu	X	-	-	-	-	
Activare/dezactivare asocieri de politică pentru domeniu	X	-	-	-	-	
Căutare domenii	X	-	-	-	-	
Adăugare registru sistem	X	-	-	-	-	
Adăugare registru aplicație	X	-	-	-	-	
Înlăturare registru	X	-	-	-	-	
Modificare registru	X	-	-	X	X	
Activare/Dezactivare căutării mapare după registru	X	-	-	X	X	
Activare/dezactivare asocieri de politică pentru registru	X	-	-	X	X	
Căutare registre	X	X	X	X	X	
Adăugare identificator	X	X	-	-	-	
Înlăturare identificator	X	-	-	-	-	
Modificare identificator	X	X	-	-	-	
Căutare identificatori	X	X	X	X	X	
Extragere identificatori asociați	X	X	X	X	X	
Adăugare/Înlăturare asociere administrativă	X	X	-	-	-	

Tabela 8. Tabela 1: Grupuri de control acces EIM (continuare)

Task EIM	Administrator EIM	Administrator identificator	Operații de căutare mapare EIM	Administrator registru	Administrator pentru registrul selectat	Căutare acreditată
Adăugare/ Înlăturare asociere sursă	X	X	-	-	-	
Adăugare/ Înlăturare asociere destinație	X	-	-	X	X	
Adăugare/ Înlăturare asociere de politică	X	-	-	X	X	
Adăugare/ Înlăturare filtru de certificate	X	-	-	X	X	
Căutare filtru de certificate	X	X	X	X	X	
Căutare asocieri	X	X	X	X	X	
Căutare asocieri de politică	X	X	X	X	X	
Extragere asociere destinație din asociere sursă	X	X	X	X	-	
Extragere asociere destinație din identificator	X	X	X	X	X	
Modificare utilizatori registru	X	-	-	X	X	
Căutare utilizatori registru	X	X	X	X	X	
Modificare alias registru	X	-	-	X	X	
Căutare alias-uri registru	X	X	X	X	X	
Extragere registru din alias	X	X	X	X	X	
Adăugare/ Înlăturare control acces EIM	X	-	-	-	-	
Afișare membri grup de control acces	X	-	-	-	-	

Tabela 8. Tabela 1: Grupuri de control acces EIM (continuare)

Task EIM	Administrator EIM	Administrator identicator	Operații de căutare mapare EIM	Administrator registru	Administrator pentru registrul selectat	Căutare acreditată
Afișare control acces EIM pentru un utilizator specificat	X	-	-	-	-	
Interogare control acces EIM	X	-	-	-	-	
Modificare acreditare	X	-	-	-	-	-
Extragere acreditare	X	-	-	-	-	X
1 - Dacă definiția registrului specificat este o definiție grup de registre, un utilizator cu control de acces Administrator pentru registrele selectate are acces administrator doar pentru grup, nu și pentru membrii grupului.						

## Concepte LDAP pentru EIM

EIM utilizează un server LDAP ca un controler de domeniu pentru a memora date EIM. De aceea trebuie să înțelegeți ceva concepte LDAP care se leagă de configurarea și folosirea EIM în întreprinderea dumneavoastră. De exemplu, puteți folosi un nume distinctiv LDAP ca identitate utilizator pentru a configura EIM și pentru a vă autentifica la controlerul de domeniu EIM.

Pentru a avea o mai bună înțelegere despre configurarea și folosirea EIM, trebuie să înțelegeți următoarele concepte LDAP:

### Concepte înrudite

“Concepte EIM” la pagina 4

Este necesară o înțelegere conceptuală a modului în care lucrează EIM pentru a înțelege complet modul în care puteți folosi EIM în întreprinderea dumneavoastră. Deși configurarea și implementarea API-urilor EIM pot diferi între platforme server, conceptele EIM sunt obișnuite de-a lungul platformelor IBM eServer.

### Numele distinctiv

Un DN (distinguished name) este o intrare LDAP care identifică și descrie în mod unic o intrare într-un server (LDAP) director. Utilizați vrăjitorul Configurare EIM (Enterprise Identity Mapping) pentru a configura serverele de director să memoreze informațiile domeniului EIM. Deoarece EIM folosește serverul de director pentru a memora datele EIM, puteți folosi numele distinctiv ca un mijloc de autentificare la controlerul de domeniu EIM.

Numele distinctive constau din însuși numele intrării, cât și din numele, în ordine de jos în sus, obiectelor de deasupra sa din directorul LDAP. Un exemplu de nume distinctiv complet poate fi `cn=Tim Jones, o=IBM, c=US`. Fiecare intrare are cel puțin un atribut care este utilizat pentru a denumi intrarea. Acest atribut de numire este numit RDN-ul (relative distinguished name) intrării. Intrarea de mai sus, un RDN dat este numită numele distinctiv părinte. În acest exemplu, `cn=Tim Jones` numește intrarea, deci este RDN. `o=IBM, c=US` este părintele DN pentru `cn=Tim Jones`.

Deoarece EIM utilizează serverul de director pentru a memora date EIM, puteți utiliza un nume distinctiv pentru identitatea utilizatorului care se autentifică la controlerul de domeniu. De asemenea puteți utiliza un nume distinctiv pentru identitatea utilizatorului care configurează EIM pentru platforma System i. De exemplu, puteți folosi un nume distinctiv când faceți următoarele:

- Configurați serverul de director să funcționeze ca un controler de domeniu EIM. Faceți aceasta prin crearea și folosirea numelui distinctiv care identifică administratorul LDAP pentru serverul de director. Dacă serverul de director nu a fost configurat înainte, puteți configura serverul de director când folosiți vrăjitorul de configurare EIM pentru crearea și alăturarea la un nou domeniu.
- Utilizați vrăjitorul Configurare EIM pentru a selecta tipul identității 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 puteți selecta. Numele distinctiv trebuie să reprezinte un utilizator care este autorizat la crearea obiectelor în spațiu nume local al serverului de director.
- Utilizați vrăjitorul Configurare EIM pentru a selecta tipul utilizatorului care să efectueze operații EIM în numele funcțiilor sistemului de operare. Aceste operații includ operațiile de căutare mapare și ștergere asocieri la ștergerea unui profil utilizator i5/OS local. Numele distinctiv este unul dintre tipurile de utilizatori pe care le puteți selecta.
- Vă conectați la controlerul de domeniu pentru a efectua administrarea EIM, de exemplu, pentru a gestiona registrele și identificatorii și pentru a efectua operații de căutare de mapări.
- Creați filtre de certificate pentru a determina domeniul unei asocieri de politică filtru de certificate. Când creați un filtru de certificate, trebuie să furnizați informațiile de nume distinctiv, fie pentru DN Subiect, fie pentru DN Emitent sau certificatul să specifice criteriul pe care îl folosește filtru pentru a determina ce certificate sunt afectate de asocierea de politică.

#### **Concepte înrudite**

“Numele distinctiv părinte”

Un nume distinctiv (DN) părinte este o intrare în spațiul de nume al serverului de director LDAP (Lightweight Directory Access Protocol). Intrările serverului LDAP sunt aranjate într-o structură ierarhică ce poate reflecta granițele politice, geografice, organizaționale sau de domeniu. Un nume distinctiv este considerat un DN părinte când DN este intrarea în director imediat superioară unui DN dat.

“Filtrele de certificate” la pagina 26

Un filtru de certificate definește un set de atribute cu nume distinctiv similare pentru un grup de certificate utilizator într-un registru de utilizatori sursă X.509. Puteți folosi filtrul de certificate ca baza unei asocieri de politică de filtrare certificate.

#### **Informații înrudite**

Concepte server director

## **Numele distinctiv părinte**

Un nume distinctiv (DN) părinte este o intrare în spațiul de nume al serverului de director LDAP (Lightweight Directory Access Protocol). Intrările serverului LDAP sunt aranjate într-o structură ierarhică ce poate reflecta granițele politice, geografice, organizaționale sau de domeniu. Un nume distinctiv este considerat un DN părinte când DN este intrarea în director imediat superioară unui DN dat.

Un exemplu de nume distinctiv complet poate fi `cn=Tim Jones, o=IBM, c=US`. Fiecare intrare are cel puțin un atribut care este utilizat pentru a denumi intrarea. Acest atribut de numire este numit RDN-ul (relative distinguished name) intrării. Intrarea de mai sus unui RDN este numită DN-ul părintelui. În acest exemplu, `cn=Tim Jones` numește intrarea, deci este RDN. `o=IBM, c=US` este părintele DN pentru `cn=Tim Jones`.

EIM utilizează un server director ca un controler de domeniu pentru memorarea datelor de domeniu EIM. DN-ul părinte combinat cu numele de domeniu EIM determină locul datelor de domeniu EIM în spațiul de nume al serverului de director. Când folosiți vrăjitorul de configurare EIM pentru a crea și a vă alătura la un nou domeniu, puteți alege să specificați un DN părinte pentru domeniul pe care îl creați. Prin folosirea unui DN părinte, puteți specifica unde să se afle în spațiul de nume LDAP, pentru domeniu, acele date EIM. Când nu specificați un DN părinte, datele EIM se află în propriul lor sufix din spațiul de nume și locația implicită pentru datele de domeniu EIM este `ibm-eimDomainName=EIM`.

#### **Concepte înrudite**

“Numele distinctiv” la pagina 46

Un DN (distinguished name) este o intrare LDAP care identifică și descrie în mod unic o intrare într-un server (LDAP) director. Utilizați vrăjitorul Configurare EIM (Enterprise Identity Mapping) pentru a configura serverele de

director să memoreze informațiile domeniului EIM. Deoarece EIM folosește serverul de director pentru a memora datele EIM, puteți folosi numele distinctiv ca un mijloc de autentificare la controlerul de domeniu EIM.

### **Informații înrudite**

Concepte server director

## **Schema LDAP și alte considerente pentru EIM**

Utilizați aceste informații pentru a afla ce este cerut pentru ca serverul de director să funcționeze cu EIM (Enterprise Identity Mapping).

EIM necesită controlerul de domeniu să fie găzduit de un server de director care suportă LDAP (Lightweight Directory Access Protocol) Versiunea 3. În plus, produsul serverului de director trebuie să poată accepta schema EIM și înțelege următoarele atribute și clase obiect:

- Atributul `ibm-entryUUID`.
- `ibmattributetype-uri`:
  - `acIEntry`
  - `acIPropagate`
  - `acISource`
  - `entryOwner`
  - `ownerPropagate`
  - `ownerSource`
- Atribute EIM, inclusiv trei atribute noi pentru suport asociere politică:
  - `ibm-eimAdditionalInformation`
  - `ibm-eimAdminUserAssoc`
  - `ibm-eimDomainName`, `ibm-eimDomainVersion`,
  - `ibm-eimRegistryAliases`
  - `ibm-eimRegistryEntryName`
  - `ibm-eimRegistryName`
  - `ibm-eimRegistryType`
  - `ibm-eimSourceUserAssoc`
  - `ibm-eimTargetIdAssoc`
  - `ibm-eimTargetUserName`
  - `ibm-eimUserAssoc`
  - `ibm-eimFilterType`
  - `ibm-eimFilterValue`
  - `ibm-eimPolicyStatus`
- Clase obiect EIM, inclusiv trei atribute noi pentru suport asociere politică:
  - `ibm-eimApplicationRegistry`
  - `ibm-eimDomain`
  - `ibm-eimIdentifier`
  - `ibm-eimRegistry`
  - `ibm-eimRegistryUser`
  - `ibm-eimSourceRelationship`
  - `ibm-eimSystemRegistry`
  - `ibm-eimTargetRelationship`
  - `ibm-eimFilterPolicy`
  - `ibm-eimDefaultPolicy`
  - `ibm-eimPolicyListAux`

### Concepte înrudite

“Controlerul de domeniu EIM” la pagina 5

Un controler de domeniu EIM este un server LDAP (Lightweight Directory Access Protocol) care este configurat pentru a gestiona unul sau mai multe domenii EIM. Un domeniu EIM conține toate identificatoarele EIM, asocierile EIM și registrele de utilizatori care sunt definite în acest domeniu. Sistemele (clienți EIM) participă în domeniul EIM prin utilizarea datelor de domeniu pentru operații de căutare EIM.

## Concepte EIM pentru i5/OS

- | Puteți implementa EIM pe orice platformă IBM eServer. Totuși, când implementați EIM pe un model System i, ar trebui să aveți grijă de unele informații care sunt specifice la implementarea System i.

Consultați următoarele informații pentru a afla despre aplicațiile i5/OS care sunt activate pentru EIM, despre considerentele legate de un profil utilizator și alte subiecte care vă poate ajuta să utilizați EIM eficace pe o platformă System i:

### Concepte înrudite

“Concepte EIM” la pagina 4

Este necesară o înțelegere conceptuală a modului în care lucrează EIM pentru a înțelege complet modul în care puteți folosi EIM în întreținerea dumneavoastră. Deși configurarea și implementarea API-urilor EIM pot diferi între platforme server, conceptele EIM sunt obișnuite de-a lungul platformelor IBM eServer.

## Considerente pentru profilul utilizator i5/OS pentru EIM.

Capacitatea de a realiza taskuri în EIM (Enterprise Identity Mapping) nu este bazată pe autoritatea profilului dumneavoastră de utilizator i5/OS, ci mai degrabă pe autoritatea dumneavoastră de control acces EIM.

Sunt unele taskuri suplimentare care trebuie să fie utilizate pentru a seta i5/OS pentru a utiliza EIM. Aceste task-uri adiționale necesită să aveți un profil utilizator i5/OS cu autorizările speciale corespunzătoare.

Pentru a seta i5/OS la utilizarea EIM folosind Navigator System i, profilul dumneavoastră utilizator trebuie să aibă următoarele autorizări speciale :

- Administrator securitate (\*SECADM).
- Toate obiectele (\*ALLOBJ).
- Configurare sistem (\*IOSYSCFG).

## Îmbunătățirile comenzii profilului utilizator i5/OS pentru identificatorii EIM

Odată ce configurați EIM pentru sistemul dumneavoastră, puteți lua avantaj de un nou parametru atât pentru comanda Creare profil utilizator (CRTUSRPRF) cât și pentru comanda Modificare profil utilizator (CHGUSRPRF), numit EIMASSOC. Puteți folosi acest parametru pentru a defini asociațiile identificator EIM pentru profilul utilizator specificat pentru registrul local.

Când folosiți acest parametru, puteți specifica informațiile următoare:

- Nume identificator EIM, ce poate fi un nume nou sau un nume identificator existent.
- O opțiune pentru asociere poate fi de adăugare (\*ADD), de înlocuire (\*REPLACE), sau de înlăturare (\*REMOVE) a asocierii specificată.

**Notă:** Folosiți \*ADD pentru a seta asocieri noi. Folosiți opțiunea \*REPLACE, de exemplu, dacă ați definit anterior asocieri la identificatorul greșit. Opțiunea \*REPLACE înlătură orice asocieri existente ale tipului specificat pentru registrul local către oricare alți identificatori și apoi adaugă unul care este specificat pentru parametru. Folosiți opțiunea \*REMOVE pentru a înlătura orice asocieri specificate de la identificatorul specificat.

- Tipul asocierii identificator, ce poate fi destinație, sursă, atât destinație cât și sursă, sau o asociere administrativă.
- Dacă să creați identificatorul EIM specificat dacă nu există deja.

Creați tipic o asocieră destinație pentru un profil i5/OS, în special într-un mediu de semnare unică. După ce folosiți comanda pentru a crea asocieră destinație dorită pentru profilul utilizator (și identificatorul EIM, dacă e necesar), puteți avea nevoie să creați o asocieră sursă corespunzătoare. Puteți utiliza Navigator System i pentru a crea o asocieră sursă pentru altă identitate de utilizator, ca principal Kerberos cu care utilizatorul se semnează pe rețea .

Când ați configurat EIM pentru sistem, ați specificat o identitate utilizator și parola pentru sistem pentru a o folosi atunci când executați operații EIM în numele sistemului de operare. Această identitate de utilizator trebuie să aibă autorizare de control acces EIM suficientă pentru a crea identificatori și pentru a adăuga asocieri.

## Parolele profilului de utilizator i5/OS și EIM

Ca administrator, țelul dumneavoastră principal pentru configurarea EIM ca parte componentă a mediului de semnare unică este de a reduce numărul de gestionare parolă utilizator pe care îl realizați pentru utilizatorii finali din întreprinderea dumneavoastră. Prin folosirea mapării de identitate pe care o furnizează EIM în combinație cu autentificarea Kerberos, știți că utilizatorii dumneavoastră vor trebui să execute mai puține logări și să își amintească și să gestioneze mai puține parole. Beneficiați de faptul că aveți mai puține apeluri de rezolvare a problemelor pentru identitățile de utilizator mapate, cum ar fi apeluri la a reseta aceste parole, atunci când utilizatorii le uită. Totuși, regulile parolă de securitate au încă efect și trebuie să gestionați încă aceste profiluri utilizator oricând parola expiră.

Pentru a beneficia mai mult de mediul de semnare unică al dumneavoastră, ar trebui să luați în considerare modificarea setării parolei pentru acele profiluri de utilizator care sunt ținta mapărilor de identitate. Ca destinație a mapării de identitate, utilizatorul nu mai are nevoie să furnizeze parola pentru profilul utilizator când utilizatorul accesează o platformă System i sau o resursă EIM-activată i5/OS. Pentru utilizatorii obișnuiți, puteți modifica setarea parolă la \*NONE astfel încât nici o parolă nu poate fi utilizată cu profilul utilizator. Deținătorului acestui profil de utilizator nu îi mai trebuie parolă din cauza mapării identității și semnării unice. Prin setarea parolei la \*NONE, beneficiați mai departe deoarece dumneavoastră și utilizatorii dumneavoastră nu mai trebuie să gestionați expirarea parolei; suplimentar, nimeni nu poate utiliza profilul la semnarea directă la o platformă System i sau la accesarea resurseleor EIM-activate i5/OS. Totuși, s-ar putea să preferați ca administratorii să continue să aibă o valoare de parolă pentru profilurile lor utilizator în caz că trebuie să se semneze direct pe platforma System i. De exemplu, dacă controlerul de domeniu EIM este jos și maparea de identitate nu poate surveni, un administrator s-ar putea să fie nevoit să se semneze direct la platforma System i până când problema cu controlerul de domeniu este rezolvată.

### Concepte înrudite

“Controlul accesului în EIM” la pagina 38

Un utilizator EIM (Enterprise Identity Mapping) este un utilizator care are control acces EIM bazat pe calitatea sa de membru într-un grup de utilizatori predefinit LDAP (Lightweight Directory Access Protocol) pentru un domeniu specific.

### Informații înrudite

Comanda Creare profil utilizator (CRTUSRPRF)

## Auditarea i5/OS pentru EIM

Unul dintre considerentele importante privind planul dumneavoastră general de securitate este felul auditării pe care o realizați.

Când configurați și folosiți EIM (Enterprise Identity Mapping), puteți dori să configurați suportul de auditare pentru serverul director, pentru a vă asigura că furnizați nivelul corespunzător de responsabilitate pe care îl cere politica dumneavoastră de securitate. De exemplu, suportul de auditare poate fi de ajutor în determinarea căruia dintre utilizatorii mapați de o asocieră de politică a realizat o acțiune pe sistemul dumneavoastră sau a modificat un obiect.

### Informații înrudite

Auditare server de director

## Aplicațiile permise EIM pentru i5/OS

EIM poate utiliza o varietate de aplicații i5/OS.

Următoarele aplicații i5/OS pot fi configurate să utilizeze EIM (Enterprise Identity Mapping):



- Serverele gazdă i5/OS (utilizate în mod curent de System i Access pentru Windows și Navigator System i)
- Server Telnet (folosit curent de PC5250 și IBM Websphere host on demand)
- QFileSrv.400 ODBC (permite folosirea semnării unice prin SQL)
- JDBC (permite folosirea EIM prin SQL)
- Arhitectură bază de date relațională distribuită (DRDA) (permite folosirea EIM prin SQL)
- IBM WebSphere Host On-Demand Versiunea 8, (caracteristica Web Express Logon)
- i5/OS NetServer
- QFileSvr.400

---

## Scenarii: EIM (Enterprise Identity Mapping)

Utilizați aceste informații pentru a învăța cum să gestionați identități utilizator de-a lungul diferitelor sisteme într-un mediu de semnare unică.

EIM (Enterprise Identity Mapping) este o tehnologie de infrastructură IBM care vă permite să urmăriți și să gestionați identitățile utilizator într-o întreprindere. Tipic, dumneavoastră utilizați EIM cu o tehnologie de autentificare, cum ar fi serviciul de autentificare în rețea, pentru a implementa un mediu de semnare unică.

### Informații înrudite

Scenariu semnare unică

---

## Planificarea pentru EIM (Enterprise Identity Mapping)

Înainte să setați EIM ar trebui să dezvoltați planul de implementare EIM (Enterprise Identity Mapping) pentru a vă asigura că ați configurat EIM pentru un mediu System i sau într-un mediu platformă amestecat.

Un plan de implementare este esențial pentru a configura și a folosi cu succes EIM în întreprinderea dumneavoastră. Pentru a dezvolta planul dumneavoastră, trebuie să colectați date despre sisteme, aplicații și utilizatori care folosesc EIM. Veți folosi informațiile pe care le adunați pentru a lua decizii de cum să configurați cât mai bine EIM în întreprinderea dumneavoastră.

Deoarece EIM este o tehnologie de infrastructură IBM eServer disponibilă pentru toate platformele IBM, cum vă planificați implementarea depinde de ce platforme sunt în întreprinderea dumneavoastră. Deși există un număr de activități de planificare pentru fiecare platformă, multe activități de planificare EIM se aplică tuturor platformelor IBM. Trebuie să folosiți activitățile de planificare EIM comune pentru a crea un plan de implementare general. Pentru a afla cum să vă planificați implementarea EIM, examinați aceste pagini:

## Planificarea EIM (Enterprise Identity Mapping) pentru eServer

Un plan de implementare este esențial pentru a configura cu succes și a folosi EIM (Enterprise Identity Mapping) într-o întreprindere cu platforme mixte. Pentru a vă dezvolta planul de implementare, aveți nevoie să colectați date despre sistemele, aplicațiile și utilizatorii care vor folosi EIM. Veți folosi informațiile pe care le adunați pentru a lua decizii despre cum e mai bine să configurați EIM pentru un mediu cu platforme mixte.

Următoarea listă furnizează un traseu al task-urilor de planificare pe care ar trebui să-l urmați înainte de a configura și folosi EIM într-un mediu cu platforme mixte. Citiți informațiile din aceste pagini pentru a învăța cum să vă planificați cu succes nevoile de configurație EIM, inclusiv de ce abilități are nevoie echipa dumneavoastră de implementare, ce informații trebuie să adunați și deciziile de configurare pe care trebuie să le faceți. Vă va fi de ajutor să tipăriți fișele de lucru pentru planificarea EIM (numărul 8 în lista de mai jos), astfel încât să le puteți efectua pe măsură ce treceți prin procesul de planificare.

## Cerințele de setare EIM (Mapare de identități în întreprindere) pentru eServer

Pentru a implementa EIM cu succes, trebuie să îndepliniți aceste cerințe: nivel întreprindere sau rețea, sistem și aplicație.

## Cerințele la nivel de întreprindere sau de rețea

Trebuie să configurați un sistem din întreprinderea sau rețeaua dumneavoastră să acționeze ca un controler de domeniu EIM, care e un server LDAP (Lightweight Directory Access Protocol) special configurat care memorează și furnizează date domeniu EIM. Sunt un număr de considerente pentru a alege care produs de servicii director să-l folosiți ca un controler de domeniu, inclusiv faptul că nu toate produsele server LDAP furnizează suport pentru controler de domeniu EIM.

Un alt considerent este disponibilitatea uneltelor de administrare. O opțiune e că puteți folosi API-urile EIM în propriile dumneavoastră aplicații pentru a realiza funcții administrative. Dacă aveți de gând să utilizați IBM Tivoli Directory Server for i5/OS ca un controler de domeniu EIM, puteți utiliza Navigator System i pentru a gestiona EIM. Dacă plănuți să folosiți produsul IBM Directory, puteți folosi utilitarul eimadmin care este parte din LDAP SPE V1R4.

Următoarele informații furnizează informații de bază despre care platforme IBM furnizează un produs server director care suportă EIM. Puteți găsi informații mai detaliate despre alegerea unui server director pentru a furniza suport controler de domeniu EIM în Planificarea unui controler de domeniu EIM.

## Cerințele pentru aplicații și sisteme

Fiecare sistem care participă într-un domeniu EIM trebuie să îndeplinească următoarele cerințe:

- Să aibă software-ul client LDAP instalat.
- Să aibă o implementare a API-urilor EIM.

Fiecare aplicație care va participa într-un domeniu EIM trebuie să fie capabilă să folosească API-urile EIM pentru a realiza operații de căutare mapare și alte operații.

**Notă:** În cazul unei aplicații distribuite, s-ar putea să nu fie necesar ca atât partea server cât și partea client să fie capabile să folosească API-urile EIM. Tipic, doar partea server a aplicației are nevoie să folosească API-urile EIM.

Următoarea tabelă furnizează informații despre suportul EIM pe care platforma eServer îl furnizează. Informațiile sunt organizate de platformă cu coloane care indică următoarele:

- Clientul EIM necesar pentru ca platforma să suporte API-urile EIM.
- Tipul configurației EIM și al uneltelor de administrare care sunt disponibile pentru platformă.
- Produsul server director care poate fi instalat pentru platformă pentru a servi ca un controler de domeniu EIM.

O platformă nu trebuie să fie capabilă să servească ca un controler de domeniu EIM pentru a participa într-un domeniu EIM.

Tabela 9. Suportul EIM pentru eServer EIM


Platformă	Client EIM (suport API)	Controler de domeniu	Unelte administrare EIM
AIX pe System p	AIX R5.2	IBM Directory V5.1	Nu e disponibil
Linux <ul style="list-style-type: none"><li>• SLES8 on PPC64</li><li>• Red Hat 7.3 pe i386</li><li>• SLES7 pe System z</li></ul>	Descărcați una din următoarele: <ul style="list-style-type: none"><li>• IBM Directory V4.1 client</li><li>• IBM Directory V5.1 client</li><li>• Open LDAP v2.0.23 client</li></ul> 	IBM Directory V5.1	Nedisponibil
i5/OS pe System i	i5/OS V5R3 sau ulterior	IBM Tivoli Directory Server for i5/OS	Navigator System i

Tabela 9. Suportul EIM pentru eServer EIM (continuare)

Platformă	Client EIM (suport API)	Controler de domeniu	Unelte administrare EIM
Windows 2000 pe System x	Descărcați una din următoarele: <ul style="list-style-type: none"> <li>• Clientul IBM Directory V4.1</li> <li>• IBM Directory V5.1 client</li> </ul>	IBM Directory V5.1 client	Nedisponibil
z/OS pe System z	z/OS V1R4 LDAP SPE OW57137	z/OS V1R4 LDAP	V1R4 LDAP SPE OW57137

Cât timp o platformă furnizează suport client EIM (API) acel sistem poate participa într-un domeniu EIM. Nu e necesar ca o platformă să furnizeze suport pentru controler de domeniu EIM decât dacă vreți să folosiți acea platformă particulară ca și controler de domeniu EIM pentru întreprinderea dumneavoastră.

### Informații înrudite



IBM Tivoli Directory Server

## Identificarea rolurilor și calificărilor necesare

EIM (Enterprise Identity Mapping) este proiectat astfel încât o singură persoană poate fi responsabilă ușor pentru configurare și administrare într-o organizație mică. Sau, într-o organizație mai mare, poate preferați să aveți un număr de indivizi diferiți care să trateze aceste responsabilități.

Numărul de persoane de care aveți nevoie în echipa dumneavoastră variază în funcție de numărul de abilități necesare pe care fiecare membru le posedă, tipul platformelor implicate în implementarea dumneavoastră EIM și de modul în care organizația dumneavoastră preferă să-și împartă rolurile de securitate și responsabilitățile.

O implementare EIM cu succes necesită configurarea și interacțiunea câtorva produse software. Deoarece fiecare din aceste produse necesită abilități și roluri specifice, puteți alege să creați o echipă de implementare EIM care conține oameni din discipline diferite, în special dacă lucrați într-o organizație mare.

Următoarele informații descriu calificările și autoritatea de control acces EIM necesare pentru a implementa EIM cu succes. Aceste abilități sunt prezentate în termeni de titluri de joburi pentru oamenii care se specializează în ele. De exemplu, un task care cere abilități LDAP (Lightweight Directory Access Protocol) este văzut ca un task pentru un administrator de Server director.

## Membrii echipei și rolurile lor

Următoarele informații descriu responsabilitățile și autorizarea necesară a rolurilor care sunt necesare pentru gestionarea EIM. Puteți folosi această listă de roluri pentru a determina membrii echipei care sunt necesari pentru a instala și configura produse date de cerințele preliminare și pentru a configura EIM și unul sau mai multe domenii EIM.

Unul din primele seturi de roluri pe care trebuie să le definiți este numărul și tipul administratorilor pentru domeniul dumneavoastră EIM. Întregului personal căruia îi dați sarcini administrative și autorizare EIM trebuie să fie implicat în procesul de planificare EIM ca membri ai echipei de implementare EIM.

**Notă:** Administratorii EIM joacă un rol important în organizația dumneavoastră și au tot la fel de multă putere ca indivizii cărora le e permis să creeze identități utilizator pe sistemele dumneavoastră. Când creează asocieri EIM pentru identități utilizator, ei determină cine poate accesa sistemele dumneavoastră și ce privilegii are când face asta. IBM recomandă să dați această autorizare acelor indivizi în care aveți un nivel mare de încredere pe baza politicii de securitate a companiei dumneavoastră.

Următoarea tabelă listează roluri potențiale pentru membrii echipei și task-urile și abilitățile necesare pentru configurarea și gestionarea EIM.

**Notă:** Dacă o singură persoană din organizația dumneavoastră va fi responsabilă pentru toate task-urile de configurare și administrare EIM, aceluși persoană ar trebui să i se dea rolul și autorizarea de administrator EIM.

*Tabela 10. Rolurile, taskurile și calificările pentru configurarea EIM*

<b>Rol</b>	<b>Taskuri autorizate</b>	<b>Calificări necesare</b>
Administrator EIM	<ul style="list-style-type: none"> <li>• Coordonarea operațiilor domeniu</li> <li>• Adăugarea, înlăturarea și modificarea definițiilor registrelor, identificatorilor EIM și asocierilor pentru identități utilizator</li> <li>• Autorizare controler la datele din domeniul EIM</li> </ul>	Cunoștințe despre uneltele de administrare EIM
Administrator identificatori EIM	<ul style="list-style-type: none"> <li>• Crearea și modificarea identificatorilor EIM</li> <li>• Adăugarea și înlăturarea asocierilor administrative și sursă (nu se pot adăuga sau înlătura asocieri destinație)</li> </ul>	Cunoștințe despre uneltele de administrare EIM
Administrator registre EIM	<p>Gestionarea tuturor definițiilor registrelor EIM:</p> <ul style="list-style-type: none"> <li>• Adăugarea și înlăturarea asocierilor destinație (nu se pot adăuga sau înlătura asocieri sursă sau administrative)</li> <li>• Actualizare definiții registru EIM</li> </ul>	<p>Cunoștințe despre:</p> <ul style="list-style-type: none"> <li>• Toate registrele de utilizatori definite în domeniul EIM (cum ar fi informații despre identitățile utilizator)</li> <li>• Uneltele de administrare EIM</li> </ul>
Administrator registru EIM X	<p>Gestionare definiție pentru registru EIM specific:</p> <ul style="list-style-type: none"> <li>• Adăugarea și înlăturarea asocierilor destinație pentru un registru de utilizatori specific (de exemplu, registrul X)</li> <li>• Actualizarea unei definiții de registru EIM specific</li> </ul>	<p>Cunoștințe despre:</p> <ul style="list-style-type: none"> <li>• Registrul utilizator particular definit în domeniul EIM (cum ar fi informații despre identitățile utilizator)</li> <li>• Uneltele de administrare EIM</li> </ul>
Administrator Server director (LDAP)	<ul style="list-style-type: none"> <li>• Instalarea și configurarea unui server director (dacă e necesar)</li> <li>• Personalizarea configurațiilor serverului director pentru</li> <li>• Crearea unui domeniu EIM (vedeți nota)</li> <li>• Definirea utilizatorilor care sunt autorizați să acceseze controlerul de domeniu EIM</li> <li>• Opțional: Definirea primului administrator EIM</li> </ul> <p><b>Notă:</b> Administratorul serverului director poate face tot ce face un administrator EIM.</p>	<p>Cunoștințe despre:</p> <ul style="list-style-type: none"> <li>• Instalarea, configurarea și personalizarea serverului director</li> <li>• Unelte administrare EIM</li> </ul>
Administrator registru de utilizatori	<ul style="list-style-type: none"> <li>• Setare profiluri utilizator sau identități utilizator pentru un registru de utilizatori specific</li> <li>• Opțional: Să servească ca un administrator de registru EIM pentru registre de utilizatori specifice</li> </ul>	<p>Cunoștințe despre:</p> <ul style="list-style-type: none"> <li>• Unelte pentru administrarea registrului de utilizatori</li> <li>• Unelte administrare EIM</li> </ul>

Tabela 10. Rolurile, taskurile și calificările pentru configurarea EIM (continuare)

Rol	Taskuri autorizate	Calificări necesare
Programator sistem sau administrator sistem	Instalarea produselor software necesare (poate include instalarea EIM)	Cunoștințe despre: <ul style="list-style-type: none"> <li>• Programarea sistemului sau abilități de administrare</li> <li>• Proceduri de instalare pentru platformă</li> </ul>
Programator aplicații	Scrierea aplicațiilor care folosesc API-uri EIM	Cunoștințe despre: <ul style="list-style-type: none"> <li>• Platformă</li> <li>• Abilități de programare</li> <li>• Compilarea programelor</li> </ul>

### Concepte înrudite

“Controlul accesului în EIM” la pagina 38

Un utilizator EIM (Enterprise Identity Mapping) este un utilizator care are control acces EIM bazat pe calitatea sa de membru într-un grup de utilizatori predefinit LDAP (Lightweight Directory Access Protocol) pentru un domeniu specific.

### Planificarea domeniului EIM

O parte critică a procesului de planificare a implementării EIM (Enterprise Identity Mapping) cere să definiți un domeniu EIM. Pentru a obține beneficii maxime având un depozit central de informații mapate, trebuie să planificați ca domeniul să fie partajat între mai multe aplicații și sisteme.

Pe măsură ce parcurgeți subiectul Planificarea EIM, veți aduna informațiile de care aveți nevoie pentru a defini domeniul și pentru a-l înregistra în fișele de lucru pentru planificare. Secțiunile de exemple din fișele de lucru vă pot ajuta să vă ghidați să adunați și să înregistrați aceste informații la fiecare etapă de planificare din acest subiect.

Următoarea tabelă listează informațiile pe care trebuie să le adunați la planificarea domeniului dumneavoastră și sugerează rolul sau rolurile echipei de implementare EIM care poate fi responsabilă pentru fiecare element de informație necesar.

**Notă:** Deși tabela listează un rol particular ca o sugestie pentru alocarea responsabilității adunării informațiilor descrise, ar trebui să alocați roluri pe baza nevoilor dumneavoastră și a politicii de securitate pentru organizația dumneavoastră. De exemplu, într-o organizație mai mică poate preferați să desemnați o singură persoană drept administrator EIM pentru a fi responsabilă cu toate aspectele planificării, configurării și gestionării EIM.

Tabela 11. Informațiile necesare pentru planificarea domeniului EIM

Informații necesare	Role
1. Dacă este un domeniu existent pentru folosire care îndeplinește nevoile dumneavoastră sau dacă trebuie să creați unul.	Administrator EIM
2. Care server director va acționa ca și controler de domeniu EIM. (Trecere în revistă “Planificarea unui controler de domeniu EIM” la pagina 56 pentru informații detaliate despre alegerea controlerului de domeniu.)	Administratorul Serverului director (LDAP) sau administratorul EIM
3. Un nume pentru domeniu. (Puteți de asemenea să furnizați o descriere opțională.)	Administrator EIM
4. Unde în director se vor memora datele domeniului EIM. <b>Notă:</b> În funcție de alegerea dumneavoastră a sistemului pentru găzduirea serverului director și alegerea directorului pentru memorarea datelor domeniului EIM, ați putea avea nevoie să realizați unele task-uri de configurare servicii asupra directorului înainte ca domeniul să fie creat.	Atât administratorul Serverului director (LDAP) cât și administratorul EIM

Tabela 11. Informațiile necesare pentru planificarea domeniului EIM (continuare)

Informații necesare	Role
5. Aplicațiile și sistemele de operare care vor participa în domeniu. Dacă configurați primul dumneavoastră domeniu, acest set inițial poate conține cel puțin un sistem. (Trecere în revistă “Dezvoltarea unui plan de numire definiții de registru EIM (Enterprise Identity Mapping)” la pagina 58 pentru informații suplimentare.)	Echipă EIM
6. Oamenii și entitățile care vor participa în domeniu. <b>Notă:</b> Pentru a face testele inițiale mai ușoare, poate vreți să limitați numărul de participanți la unul sau doi.	Echipă EIM

## Planificarea unui controler de domeniu EIM

În timp ce strângeți informații pentru a defini domeniul EIM, trebuie să determinați care produs server de director se va comporta ca și controlerul de domeniu EIM.

EIM necesită controlerul de domeniu să fie găzduit de un server director care suportă LDAP (Lightweight Directory Access Protocol (LDAP) Versiunea 3. Suplimentar, produsul server director trebuie să fie capabil să accepte Schema LDAP și alte considerente privind EIM și să înțeleagă anumite atribute și clase obiect.

Dacă întreprinderea dumneavoastră posedă mai mult de un server director care poate găzdui un controler de domeniu EIM, ar trebui să considerați folosirea controlerelor domeniu replicate secundare. De exemplu, dacă vă așteptați să aveți un număr mare de operații de căutare mapare EIM, replicile pot îmbunătăți performanțele operațiilor de căutare.

De asemenea, ar trebui să considerați dacă să faceți controlerul de domeniu *local* sau *la distanță* în relație cu sistemul care vă așteptați să ruleze numărul cel mai mare de operații de căutare mapare. Având controlerul de domeniu local pe sistemul de volum înalt, puteți îmbunătăți performanța operațiilor de căutare pe sistemul local. Folosiți fișele de lucru pentru planificare pentru a înregistra aceste decizii de planificare, precum și acelea pe care le faceți pentru domeniul dumneavoastră și alte informații despre director.

După ce determinați care server director din întreprinderea dumneavoastră va găzdui controlerul de domeniu EIM, trebuie să luați unele decizii despre accesul la controlerul de domeniu.

## Planificarea accesului la controlerul de domeniu

Trebuie să planificați cum veți accesa dumneavoastră și aplicațiile și sistemele de operare activate EIM serverul director care găzduiește controlerul de domeniu EIM. Pentru a accesa un domeniu EIM trebuie:

1. Să fiți capabil să vă legați la controlerul de domeniu EIM
2. Să fiți sigur că subiectul de legare este un membru al unui grup de control acces EIM sau este administratorul LDAP. Referiți-vă la Gestionare control acces EIM pentru informații suplimentare.

## Selectarea tipului legăturii EIM

API-urile EIM suportă câteva mecanisme diferite pentru stabilirea unei conexiuni, cunoscută de asemenea ca legare, cu controlerul de domeniu EIM. Fiecare tip de mecanism de legare furnizează un nivel diferit de autentificare și criptare pentru conexiune. Alegerile posibile sunt:

### Legături Simple

O legătură simplă este o conexiune LDAP unde un client LDAP furnizează un nume distinctiv al legăturii și o parolă de legătură la serverul LDAP pentru autentificare. Numele distinctiv și parola de legătură sunt definite de administratorul LDAP în directorul LDAP. Aceasta este cea mai slabă formă de autentificare și cea mai puțin sigură deoarece numele distinctiv și parola de legătură sunt trimise necriptate și sunt vulnerabile. Utilizați CRAM-MD5 (mecanism de autentificare cerere de identificare-răspuns) pentru a adăuga un nivel de protecție adițional pentru parola de legătură. Cu protocolul CRAM-MD5, clientul trimite o valoare hash în locul parolei necriptate la server pentru autentificare.

### Autentificare server cu SSL - autentificare parte server

Un server LDAP poate fi configurat pentru conexiuni SSL sau TLS. Serverul LDAP folosește un certificat digital pentru a se autentifica pe el însuși la clientul LDAP și stabilește o sesiune de comunicații criptate între ei. Doar serverul LDAP este autentificat prin intermediul unui certificat. Capătul utilizator este autentificat prin intermediul unui nume distinctiv și parolă de legătură. Tăria autentificării este aceeași cu cea pentru o legătură simplă, dar toate datele (inclusiv numele distinctiv și parola de legătură) sunt criptate pentru protecție.

### Autentificare client cu SSL

Un server LDAP poate fi configurat să necesite ca utilizatorul final să fie autentificat prin mijlocul unui certificat digital decât printr-un nume distinctiv de legătură și parolă pentru SSL sau conexiuni sigure TLS la serverul LDAP. Atât clientul, cât și serverului sunt autentificate și sesiunea este criptată. Această opțiune furnizează un nivel mai puternic de autentificare a utilizatorului și protejează confidențialitatea tuturor datelor transmise.

### Autentificare Kerberos

Un client LDAP poate fi autentificat la server utilizând tichetul Kerberos ca un înlocuitor suplimentar pentru un nume distinctiv legătură și parolă. Kerberos, care este un sistem de autentificare în rețea terță-partie de încredere, permite unui principal (un utilizator sau un serviciu) să-și demonstreze identitatea altui serviciu în interiorul unei rețele care nu e de încredere. Autentificarea principalilor este efectuată printr-un server centralizat numit KDC (key distribution center). KDC autentifică un utilizator cu un tichet Kerberos. Aceste tichete dovedesc identitatea principalului altor servicii dintr-o rețea. După ce un principal este autentificat cu aceste tichete, el și serviciul pot schimba date criptate cu un serviciu destinație. Această opțiune furnizează un nivel mai mare de autentificare utilizator și protejează intimitatea informațiilor de autentificare.

Alegerea unui mecanism de legare este bazată pe nivelul de securitate cerut de aplicația cu EIM activ și de mecanismele de autentificare suportate de serverul LDAP care găzduiește domeniul EIM.

De asemenea, s-ar putea să fie nevoie să realizați task-uri de configurare suplimentare pentru ca serverul LDAP să activeze mecanismele de autentificare pe care alegeți să le folosiți. Verificați documentația pentru serverul LDAP care vă găzduiește controlerul de domeniu pentru a determina ce alte task-uri de configurare trebuie să realizați.

### Exemplu de fișă de lucru planificare: informații despre controler de domeniu

După ce luați deciziile referitoare la controlerul de domeniu EIM, folosiți fișele de lucru pentru planificare pentru a înregistra informațiile despre controlerul de domeniu EIM de care au nevoie sistemele de operare și aplicațiile dumneavoastră cu EIM activ. Informațiile pe care le adunați ca parte a acestui proces pot fi folosite de administratorul LDAP pentru a defini identitatea de legătură a aplicației sau a sistemului de operare la serverul director LDAP care găzduiește controlerul de domeniu EIM.

Următoarea porțiune exemplu a fișelor de lucru pentru planificare arată tipul informațiilor pe care trebuie să le adunați. De asemenea include valori exemplu pe care le-ați putea folosi când configurați controlerul de domeniu EIM.

Tabela 12. Informațiile despre domeniu și despre controlerul de domeniu pentru fișa de lucru pentru planificare EIM

Informații necesare pentru a configura domeniul EIM și controlerul de domeniu	Răspunsuri exemplu
Un nume cu sens pentru domeniu. Acesta poate fi numele unei companii, al unui departament sau al unei aplicații care folosește domeniul.	MyDomain
Opțional: Dacă configurați un domeniu EIM într-un director LDAP existent deja, specificați un nume distinctiv părinte pentru domeniu. Acesta este numele distinctiv care reprezintă intrarea imediat mai sus de intrarea nume domeniu din ierarhia arbore a informațiilor director, de exemplu, o=ibm,c=us.	o=ibm,c=us

Tabela 12. Informațiile despre domeniu și despre controlerul de domeniu pentru fișa de lucru pentru planificare EIM (continuare)

Informații necesare pentru a configura domeniul EIM și controlerul de domeniu	Răspunsuri exemplu
Nume distinctiv domeniu EIM complet calificat rezultat. Acesta este numele complet al domeniului EIM care descrie locația directorului pentru datele domeniului EIM. Numele distinctiv complet calificat al domeniului conține, cel puțin, DN-ul pentru domeniu (ibm-eimDomainName=), plus numele domeniului pe care l-ați specificat. Dacă alegeți să specificați un DN părinte pentru domeniu, atunci DN-ul complet calificat al domeniului conține DN-ul relativ al domeniului (ibm-eimDomainName=), numele domeniului (MyDomain) și DN-ul părinte (o=ibm,c=us). <b>Notă:</b>	Oricare din acestea, depinde dacă alegeți un DN părinte: <ul style="list-style-type: none"> <li>• ibm-eimDomainName=MyDomain</li> <li>• ibm-eimDomainName=MyDomain,o=ibm,c=us</li> </ul>
Adresa conexiunii pentru controlerul de domeniu. Aceasta conține tipul conexiunii (ldap de bază sau ldap securizat, de exemplu, ldap:// sau ldaps://) plus următoarele informații:	ldap://
<ul style="list-style-type: none"> <li>• Opțional: Numele adresă sau adresa IP</li> <li>• Opțional: Numărul portului</li> </ul>	<ul style="list-style-type: none"> <li>• some.ldap.host</li> <li>• 389</li> </ul>
Adresa completă rezultată a conexiunii pentru controlerul de domeniu.	ldap://some.ldap.host:389
Mecanisme de legare cerute de aplicații sau sisteme. Alegerile includ: <ul style="list-style-type: none"> <li>• Legătură simplă</li> <li>• CRAM MD5</li> <li>• Autentificare server</li> <li>• Autentificare client</li> <li>• Kerberos</li> </ul>	Kerberos

Dacă configurația dumneavoastră EIM și echipa de administrare conține mai mulți membri ai echipei, va fi nevoie să determinați identitatea de legătură și mecanismul pe care le vor folosi fiecare membru al echipei pentru accesarea domeniului EIM pe baza rolului lor. De asemenea, trebuie să determinați identitatea de legătură și mecanismul pentru utilizatorii finali ai aplicației EIM. Ați putea găsi fișa de lucru următoare foarte folositoare ca exemplu pentru adunarea acestor informații.

Tabela 13. Exemplu de fișă de lucru pentru planificarea identității de legătură

Autorizare sau rol EIM	Identitate de legătură	Mecanism de legătură	Motiv necesar
EIM administrator	eimadmin@krbrealml.com	kerberos	configurare și gestionare EIM
Administrator LDAP	cn=administrator	legătură simplă	configurare controler de domeniu EIM
Administrator registru EIM X	cn=admin2	CRAM MD5	gestionare definiții registru specific
Căutare mapări EIM	cn=MyApp,c=US	legătură simplă	realizare operații de căutare mapare aplicație

## Dezvoltarea unui plan de numire definiții de registru EIM (Enterprise Identity Mapping)

Pentru a folosi EIM (Enterprise Identity Mapping) pentru a mapa identitatea utilizator dintr-un registru de utilizatori la o identitate utilizator echivalentă din alt registru de utilizatori, ambele registre de utilizatori trebuie să fie definite pentru EIM.



Trebuie să creați o definiție de registru EIM pentru fiecare operație sau registru de utilizatori al sistemului de operare care va participa în domeniul EIM. Registrele de utilizatori pot reprezenta registrele sistemelor de operare precum RACF (Resource Access Control Facility) sau i5/OS, un registru distribuit precum Kerberos sau un subset de registre de sistem care este utilizat exclusiv de o aplicație.

Un domeniu EIM poate conține definiții de registre pentru registre de utilizatori care există pe orice platformă. De exemplu, un domeniu gestionat de un controler de domeniu pe i5/OS ar putea conține definiții de registre pentru platforme non-i5/OS (precum un registru AIX). Deși puteți defini oricare registru de utilizatori pe un domeniu EIM, trebuie să definiți registre de utilizatori pentru acele aplicații și sisteme de operare care sunt active EIM.

Puteți numi o definiție de registru EIM orice vreți cu condiția ca numele să fie unic în domeniul EIM. De exemplu, ați putea numi definiția registrului EIM pe baza numelui sistemului care găzduiește registrul de utilizatori. Dacă asta nu e suficient pentru a distinge definiția registrului din definiții similare, ați putea folosi un punct (.) sau o liniuță de subliniere (\_) pentru a adăuga tipul registrului de utilizatori pe care îl definiți. Indiferent de criteriile pe care alegeți să le folosiți, ar trebui să considerați dezvoltarea unei convenții de numire pentru definițiile registrului EIM. Făcând așa vă asigurați că numele definițiilor sunt consistente în domeniu și că descriu adecvat tipul și instanța registrului de utilizatori definit și modul în care e folosit. De exemplu, ați putea alege numele fiecărei definiții de registru folosind o combinație a numelui aplicației sau al sistemului de operare care folosește registrul și locația fizică a acestuia în întreprinderea dumneavoastră.

O aplicație care e scrisă pentru a folosi EIM poate specifica fie un alias de registru sursă sau destinație fie alias-uri pentru ambele. Când creați definiții de registre EIM trebuie să verificați documentația pentru aplicațiile dumneavoastră pentru a determina dacă trebuie să specificați unul sau mai multe alias-uri pentru definiții de registre. Când alocați aceste alias-uri definițiilor de registre corespunzătoare, aplicația poate realiza o căutare de alias pentru a găsi definiția sau definițiile registrului EIM care se potrivește aliasurilor din aplicație.

Puteți considera următoarea porțiune exemplu din fișa de lucru pentru planificare ca fiind de ajutor ca un ghid pentru a folosi informațiile înregistrate despre registrele de utilizatori participante. Puteți folosi fișa de lucru reală pentru a specifica un nume de definiție registru pentru fiecare registru de utilizatori, pentru a specifica dacă folosește un alias și pentru a descrie locația registrului de utilizatori și folosirea sa. Documentația pentru instalarea și configurarea aplicației vă va furniza unele dintre informațiile de care aveți nevoie pentru fișa de lucru.

*Tabela 14. Exemplu de fișă de lucru pentru planificarea informațiilor definițiilor de registre EIM*

Nume definiție pentru registru	Tip registru de utilizatori	Alias definiție pentru registru	Descriere registru
System_C	Registru de utilizatori sistem i5/OS	Examinați documentația aplicației	Registru de utilizatori principal al sistemului pentru i5/OS pe System C
System_A_WAS	WebSphere LTPA	app_23_alias_source	Registru de utilizatori WebSphere LTPA pe System A
System_B	Linux	Examinați documentația aplicației	Registru de utilizatori Linux pe System B
System_A	Registru de utilizatori sistem i5/OS	app_23_alias_target app_xx_alias_target	Registru de utilizatori principal al sistemului pentru i5/OS pe System A
System_D	Registru de utilizatori Kerberos	app_xx_alias_source	regiune Kerberos legal.mydomain.com
System_4	Registru de utilizatori pentru Windows 2000	Examinați documentația aplicației	Registru de utilizatori aplicație de resurse umane pe sistemul 4

**Notă:** Tipurile asocierii pentru fiecare registru vor fi determinate mai târziu în procesul de planificare.

După ce terminați această secțiune a fișei de lucru pentru planificare, ar trebui să vă dezvoltați planul de mapare a identității pentru a determina dacă să folosiți asocieri identificator, asocieri de politică sau ambele tipuri pentru a crea mapările de care aveți nevoie pentru identitățile utilizator din fiecare registru de utilizatori definit.

## Dezvoltarea unui plan de mapare identități

O parte critică a procesului de planificare a implementării EIM (Enterprise Identity Mapping) cere să determinați cum vreți să folosiți maparea identității în întreprinderea dumneavoastră.

Sunt două metode pe care le puteți folosi pentru a mapa identități în EIM:

- **Asocierile de identificator** descriu relații între un identificator EIM și identitățile utilizator din registrele de utilizatori care reprezintă persoana. O asociere identificator creează o mapare directă unu-la-unu între un identificator EIM și o identitate utilizator specifică. Puteți folosi asocieri identificator pentru a defini indirect o relație între identități utilizator prin identificatorul EIM.

Dacă politica dumneavoastră de securitate necesită un grad mare de responsabilitate, aveți nevoie să folosiți asocieri identificator aproape exclusiv pentru implementarea mapării identității dumneavoastră. Deoarece folosiți asocieri de identitate pentru a crea mapări unu-la-unu pentru identitățile utilizator pe care aceștia le dețin, puteți să determinați mereu cu exactitate cine a realizat o acțiune asupra unui obiect sau asupra sistemului.

- **Asocierile de politică** descriu o relație între mai multe identități utilizator și o singură identitate utilizator dintr-un registru de utilizatori. Asocierile de politică folosesc suport pentru politica de mapare EIM pentru a crea mapări multe-la-una între identități utilizator fără a invoca un identificator EIM.

Asocierile de politică pot fi folositoare când aveți unul sau mai multe grupuri mari de utilizatori care au nevoie de acces la sisteme sau aplicații din întreprinderea dumneavoastră unde nu vreți ca ei să aibă identități utilizator specifice pentru a primi acest acces. De exemplu, mențineți o aplicație Web care accesează o aplicație internă specifică. Nu vreți să setați sute sau mii de identități utilizator pentru a autentifica utilizatorii pentru această aplicație internă. În această situație, poate vreți să configurați maparea identității astfel încât toți utilizatorii acestei aplicații Web sunt mapați la o singură identitate utilizator cu nivelul minim de autorizare necesar pentru a rula aplicația. Puteți face acest tip de mapare identitate folosind asocieri de politică.

Poate decideți să folosiți asocieri identificator pentru a furniza cel mai bun control al identităților utilizator din întreprinderea dumneavoastră cu cel mai mare grad de gestiuni simplificată a parolelor. Sau vă puteți decide să utilizați un amestec de asocieri de politică și asocieri de identificatoare pentru a fluidiza semnarea unică, când corespunzător, în timp ce mențineți control specific peste identitățile utilizator pentru administratori. Indiferent de ce tip de mapare decideți că îndeplinește cel mai bine nevoile afacerii dumneavoastră și se potrivește corespunzător politicii dumneavoastră de securitate, aveți nevoie să creați un plan de mapare identitate pentru a vă asigura că implementați maparea identității corespunzător.

Pentru a crea un plan de mapare a identității, trebuie să faceți următoarele:

### Concepte înrudite

“Crearea asocierilor EIM” la pagina 100

Sunt două tipuri de asocieri EIM pe care le puteți crea. Puteți crea fie o asociere identificator sau o asociere de politică.

“Crearea unei asocieri de politică” la pagina 102

O asociere de politică furnizează un mod de a defini o relație dintre mai multe identități de utilizatori din unul sau mai multe registre și o identitate de utilizator unică în alt registru.

### Planificarea asocierilor EIM:

Asocierile sunt intrări pe care le creați într-un domeniu EIM pentru a defini relațiile între identități utilizator în diferite registre de utilizatori.

Puteți crea unul din cele două tipuri de asocieri în EIM: asocieri identificator pentru a defini mapări unu-la-unu și asocieri de politică pentru a defini mapări multi-la-unu. Puteți folosi asocierile de politică în locul sau în combinație cu asocierile identificator.

Tipurile specifice de asocieri pe care alegeți să le creați depinde de cum folosește un utilizator o anumită identitate utilizator, precum și de planul general de mapare identitate al dumneavoastră.

Puteți crea oricare din următoarele tipuri de asocieri identificator:

- **Asocierile destinație**

Definiți asocieri destinație pentru utilizatori care în mod normal accesează sistemul ca un server de pe un alt sistem client. Acest tip de asociere e folosit când o aplicație realizează operații de căutare mapare.

- **Asocierile sursă**

Definiți asocieri sursă când identitatea utilizator este prima pe care utilizatorul o furnizează pentru a se înregistra pe sistem sau rețea. Acest tip de asociere e folosit când o aplicație realizează operații de căutare mapare.

- **Asocierile administrative**

Definiți asocieri administrative când vreți să fiți capabil să urmăriți faptul că identitatea utilizator aparține unui utilizator specific, dar nu vreți ca ea să fie disponibilă pentru operații de căutare mapare. Puteți folosi acest tip de asociere pentru a urmări toate identitățile utilizator pe care o persoană le folosește în întreprindere.

O **asociere de politică** definește mereu o asociere destinație.

E posibil ca o singură definiție pentru registru să aibă mai mult de un tip de asocieri în funcție de cum e folosit registrul de utilizatori la care se referă. Deși nu există limite pentru numărul sau combinațiile de asocieri pe care le puteți defini, păstrați acest număr minim pentru a simplifica administrarea domeniului dumneavoastră EIM.

Tipic, o aplicație va furniza o ghidare pentru definițiile registrelor pe care le așteaptă ca registre sursă și destinație, dar nu și pentru tipurile asocierii. Fiecare capăt utilizator al aplicației trebuie să fie mapat pe ea prin cel puțin o asociere. Această asociere poate fi o mapare unu-la-unu între identificatorul EIM unic și o identitate utilizator din registrul destinație cerut sau o mapare multi-la-unu între un registru sursă pentru care identitatea utilizator este membru și registrul destinație cerut. Care tip de asociere folosiți depinde de cerințele dumneavoastră de mapare identitate și criteriile pe care le furnizează aplicația.

Anterior, ca parte a procesului de planificare, ați completat două fișe de lucru pentru planificarea identităților de utilizator din organizația dumneavoastră cu informații despre identificatorii EIM și definițiile de registru EIM de care aveți nevoie. Acum trebuie să unificați aceste informații specificând tipurile asocierilor pe care vreți să le folosiți pentru a mapa identitățile utilizatorilor din întreprinderea dumneavoastră. Trebuie să determinați dacă să definiți o asociere de politică pentru o anumită aplicație și registrele ei de utilizatori sau să definiți asocieri identificator specifice (sursă, destinație sau administrativă) pentru fiecare identitate utilizator din sistem sau registru aplicație. Puteți face aceasta înregistrând informații despre tipurile de asocieri cerute atât în fișele de lucru pentru planificarea definițiilor de registre, cât și în rândurile corespondente din fiecare fișă de lucru pentru asociere.

Pentru a vă finaliza planul de mapare a identității, puteți folosi următoarele fișe de lucru exemplu drept ghid, pentru a vă ajuta să înregistrați informațiile asocierii cu care trebuie să descrieți imaginea completă a modului în care intenționați să implementați maparea identității.

*Tabela 15. Exemplu de fișă de lucru pentru planificarea informațiilor definițiilor de registre*

Nume definiție pentru registru	Tip registru de utilizatori	Alias definiție pentru registru	Descriere registru	Tipuri asociere
System_C	Registru de utilizatori sistem i5/OS	Trecere în revistă documentație aplicație	Registru de utilizatori principal al sistemului pentru i5/OS pe System C	Destinație
System_A_WAS	WebSphere LTPA	app_23_alias_source	Registru de utilizatori WebSphere LTPA pe System A	Sursă primară
System_B	Linux	Trecere în revistă documentație aplicație	Registru de utilizatori Linux pe System B	Sursă și destinație

Tabela 15. Exemplu de fișă de lucru pentru planificarea informațiilor definițiilor de registre (continuare)

Nume definiție pentru registru	Tip registru de utilizatori	Alias definiție pentru registru	Descriere registru	Tipuri asociere
System_A	Registru de utilizatori sistem i5/OS	app_23_alias_target app_xx_alias_target	Registru de utilizatori principal al sistemului pentru i5/OS pe System A	Destinație
System_D	Registru de utilizatori Kerberos	app_xx_alias_source	regiune Kerberos legal.mydomain.com	Sursă
System_4	Registru de utilizatori pentru Windows 2000	Trecere în revistă documentație aplicație	Registru de utilizatori aplicație de resurse umane pe System 4	Administrativă
order.mydomain.com	Registru de utilizatori pentru Windows 2000		Registru principal pentru logare al angajaților departamentului de comenzi	Politică registru implicită (registru sursă)
System_A_order_app	Aplicație departament de comenzi		Registru specific aplicației pentru actualizări comenzi	Politică registru implicită (registru destinație)
System_C_order_app	Aplicație departament de comenzi		Registru specific aplicației pentru actualizări comenzi	Politică registru implicită (registru destinație)

Tabela 16. Exemplu de fișă de lucru pentru planificarea identificatorilor EIM

Nume identificator unic	Identificator sau descriere identitate utilizator	Alias identificator
John S Day	Manager resurse umane	app_23_admin
John J Day	Departamentul juridic	app_xx_admin
Sharon A. Jones	Administrator alt departament	

Tabela 17. Exemplu de fișă de lucru pentru planificarea asocierii de identificator

Nume unic identificator: _____ John S Day _____		
Registru de utilizatori	Identitate utilizator	Tipuri asociere
WAS System A pe System A	johnday	Sursă
Linux pe System B	jsdl	Sursă și destinație
i5/OS pe System C	JOHND	Destinație
Registru 4 pe sistemul Windows 2000 pentru resurse umane	JDAY	Administrativă

Tabela 18. Exemplu de fișă de lucru pentru planificarea asocierii de politică

Tip asociere de politică	Registru de utilizatori sursă	Registru de utilizatori destinație	Identitate utilizator	Descriere
Registru implicit	order.mydomain.com	System_A_order_app	SYSUSERA	Mapează utilizatorii departamentului de comenzi autentificați Windows la identitatea de utilizator aplicație corespunzătoare

Tabela 18. Exemplu de fișă de lucru pentru planificarea asocierii de politică (continuare)

Tip asociere de politică	Registru de utilizatori sursă	Registru de utilizatori destinație	Identitate utilizator	Descriere
Registru implicit	order.mydomain.com	System_C_order_app	SYSUSERB	Mapează utilizatorii departamentului de comenzi autentificați Windows la identitatea de utilizator aplicație corespunzătoare

### Dezvoltarea unui plan de numire identicatori EIM:

Când planificați cerințele mapeării identitate EIM, puteți crea identicatori EIM unici pentru utilizatori ai aplicațiilor EIM-activate și sistemelor de operare din întreprinderea dumneavoastră când vreți să creați mapeări unu la unu între identități utilizator pentru un utilizator. Folosind asocieri identicator pentru a crea mapeări unu-la-unu puteți maximiza beneficiile gestiunii parolelor pe care le furnizează EIM.

Planul de numire pe care îl dezvoltați depinde de nevoile și preferințele afacerii dumneavoastră; singura cerință pentru numele identicatorilor EIM este să fie unici. Unele companii pot prefera să folosească numele complet, legal al fiecărei persoane; alte companii pot prefera să folosească un tip diferit de date, cum ar fi numărul de angajat al fiecărei persoane. Dacă vreți să creați nume de identicator EIM pe baza numelui complet al unei persoane, trebuie să anticipați posibilele nume duplicate. Cum tratați numele duplicate potențiale ale identicatorilor este o problemă legată de preferința dumneavoastră personală. Poate vreți să tratați fiecare caz manual adăugând un șir de caractere predeterminat la fiecare nume de identicator pentru a asigura unicitatea de exemplu, puteți decide să adăugați numărul departamentului fiecărei persoane.

Ca parte a dezvoltării unui plan de numire identicatori EIM, trebuie să decideți asupra planului general de mapare identitate. Făcând asta vă ajută să decideți când aveți nevoie să folosiți identicatori și asocieri identicator versus folosirea asocierea de politică pentru mapearea identităților în interiorul întreprinderii dumneavoastră. Pentru a dezvolta planul de numire al identicatorilor EIM, puteți folosi fișa de lucru de mai jos pentru a vă ajuta să strângeți informații despre identitățile utilizator din organizația dumneavoastră și să planificați identicatori EIM pentru certificatele utilizator. Fișa de lucru reprezintă tipul de informații pe care trebuie să le cunoască administratorul EIM pentru a ști când creează identicatori EIM sau asocieri de politică pentru utilizatorii unei aplicații.

Tabela 19. Exemplu de fișă de lucru pentru planificarea identicatorilor EIM

Nume identicator unic	Identicator sau descriere identitate utilizator	Alias identicator
John S Day	Manager resurse umane	app_23_admin
John J Day	Departamentul juridic	app_xx_admin
Sharon A. Jones	Administrator alt departament	

O aplicație care e scrisă pentru a folosi EIM poate specifica un alias pe care îl folosește pentru a găsi identicatorul EIM corespunzător pentru aplicație, pe care aplicația îl poate folosi în schimb pentru a determina o identitate utilizator specifică care va fi folosită. Trebuie să verificați documentația pentru aplicațiile dumneavoastră pentru a determina dacă trebuie să specificați unul sau mai multe alias-uri pentru identicator. Câmpurile identicator EIM sau descriere identitate utilizator sunt formular liber și pot fi folosite pentru a furniza informații descriptive despre utilizator.

Nu trebuie să creați identicatori EIM pentru toți membrii întreprinderii dumneavoastră odată. După crearea unui identicator EIM inițial și folosirea lui pentru a vă testa configurația EIM, puteți crea identicatori EIM suplimentare pe baza scopurilor organizației dumneavoastră pentru folosirea EIM. De exemplu, puteți adăuga identicatori EIM pe o bază departamentală sau zonală. Sau, puteți adăuga identicatori EIM pe măsură ce dezvoltați aplicații EIM suplimentare.

După ce adunați informațiile de care aveți nevoie pentru a dezvolta un plan de numire a identificatorilor EIM, puteți plănuți asocieri pentru identitățile utilizatorilor dumneavoastră.

## Fișele de lucru pentru planificarea implementării EIM

Pe măsură ce avansați prin procesul de planificare EIM (Enterprise Identity Mapping), veți găsi folositor să utilizați aceste fișe de lucru pentru a aduna informații pe care va trebui să le configurați și să folosiți EIM în întreprinderea dumneavoastră. Exemplele de secțiuni efectuate ale fișelor de lucru sunt furnizate în paginile de planificare corespunzătoare.

Aceste fișe de lucru sunt furnizate ca un exemplu al tipurilor de care aveți nevoie pentru a vă crea planul de implementare EIM. Numărul de intrări furnizate e mai mic decât numărul de care veți avea nevoie pentru informațiile EIM ale dumneavoastră. Puteți edita aceste fișe de lucru pentru a le face mai folositoare pentru situația dumneavoastră.

*Tabela 20. Fișa de lucru cu informații despre domeniu și controler de domeniu*

Informațiile cerute pentru configurarea domeniului EIM și controlerului domeniului	Răspunsuri
Un nume cu sens pentru domeniu. Acesta poate fi numele unei companii, al unui departament sau al unei aplicații care folosește domeniul.	
Opțional: Un nume distinctiv părinte pentru domeniu. Acesta este numele distinctiv care reprezintă intrarea imediat mai sus de intrarea nume domeniu din ierarhia arbore a informațiilor director, de exemplu, o=ibm,c=us.	
Nume distinctiv domeniu EIM complet calificat rezultat. Acesta este numele complet al domeniului EIM care descrie locația directorului pentru datele domeniului EIM. Numele distinctiv complet calificat al domeniului conține, cel puțin, DN-ul pentru domeniu (ibm-eimDomainName=), plus numele domeniului pe care l-ați specificat. Dacă alegeți să specificați un DN părinte pentru domeniu, atunci DN-ul complet calificat al domeniului conține DN-ul relativ al domeniului (ibm-eimDomainName=), numele domeniului (MyDomain)și DN-ul părinte (o=ibm,c=us).	
Adresa conexiunii pentru controlerul de domeniu. Aceasta conține tipul conexiunii (ldap de bază sau ldap securizat, de exemplu, ldap:// sau ldaps://) plus următoarele informații:	
<ul style="list-style-type: none"> <li>Opțional: Numele adresă sau adresa IP</li> <li>Opțional: Numărul portului</li> </ul>	
Adresa completă rezultată a conexiunii pentru controlerul de domeniu.	
Mecanismul de legare cerute de aplicații sau sisteme. Alegerile includ: <ul style="list-style-type: none"> <li>Legătură simplă</li> <li>CRAM MD5</li> <li>Autentificare server</li> <li>Autentificare client</li> <li>Kerberos</li> </ul>	

Consultați Planificarea pentru un controler de domeniu EIM pentru un exemplu de cum să folosiți această fișă de lucru.

*Tabela 21. Fișa de lucru pentru planificarea identităților de legătură*

Autorizarea sau rolul EIM	Identitatea de legătură	Mecanismul de legătură	Motivul pentru care este cerut

Tabela 21. Fișa de lucru pentru planificarea identităților de legătură (continuare)


Trecere în revistă Planificare un controler de domeniu EIM pentru un exemplu cumse face pentru a utiliza această fișă de lucru.

Tabela 22. Fișa de lucru pentru planificarea informațiilor despre definițiile de registre

Nume definiție pentru registru	Tip registru de utilizatori	Alias definiție registru	Descriere registru	Tipuri asociere

Trecere în revistă Dezvoltare planificare numire definiție EIM pentru un exemplu despre cum a utiliza această fișă de lucru.

Tabela 23. Fișa de lucru pentru planificarea identicatorului EIM

Nume identicator unic	Descriere identicator sau identitate utilizator	Alias identicator

Tabela 23. Fișa de lucru pentru planificarea identificatorului EIM (continuare)


Trecere în revistă Dezvoltare planificare numire definiție EIM pentru un exemplu despre cum a utiliza această fișă de lucru.

Tabela 24. Fișa de lucru pentru planificarea asocierii de identificatori

Nume unic identificator: _____John S Day_____		
Registru de utilizatori	Identitate utilizator	Tipuri asociere

Trecere în revistă Planificare asocieri EIM pentru un exemplu despre cum a utiliza această fișă de lucru.

Tabela 25. Fișa de lucru pentru planificarea asocierii de politică

Tip asociere de politică	Registru de utilizatori sursă	Registru de utilizatori destinație	Identitate utilizator	Descriere

Trecere în revistă Planificare asocieri EIM pentru un exemplu despre cum a utiliza această fișă de lucru.

## Planificarea pentru dezvoltarea aplicațiilor de mapare EIM (Enterprise Identity Mapping)

Pentru ca o aplicație să folosească EIM (Enterprise Identity Mapping) și să participe într-un domeniu, ea trebuie să fie capabilă să folosească API-urile EIM.

Trebuie să consultați documentația API EIM și documentația de platformă EIM specifică pentru a determina dacă sunt considerente speciale de planificare pe care ar trebui să le înțelegeți când scrieți sau adaptați aplicații pentru a utiliza API-urile EIM. De exemplu, ar putea fi considerente de compilare sau altele pentru aplicații în C sau C++ care cheamă API-urile EIM. În funcție de platforma aplicației, s-ar putea să fie considerente de editare-legătură sau altele de asemenea.

### Operații înrudite

“API-urile EIM” la pagina 122

EIM furnizează mecanismul pentru gestionarea identității utilizatorului pe mai multe platforme. EIM are mai multe API-uri care pot fi folosite de către aplicații pentru a realiza operații EIM în numele aplicației sau în numele unui utilizator de aplicație.



## Planificarea EIM (Enterprise Identity Mapping) pentru i5/OS

Sunt multiple tehnologii și servicii pe care EIM (Enterprise Identity Mapping) le conține pe platforma System i. Prioritar la configurarea EIM-ului pe serverul dumneavoastră, ar trebui să decideți ce funcționalitate să implementați utilizând EIM capabilități semnare unică.

Înainte de a implementa EIM, trebuie să fi decis cerințele de securitate de bază pentru rețeaua dumneavoastră și să fi implementat aceste măsuri de securitate. EIM furnizează administratorilor și utilizatorilor o modalitate mai ușoară de gestiune a identităților în cadrul întreprinderii. Când utilizat cu serviciul de autentificare în rețea, EIM furnizează capabilități de semnare unică pentru întreprinderea dumneavoastră.

Dacă plănuieți să folosiți Kerberos pentru a autentifica utilizatori ca parte a unei implementări de semnare unică, ar trebui de asemenea să configurați serviciul de autentificare în rețea.

Pentru a învăța mai multe despre cum să planificați configurația EIM a sistemului dumneavoastră, treceți în revistă următoarele informații:


### Informații înrudite

Planificare serviciu de autentificare în rețea

## Cerințe preliminare instalare EIM pentru i5/OS

Foaia de lucru de planificare identifică serviciile pe care ar trebui să le instalați prioritar configurației EIM.

Tabela 26. Fișa de lucru pentru planificarea instalării EIM

Fișă de lucru pentru planificarea cerințelor preliminare EIM	Răspunsuri
Sistemul dumneavoastră rulează i5/OS V5R4 sau mai ulterior?	
Sunt următoarele opțiuni și produse instalate pe sistemul dumneavoastră? <ul style="list-style-type: none"><li>• i5/OS Servere gazdă (5761-SS1 Opțiunea 12)</li><li>• System i Access pentru Windows (5761-XE1)</li><li>• Interpretorul Qshell (5761-SS1 Opțiunea 30) Necesară dacă intenționați să configurați serviciul de autentificare în rețea ca și EIM.</li></ul> <b>Notă:</b> 5722 este codul produs pentru opțiuni și produse i5/OS, prioritar la V6R1.	
Este Navigator System i instalat pe PC-ul administratorului, inclusiv următoarele subcomponente? <ul style="list-style-type: none"><li>• Rețea</li><li>• Securitatea (necesară dacă intenționați pentru a configura serviciul de autentificare în rețea ca și EIM)</li></ul>	
Ați instalat ultimul pachet de service System i Access pentru Windows? Pentru ultimul pachet de service vedeți System i Access 	
Dacă un server de director, de exemplu, IBM Tivoli Directory Server for i5/OS este configurat curent și vreți să îl utilizați ca și controler de domeniu EIM, știți numele distinctiv al administratorului LDAP (DN) și parola?	
Dacă este instalat un server de director, poate fi oprit temporar? (Aceasta lucru va fi necesar pentru a efectua procesul de configurare EIM.)	
Aveți autorizările speciale *SECADM, *ALLOBJ și *IOSYSCFG?	
Ați aplicat cele mai recente corecții temporare de program (PTF-uri)?	

## Instalarea opțiunilor Navigator System i necesare

Pentru a activa un mediu de semnare unică cu EIM (Enterprise Identity Mapping) și serviciu autentificare în rețea, trebuie să instalați atât opțiunea **Rețea** și opțiunea **Securitate** a Navigator System i.

EIM se află în cadrul opțiunii **Rețea** și serviciul de autentificare în rețea se află în opțiunea **Securitate**. Dacă nu plănuieți să utilizați serviciul de autentificare în rețea în rețeaua dumneavoastră, nu trebuie să instalați opțiunea **Securitate** a Navigator System i.

Pentru a instala opțiunea Rețea a Navigator System i sau pentru a verifica dacă aveți această opțiune instalată, asigurați-vă că System i Access pentru Windows este instalată pe PC-ul pe care îl utilizați pentru a administra modelul System i.

Pentru a instala opțiunea **Rețea**:

1. Faceți clic pe **Pornire > Programe > System i Access pentru Windows > Setare selectivă**.
2. Urmați instrucțiunile din dialog. Pe dialogul **Selectare componentă**, expandați **Navigator System i** și apoi selectați opțiunea **Rețea**. Dacă planificați să utilizați serviciul de autentificare în rețea, trebuie să selectați, de asemenea, opțiunea **Securitate**.
3. Continuați apoi cu **Setarea selectivă**.

#### **Informații înrudite**

Network authentication service

### **Considerațiile de salvare și recuperare pentru EIM**

Trebuie să dezvoltați un plan de salvare de rezervă și recuperare a datelor EIM (Enterprise Identity Mapping) pentru a vă asigura că sunt protejate și pot fi recuperate dacă va fi vreodată o problemă cu serverul director care găzduiește controlerul de domeniu EIM. Sunt de asemenea informații de configurație EIM importante pe care trebuie să înțelegeți cum să le recuperați.

#### **Informații înrudite**

Replicare server de director

Taskuri replicare

Considerente salvare și restaurare server de director

### **Salvarea de rezervă și recuperarea datelor domeniului EIM:**

Cum salvați datele dumneavoastră EIM depinde de felul în care decideți să gestionați acest aspect al serverului director care acționează ca și controlerul de domeniu pentru datele dumneavoastră EIM.

O cale de a face o copie de rezervă a datelor, în special pentru scopuri de recuperare a dezastrelor este să salvați biblioteca bazei de date. Implicit, aceasta e QUSRDIRDB. Dacă changelog e activat, ar trebui să salvați de asemenea biblioteca QUSRDIRCL. Serverul director de pe sistemul pe care vreți să restaurați biblioteca trebuie să aibă aceeași schemă și configurație LDAP ca serverul director original. Fișierele care memorează aceste informații sunt în /QIBM/UserData/OS400/DirSrv. Datele de configurare suplimentare sunt memorate în QUSRSYS/QGLDCLCFG (obiectul \*USRSPC) și QUSRSYS/QGLDVLDL (obiectul \*VLDL). Pentru a avea o copie de rezervă completă pentru serverul dumneavoastră director, trebuie să salvați ambele biblioteci, fișierele sistemului de fișiere integrate și obiectele QUSRSYS.

De exemplu, puteți folosi un fișier LDIF pentru a salva tot sau o parte din conținutul serverului director. Pentru a salva de rezervă informațiile domeniului pentru un controler de domeniu IBM Tivoli Directory Server for i5/OS urmați acești pași:

1. În Navigator System i, expandați **Rețea > Servere > TCP/IP**.
2. Faceți clic dreapta pe **Server de director**, selectați **Unelte**, apoi selectați **Export fișier** pentru a afișa o pagină care vă permite să specificați care părți din conținutul serverului de director să fie exportate la un fișier.
3. Transferați fișierul de export la System i platforma pe care vreți să o utilizați ca serverul de director copie de rezervă.
4. În Navigator System i pe serverul de salvare de rezervă, expandați **Rețea > Servere > TCP/IP**.
5. Faceți clic dreapta pe **Server de director**, selectați **Unelte**, apoi selectați **Import** pentru a încărca conținuturile a fișierului transferat pentru noul server de director.

O altă metodă pe care o puteți considera pentru salvarea datelor domeniului EIM, este să configurați și să folosiți un server director replică. Toate modificările asupra datelor din domeniul EIM sunt automat expediate serverului director replică astfel încât dacă serverul director care găzduiește controlerul de domeniu eșuează sau pierde date EIM, le puteți extrage din serverul replică.

Cum configurați și folosiți un server director replică variază în funcție de tipul modelului de replicare pe care ați ales să-l folosiți.

### **Salvarea de rezervă și recuperarea informațiilor de configurare EIM:**

În caz că sistemul dumneavoastră va cădea, s-ar putea să fie nevoie să restaurați informațiile de configurare EIM pentru acel sistem. Aceste informații nu pot fi salvate și restaurate ușor peste sisteme.

Aceste opțiuni vă sunt disponibile pentru a salva și restaura configurația EIM:

- Folosiți comanda SAVSECDTA (Save Security Data - Salvare date securitate) pe fiecare sistem pentru a salva informații EIM și alte informații importante de configurare. Apoi restaurați obiectul profil utilizator QSYS pe fiecare sistem.

**Notă:** Trebuie să folosiți comanda SAVSECDTA și să restaurați obiectul profil utilizator QSYS pe fiecare sistem cu o configurație EIM individual. Puteți întâlni probleme dacă încercați să recuperați obiectul profil utilizator QSYS pe un sistem când el a fost salvat pe un sistem diferit.

- Fie rulați din nou vrăjitorul de configurare EIM, fie actualizați manual proprietățile folderului Configurare EIM. Pentru a face acest proces mai ușor, ar trebui să salvați fișele de lucru pentru planificarea implementării EIM sau să faceți o înregistrare a informațiilor de configurare pentru fiecare sistem.

Suplimentar, trebuie să luați în considerare și să planificați cum să salvați de rezervă și recuperați datele serviciului de autentificare în rețea al dumneavoastră dacă ați configurat serviciul de autentificare în rețea ca parte componentă a implementării unui mediu de semnare unică.

---

## **Configurarea EIM (Enterprise Identity Mapping)**

Vrăjitorul de configurare EIM vă permite să finalizați o configurare de bază EIM pentru sistemul dumneavoastră ușor și rapid. Vrăjitorul vă furnizează trei opțiuni de configurare sistem EIM.

Cum folosiți vrăjitorul pentru a configura EIM pe un sistem specific depinde de planul general de folosire a EIM în întreprinderea dumneavoastră și cerințele de configurare EIM. De exemplu, mulți administratori doresc să utilizeze EIM în conjunctură cu serviciul autentificare în rețea pentru a crea un mediu de semnare unică peste platforme și sisteme multiple fără a fi nevoie să modifice politicile de securitate. În consecință, vrăjitorul de configurare EIM vă permite să configurați serviciul de autentificare în rețea ca parte a configurației dumneavoastră EIM. Totuși, configurarea și utilizarea serviciului de autentificare în rețea nu este o cerință preliminară sau o necesitate pentru configurarea și folosirea EIM.

Înainte de a începe să configurați EIM pentru unul sau mai multe sisteme, planificați implementarea EIM pentru a aduna informațiile de care aveți nevoie. De exemplu, trebuie să decideți în legătură cu următoarele :

- Care platformă System i vreți să o configurați ca și controler de domeniu EIM pentru do meniul EIM? Utilizați vrăjitorul de configurare EIM pentru a crea pentru prima oară un nou domeniu pe acest sistem, apoi utilizați vrăjitorul pentru a configura toate sisteme suplimentare să se alăture acestui domeniu.
- Vreți să configurați un serviciu de autentificare în rețea pentru orice sistem pe care îl configurați pentru EIM? Dacă astfel, puteți utiliza vrăjitorul de configurare EIM pentru a crea o configurație serviciu de autentificare în rețea pe fiecare model System i. Cu toate acestea, trebuie să realizați alte operații pentru a termina configurarea de servicii de autentificare în rețea.

După ce utilizați vrăjitorul de configurare EIM pentru a crea o configurație de bază pentru fiecare platformă System i, există încă un număr de taskuri de configurare EIM pe care trebuie să le realizați înainte de a finaliza configurarea EIM.

Examinați Scenariu: Activare semnare unică pentru un exemplu care arată cum o companie fictivă a configurat un mediu de semnare unică folosind serviciul de autentificare în rețea și EIM.

Pentru a configura EIM, trebuie să aveți toate autorizările speciale următoare:

- Administrator de securitate (\*SECADM).
- Toate obiectele(\*ALLOBJ).
- Configurare sistem (\*IOSYSCFG).

Înainte de a utiliza vrăjitorul pentru configurare EIM, ar trebui să parcurgeți toți pașii din “Planificarea pentru EIM (Enterprise Identity Mapping)” la pagina 51 pentru a determina exact cum veți utiliza EIM. Dacă configurați EIM ca parte a creării unui mediu de semnare unică, atunci ar trebui să finalizați toți pașii planificărilor de semnare unică de asemenea.

Pentru a accesa vrăjitorul de configurare EIM, urmați acești pași :

1. Porniți Navigator System i.
2. Semnați-vă pe sistemul pe care vreți să îl configurați pentru EIM. Dacă configurați EIM pentru mai mult de un sistem, începeți cu cel pe care vreți să îl configurați controler de domeniu pentru EIM.
3. Expandați **Rețea** → **Mapare identitate în întreprindere**.
4. Faceți clic dreapta pe **Configurare** și selectați **Configurare** pentru a lansa în execuție vrăjitorul de configurare EIM.
5. Selectați o opțiune de configurare EIM și urmați instrucțiunile pe care le furnizează vrăjitorul pentru a completa vrăjitorul.
6. Faceți clic pe **Ajutor**, dacă este necesar, pentru a determina ce informație să specificați pe măsură ce continuați să folosiți vrăjitorul.

Odată planificarea încheiată, puteți utiliza vrăjitorul pentru configurații EIM pentru a crea una dintre cele trei configurații de bază. Puteți utiliza vrăjitorul pentru a uni un domeniu existent sau pentru a crea și uni un nou domeniu. Atunci când utilizați vrăjitorul pentru configurare EIM pentru a crea și a vă alătura la un nou domeniu, puteți alege să configurați un controler de domeniu EIM fie pe un sistem local, fie un sistem la distanță. Informațiile următoare furnizează instrucțiuni pentru configurarea EIM bazată pe felul de configurare EIM de bază de care aveți nevoie:

#### **Informații înrudite**

Network authentication service

Semnare unică

## **Crearea și alăturarea la un domeniu local nou**

Atunci când utilizați vrăjitorul pentru configurare EIM pentru a crea și a vă alătura unui nou domeniu, puteți alege să configurați un controler de domeniu EIM pe un sistemul local ca parte a creării configurației EIM.

Dacă este necesar, vrăjitorul de configurare EIM asigură să furnizați informațiile de configurație de bază pentru serverul de director. De asemenea, dacă Kerberos nu este configurat actual pe platforma System i, vrăjitorul vă invită să lansați în execuție vrăjitorul Configurare serviciu de autentificare în rețea.

Când terminați vrăjitorul de configurare EIM, puteți realiza următoarele task-uri:

- Crearea unui nou domeniu EIM.
- Configurarea serverului de director local să funcționeze ca un controler de domeniu EIM.
- Configurarea serviciului de autentificare în rețea pentru sistem.
- Crearea definițiilor registru pentru registrul local i5/OS și pentru registrul Kerberos.
- Configurarea sistemului ca să participe într-un domeniu nou EIM.

Pentru a configura sistemul să creeze și să se alătore unui domeniu EIM nou, trebuie să aveți toate autorizările speciale următoare:

- Administrator de securitate(\*SECADM).
- Toate obiectele (\*ALLOBJ).
- Configurare sistem (\*IOSYSCFG).

Pentru a folosi vrăjitorul de configurare EIM pentru a crea și a vă alătura la un nou domeniu, realizați următorii pași:

1. În Navigator System i, selectați sistemul pentru care vreți să configurați EIM și expandați **Rețea > EIM (Enterprise Identity Mapping)**.
2. Faceți clic dreapta pe **Configurație** și selectați **Configurare** pentru a porni vrăjitorul de configurare EIM.

**Notă:** Această opțiune este etichetată **Reconfigurare** dacă EIM a fost configurat anterior pe sistem.

3. Pe pagina de **Bun venit** a vrăjitorului, selectați **Creare și alăturare la un domeniu nou** și apoi apăsați **Următorul**.
4. Pe pagina **Specificare locație domeniu EIM**, selectați **Pe serverul de director local** și faceți clic **Următorul**.

**Notă:** Această opțiune configurează serverul de director local ca să funcționeze ca un controler de domeniu EIM. Deoarece serverul de director memorează toate datele EIM pentru domeniu, trebuie să fie activ și să rămână activ pentru a suporta căutările de mapări EIM și celelalte operații.

Dacă serviciul de autentificare în rețea nu este configurat actual pe platforma System i sau informații configurație autentificare în rețea sunt necesare pentru a configura un mediu semnare unică, este afișată pagina **Configurare serviciu autentificare în rețea**. Această pagină vă permite să porniți vrăjitorul Configurare serviciu de autentificare în rețea astfel încât să puteți configura serviciul de autentificare în rețea. Sau, puteți configura Serviciul de autentificare în rețea mai târziu utilizând vrăjitorul de configurare pentru acest serviciu prin Navigator System i. După ce efectuați configurarea serviciului de autentificare în rețea, continuă vrăjitorul de configurare EIM.

5. Pentru a configura serviciul de autentificare în rețea, terminați acești pași:
  - a. Pe pagina **Configurare NAS (Network Authentication Service)**, selectați **Da** pentru a porni vrăjitorul de configurare NAS. Cu acest vrăjitor, puteți configura mai multe interfețe și servicii i5/OS pentru a participa într-o regiune Kerberos și pentru a configura un mediu semnare unică care utilizează ambele EIM și serviciul de autentificare în rețea.
  - b. Pe pagina **Specificare informații regiune**, specificați numele regiunii implicite în câmpul **Regiune implicită**. Dacă utilizați Microsoft Active Directory pentru autentificarea Kerberos, selectați **Microsoft Active Directory este utilizat pentru autentificarea Kerberos** și faceți clic pe **Următorul**.
  - c. Pe pagina **Specificare informații KDC**, specificați numele complet calificat al serverului Kerberos pentru această regiune în câmpul **KDC**, specificați **88** în câmpul **Port** și faceți clic pe **Următorul**.
  - d. Pe pagina **Specificare informații pentru server de parole**, selectați fie **Da**, fie **Nu** pentru setarea unui server de parole. Serverul de parole permite principalilor să modifice parolele pe serverul Kerberos. Dacă selectați **Da**, introduceți numele serverului de parole în câmpul **Server de parole**. În câmpul **Port**, acceptați valoarea implicită de 464 și faceți clic pe **Următorul**.
  - e. Pe pagina **Selectare intrări tabelă de chei**, selectați **Autentificare Kerberos i5/OS** și faceți clic pe **Următorul**.

**Notă:** În plus puteți de asemenea crea intrări tabelă de chei pentru IBM Tivoli Directory Server for i5/OS, i5/OS NetServer și IBM HTTP Server for i5/OS dacă vreți ca aceste servicii să utilizeze autentificare Kerberos. Este posibil să aveți nevoie de configurări suplimentare pentru aceste servicii, înainte ca ele să poată folosi autentificarea Kerberos.

- f. Pe pagina **Creare intrare tabelă de chei i5/OS**, introduceți și confirmați o parolă și faceți clic pe **Următorul**. Aceasta este aceeași parolă pe care o veți utiliza când adăugați principalii i5/OS la serverul Kerberos.
- g. Opțional: Pe pagina **Creare fișier batch**, selectați **Da**, specificați informațiile următoare și faceți clic pe **Următorul**:
  - În câmpul **Fișier batch**, actualizați calea de directoare. Faceți clic pe **Răsfoire** pentru a găsi calea de directoare corespunzătoare sau editați calea în câmpul **Fișier batch**.

- În câmpul **Includere parolă**, selectați **Da**. Aceasta asigură că toate parolele asociate cu principalul serviciului i5/OS sunt incluse în fișierul batch. Este important de reținut că parolele sunt în text clar și pot fi citite de oricine are acces de citire la fișierul batch. De aceea este esențial să ștergeți fișierul batch de pe serverul Kerberos și de pe PC imediat ce l-ați folosit. Dacă nu includeți parola, va apare un prompt pentru parolă, când rulați fișierul batch.

**Notă:** Puteți de asemenea adăuga manual principalii serviciului care sunt generați de vrăjitor la Microsoft Active Directory. Pentru a afla cum să faceți asta, vedeți Adăugare principalii i5/OS la serverul Kerberos

- Pe pagina **Sumar**, treceți în revistă detaliile de configurare serviciu de autentificare în rețea și faceți clic pe **Sfârșit** pentru a vă întoarce la vrăjitorul de configurare EIM.
6. Dacă serverul de director local nu este configurat, pagina **Configurare server de director** afișează rezumatele vrăjitorului de configurare EIM. Furnizați următoarele informații pentru a configura serverul de director local:

**Notă:** Dacă configurați serverul de director local înainte de a folosi vrăjitorul de configurare EIM, atunci se afișează pagina **Specificare utilizator pentru conexiune**. Folosiți această pagină pentru a specifica numele distinctiv și parola pentru administratorul LDAP pentru a vă asigura că vrăjitorul are destulă autorizare pentru a administra domeniul EIM și obiectele din el și continuați cu următorul pas din procedură. Faceți clic pe **Ajutor**, dacă este necesar, pentru a determina ce informații să fie furnizate pentru această pagină.

- În câmpul **Port**, acceptați numărul de port implicit **389** sau specificați un alt număr de port de folosit pentru comunicațiile EIM nesecurizate cu serverul de director.
  - În câmpul **Nume distinctiv**, specificați numele distinctiv (DN) LDAP care identifică administratorul LDAP pentru serverul de director. Vrăjitorul de configurare EIM creează acest DN administrator LDAP și îl folosește pentru a configura serverul de director ca și controler de domeniu pentru noul domeniu pe care-l creați.
  - În câmpul **Parolă**, introduceți parola pentru administratorul LDAP.
  - În câmpul **Confirmare parolă**, specificați parola a doua oară în scopul validării ei.
  - Faceți clic pe **Următorul**.
7. Pe pagina **Specificare domeniu** furnizați următoarele informații:
- În câmpul **Domeniu**, specificați numele domeniului EIM pe care doriți să-l creați. Acceptați numele implicit al EIM sau folosiți orice șir de caractere care vă convin. Totuși, nu puteți utiliza caractere speciale ca = + < > , # ; \ și \*.
  - În câmpul **Descriere**, introduceți un text de descriere a domeniului.
  - Faceți clic pe **Următorul**.
8. Pe pagina **Specificare DN părinte pentru domeniu**, selectați **Da** pentru a specifica un DN părinte pentru domeniul pe care-l creați sau specificați **Nu** pentru a avea datele EIM memorate într-o locație director cu un sufix al cărui nume este derivat din numele domeniului EIM.

**Notă:** Când creați un domeniu pe un server de director local, un DN părinte este opțional. Prin specificarea unui părinte DN, puteți specifica unde să se afle datele EIM spațiu de nume al serverului LDAP pentru domeniu. Când nu specificați un DN părinte, datele EIM se află în sufixul propriu în spațiul de nume. Dacă selectați **Da**, folosiți caseta listă pentru a selecta sufixul LDAP de folosire ca DN părinte sau introduceți text pentru a crea și numi un nou DN părinte. Nu este necesar să specificați un DN părinte pentru noul domeniu. Faceți clic pe **Ajutor** pentru mai multe informații despre folosirea unui DN părinte.

9. Pe pagina **Informații registru**, specificați dacă să se adauge registrele de utilizatori locali la domeniul EIM ca și definiții de registre. Selectați unul sau amândouă din aceste tipuri de registre de utilizatori:

**Notă:** Nu trebuie să creați la acest moment definițiile de registru. Dacă alegeți să creați definițiile de registru mai târziu, trebuie să adăugați definițiile de registru sistem și să actualizați proprietățile configurației EIM.

- a. Selectați **i5/OS local** pentru a adăuga o definiție registru pentru registrul local. În câmpul oferit, acceptați valoarea implicită pentru numele definiției de registru sau specificați o valoare diferită pentru numele definiției de registru. Numele registrului EIM este un șir arbitrar care reprezintă tipul registrului și instanța specifică a celui registru.
  - b. Selectați **Kerberos** pentru a adăuga o definiție de registru pentru registrul Kerberos. În câmpul oferit, acceptați valoarea implicită pentru numele definiției de registru sau specificați o valoare diferită pentru numele definiției de registru. Numele definiției de registru implicit este același cu numele regiunii. Acceptând numele implicit și folosind același nume de registru Kerberos ca și numele regiunii, puteți crește performanțele la extragerea informațiilor din registru. Selectați, dacă este necesar, **Identitățile utilizatorului Kerberos sunt sensibile la majuscule**.
  - c. Faceți clic pe **Următorul**.
10. Pe pagina **Specificare utilizator sistem EIM**, selectați un **Tip de utilizator** pe care vreți să-l folosească sistemul la realizarea operațiilor EIM pentru funcțiile sistemului de operare. Aceste operații includ operațiile de căutare mapare și de ștergere a asocierii la ștergerea unui profil utilizator i5/OS. Puteți selecta unul din următoarele tipuri de utilizatori: **Nume distinctiv și parolă**, **Fișier tabelă de chei Kerberos și principal** sau **Principal Kerberos și parolă**. Ce tipuri de utilizator puteți selecta depinde de configurația curentă a sistemului. De exemplu, dacă serviciul de autentificare în rețea nu este configurat pentru sistem, atunci tipul de utilizatori Kerberos nu sunt disponibili pentru selecție. Tipul de utilizator pe care îl selectați determină celelalte informații pe care trebuie să le furnizați pentru a completa pagina după cum urmează:

**Notă:** Trebuie să specificați un utilizator care este definit curent pe serverul de director care găzduiește controlerul de domeniu EIM. Utilizatorul pe care îl specificați trebuie să aibă privilegiile de efectuare a căutărilor de mapare și administrare de registre pentru registrul de utilizatori local. Dacă utilizatorul pe care îl specificați nu are aceste privilegii, atunci anumite funcții ale sistemului de operare înrudite cu utilizarea semnării unice și ștergerea profilurilor utilizator ar putea eșua.

Dacă nu ați configurat serverul de director înainte de a rula acest vrăjitor, singurul tip de utilizator pe care-l puteți selecta este **Nume distinctiv și parolă** și singurul nume distinctiv pe care-l puteți specifica este DN-ul administratorului LDAP.

- Dacă selectați **Nume distinctiv și parolă**, furnizați informațiile următoare:
  - În câmpul **Nume distinctiv**, specificați numele distinctiv LDAP care identifică utilizatorul pe care să-l folosească sistemul atunci când realizează operații EIM.
  - În câmpul **Parolă**, introduceți parola pentru numele distinctiv.
  - În câmpul **Confirmare parolă**, specificați parola a doua oară în scopul verificării ei.
- Dacă selectați **Principal Kerberos și parolă**, furnizați informațiile următoare:
  - În câmpul **Principal**, specificați numele principalului Kerberos de folosit de sistem la realizarea operațiilor EIM.
  - În câmpul **Regiune**, specificați numele de regiune Kerberos complet calificat la care este membru principalul. Numele principalului și al regiunii ce identifică în mod unic utilizatorii Kerberos din fișierul tabelă de chei. De exemplu, principalul jsmith din regiunea ordept.myco.com este reprezentat în fișierul tabelă de chei ca jsmith@ordept.myco.com.
  - În câmpul **Parolă**, introduceți parola pentru utilizator.
  - În câmpul **Confirmare parolă**, specificați parola a doua oară în scopul verificării ei.
- Dacă selectați **Fișier tabelă de chei Kerberos și principal**, furnizați informațiile următoare:
  - În câmpul **Fișier tabelă de chei**, specificați calea complet calificată și numele de fișier tabelă de chei care conține principalul Kerberos, de folosit de sistem pentru realizarea operațiilor EIM. Sau, faceți clic pe **Răsfoire** pentru a răsfoi prin directoare în sistemul de fișiere integrat System i pentru a selecta un fișier tabelă de chei.
  - În câmpul **Principal**, specificați numele principalului Kerberos de folosit de sistem la realizarea operațiilor EIM.

- În câmpul **Regiune**, specificați numele de regiune Kerberos complet calificat la care este membru principalul. Numele principalului și al regiunii ce identifică în mod unic utilizatorii Kerberos din fișierul tabelă de chei. De exemplu, principalul jsmith din regiunea ordept.myco.com este reprezentat în fișierul tabelă de chei ca jsmith@ordept.myco.com.
  - Faceți clic pe **Verificare conexiune** pentru a vă asigura că vrăjitorul poate folosi informațiile de utilizator specificate pentru a stabili o conexiune la controlerul de domeniu EIM.
  - Faceți clic pe **Următorul**.
11. În panoul **Rezumat**, revizualizați informațiile de configurare pe care le-ați furnizat. Dacă toate informațiile sunt corecte, apăsați **Sfârșit**.

## Finalizarea configurației EIM pentru domeniu

Când vrăjitorul se termină, adaugă domeniul nou la folderul **Gestionare domeniu** și ați creat o configurație EIM de bază pentru acest server. Totuși, s-ar putea să fie nevoie să terminați aceste task-uri pentru a finaliza configurarea EIM pentru domeniu.

1. Folosiți vrăjitorul de configurare EIM pe fiecare server suplimentar care vreți să se alăture la domeniu.
2. Adăugare definiții registru EIM la domeniul EIM, dacă necesar, pentru alte platforme și aplicații non-System i care vreți să participe la domeniul EIM. Aceste definiții de registre se referă la registrele de utilizatori reali care trebuie să participe în domeniu. Puteți, fie adăuga definiții de registru sistem fie adăuga definiții de registru aplicație în funcție de ce are nevoie implementarea dumneavoastră EIM.
3. Bazat pe implementarea dumneavoastră EIM, determinați dacă să:
  - Creați identificatori EIM pentru fiecare utilizator sau entitate unică în domeniu și să creați asocieri de identificatori pentru ei.
  - Creați asocieri de politică pentru a mapa un grup de utilizatori la o singură identitate de utilizator destinație.
  - Creați o combinație a acestora.
4. Folosiți funcția EIM de testare a unei mapări pentru a testa mapările de identificatori pentru configurația EIM.
5. Dacă singurul utilizator EIM pe care l-ați definit este DN pentru administratorul LDAP, atunci utilizatorul EIM are un nivel de autorizări înalt la toate datele din serverul de director. Prin urmare, ați putea considera crearea unui sau mai multor DN-uri ca utilizatori adiționali care au control acces pentru date EIM mai corespunzătoare și mai limitate. Pentru a învăța mai multe despre crearea DN-urilor pentru serverul de director, consultați Nume distinctive în Centrul de informare i5/OS. Numărul de utilizatori EIM suplimentari depinde de accentul pus în politicile de securitate pe îndatoririle și responsabilitățile privitoare la securitate. Tipic, puteți crea cel puțin următoarele două tipuri de nume distinctive (DN):

- **Un utilizator care are control de acces de administrator EIM**

Acest DN de administrator EIM oferă nivelul corespunzător de autorizare pentru un administrator care este responsabil pentru gestionarea domeniului EIM. Acest DN administrator EIM ar putea fi utilizat la conectarea la controlerul de domeniu când gestionați toate aspectele domeniului EIM prin mijloace ale Navigator System i.

- **Sau cel puțin cu un utilizator care are următoarele controale de acces:**

- Administrator de identificatori
- Administrator de registru
- Operații de mapare EIM

Acest utilizator furnizează nivelul corespunzător de control acces necesar pentru utilizatorul sistem care realizează operațiile EIM din partea sistemului de operare.

**Notă:** Pentru a utiliza noul DN pentru utilizatorul sistemului în loc de DN-ul administratorului LDAP, trebuie să modificați proprietățile configurației EIM pentru platforma System i. Consultați Gestiune proprietăți configurație EIM pentru a învăța cum să modificați DN-ul de utilizator sistem.

În plus, poate doriți să folosiți protocolul SSL (Secure Sockets Layer) sau TLS (Transport Layer Security) pentru a configura o conexiune securizată la controlerul de domeniu EIM pentru a proteja transmisia datelor EIM. Dacă activați SSL pentru serverul de director, trebuie să actualizați proprietățile configurației EIM pentru a specifica că platforma



System i folosește o conexiune sigură SSL. De asemenea, trebuie să actualizați proprietățile pentru domeniu pentru a specifica că EIM utilizează conexiuni SSL pentru gestionarea domeniului prin Navigator System i.

**Notă:** S-ar putea să fie nevoie să realizați taskuri suplimentare dacă ați creat o configurație serviciu de autentificare în rețea, în special dacă implementați un mediu de semnare unică. Puteți găsi informații despre acești pași suplimentari trecând în revistă pașii de configurare finalizați demonstrați de scenariul, Activare semnare unică pentru i5/OS.

## Crearea și alăturarea la un nou domeniu la distanță

Când folosiți vrăjitorul Configurare EIM pentru a crea și a vă alătura unui domeniu nou, puteți opta pentru configurarea unui server de director pe un sistem la distanță care să acționeze ca un controler de domeniu EIM ca parte a creării configurației dumneavoastră EIM.

Trebuie să specificați informațiile corespunzătoare pentru conectarea la serverul de director la distanță, pentru a vă permite să configurați EIM. Dacă Kerberos nu este configurat actual la platforma System i, vrăjitorul vă promptează să porniți vrăjitorul de configurare serviciu de autentificare în rețea.

**Notă:** Serverul de director de pe sistemul la distanță trebuie să asigure suportul EIM. EIM necesită găzduirea controlerului de domeniu pe un server de director care suportă LDAP (Lightweight Directory Access Protocol) Versiunea 3. În plus, produsul server de director trebuie să aibă configurată schema EIM. De exemplu, IBM Directory Server V5.1 furnizează acest suport. Pentru informații suplimentare despre cerințele controlerului de domeniu EIM, vedeți “Planificarea unui controler de domeniu EIM” la pagina 56.

După ce finalizați vrăjitorul Configurare EIM, puteți realiza următoarele operații:

- Crearea unui domeniu EIM nou.
- Configurarea unui server de director la distanță care să acționeze ca un controler de domeniu EIM.
- Configurarea serviciului de autentificare în rețea pentru sistem.
- Crearea definițiilor registrului pentru registrul local i5/OS și pentru registrul Kerberos.
- Configurarea sistemului pentru a participa la noul domeniu EIM.

Pentru a vă configura sistemul pentru crearea și alăturarea la un nou domeniu EIM, trebuie să aveți toate autorizările speciale următoare:

- Administrator securitate (\*SECADM).
- Toate obiectele (\*ALLOBJ).
- Configurare sistem (\*IOSYSCFG).

Pentru a folosi vrăjitorul Configurare EIM la crearea și alăturarea la un domeniu pe un sistem la distanță, parcurgeți pașii următori:

1. Verificați dacă serverul de director de pe sistemul la distanță este activ.
2. În Navigator System i, selectați sistemul pentru care vreți să configurați EIM și expandați **Rețea > EIM (Enterprise Identity Mapping)**.
3. Faceți clic dreapta pe **Configurație** și selectați **Configurare** pentru a porni vrăjitorul de configurare EIM.

**Notă:** Această opțiune este etichetată **Reconfigurare** dacă EIM a fost configurat anterior pe sistem.

4. Pe pagina de **Bun venit** a vrăjitorului, selectați **Creare și alăturare la un domeniu nou** și apoi apăsați **Următorul**.
5. Pe pagina **Specificare locație domeniu EIM**, selectați **Pe serverul de director local** și faceți clic pe **Următorul**.

**Notă:** Această opțiune configurează serverul de director local ca să funcționeze ca un controler de domeniu EIM. Deoarece serverul de director memorează toate datele EIM pentru domeniu, trebuie să fie activ și să rămână activ pentru a suporta căutările de mapări EIM și celelalte operații.

Dacă serviciul de autentificare în rețea nu este configurat actual pe platforma System i sau informații configurație autentificare în rețea sunt necesare pentru a configura un mediu semnare unică, este afișată pagina **Configurare serviciu autentificare în rețea**. Această pagină vă permite să porniți vrăjitorul Configurare serviciu de autentificare în rețea astfel încât să puteți configura serviciul de autentificare în rețea. Sau, puteți configura Serviciul de autentificare în rețea mai târziu utilizând vrăjitorul de configurare pentru acest serviciu prin Navigator System i. După ce efectuați configurarea serviciului de autentificare în rețea, vrăjitorul de configurare EIM continuă.

6. Pentru a configura serviciul de autentificare în rețea, parcurgeți pașii următori:
  - a. În pagina **Configurare NAS**, selectați **Da** pentru a lansa vrăjitorul Configurare NAS. Cu acest vrăjitor, puteți configura mai multe interfețe și servicii i5/OS pentru a participa într-o regiune Kerberos și pentru a configura un mediu semnare unică care utilizează ambele EIM și serviciul de autentificare în rețea.
  - b. În pagina **Specificare informații regiune**, specificați numele regiunii implicite în câmpul **regiune implicită**. Dacă utilizați Microsoft Active Directory pentru autentificarea Kerberos, selectați **Microsoft Active Directory este utilizat pentru autentificarea Kerberos** și faceți clic pe **Următorul**.
  - c. În pagina **Specificare informații KDC**, specificați numele complet calificat al serverului Kerberos pentru această regiune, în câmpul **KDC**, apoi specificați **88** în câmpul **Port** și faceți clic pe **Următorul**.
  - d. În pagina **Specificare informații server de parole**, selectați **Da** sau **Nu** pentru setarea unui server de parole. Serverul de parole permite principalilor să schimbe parolele de pe serverul Kerberos. Dacă selectați **Da**, introduceți un nume de server de parole în câmpul **Server de parole**. În câmpul **Port**, lăsați valoarea implicită, **464** și faceți clic pe **Următorul**.
  - e. Pe pagina **Selectați intrări tabelă de chei**, selectați **Autentificare Kerberos i5/OS** și faceți clic pe **Următorul**.

**Notă:** În plus puteți de asemenea crea intrări tabelă de chei pentru IBM Tivoli Directory Server for i5/OS, i5/OS NetServer și IBM HTTP Server for i5/OS, dacă vreți ca aceste servicii să utilizeze autentificare Kerberos. Pentru ca aceste servicii să poată folosi autentificarea Kerberos, pot fi necesare operații suplimentare de configurare.

- f. Pe pagina **Creare intrare tabelă chei i5/OS** introduceți și confirmați o parolă și faceți clic pe **Următorul**. Aceasta este aceeași parolă pe care o veți utiliza când adăugați principalii i5/OS la serverul Kerberos.
- g. Opțional: În pagina **Creare fișier batch**, selectați **Da**, specificați următoarele informații și faceți clic pe **Următorul**:
  - În câmpul **Fișier batch**, actualizați calea de director. Faceți clic pe **Răsfoire** pentru a localiza calea corespunzătoare de director sau editați calea în câmpul **Fișier batch**.
  - În câmpul **Includere parolă**, selectați **Da**. Aceasta asigură că toate parolele asociate cu principalul serviciului i5/OS sunt incluse în fișierul batch. Este important să rețineți că parolele sunt afișate în text clar și că pot fi citite de oricine are acces cu citire la fișierul batch. De aceea, este esențial să ștergeți fișierul batch de pe serverul Kerberos și de pe PC imediat după ce îl folosiți. Dacă nu includeți parola, veți fi promptat pentru parolă atunci când rulați fișierul batch.

**Notă:** Puteți de asemenea adăuga manual principalii serviciului care sunt generați de vrăjitor la Microsoft Active Directory. Pentru a afla cum să faceți asta, vedeți Adăugare principalii i5/OS la serverul Kerberos.

- În pagina **Sumar**, treceți în revistă detaliile configurației serviciului de autentificare în rețea și faceți clic pe **Sfârșit** pentru a reveni la vrăjitorul Configurare EIM.

7. Folosiți pagina **Specificare controler de domeniu EIM** pentru a specifica următoarele informații de conexiune pentru controlerul de domeniu EIM la distanță pe care doriți să-l configurați:
  - a. În câmpul **Nume controler de domeniu**, specificați numele serverului de director la distanță pe care doriți să-l configurați drept controler de domeniu EIM pentru domeniul pe care îl creați. Numele de controler de domeniu EIM poate fi numele de gază și de domeniu TCP/IP al serverului de director sau adresa serverului de director.
  - b. Specificați informațiile de conexiune pentru conexiunea la controlerul de domeniu, după cum urmează:

- Selectați **Folosire conexiune sigură (SSL sau TLS)** pentru a utiliza o conexiune sigură cu controlerul de domeniu EIM. Dacă este selectată această opțiune, conexiunea folosește SSL (Secure Sockets Layer) sau TLS (Transport Layer Security) pentru a proteja transmiterea datelor EIM printr-o rețea care nu este încredere, așa cum este Internetul.

**Notă:** Trebuie să verificați dacă este configurat controlerul de domeniu EIM pentru a folosi o conexiune sigură. Dacă nu este, conexiunea la controlerul de domeniu poate eșua.

- În câmpul **Port**, specificați portul TCP/IP pe care ascultă serverul de director. Dacă este selectată opțiunea **Folosire conexiune sigură**, portul implicit este 636; dacă nu, portul implicit este 389.
- c. Faceți clic pe **Verificare conexiune** pentru a testa dacă vrăjitorul poate folosi informațiile specificate pentru stabili cu succes o conexiune la controlerul de domeniu EIM la distanță.
- d. Faceți clic pe **Următorul**.
8. În pagina **Specificare utilizator pentru conexiune**, selectați un **Tip de utilizator** pentru conexiune. Puteți selecta unul dintre următoarele tipuri de utilizatori: **Nume distinctiv și parolă**, **Fișier tabelă de chei Kerberos și principal**, **Principal Kerberos și parolă** sau **Profil de utilizator și parolă**. Cele două tipuri de utilizator Kerberos sunt disponibile numai dacă serviciul de autentificare în rețea este configurat pentru platforma locală System i. Tipul de utilizator pe care îl selectați determină celelalte informații pe care trebuie să le furnizați pentru a efectua dialogul care urmează:

**Notă:** Pentru a vă asigura că vrăjitorul are destulă autorizare pentru a crea în director obiectele EIM necesare, selectați ca tip de utilizator **Nume distinctiv și parolă** și specificați ca utilizator DN pentru administratorul LDAP și parola.

Puteți specifica un utilizator diferit pentru conexiune; însă utilizatorul pe care îl specificați trebuie să aibă o autorizare echivalentă cu cea a administratorului LDAP pentru serverul de director la distanță.

- a. Dacă selectați **Nume distinctiv și parolă**, furnizați informațiile următoare:
- În câmpul **Nume distinctiv**, specificați DN-ul (distinguished name) și parola administratorului LDAP pentru a vă asigura că vrăjitorul are suficientă autorizare pentru a administra domeniul EIM și obiectele din el.
  - În câmpul **Parolă**, introduceți parola pentru numele distinctiv.
  - În câmpul **Confirmare parolă**, specificați parola a doua oară în scopul validării ei.
- b. Dacă selectați **Fișier tabelă de chei Kerberos și principal**, furnizați informațiile următoare:
- În câmpul **Fișier tabelă de chei**, specificați calea complet calificată și numele de fișier tabelă de chei care conține principalul Kerberos, pentru a fi folosit de vrăjitor la conectarea în domeniul EIM. Sau, faceți clic pe **Răsfoire** pentru a răsfoi prin directoare în sistemul de fișiere integrat i5/OS pentru a selecta un fișier tabelă de chei.
  - În câmpul **Principal**, specificați numele principalului Kerberos care să fie folosit pentru a identifica utilizatorul.
  - În câmpul **Regiune**, specificați numele de regiune Kerberos complet calificat în care este membru principalul. Numele principalului și al regiunii ce identifică în mod unic utilizatorii Kerberos din fișierul tabelă de chei. De exemplu, principalul jsmith din regiunea ordept.myco.com, este reprezentat în fișierul tabelă de chei ca jsmith@ordept.myco.com.
- c. Dacă selectați **Principal Kerberos și parolă**, furnizați informațiile următoare:
- În câmpul **Principal**, specificați numele principalului Kerberos, de folosit de vrăjitor la conectarea în domeniul EIM.
  - În câmpul **Regiune**, specificați numele de regiune Kerberos complet calificat în care este membru principalul. Numele principalului și al regiunii ce identifică în mod unic utilizatorii Kerberos din fișierul tabelă de chei. De exemplu, principalul jsmith din regiunea ordept.myco.com este reprezentat în fișierul tabelă de chei ca jsmith@ordept.myco.com.
  - În câmpul **Parolă**, introduceți parola pentru principalul Kerberos.
  - În câmpul **Confirmare parolă**, specificați parola a doua oară în scopul validării ei.

- d. Dacă selectați **Profil utilizator și parolă**, furnizați informațiile următoare:
    - În câmpul **Profil utilizator**, specificați numele profilului de utilizator de folosit de vrăjitor la conectarea în domeniul EIM.
    - În câmpul **Parolă**, introduceți parola pentru profilul utilizator.
    - În câmpul **Confirmare parolă**, specificați parola a doua oară în scopul validării ei.
  - e. Faceți clic pe **Verificare conexiune** pentru a testa că vrăjitorul poate folosi informațiile de utilizator specificate pentru a stabili o conexiune la controlerul de domeniu EIM.
  - f. Faceți clic pe **Următorul**.
9. Pe pagina **Specificare domeniu** furnizați următoarele informații:
- a. În câmpul **Domeniu**, specificați numele domeniului EIM pe care doriți să-l creați. Acceptați numele implicit al EIM sau folosiți orice șir de caractere care vă convin. Totuși, nu puteți utiliza caractere speciale ca = + < > , # ; \ și \*.
  - b. În câmpul **Descriere**, introduceți un text de descriere a domeniului.
  - c. Faceți clic pe **Următorul**.
10. În dialogul **Specificare DN părinte pentru domeniu**, selectați **Da** pentru a specifica DN-ul părintelui pe care să-l folosească vrăjitorul pentru locația domeniului EIM pe care îl creați. Acesta este DN-ul care reprezintă intrarea aflată imediat deasupra intrării numelui domeniului dumneavoastră în ierarhia arborelui cu informațiile despre director. Sau specificați **Nu** pentru ca datele EIM să fie stocate într-o locație de director cu un sufix al cărui nume este derivat din numele domeniului EIM.

**Notă:** Atunci când folosiți vrăjitorul pentru a configura un domeniu pe un controler de domeniu de la distanță, trebuie să specificați un DN de părinte corespunzător pentru domeniu. Deoarece toate obiectele configurație necesare pentru DN-ul părinte trebuie să existe deja pentru a nu eșua configurarea EIM, trebuie să răsfoiți după un DN părinte corespunzător, în loc să introduceți manual informațiile DN. Faceți clic pe **Ajutor** pentru mai multe informații despre folosirea unui DN părinte.

11. Pe pagina **Informații registru**, specificați dacă să se adauge registrele de utilizatori locali la domeniul EIM ca și definiții de registre. Selectați unul dintre aceste tipuri de registre de utilizatori sau pe amândouă:

**Notă:** Nu trebuie să creați în acest moment definițiile de registru. Dacă alegeți să creați definițiile registru mai târziu, vedeți adăugarea definiție registru și proprietăți registru EIM .

- a. Selectați **i5/OS local** pentru a adăuga o definiție registru pentru registrul local. În câmpul oferit, acceptați valoarea implicită pentru numele definiției de registru sau specificați o valoare diferită pentru numele definiției de registru. Numele registrului EIM este un șir arbitrar care reprezintă tipul registrului și instanța specifică a celui registru.
  - b. Selectați **Kerberos** pentru a adăuga o definiție de registru pentru registrul Kerberos. În câmpul oferit, acceptați valoarea implicită pentru numele definiției de registru sau specificați o valoare diferită pentru numele definiției de registru. Numele definiției de registru implicit este același cu numele regiunii. Acceptând numele implicit și folosind același nume de registru Kerberos ca și numele regiunii, puteți crește performanțele la extragerea informațiilor din registru. Selectați, dacă este necesar, **Identitățile utilizatorului Kerberos sunt sensibile la majuscule**.
  - c. Faceți clic pe **Următorul**.
12. Pe pagina **Specificare utilizator sistem EIM**, selectați un **Tip de utilizator** pe care vreți să-l folosească sistemul la realizarea operațiilor EIM pentru funcțiile sistemului de operare. Aceste operații includ operațiile de căutare mapare și de ștergere a asocierii la ștergerea unui profil utilizator i5/OS. Puteți selecta unul din următoarele tipuri de utilizator: **Nume distinctiv și parolă**, **Fișier tabelă de chei Kerberos și principal** sau **Principal Kerberos și parolă**. Ce tipuri de utilizator puteți selecta depinde de configurația curentă a sistemului. De exemplu, dacă serviciul de autentificare în rețea nu este configurat pentru sistem, atunci este posibil ca tipul de utilizator Kerberos să nu fie disponibil pentru selecție. Tipul de utilizator pe care îl selectați determină celelalte informații pe care trebuie să le furnizați pentru a completa pagina, după cum urmează:

**Notă:** Trebuie să specificați un utilizator care este definit curent pe serverul de director care găzduiește controlerul de domeniu EIM. Utilizatorul pe care îl specificați trebuie să aibă privilegiile de efectuare a

căutărilor de mapare și administrare de registre pentru registrul de utilizatori local. Dacă utilizatorul pe care îl specificați nu are aceste privilegii, atunci anumite funcții ale sistemului de operare înrudite cu utilizarea semnării unice și ștergerea profilurilor de utilizator ar putea eșua.

Dacă nu ați configurat serverul de director înainte de a rula acest vrăjitor, singurul tip de utilizator pe care-l puteți selecta este **Nume distinctiv și parolă** și singurul nume distinctiv pe care-l puteți specifica este DN-ul administratorului LDAP.

- a. Dacă selectați **Nume distinctiv și parolă**, furnizați informațiile următoare:
    - În câmpul **Nume distinctiv**, specificați numele distinctiv LDAP care identifică utilizatorul pe care să-l folosească sistemul atunci când realizează operații EIM.
    - În câmpul **Parolă**, introduceți parola pentru numele distinctiv.
    - În câmpul **Confirmare parolă**, specificați parola a doua oară în scopul verificării ei.
  - b. Dacă selectați **Principal Kerberos și parolă**, furnizați informațiile următoare:
    - În câmpul **Principal**, specificați numele principalului Kerberos pe care să-l folosească sistemul la realizarea operațiilor EIM.
    - În câmpul **Regiune**, specificați numele de regiune Kerberos complet calificat în care este membru principalul. Numele principalului și al regiunii ce identifică în mod unic utilizatorii Kerberos din fișierul tabelă de chei. De exemplu, principalul jsmith din regiunea ordept.myco.com este reprezentat în fișierul tabelă de chei ca jsmith@ordept.myco.com.
    - În câmpul **Parolă**, introduceți parola pentru utilizator.
    - În câmpul **Confirmare parolă**, specificați parola a doua oară în scopul verificării ei.
  - c. Dacă selectați **Fișier tabelă de chei Kerberos și principal**, furnizați informațiile următoare:
    - În câmpul **Fișier tabelă de chei**, specificați calea complet calificată și numele de fișier tabelă de chei care conține principalul Kerberos, de folosit de sistem pentru realizarea operațiilor EIM. Sau, faceți clic pe **Răsfoire** pentru a răsfoi prin directoare în sistemul de fișiere integrat System i pentru a selecta un fișier tabelă de chei.
    - În câmpul **Principal**, specificați numele principalului Kerberos pe care să-l folosească sistemul la realizarea operațiilor EIM.
    - În câmpul **Regiune**, specificați numele de regiune Kerberos complet calificat în care este membru principalul. Numele principalului și al regiunii ce identifică în mod unic utilizatorii Kerberos din fișierul tabelă de chei. De exemplu, principalul jsmith din regiunea ordept.myco.com este reprezentat în fișierul tabelă de chei ca jsmith@ordept.myco.com.
  - d. Faceți clic pe **Verificare conexiune** pentru a vă asigura că vrăjitorul poate folosi informațiile de utilizator specificate pentru a stabili o conexiune la controlerul de domeniu EIM.
  - e. Faceți clic pe **Următorul**.
13. În panoul **Rezumat**, revizualizați informațiile de configurare pe care le-ați furnizat. Dacă toate informațiile sunt corecte, apăsați **Sfârșit**.

## Finalizarea configurației EIM pentru domeniu

Când vrăjitorul se termină, adaugă domeniul nou la folderul **Gestionare domeniu** și cu aceasta ați creat o configurație EIM de bază pentru acest server. Este însă posibil să fie necesar să executați operațiile următoare pentru a finaliza configurarea EIM pentru domeniu.

1. Utilizați vrăjitorul de configurare EIM pe fiecare server adițional pe care vreți să îl alăturați unui domeniu existent. Vedeți subiectul “Alăturarea la un domeniu existent” la pagina 80 pentru informații suplimentare.
2. Adăugați definiții registru EIM la domeniul EIM, dacă este necesar, pentru alte platforme și aplicații non-System i care vor să participe la domeniul EIM. Aceste definiții de registre se referă la registrele de utilizatori reale care trebuie să participe în domeniu. Depinzând de cerințele implementării EIM ar trebui să vedeți fie “Adăugarea unei definiții de registru sistem” la pagina 91, fie “Adăugarea unei definiții de registru aplicație” la pagina 91.
3. Bazat pe implementarea dumneavoastră EIM, determinați dacă să:
  - a. “Crearea unui identificator EIM” la pagina 97 pentru fiecare utilizator unic sau entitate în domeniu și “Crearea unei asocieri de identificator EIM” la pagina 101 pentru ele.

- b. “Crearea unei asocieri de politică” la pagina 102 pentru a mapa un grup de utilizatori la o identitate utilizator destinație.
  - c. Creați o combinație a acestora.
4. Utilizați funcția EIM “Testarea mapărilor EIM” la pagina 88 pentru a testa mapările de identitate pentru configurația EIM a dumneavoastră.
  5. Dacă singurul utilizator EIM pe care l-ați definit este DN pentru administratorul LDAP, atunci utilizatorul EIM are un nivel de autorizări înalt pentru toate datele din serverul de director. Prin urmare, ați putea considera crearea unui sau mai multor DN-uri ca utilizatori adiționali care au control acces pentru date EIM mai corespunzătoare și mai limitate. Pentru a învăța mai multe despre crearea DN-urilor pentru serverul de director, vedeți Nume distinctive în Centrul de informare i5/OS. Numărul de utilizatori EIM suplimentari depinde de accentul pus în politicile de securitate pe îndatoririle și responsabilitățile privitoare la securitate. Tipic, puteți crea cel puțin următoarele două tipuri de nume distinctive (DN):
    - **Un utilizator care are control de acces de administrator EIM**

Acest DN de administrator EIM oferă nivelul corespunzător de autorizare pentru un administrator care este responsabil cu gestionarea domeniului EIM. Acest DN administrator EIM ar putea fi utilizat la conectarea la controlerul de domeniu când gestionați toate aspectele domeniului EIM prin mijloace ale Navigator System i.
    - **Sau cel puțin cu un utilizator care are următoarele controale de acces:**
      - Administrator de identificatori
      - Administrator de registru
      - Operații de mapare EIM

Acest utilizator furnizează nivelul corespunzător de control acces, necesar pentru utilizatorul de sistem care realizează operațiile EIM din partea sistemului de operare.

**Notă:** Pentru a utiliza noul DN pentru utilizatorul sistemului în loc de DN-ul administratorului LDAP, trebuie să modificați proprietățile configurației EIM pentru platforma System i. Vedeți “Gestionarea proprietăților de configurare EIM” la pagina 115 pentru a afla cum să modificați DN-ul utilizatorului sistemului.

S-ar putea să fie nevoie să realizați taskuri suplimentare dacă ați creat o configurație serviciu de autentificare de bază, în special dacă implementați un mediu de semnare unică. Puteți găsi informații despre acești pași suplimentari trecând în revistă pașii de configurare finalizați demonstrați de scenariul, Activare semnare unică pentru i5/OS.

## Alăturarea la un domeniu existent

Utilizați vrăjitorul de configurare EIM (Enterprise Identity Mapping) pe o platformă System i pentru a configura un controler de domeniu și a crea un domeniu EIM, apoi puteți utiliza vrăjitorul pentru a configura alte sisteme să participe în domeniu.

După ce creați un domeniu EIM și configurați un controler de domeniu pe un sistem, puteți configura toate celelalte platforme System i să se alătore domeniului EIM. Pe măsură ce lucrați cu vrăjitorul trebuie să furnizați informații despre domeniu, incluzând informații de conexiune la controlerul de domeniu EIM. Când folosiți vrăjitorul de configurare EIM pentru a vă alătura unui domeniu existent, vrăjitorul tot vă oferă opțiunea de lansarea a vrăjitorului de configurare NAS (Network Authentication Service) dacă ați ales să configurați Kerberos ca parte a configurării EIM pe sistem.

Când terminați să vă alăturați unui domeniu existent cu vrăjitorul de configurare EIM, puteți realiza următoarele task-uri:

- Configurarea serviciului de autentificare în rețea pentru sistem.
- Crearea definițiilor registru pentru registrul local i5/OS și pentru registrul Kerberos.
- Configurarea sistemului ca să participe într-un domeniu existent EIM.

Pentru a configura sistemul să se alătore unui domeniu EIM existent, trebuie să aveți toate din următoarele autorizări speciale:

- Administrator securitate (\*SECADM).

- Toate obiectele (\*ALLOBJ).

Pentru a porni și folosi vrăjitorul de configurare EIM pentru a vă alătura unui domeniu existent, realizați următorii pași:

1. Verificați că serverul de director de pe sistemul de la distanță este activ.
2. În Navigator System i, selectați sistemul pentru care vreți să configurați EIM și expandați **Rețea > EIM (Enterprise Identity Mapping)**.
3. Faceți clic dreapta **Configurare** și selectați **Configurare...** pentru a porni vrăjitorul de configurare EIM.

**Notă:** Această opțiune este etichetată **Reconfigurare...**, dacă EIM a fost configurat anterior pe sistem.

4. Pe pagina de **Bun venit** a vrăjitorului, selectați **Alăturare la un domeniu existent** și apoi apăsați **Următorul**.

**Notă:** Dacă serviciul de autentificare în rețea nu este configurat curent pe modelul System i sau informații suplimentare configurare autentificare în rețea sunt necesare pentru a configura un mediu de semnare unică, pagina **Configurare servicii autentificare în rețea** se afișează. Această pagină vă permite să porniți vrăjitorul Configurare servicii de autentificare în rețea astfel încât să puteți configura serviciul de autentificare în rețea. Sau, puteți configura Serviciu autentificare în rețea mai târziu utilizând vrăjitorul de configurare pentru acest serviciu prin Navigator System i. După ce efectuați configurarea serviciului de autentificare în rețea, continuați vrăjitorul de configurare EIM.

5. Pentru a configura serviciul de autentificare în rețea, terminați acești pași:

- a. Pe pagina **Configurare NAS (Network Authentication Service)**, selectați **Da** pentru a porni vrăjitorul de configurare NAS. Cu acest vrăjitor, puteți configura mai multe interfețe și servicii i5/OS pentru a participa într-o regiune Kerberos și pentru a configura un mediu semnare unică care utilizează ambele EIM și serviciul de autentificare în rețea.
- b. Pe pagina **Specificare informații regiune**, specificați numele regiunii implicite în câmpul **Regiune implicită**. Dacă utilizați Microsoft Active Directory pentru autentificarea Kerberos, selectați **Microsoft Active Directory este utilizat pentru autentificarea Kerberos** și faceți clic pe **Următorul**.
- c. Pe pagina **Specificare informații KDC**, specificați numele complet calificat al serverului Kerberos pentru această regiune în câmpul **KDC**, specificați **88** în câmpul **Port** și faceți clic pe **Următorul**.
- d. Pe pagina **Specificare informații pentru server de parole**, selectați fie **Da**, fie **Nu** pentru setarea unui server de parole. Serverul de parole permite principalilor să modifice parolele pe serverul Kerberos. Dacă selectați **Da**, introduceți numele serverului de parole în câmpul **Server de parole**. În câmpul **Port**, acceptați valoarea implicită de **464** și faceți clic pe **Următorul**.
- e. Pe pagina **Selectare intrări tabelă de chei** selectați **Autentificare Kerberos i5/OS** și faceți clic pe **Următorul**.

**Notă:** În plus puteți de asemenea crea intrări tabelă de chei pentru IBM Tivoli Directory Server for i5/OS, i5/OS NetServer și IBM HTTP Server for i5/OS dacă vreți ca aceste servicii să utilizeze autentificare Kerberos. Este posibil să aveți nevoie de configurări suplimentare pentru aceste servicii, înainte ca ele să poată folosi autentificarea Kerberos.

- f. Pe pagina **Creare Intrare tabelă chei i5/OS** introduceți și confirmați o parolă și faceți clic pe **Următorul**. Aceasta este aceeași parolă pe care o veți utiliza când adăugați principalii i5/OS la serverul Kerberos.
- g. Opțional: Pe pagina **Creare fișier batch**, selectați **Da**, specificați informațiile următoare și faceți clic pe **Următorul**:
  - În câmpul **Fișier batch**, actualizați calea de directoare. Faceți clic pe **Răsfoire** pentru a găsi calea de directoare corespunzătoare sau editați calea în câmpul **Fișier batch**.
  - În câmpul **Includere parolă**, selectați **Da**. Aceasta asigură că toate parolele asociate cu principalul serviciului i5/OS sunt incluse în fișierul batch. Este important de reținut că parolele sunt în text clar și pot fi citite de oricine are acces de citire la fișierul batch. De aceea este esențial să ștergeți fișierul batch de pe serverul Kerberos și de pe PC imediat ce l-ați folosit. Dacă nu includeți parola, va apare un prompt pentru parolă, când rulați fișierul batch.

**Notă:** Puteți de asemenea adăuga manual principalii serviciului care sunt generați de vrăjitor la Microsoft Active Directory. Pentru a afla cum să faceți asta, vedeți Adăugare principalii i5/OS la serverul Kerberos

- Pe pagina **Sumar**, treceți în revistă detaliile de configurare serviciu de autentificare în rețea și faceți clic pe **Sfârșit** pentru a vă întoarce la vrăjitorul de configurare EIM.

6. Pe pagina **Specificare controler de domeniu** furnizați următoarele informații:

**Notă:** Serverul de director care acționează ca și controler de domeniu, trebuie să fie activ pentru a termina cu succes această configurare de EIM.

- a. În câmpul **Nume controler de domeniu**, specificați numele sistemului care servește ca și controler de domeniu pentru domeniul EIM pentru care vreți ca platforma System i să se alăture.
- b. Faceți clic pe **Folosirea conexiunii securizate (SSL sau TLS)**, dacă doriți să folosiți o conexiune securizată la controlerul de domeniu EIM. Când este selectată, conexiunea folosește fie SSL (Secure Sockets Layer), fie TLS (Transport Layer Security) pentru a stabili o conexiune securizată pentru a proteja transmisia datelor EIM peste o rețea care nu este de încredere, cum ar fi Internetul.

**Notă:** Trebuie să verificați dacă este configurat controlerul de domeniu EIM să folosească o conexiune securizată. Dacă nu, conectarea la controlerul de domeniu eșuează.

- c. În câmpul **Port**, specificați portul TCP/IP la care ascultă serverul de director. Dacă este selectat **Folosirea conexiunii securizate**, portul implicit este 636; altfel, portul implicit este 389.
- d. Faceți clic pe **Verificare conexiune** pentru a testa că vrăjitorul poate folosi informațiile specificate pentru a stabili o conexiune la controlerul de domeniu EIM.
- e. Faceți clic pe **Următorul**.

7. Pe pagina **Specificare utilizator pentru conexiune**, selectați un **Tip de utilizator** pentru conexiune. Puteți selecta unul din următoarele tipuri de utilizatori: **Nume și parolă distinctive**, **Fișierul tabelă de chei și principalul Kerberos**, **Principalul și parola Kerberos** sau **Profilul utilizator și parola**. Cele două tipuri de utilizator Kerberos sunt disponibile numai dacă serviciul de autentificare în rețea este configurat pentru platforma locală System i. Tipul de utilizator pe care îl selectați determină celelalte informații pe care trebuie să le furnizați pentru a efectua dialogul care urmează:

**Notă:** Pentru a vă asigura că vrăjitorul are destulă autorizare pentru a crea în director obiectele EIM necesare, selectați ca tip de utilizator **Nume distinctiv și parolă** și specificați ca utilizator DN pentru administratorul LDAP și parola.

Puteți specifica un utilizator diferit pentru conexiune; dar utilizatorul pe care-l specificați trebuie să aibă autorizarea echivalentă cu administratorul LDAP pentru serverul de director de la distanță.

- Dacă selectați **Nume distinctiv și parolă**, furnizați informațiile următoare:
  - În câmpul **Nume distinctiv**, specificați numele distinctiv (DN) LDAP care identifică utilizatorul care este autorizat să creeze obiecte în spațiul de nume local al serverului LDAP. Dacă ați folosit acest vrăjitor să configurați serverul LDAP într-un pas anterior, trebuie să introduceți numele distinctiv pentru administratorul LDAP pe care l-ați creat în acel pas.
  - În câmpul **Parolă**, introduceți parola pentru numele distinctiv.
  - În câmpul **Confirmare parolă**, specificați parola a doua oară în scopul validării ei.
- Dacă selectați **Fișier tabelă de chei Kerberos și principal**, furnizați informațiile următoare:
  - În câmpul **Fișier tabelă de chei**, specificați calea complet calificată și numele de fișier tabelă de chei care conține principalul Kerberos, de folosit de vrăjitor la conectarea în domeniul EIM. Sau, faceți clic pe **Răsfoire...** pentru a răsfoi printre directoarele din System i sistemul de fișiere integrat pentru a selecta un fișier tabelă de chei.
  - În câmpul **Principal**, specificați numele principalului Kerberos care să fie folosit pentru a identifica utilizatorul.



- În câmpul **Regiune**, specificați numele de regiune Kerberos complet calificat la care este membru principalul. Numele principalului și al regiunii identifică în mod unic utilizatorii Kerberos din fișierul tabelă de chei. De exemplu, principalul jsmith din regiunea ordept.myco.com, este reprezentat în fișierul tabelă de chei ca jsmith@ordept.myco.com.
  - Dacă selectați **Principal Kerberos și parolă**, furnizați informațiile următoare:
    - În câmpul **Principal**, specificați numele principalului Kerberos, de folosit de vrăjitor la conectarea în domeniul EIM.
    - În câmpul **Regiune**, specificați numele de regiune Kerberos complet calificat la care este membru principalul. Numele principalului și al regiunii identifică în mod unic utilizatorii Kerberos din fișierul tabelă de chei. De exemplu, principalul jsmith din regiunea ordept.myco.com este reprezentat în fișierul tabelă de chei ca jsmith@ordept.myco.com.
    - În câmpul **Parolă**, introduceți parola pentru principalul Kerberos.
    - În câmpul **Confirmare parolă**, specificați parola a doua oară în scopul validării ei.
  - Dacă selectați **Profil utilizator și parolă**, furnizați informațiile următoare:
    - În câmpul **Profil utilizator**, specificați numele profilului de utilizator de folosit de vrăjitor la conectarea în domeniul EIM.
    - În câmpul **Parolă**, introduceți parola pentru profilul utilizator.
    - În câmpul **Confirmare parolă**, specificați parola a doua oară în scopul validării ei.
  - Faceți clic pe **Verificare conexiune** pentru a testa că vrăjitorul poate folosi informațiile de utilizator specificate pentru a stabili o conexiune la controlerul de domeniu EIM.
  - Faceți clic pe **Următorul**.
8. În pagina **Specificați domeniul**, selectați numele domeniului la care doriți să vă alăturați și apăsați **Următorul**.
9. Pe pagina **Informații registru**, specificați dacă să se adauge registrele de utilizatori locali la domeniul EIM ca și definiții de registre. Selectați unul sau amândouă din aceste tipuri de registre de utilizatori:
- Selectați **i5/OS local** pentru a adăuga o definiție registru pentru registrul local. În câmpul oferit, acceptați valoarea implicită pentru numele definiției de registru sau specificați o valoare diferită pentru numele definiției de registru. Numele registrului EIM este un șir arbitrar care reprezintă tipul registrului și instanța specifică a acelui registru.
- Notă:** Nu aveți nevoie să creați definiția pentru registrul i5/OS local la acest moment. Dacă alegeți să creați definiția pentru registrul i5/OS mai târziu, trebuie să adăugați definiția pentru registrul sistem și actualiza proprietățile configurației EIM.
- Selectați **Kerberos** pentru a adăuga o definiție de registru pentru registrul Kerberos. În câmpul oferit, acceptați valoarea implicită pentru numele definiției de registru sau specificați o valoare diferită pentru numele definiției de registru. Numele definiției de registru implicit este același cu numele regiunii. Acceptând numele implicit și folosind același nume de registru Kerberos ca și numele regiunii, puteți crește performanțele la extragerea informațiilor din registru. Selectați, dacă este necesar, **Identitățile utilizatorului Kerberos sunt sensibile la majuscule**.
- Notă:** Dacă ați utilizat vrăjitorul de configurare EIM pe alt sistem pentru a adăuga o definiție registru pentru registrul Kerberos pentru care acest model System i are un serviciu principal, apoi nu aveți nevoie să adăugați o definiție registru Kerberos ca parte componentă a acestei configurații. Dar, va fi nevoie să specificați numele acelui registru Kerberos în proprietățile configurației pentru acest sistem, după ce ați terminat vrăjitorul.
- Faceți clic pe **Următorul**.
10. Pe pagina **Specificare utilizator sistem EIM**, selectați un **Tip de utilizator** pe care vreți să-l folosească sistemul la realizarea operațiilor EIM pentru funcțiile sistemului de operare. Aceste operații includ operațiile de căutare mapare și de ștergere a asocierii la ștergerea unui profil utilizator i5/OS. Puteți selecta unul din următoarele tipuri de utilizatori: **Nume distinctiv și parolă**, **Fișier tabelă de chei Kerberos și principal** sau **Principal Kerberos și parolă**. Ce tipuri de utilizator puteți selecta depinde de configurația curentă a sistemului. De exemplu, dacă

serviciul de autentificare în rețea nu este configurat pentru sistem, atunci tipul de utilizatori Kerberos nu sunt disponibili pentru selecție. Tipul de utilizator pe care îl selectați determină celelalte informații pe care trebuie să le furnizați pentru a completa pagina după cum urmează:

**Notă:** Trebuie să specificați un utilizator care este definit curent pe serverul de director care găzduiește controlerul de domeniu EIM. Utilizatorul pe care îl specificați trebuie să aibă privilegiile de efectuare a căutărilor de mapare și administrare de registre pentru registrul de utilizatori local. Dacă utilizatorul pe care îl specificați nu are aceste privilegii, atunci anumite funcții ale sistemului de operare înrudite cu utilizarea semnării uniceși ștergerea profilurilor utilizator ar putea eșua.

- Dacă selectați **Nume distinctiv și parolă**, furnizați informațiile următoare:
    - În câmpul **Nume distinctiv**, specificați numele distinctiv LDAP care identifică utilizatorul pe care să-l folosească sistemul atunci când realizează operații EIM.
    - În câmpul **Parolă**, introduceți parola pentru numele distinctiv.
    - În câmpul **Confirmare parolă**, specificați parola a doua oară în scopul verificării ei.
  - Dacă selectați **Principal Kerberos și parolă**, furnizați informațiile următoare:
    - În câmpul **Principal**, specificați numele principalului Kerberos de folosit de sistem la realizarea operațiilor EIM.
    - În câmpul **Regiune**, specificați numele de regiune Kerberos complet calificat la care este membru principalul. Numele principalului și al regiunii identifică în mod unic utilizatorii Kerberos din fișierul tabelă de chei. De exemplu, principalul jsmith din regiunea ordept.myco.com este reprezentat în fișierul tabelă de chei ca jsmith@ordept.myco.com.
    - În câmpul **Parolă**, introduceți parola pentru utilizator.
    - În câmpul **Confirmare parolă**, specificați parola a doua oară în scopul verificării ei.
  - Dacă selectați **Fișier tabelă de chei Kerberos și principal**, furnizați informațiile următoare:
    - În câmpul **Fișier tabelă de chei**, specificați calea complet calificată și numele de fișier tabelă de chei care conține principalul Kerberos, de folosit de sistem pentru realizarea operațiilor EIM. Sau, faceți clic pe **Răsfoire...** pentru a răsfoi printre directoarele din System i sistemul de fișiere integrat pentru a selecta un fișier tabelă de chei.
    - În câmpul **Principal**, specificați numele principalului Kerberos de folosit de sistem la realizarea operațiilor EIM.
    - În câmpul **Regiune**, specificați numele de regiune Kerberos complet calificat la care este membru principalul. Numele principalului și al regiunii identifică în mod unic utilizatorii Kerberos din fișierul tabelă de chei. De exemplu, principalul jsmith din regiunea ordept.myco.com este reprezentat în fișierul tabelă de chei ca jsmith@ordept.myco.com.
  - Faceți clic pe **Verificare conexiune** pentru a vă asigura că vrăjitorul poate folosi informațiile de utilizator specificate pentru a stabili o conexiune la controlerul de domeniu EIM.
  - Faceți clic pe **Următorul**.
11. În pagina **Rezumat**, treceți în revistă informațiile de configurare pe care le-ați furnizat. Dacă toate informațiile sunt corecte, apăsați **Sfârșit**.

## Finalizarea configurației EIM pentru domeniu

Când vrăjitorul se termină, adaugă domeniul la folderul **Domain Management** și ați creat o configurație EIM de bază pentru acest server. Totuși, s-ar putea să fie nevoie să terminați acești pași pentru a finaliza configurarea EIM pentru domeniu.

1. Adăugați definiții registru EIM la domeniul EIM, dacă este necesar, sistemele la care nu rulează sisteme și aplicații i5/OS pe care vreți să participe la domeniul EIM. Aceste definiții de registre se referă la registrele de utilizatori reali care trebuie să participe în domeniu. Puteți, fie adăuga definiții de registru sistem fie adăuga definiții de registru aplicație în funcție de ce are nevoie implementarea dumneavoastră EIM.
2. Bazat pe implementarea dumneavoastră EIM, determinați dacă să:
  - Creați identificatori EIM pentru fiecare utilizator sau entitate unică în domeniu și să creați asocieri de identificatori pentru ei.

- Creați asocieri de politică pentru a mapa un grup de utilizatori la o singură identitate de utilizator destinație.
  - Creați o combinație a acestora.
3. Folosiți funcția EIM de testare a unei mapări pentru a testa mapările de identificatori pentru configurația EIM.
  4. Dacă singurul utilizator EIM pe care l-ați definit este DN pentru administratorul LDAP, atunci utilizatorul dumneavoastră EIM are un nivel înalt de autorizare la toate datele de pe serverul director. Prin urmare, ați putea considera crearea unui sau mai multor DN-uri ca utilizatori adiționali care au control acces pentru date EIM mai corespunzătoare și mai limitate. Pentru a învăța mai multe despre crearea DN-urilor pentru serverul de director, consultați Nume distinctive în Centrul de informare i5/OS. Numărul de utilizatori EIM suplimentari depinde de accentul pus în politicile de securitate pe îndatoririle și responsabilitățile privitoare la securitate. Tipic, puteți crea cel puțin următoarele două tipuri de nume distinctive (DN):
    - **Un utilizator care are control de acces de administrator EIM**  
Acest DN de administrator EIM oferă nivelul corespunzător de autorizare pentru un administrator care este responsabil pentru gestionarea domeniului EIM. Acest DN administrator EIM ar putea fi utilizat la conectarea la controlerul de domeniu când gestionați toate aspectele domeniului EIM prin mijloace ale Navigator System i.
    - **Sau cel puțin cu un utilizator care are următoarele controale de acces:**
      - Administrator de identificatori
      - Administrator de registru
      - Operații de mapare EIM

Acest utilizator furnizează nivelul corespunzător de control acces necesar pentru utilizatorul sistem care realizează operațiile EIM din partea sistemului de operare.

**Notă:** Pentru a utiliza noul DN pentru utilizatorul sistemului în loc de DN-ul administratorului LDAP, trebuie să modificați proprietățile configurației EIM pentru platforma System i. Consultați Gestiune proprietăți configurație EIM pentru a învăța cum să modificați DN-ul de utilizator sistem.

S-ar putea să fie nevoie să realizați taskuri suplimentare dacă ați creat o configurație serviciu de autentificare de bază, în special dacă implementați un mediu de semnare unică. Puteți găsi inform ații despre acești pași suplimentari trecând în revistă pașii de configurare finalizați demonstrați de scenariul, Activare semnare unică pentru i5/OS.

## Configurarea unei conexiuni securizate la controlerul de domeniu EIM

Ați putea dori să folosiți protocoalele SSL (Secure Sockets Layer) sau TLS (Transport Layer Security) pentru a stabili o conexiune securizată cu controlerul de domeniu EIM (Enterprise Identity Mapping), pentru a proteja transmisia datelor EIM.

Pentru a configura SSL sau TLS pentru EIM, trebuie să efectuați aceste operații:

1. Dacă este necesar, utilizați DCM (Digital Certificate Manager) pentru a crea un certificat pentru serverul de director pentru a-l folosi cu SSL.
2. Activarea SSL pentru serverul de director local care găzduiește domeniul EIM.
3. Actualizați proprietățile configurării EIM pentru a specifica că modelul System i utilizează o conexiune SSL sigură. Pentru a actualiza proprietățile Configurației EIM, terminați acești pași:
  - a. În Navigator System i, selectați sistemul în care ați configurat EIM și expandați **Rețea** → **EIM (Enterprise Identity Mapping)**.
  - b. Faceți clic-dreapta **Configurare** și selectați **Proprietăți**.
  - c. Pe pagina **Domeniu**, selectați **Folosirea conexiunii securizate (SSL sau TLS)**, specificați portul securizat la care ascultă serverul de director sau acceptați valoarea implicită **636** în câmpul **Port** și faceți clic pe **OK**.
4. Actualizați proprietățile domeniului EIM pentru fiecare domeniu EIM pentru a specifica că EIM utilizează o conexiune SSL când gestionează domeniul prin Navigator System i. Pentru a actualiza proprietățile domeniului EIM, terminați acești pași:
  - a. În Navigator System i, selectați sistemul în care ați configurat EIM și expandați **Rețea** → **EIM (Enterprise Identity Mapping)** → **Gestionare domeniu**.

- b. Selectați domeniul EIM în care vreți să lucrați.
  - Dacă domeniul EIM cu care vreți să lucrați nu este listat sub **Gestionare domeniu**, vedeți adăugarea unui domeniu EIM la Gestionare domeniu.
  - Dacă nu sunteți conectat curent la domeniul EIM în care vreți să lucrați, vedeți Conectarea la controlerul de domeniu EIM.
- c. Faceți clic-dreapta pe domeniul EIM la care sunteți acum conectat și selectați **Proprietăți**.
- d. Pe pagina **Domeniu**, selectați **Folosirea conexiunii securizate (SSL sau TLS)**, specificați portul securizat la care ascultă serverul de director sau acceptați valoarea implicită 636 în câmpul **Port** și faceți clic pe **OK**.

---

## Gestionarea EIM (Enterprise Identity Mapping)

După ce configurați EIM (Enterprise Identity Mapping) pentru platforma dumneavoastră System i, sunt multe taskuri administrative pe care va trebui să le realizați în timp pentru a gestiona domeniul dumneavoastră EIM și datele pentru domeniu.

Pentru a învăța mai multe despre gestionarea EIM în întreprinderea dumneavoastră, examinați aceste pagini.

### Gestionarea domeniilor EIM (Enterprise Identity Mapping)

Utilizați Navigator System i pentru a gestiona toate domeniile dumneavoastră EIM.

Pentru a gestiona orice domeniu EIM, domeniul trebuie să fie menționat sau trebuie să îl adăugați la folderul **Gestionare domeniu** sub folderul **Rețea** în Navigator System i. Când folosiți Configurația EIM pentru a crea și configura un nou domeniu EIM, domeniul este adăugat automat la folderul **Gestionare domeniu** astfel încât puteți gestiona domeniul și informația din domeniu.

Puteți utiliza orice conexiune System i pentru a gestiona un domeniu EIM care se află oriunde în aceeași rețea, chiar și când sistemul pe care îl utilizați nu este participant în domeniu.

Puteți realiza următoarele operații de gestiune pentru un domeniu:

#### Adăugarea unui domeniu EIM la folderul Gestionare domeniu

Pentru a adăuga un domeniu EIM la folderul Gestionare domeniu, trebuie să aveți autorizare specială \*SECADM și domeniul pe care vreți să îl adăugați trebuie să existe înaintea adăugării sale la folderul Gestionare domeniu.

Pentru a adăuga un domeniu EIM existent la folderul **Gestionare domeniu**, efectuați următorii pași:

1. Expandați **Rețea >Mapare identitate în întreprindere**.
2. Faceți clic dreapta pe **Gestionare domeniu** și selectați **Adăugare domeniu**
3. În fereastra de dialog **Adăugare domeniu**, specificați domeniul cerut și informații de conectare. Sau, faceți clic pe **Răsfoire** pentru a vizualiza o listă de domenii pe care controlerul de domenii le gestionează.

**Notă:** Dacă faceți clic pe **Răsfoire**, dialogul **Conectare la Controler domenii EIM** se afișează. Pentru a vedea o listă de domenii, trebuie să vă conectați la controlerul de domenii fie cu control acces administrator LDAP sau cu control acces administrator EIM. Conținutul listei domeniului variază în funcție de controlul accesului EIM pe care îl aveți. Dacă aveți control de acces Administrator LDAP, puteți vizualiza o listă a tuturor domeniilor pe care le gestionează controlerul de domenii. Altfel lista afișează doar acele domenii pentru care aveți control de acces Administrator EIM.

4. Faceți clic pe **Ajutor**, dacă este necesar, pentru a determina ce informații să specificați pentru fiecare câmp.
5. Apăsați **OK** pentru a adăuga domeniul.

#### Conectarea la domeniul EIM

Înainte să puteți lucra cu un domeniu EIM (Enterprise Identity Mapping), trebuie mai întâi să vă conectați la controlerul de domenii EIM pentru domeniu. Vă puteți conecta la un domeniu EIM chiar dacă modelul dumneavoastră System i nu este actual configurat pentru a participa la domeniu.

Pentru a vă conecta la controlerul de domenii EIM, utilizatorul la care vă conectați trebuie să fie membru al unui grup de control acces EIM. Apartenența dumneavoastră la un grup de control acces EIM determină ce operații puteți realiza în domeniu și ce date EIM puteți vizualiza sau schimba.

Pentru a vă conecta la un domeniu EIM, efectuați pașii următori:

1. Expandați **Rețea > EIM (Enterprise Identity Mapping) > Gestionare domeniu**.
2. Faceți clic-dreapta pe domeniul la care vreți să vă conectați..

**Notă:** Dacă domeniul cu care vreți să lucrați nu este menționat sub **Gestiune domenii**, trebuie să adăugați un domeniu EIM la folderul de gestiune domenii.

3. Faceți clic dreapta pe domeniul EIM la care vreți să vă conectați și selectați **Conectare**.
4. În fereastra **Conectare la controlerul de domeniu EIM**, specificați **Tipul utilizatorului**, furnizați informațiile de identificare cerute pentru utilizator selectați o opțiune de parolă pentru conectarea la un controler de domeniu.
5. Faceți clic pe **Ajutor**, dacă este necesar, pentru a determina ce informații să specificați pentru fiecare câmp din fereastra de dialog.
6. Faceți clic pe **OK** pentru conectare la controlerul de domeniu.

## Activarea asocierilor de politică pentru un domeniu

O asociere de politică furnizează un mijloc de creare mapări multe-la-una în situații unde asocierile între identitățile utilizator și identificatorul EIM (Enterprise Identity Mapping) nu există.

Puteți folosi o asociere de politică pentru a mapa un set sursă de identități de utilizator (în loc de o singură identitate de utilizator) la o unică identitate destinație de utilizator dintr-un registru de utilizatori destinație, specificat. Pentru a putea folosi asocieri de politică, trebuie însă mai întâi să vă asigurați că ați activat domeniul pentru a utiliza asocierile de politică pentru operații de căutare mapare.

Pentru a activa suportul de politică de mapare pentru a utiliza asocierile de politică pentru un domeniu, trebuie să fiți conectat la domeniul EIM în care vreți să lucrați și trebuie să aveți control acces administrator EIM.

Pentru a activa suportul de căutare mapare pentru utilizare asocieri de politică într-un domeniu, parcurgeți pașii următori:

1. Expandați **Rețea > EIM (Enterprise Identity Mapping) > Gestionare domeniu**.
2. Faceți clic dreapta pe domeniul EIM în care vreți să lucrați și selectați **Politică mapare**.
  - Dacă domeniul EIM cu care vreți să lucrați nu este menționat sub **Gestionare domeniu**, trebuie să adăugați un domeniu EIM la folderul Gestionare domeniu.
  - Dacă nu sunteți conectat curent la domeniul EIM în care vreți să lucrați, trebuie să vă conectați la controlerul de domeniu EIM. (Opțiunea de **Politică mapare** nu este disponibilă până vă conectați la domeniu.)
3. În pagina **General**, selectați **Activare căutări mapare folosind asocieri de politică pentru domeniu**.
4. Selectați **OK**.

**Notă:** Trebuie să activați căutările de mapare și utilizarea asocierilor de politică pentru fiecare definiție registru destinație pentru care sunt asocieri de politică definite. Dacă nu activați căutările de mapare pentru definiția de registru destinație, registrul respectiv nu poate participa la operațiile de căutare mapare EIM. Dacă nu specificați faptul că registrul destinație poate folosi asocieri de politică, asocierile de politică definite pentru acel registru sunt ignorate de operațiile de căutare mapare EIM.

### Concepte înrudite

“Suportul pentru politica EIM și activarea” la pagina 37

Suportul politicii de mapare EIM (Enterprise Identity Mapping) vă permite să folosiți asocieri de politică precum și asocieri identificator specifice într-un domeniu EIM. Puteți folosi asocierile de politică în locul sau în combinație cu asocierile identificator.

## Testarea mapărilor EIM

Testare mapare EIM (Enterprise Identity Mapping) vă permite să emiteți operații de căutare EIM împotriva configurației EIM. Puteți folosi testul pentru a verifica că o identitate specifică de utilizator sursă se mapează corect la identitatea de utilizator destinație. Testarea asigură că operațiile de căutare mapare EIM pot returna identitatea utilizator destinație corectă bazată pe informațiile specificate.

Pentru a utiliza funcția testare mapare pentru a vă testa configurația EIM, trebuie să fiți conectat la domeniul EIM în care vreți să lucrați și trebuie să aveți control de acces EIM la unul din aceste nivele:

- Administrator EIM
- Administrator de identificatori
- Administrator de registru
- Operații de căutare mapare EIM

Pentru a folosi suportul de testare mapări pentru a testa configurația EIM, terminați acești pași:

1. Expandați **Rețea > EIM (Enterprise Identity Mapping) > Gestionare domeniu**.
2. Selectați domeniul EIM în care vreți să lucrați.
  - Dacă domeniul EIM cu care vreți să lucrați nu este listat sub **Gestionare domeniu**, vedeți adăugarea unui domeniu EIM la Gestionare domeniu.
  - Dacă nu sunteți conectat curent la domeniul EIM în care vreți să lucrați, vedeți Conectarea la controlerul de domeniu EIM.
3. Faceți clic-dreapta pe domeniul EIM la care sunteți acum conectat și selectați **Testarea unei mapări**
4. În dialogul **Testarea unei mapări**, specificați informațiile următoare:
  - a. În câmpul **Registru sursă**, furnizați numele definiției de registru care se referă la registrul de utilizatori pe care vreți să-l folosiți ca sursă pentru testarea operației de căutare mapări.
  - b. În câmpul **Utilizator sursă**, furnizați numele identității utilizatorului pe care vreți să-l folosiți ca sursă pentru testarea operației de căutare mapări.
  - c. În câmpul **Registru destinație**, furnizați numele definiției de registru care se referă la registrul de utilizatori pe care vreți să-l folosiți ca destinație pentru testarea operației de căutare mapări.
  - d. Opțional: În câmpul **Informații de căutare**, furnizați orice informații de căutare definite pentru utilizatorul destinație.
5. Faceți clic pe **Ajutor**, dacă este nevoie, pentru mai multe detalii despre ce informații sunt necesare pentru fiecare câmp în dialog.
6. Faceți clic pe **Testare** și vedeți rezultatele operației de căutare mapări, atunci când sunt afișate.

**Notă:** Dacă operația de căutare mapare returnează rezultate ambigue, dialogul Testare mapare - Rezultate este afișat indicând un mesaj de eroare și o listă de utilizatori destinație pe care le găsește câmpul operație de căutare.

- a. Pentru a depana rezultatele ambigue, selectați un utilizator destinație și faceți clic pe **Detalii**.
  - b. Dialogul Testare mapare - Detalii este afișat indicând informații despre rezultatele operației de căutare mapare pentru utilizatorul destinație specificat. Faceți clic pe **Ajutor** pentru informații suplimentare detaliate despre rezultatele operației de căutare mapare.
  - c. Faceți clic pe **Închide** pentru a ieși din dialogul **Testare mapare - Rezultate**.
7. Continuați testarea configurației sau faceți clic pe **Închidere** pentru a ieși.

### Concepte înrudite

“Depanarea problemelor de mapare EIM” la pagina 119

Există un număr de probleme obișnuite care pot duce la nefuncționarea tuturor mapărilor EIM sau la funcționarea lor necorespunzătoare. Revedeți următoarea tabelă pentru a găsi informații despre ce problemă ar putea cauza o mapare EIM să eșueze și soluțiile potențiale pentru acea problemă. Dacă mapările EIM eșuează, s-ar putea să fie nevoie să vedeți fiecare soluție din tabelă pentru a găsi și rezolva problema sau problemele care au dus la eșuarea mapărilor.

## Lucrul cu rezultatele testului și rezolvarea problemelor:

Când rulează testul, este returnată o identitate de utilizator destinație dacă procesul testării găsește o asociere dintre identitatea de utilizator sursă și identitatea de utilizator destinație pe care administratorul o furnizează. Testul indică tipul asocierii între cele două identități de utilizator pe care a găsit-o. Când procesul de testare nu găsește o asociere bazată pe informațiile furnizate, testul întoarce o identitate de utilizator destinație de none (nici una).

Testul, ca orice operație de căutare mapări EIM, caută și întoarce prima identitate de utilizator destinație corespunzătoare, prin căutarea în următoarea ordine:

1. Asociere de identificator specifică
2. Asociere de politică filtrare certificat
3. Asociere politică registru implicit
4. Asocierea de politică domeniu implicit

În anumite cazuri, testul nu întoarce nici un rezultat identitate de utilizator destinație, deși asocierile sunt configurate pentru domeniu. Verificați că ați furnizat informații corecte pentru test. Dacă informațiile sunt corecte și testul nu întoarce nici un rezultat, atunci problema poate fi cauzată de una din următoarele:

- Suportul de asocieri politică nu este activat la nivelul domeniului. S-ar putea să fie nevoie să activați asocierile de politică pentru un domeniu.
- Suportul de căutare mapări sau suportul de asocieri politică nu este activat la nivelul de registru individual. S-ar putea să fie nevoie să activați suportul de căutare mapări și folosirea de asocieri politică pentru registrul destinație
- O asociere destinație sau sursă pentru un identificator EIM nu este configurată corect. De exemplu, nu există nici o asociere sursă pentru principalul Kerberos (sau utilizatorul Windows) sau este incorectă. Sau, asocierea destinație specifică o identitate de utilizator incorectă. Afișați toate asocierile de identificatori pentru un identificator EIM pentru a verifica asocierile pentru un identificator specific.
- O asociere politică nu este configurată corect. Afișați toate asocierile politică pentru un domeniu pentru a verifica informațiile sursă și destinație pentru toate asocierile de politică definite în domeniu.
- Definiția de registru și identitățile de utilizator nu se potrivesc datorită sensibilității la majuscule. Puteți șterge și crea din nou registrul, sau șterge și crea din nou asocierea cu majuscula corespunzătoare.

În alte cazuri, testul poate avea rezultate ambigue. În asemenea caz, se afișează un mesaj de eroare care indică aceasta. Testul întoarce rezultate ambigue, când mai mult de o identitate de utilizator destinație se potrivește cu criteriul de test specificat. O operație de căutare mapări poate întoarce mai multe identități de utilizator destinație când există una sau mai multe din situațiile următoare:

- Un identificator EIM are mai multe asocieri destinație individuale la același registru destinație.
- Mai mult de un identificator EIM are aceeași identitate utilizator specificată într-o asociere sursă și fiecare din acești identificatori EIM are o asociere destinație la același registru destinație, deși identitatea utilizator specificată pentru fiecare asociere destinație poate fi diferită.
- Mai mult de o asociere politică domeniu implicită specifică același registru destinație.
- Mai mult de o asociere politică registru implicită specifică același registru sursă și același registru destinație.
- Mai mult de o asociere politică filtru certificate specifică același registru sursă X.509, filtru de certificate și registru destinație.

O operație de căutare mapare returnează mai mult de o identitate utilizator destinație poate crea probleme pentru aplicațiile permise EIM, inclusiv aplicațiile și produsele iOS. De aceea este nevoie să determinați cauza rezultatelor ambigue și ce acțiuni trebuie luate pentru rezolvarea situației. În funcție de cauză, puteți face una din următoarele:

- Testul returnează mai multe identități de destinație nedorite. Aceasta indică incorectitudinea configurației de asocieri pentru domeniu, datorită unuia din următoarele:
  - O asociere destinație sau sursă pentru un identificator EIM nu este configurată corect. De exemplu, nu există nici o asociere sursă pentru principalul Kerberos (sau utilizatorul Windows) sau este incorectă. Sau, asocierea destinație specifică o identitate de utilizator incorectă. Afișați toate asocierile de identificatori pentru un identificator EIM pentru a verifica asocierile pentru un identificator specific.

- O asociere politică nu este configurată corect. Afișați toate asocierile politică pentru un domeniu pentru a verifica informațiile sursă și destinație pentru toate asocierile de politică definite în domeniu.
- Testul întoarce mai multe identități destinație și aceste rezultate sunt corespunzătoare pentru modul cum sunt configurate asocierile, atunci este nevoie să specificați informații de căutare pentru fiecare identitate de utilizator destinație. Trebuie să definiți informații de căutare unice pentru toate identitățile de utilizator destinație care au aceeași sursă (fie un identificator EIM pentru asocierile de identificatori sau un registru de utilizatori sursă pentru asocierile de politică). Definind informații de căutare pentru fiecare identitate de utilizator destinație, vă asigurați că o operație de căutare întoarce o singură identitate de utilizator destinație, în locul tuturor identităților de utilizator posibile. Consultați Adăugarea de informații de căutare pentru o identitate utilizator destinație. Trebuie să specificați aceste operații de căutare despre operația de căutare mapare.

**Notă:** Această abordare funcționează doar dacă aplicația este activată să folosească informațiile de căutare. Totuși, aplicațiile de bază i5/OS ca System i Access pentru Windows nu pot utiliza informații de căutare pentru a distinge printre identități utilizator destinație returnate de o operație de căutare. În consecință, ați putea considera redefinirea asocierilor pentru domeniu pentru a vă asigura că o operație de căutare de mapare poate returna o singură identitate utilizator destinație pentru a se asigura că aplicațiile i5/OS de bază pot realiza operații de căutare și mapare de identități cu succes.

## Înlăturarea unui domeniu EIM din folderul Gestionare domeniu

Puteți înlătura un domeniu EIM pe care nu mai vreți să îl gestionați din folderul **Gestionare domeniu**. Cu toate acestea, înlăturarea domeniului din folderul **Gestionare domeniu** nu are același efect ca și ștergerea domeniului și nu șterge datele de domeniu din controlerul de domeniului.

Nu vă trebuie nici un control acces EIM pentru a înlătura un domeniu.

Pentru a înlătura un domeniu EIM (Enterprise Identity Mapping) pe care nu mai doriți să-l gestionați din folderul **Gestionare domeniu**, completați acești pași:

1. Expandați **Rețea >Mapare identitate în întreprindere**.
2. Faceți clic dreapta pe **Gestionare domeniu** și selectați **Înlăturare domeniu**.
3. Selectați domeniul EIM pe care doriți să îl înlăturați din **Gestionare domeniu**.
4. Apăsați **OK** pentru a înlătura domeniul.

### Operații înrudite

“Ștergerea unui domeniu EIM și a tuturor obiectelor de configurare”

Înainte să ștergeți un domeniu EIM, trebuie să ștergeți toate definițiile de registru și toți identificatorii EIM (Enterprise Identity Mapping) din domeniu. Dacă nu vreți să ștergeți domeniul și toate datele domeniului, dar nu mai vreți să gestionați domeniul, în schimb puteți înlătura domeniul.

## Ștergerea unui domeniu EIM și a tuturor obiectelor de configurare

Înainte să ștergeți un domeniu EIM, trebuie să ștergeți toate definițiile de registru și toți identificatorii EIM (Enterprise Identity Mapping) din domeniu. Dacă nu vreți să ștergeți domeniul și toate datele domeniului, dar nu mai vreți să gestionați domeniul, în schimb puteți înlătura domeniul.

Pentru a șterge un domeniu EIM, trebuie să aveți control acces EIM cel puțin la unul din nivelele:

- Administrator LDAP
  - Administrator EIM.
1. Expandați **Rețea > EIM (Enterprise Identity Mapping) > Gestionare domeniu**.
  2. Dacă este necesar, ștergeți toate definițiile de registru din domeniul EIM
  3. Dacă este necesar, ștergeți toți identificatorii EIM din domeniul EIM .
  4. Faceți clic dreapta pe domeniul pe care vreți să îl ștergeți și selectați **Ștergere**.
  5. Apăsați **Da** în dialogul **Confirmare de ștergere**.

**Notă:** Ecranele dialog Ștergere în progres indică starea ștergerii domeniului până când procesul este complet.



### Operații înrudite

“Înlăturarea unui domeniu EIM din folderul Gestionare domeniu” la pagina 90

Puteți înlătura un domeniu EIM pe care nu mai vreți să îl gestionați din folderul **Gestionare domeniu**. Cu toate acestea, înlăturarea domeniului din folderul **Gestionare domeniu** nu are același efect ca și ștergerea domeniului și nu șterge datele de domeniu din controlerul de domeniului.

## Gestionarea definițiilor de registre EIM

Pentru ca registrele de utilizatori și identitățile utilizator pe care le conțin să participe într-un domeniu EIM trebuie să creați definiții registru pentru ele. Puteți gestiona modul în care registrele de utilizator și identitățile lor de utilizator participă în EIM prin gestionarea acestor definiții de registru EIM.

Puteți realiza următoarele operații de gestiune pentru definițiile de registru:

### Concepte înrudite

“Crearea unei asocieri de politică” la pagina 102

O asociere de politică furnizează un mod de a defini o relație dintre mai multe identități de utilizatori din unul sau mai multe registre și o identitate de utilizator unică în alt registru.

### Operații înrudite

“Ștergerea unei asocieri de politică” la pagina 114

Pentru a șterge o asociere de politică, trebuie să fiți conectat la domeniul EIM (Enterprise Identity Mapping) în care vreți să lucrați și trebuie să aveți control acces EIM pentru fie administrator registru sau administrator EIM.

## Adăugarea unei definiții de registru sistem

Pentru a crea o definiție registru sistem, trebuie să fiți conectat la domeniul EIM (Enterprise Identity Mapping) în care vreți să lucrați și trebuie să aveți control acces administrator.

Pentru a adăuga o definiție pentru registrul sistem la un domeniu EIM, completați acești pași.

1. Expandați **Rețea > EIM (Enterprise Identity Mapping) > Gestionare domeniu**.
2. Selectați domeniul EIM în care doriți să lucrați.
  - Dacă domeniul EIM cu care doriți să lucrați nu este listat sub Gestionare domeniu, vedeți “Adăugarea unui domeniu EIM la folderul Gestionare domeniu” la pagina 86.
  - Dacă nu sunteți conectat momentan la domeniul EIM în care vreți să lucrați, vedeți “Conectarea la domeniul EIM” la pagina 86.
3. Expandați domeniul EIM la care sunteți conectat acum.
4. Faceți clic dreapta pe **Registre de utilizatori**, selectați **Adăugare registru**, apoi selectați **Sistem**.
5. În dialogul **Adăugare registru sistem**, furnizați informații despre definiția registru sistem, după cum urmează:
  - a. Un nume pentru definiția registru sistem.
  - b. Un tip definiție pentru registru.
  - c. O descriere a definiției registru sistem.
  - d. (Opțional.) Registru de utilizatori URL.
  - e. Unul sau mai multe alias-uri pentru definiția registru de aplicație, dacă este necesar.
6. Apăsați clic pe **OK** pentru a salva informațiile și a adăuga definiția registru la domeniul EIM.

## Adăugarea unei definiții de registru aplicație

Pentru a crea o definiție registru de aplicație, trebuie să fiți conectat la domeniul EIM (Enterprise Identity Mapping) în care vreți să lucrați și trebuie să aveți control acces EIM.

Pentru a adăuga o definiție pentru registrul aplicație la un domeniu EIM, completați acești pași:

1. Expandați **Rețea > EIM (Enterprise Identity Mapping) > Gestionare domeniu**.
2. Selectați domeniul EIM în care doriți să lucrați.

- Dacă domeniul EIM cu care doriți să lucrați nu este listat sub Gestionare domeniu, vedeți “Adăugarea unui domeniu EIM la folderul Gestionare domeniu” la pagina 86.
  - Dacă nu sunteți conectat momentan la domeniul EIM în care vreți să lucrați, vedeți “Conectarea la domeniul EIM” la pagina 86.
3. Expandați domeniul EIM la care sunteți conectat acum.
  4. Faceți clic dreapta pe **Proprietăți utilizator**, selectați **Adăugare registru**, apoi selectați **Aplicație**.
  5. În dialogul **Adăugare registru aplicație**, furnizați informații despre definiția registru aplicație, după cum urmează:
    - a. Un nume pentru definiția registru aplicație.
    - b. Numele definiției registru al sistemului a cărui registru de utilizatori aplicație pe care îl definiți este un subset. Definiția registru sistem pe care o specificați trebuie să existe deja în EIM, altfel crearea unei definiții registru de aplicații eșuează.
    - c. Un tip definiție pentru registru.
    - d. O descriere a definiției registru de aplicație.
    - e. Unul sau mai multe alias-uri pentru definiția registru de aplicație, dacă este necesar.
  6. Faceți clic pe **Ajutor**, dacă este necesar, pentru a determina ce informații să fie furnizate pentru fiecare câmp.
  7. Apăsați clic pe **OK** pentru a salva informațiile și a adăuga definiția registru la domeniul EIM.

#### Concepte înrudite

“Definițiile de registru de sistem” la pagina 13

O definiție pentru registrul sistem este o intrare pe care o creați în EIM (Enterprise Identity Mapping) pentru a reprezenta și descrie un registru utilizator distinct într-o stație de lucru sau într-un server.

## Adăugarea unei definiții de registru grup

Pentru a crea o definiție pentru registrul grup, trebuie să fiți conectat la domeniul EIM în care doriți să lucrați și trebuie să aveți control acces administrator EIM.

Pentru a adăuga o definiție pentru registrul grup la un domeniu EIM, completați acești pași:

1. Expandați **Rețea** → **EIM (Enterprise Identity Mapping)** → **Gestionare domeniu**.
2. Selectați domeniul EIM în care vreți să lucrați.
  - a. Dacă domeniul EIM cu care doriți să lucrați nu este menționat sub Gestionare domeniu, vedeți Adăugarea unui domeniu EIM la Gestionare domeniu.
  - b. Dacă nu sunteți conectat curent la domeniul EIM în care vreți să lucrați, vedeți Conectarea la controlerul de domeniu EIM.
3. Expandați domeniul EIM la care sunteți conectat acum.
4. Faceți clic dreapta pe **Registre de utilizatori**, selectați **Adăugare registru**, apoi selectați **Grup**.
5. În dialogul Adăugare registru grup, furnizați informații despre definiția pentru registrul de grup, precum urmează:
  - a. Un nume pentru definiția pentru registrul grup.
  - b. Selectați **Membrii registru grup sunt sensibili la majuscule** dacă toți membrii definiției pentru registrul grup sunt sensibili la majuscule.
  - c. O descriere a unei definiții pentru registrul grup.
  - d. Unul sau mai multe aliasuri pentru definiția pentru registrul grup, dacă este necesar.
6. Faceți clic pe **Ajutor**, dacă este necesar, pentru a determina ce informații să fie furnizate pentru fiecare câmp.
7. Apăsați clic pe **OK** pentru a salva informațiile și a adăuga definiția registru la domeniul EIM.

## Adăugarea unui alias la o definiție de registru

Dumneavoastră sau un dezvoltator de aplicație, ați putea dori să specificați informații distinctive suplimentare pentru o definiție registru. Puteți face asta prin crearea unui alias pentru definiția registru. Dvs., sau alții, puteți folosi aliasul pentru definiția registru pentru a distinge mai bine un registru de utilizatori față de altul.

Acest suport alias permite programatorilor să scrie aplicații fără să trebuiască să știe dinainte numele definiției arbitrare pentru registrul EIM (Enterprise Identity Mapping) ales de administrator care desfășoară aplicația. Documentația

aplicației poate furniza administratorului EIM numele de alias pe care îl utilizează aplicația. Utilizând această informație, administratorul EIM poate atribui acest nume de alias definiției registrului EIM care reprezintă registrul de utilizatori real pe care administratorul dorește ca aplicația să îl utilizeze.

Pentru a adăuga un alias la o definiție registru, trebuie să fiți conectat la domeniul EIM în care vreți să lucrați și trebuie să aveți control de acces EIM la unul din următoarele nivele:

- Administrator registru.
- Administrator pentru registrele selectate (pentru registrul pe care îl modificați).
- Administrator EIM.

Pentru a adăuga un alias la definiție pentru registrul EIM, efectuați acești pași:

1. Expandați **Rețea > EIM (Enterprise Identity Mapping) > Gestionare domeniu**.
2. Selectați domeniul EIM în care vreți să lucrați.
  - Dacă domeniul EIM cu care doriți să lucrați nu este listat sub Gestionare domeniu, vedeți “Adăugarea unui domeniu EIM la folderul Gestionare domeniu” la pagina 86.
  - Dacă nu sunteți conectat momentan la domeniul EIM în care vreți să lucrați, vedeți “Conectarea la domeniul EIM” la pagina 86.
3. Expandați domeniul EIM la care sunteți conectat acum.
4. Apăsați clic pe **Registre de utilizatori** pentru a afișa lista definițiilor registru din domeniu.

**Notă:** Dacă aveți Administrator pentru controlul acces la registre, lista conține doar acele definiții registru la care sunteți autorizat specific.

5. Faceți clic dreapta pe definiția de registru pentru care vreți să adăugați un alias și selectați **Proprietăți**.
6. Selectați pagina **Alias-uri** și specificați numele și tipul de alias pe care doriți să îl adăugați.

**Notă:** Puteți specifica un tip alias pe care nu îl includeți în lista de tipuri.

7. Apăsați clic pe **Ajutor**, dacă este necesar, pentru a determina ce informații să specificați pentru fiecare câmp.
8. Selectați **Adăugare**.
9. Apăsați clic pe **OK** pentru a salva modificările la definiția de registru.

## Definirea tipului de registru de utilizatori privat în EIM

Când creați o definiție registru EIM (Enterprise Identity Mapping) puteți specifica unul din numerele de tipuri de registru de utilizatori predefinite pentru a reprezenta un registru de utilizatori actual care există pe un sistem din întreprindere.

Tipurile de definiții registru predefinite acoperă unele registre de utilizatori sistem de operare, s-ar putea să fie nevoie să creați o definiție registru pentru fiecare EIM care nu include un tip registru predefinit. În această situație aveți două opțiuni. Puteți, fie să folosiți o definiție de registru care se potrivește cu caracteristicile registrului dumneavoastră de utilizatori sau puteți defini un tip de registru de utilizatori privat.

Pentru a defini un tip de registru de utilizatori pe care EIM nu este predefinit să-l recunoască, trebuie să folosiți o identitate obiect (OID) ca să specificați tipul registrului în formularul **ObjectIdentifier-normalization**, unde **ObjectIdentifier** este un identificator obiect zecimal cu puncte, cum ar fi 1.2.3.4.5.6.7 și **normalization** este fie valoare **caseExact**, fie valoarea **caseIgnore**. De exemplu, identificatorul obiect (OID) pentru System i este 1.3.18.0.2.33.2-caseIgnore.

Pentru a vă asigura că folosiți și creați OID-uri unice trebuie să obțineți toate OID-urile de care aveți nevoie de la autorități de înregistrare OID legale. OID-urile unice vă ajută să evitați conflictele potențiale cu OID-urile create de către alte organizații sau aplicații.

Există două moduri de a obține OID-uri.

- **Înregistrați obiectele la o autoritate.** Această metodă este o alegere bună atunci când aveți nevoie de un număr mic de OID-uri fixe pentru a reprezenta informația. De exemplu, acele OID-uri ar putea să reprezinte politici de certificate pentru utilizatorii din întreprinderea dumneavoastră.
- **Obțineți o alocare de arc de la o autoritate de înregistrare și alocați OID-urile dumneavoastră după necesități.** Această metodă, care este o alocare a unui interval de identificatoare obiect zecimale cu punct, este o bună alegere dacă aveți nevoie de un număr mare de OID-uri sau dacă este posibil ca alocările dumneavoastră OID să se schimbe. Alocarea arc constă din numerele de început din notația zecimală cu punct pe care trebuie să vă bazați **IdentificatorObiect**. De exemplu, alocarea arc ar putea fi 1.2.3.4.5.. Ați putea crea apoi OID-uri prin adăugarea la acest arc de bază. De exemplu, ați putea crea OID-uri sub forma 1.2.3.4.5.x.x).

Puteți învăța mai multe despre înregistrare OID-urilor dumneavoastră cu o autoritate de înregistrare prin consultarea acestor resurse Internet:

- American National Standards Institute (ANSI) este autoritatea de înregistrare pentru Statele Unite pentru nume de organizații aflate sub incidența procesului de înregistrare globală stabilit de către ISO (International Standards Organization) și ITU (International Telecommunication Union). Un formular în format Microsoft Word despre aplicarea pentru un RID (Registered Application Provider Identifier) se află pe situl web ANSI Public Document Library <http://public.ansi.org/ansionline/Documents/> . Puteți găsi foaia de întâmplări selectând **Alte servicii > Programe de înregistrare**. Arcul ANSI OID pentru organizații este 2.16.840.1. ANSI taxează pentru alocările de arc OID. Durează aproximativ două săptămâni pentru a primi un arc OID alocat de la ANSI. ANSI va alocă un număr (NEWNUM) pentru a crea un nou arc OID; de exemplu: 2.16.840.1.NEWNUM.
- În cele mai multe țări sau regiuni, asociația națională de standarde întreține un registru OID. Cât despre arcurile ANSI, acestea sunt în general alocate sub OID 2.16. Ar putea fi nevoie de anumite investigații pentru a găsi autoritatea OID pentru o anumită țară sau regiune. Adresele pentru corpurile de membru naționale ISO pot fi găsite la [http://www.wssn.net/WSSN/listings/links\\_national.html](http://www.wssn.net/WSSN/listings/links_national.html) . Informațiile includ adresa poștală și adresă de poștă electronică. În cele mai multe cazuri, este specificat și un sit Web.
- IANA (Internet Assigned Numbers Authority) alocă numere întreprinderilor private, care sunt OID-uri, în arcul 1.3.6.1.4.1. IANA a alocat arcuri la peste 7500 de companii până acum. Pagina de aplicare este localizată la <http://www.iana.org/cgi-bin/enterprise.pl> , sub Numere întreprindere private. De obicei, cu IANA, alocarea durează o săptămână. Un OID de la IANA este gratuit. IANA va alocă un număr (NEWNUM), astfel încât noul arc OID va fi 1.3.6.1.4.1.NEWNUM.
- Guvernul Federal al Statelor Unite întreține CSOR (Computer Security Objects Registry). CSOR este autoritatea care denumește arcul 2.16.840.1.101.3 și în prezent înregistrează obiectele pentru etichetele de securitate, algoritmi criptografici și politici de certificate. Politicile de certificate OID sunt definite în arcul 2.16.840.1.101.3.2.1. CSOR furnizează OID-uri agențiilor Guvernului Federal al Statelor Unite. Pentru informații suplimentare despre CSOR, consultați <http://www.csrc.nist.gov/pki/CSOR/csor.html> .

#### Concepte înrudite

“Definițiile de registru EIM” la pagina 11

O definiție registru EIM (Enterprise Identity Mapping) este o intrare în EIM pe care o creați pentru a reprezenta un registru de utilizatori real, care există pe un sistem în întreprindere. Un registru de utilizatori funcționează asemănător unui director care conține o listă a identităților utilizator valide pentru un anumit sistem sau pentru o anumită aplicație.

## Activarea suportului de căutare mapare și a utilizării asocierilor de politică pentru un registru destinație

Suportul politică de mapare EIM (Enterprise Identity Mapping) vă permite să utilizați asocieri de politică ca un mijloc de creare mapări multe-la-unul în situații unde asocieri între identități utilizator și un identificator EIM nu există. Puteți folosi o asociere de politică pentru a mapa un set sursă de identități de utilizator (în loc de o singură identitate de utilizator) la o unică identitate destinație de utilizator dintr-un registru de utilizatori destinație, specificat.

Pentru a putea folosi asocieri de politică, trebuie însă mai întâi să vă asigurați că activați căutările de mapare folosind asocieri de politică pentru domeniu. De asemenea, trebuie să activați una sau două setări pentru fiecare registru:

- **Activare căutări mapare pentru registru** Selectați această opțiune pentru a asigura că registrul poate participa la operațiile de căutare mapare EIM, indiferent dacă registrul are vreo asociere de politică definită pentru el.
- **Folosire asocieri de politică** Selectați această opțiune pentru a permite acestui registru să fie registrul destinație al asocierii de politică și a asigura că poate participa la operațiile de căutare EIM.

Dacă nu activați căutările de mapare pentru registru, acesta nu poate participa deloc la operațiile de căutare mapare EIM. Dacă nu specificați faptul că registrul folosește asocieri de politică, operațiile de căutare mapare EIM ignoră toate asocierile de politică pentru acel registru atunci când acesta este destinația operației.

Pentru a activa căutările de mapare să utilizeze asocieri de politică pentru un registru destinație, trebuie să fiți conectat la domeniul EIM în care vreți să lucrați și să aveți “Controlul accesului în EIM” la pagina 38 la unul dintre următoarele niveluri:

- Administrator EIM
- Administrator de registru
- Administrator pentru registre selectate (pentru registrul pe care vreți să-l activați)

Pentru a activa suportul de căutare mapare în general și folosirea asocierilor de politică în particular pentru un registru destinație, parcurgeți pașii următori:

1. Expandați **Rețea > EIM (Enterprise Identity Mapping) > Gestionare domeniu**.
2. Selectați domeniul EIM în care vreți să lucrați.
  - Dacă domeniul EIM cu care vreți să lucrați nu este listat sub **Gestionare domeniu**, vedeți “Adăugarea unui domeniu EIM la folderul Gestionare domeniu” la pagina 86.
  - Dacă nu sunteți conectat curent la domeniul EIM în care vreți să lucrați, vedeți Conectarea la controlerul de domeniu EIM.
3. Selectați **Registre de utilizatori** pentru a afișa lista cu definițiile de registru pentru domeniu.

**Notă:** Dacă aveți controlul de acces Administrator pentru registre selectate, lista conține numai definițiile de registru pentru care sunteți autorizat în mod specific.

4. Faceți clic dreapta pe definiția registru pentru care vreți să activați suportul de politică mapare pentru asocieri de politică și selectați **Politică mapare**
5. În pagina **General**, selectați **Activare căutări mapare pentru registru**. Dacă selectați această opțiune, permiteți registrului să participe la operațiile de căutare mapare EIM. Dacă această opțiune nu este selectată, o operație de căutare nu poate returna date pentru registru, indiferent dacă registrul este sursă sau destinație în operația de căutare.
6. Selectați **Folosire asocieri de politică**. Dacă selectați această opțiune, permiteți operațiilor de căutare să utilizeze asocierile de politică drept bază pentru returnarea datelor când registrul este destinația operației de căutare.
7. Faceți clic **OK** pentru a vă salva modificările.

**Notă:** Pentru ca un registru să poată folosi asocieri de politică, trebuie de asemenea să vă asigurați că activați asocierile de politică pentru un domeniu.

#### Concepte înrudite

“Suportul pentru politica EIM și activarea” la pagina 37

Suportul politicii de mapare EIM (Enterprise Identity Mapping) vă permite să folosiți asocieri de politică precum și asocieri identificator specifice într-un domeniu EIM. Puteți folosi asocierile de politică în locul sau în combinație cu asocierile identificator.

## Ștergerea unei definiții de registru

Când ștergeți o definiție registru dintr-un domeniu EIM (Enterprise Identity Mapping) nu afectați registrul de utilizatori la care definiția de registru se referă, dar acel registru de utilizatori nu mai poate participa în domeniul EIM.

Trebuie să luați în considerare aceste lucruri când ștergeți o definiție registru:

- Când ștergeți o definiție de registru, pierdeți toate asocierile pentru acel registru de utilizatori. Dacă redefiniți registrul la un domeniu, trebuie să creați orice asocieri necesare din nou.
- Când ștergeți o definiție de registru X.509, pierdeți de asemenea toate filtrele certificate definite pentru acest registru. Dacă redefiniți registrul X.509 la un domeniu, trebuie să creați niște filtre certificate din nou.
- Nu puteți șterge o definiție de registru sistem dacă acolo există definiții de registru care specifică definiția de registru sistem ca un registru părinte.

Pentru a șterge o definiție registru, trebuie să fiți conectat la domeniul EIM în care vreți să lucrați și trebuie să aveți control acces administrator EIM.

Pentru a șterge o definiție de registru EIM, efectuați acești pași:

1. Expandați **Rețea > EIM (Enterprise Identity Mapping) > Gestionare domeniu**.
2. Selectați domeniul EIM în care doriți să lucrați.
  - Dacă domeniul EIM cu care vreți să lucrați nu este listat sub **Gestionare domeniu**, vedeți “Adăugarea unui domeniu EIM la folderul Gestionare domeniu” la pagina 86.
  - Dacă nu sunteți conectat curent la domeniul EIM în care vreți să lucrați, vedeți Conectarea la controlerul de domeniu EIM.
3. Expandați domeniul EIM la care sunteți conectat acum.
4. Faceți clic pe **Registreele de utilizatori** pentru a afișa o listă cu definiții de registru din domeniu.

**Notă:** Dacă aveți Administrator pentru controlul accesului registrelor selectate, lista conține doar acele definiții de registru pentru care sunteți autorizat.

5. Faceți clic dreapta pe registrul de utilizatori pe care vreți să îl ștergeți și selectați **Ștergere**.
6. Faceți clic pe **Da** în fereastra **Confirmare** pentru a șterge definiția registrului.

## Înlăturarea unui alias din identificatorul de registru

Pentru a înlătura un alias de la o definiție registru EIM (Enterprise Identity Mapping), trebuie să fiți conectat la domeniul EIM în care vreți să lucrați și trebuie să aveți control acces EIM ca administrator registru, Administrator pentru registrele selectate sau administrator EIM.

Pentru a înlătura un alias de la o definiție registru EIM, finalizați acești pași:

1. Expandați **Rețea > EIM (Enterprise Identity Mapping) > Gestionare domeniu**.
2. Selectați domeniul EIM în care vreți să lucrați
  - Dacă domeniul EIM cu care vreți să lucrați nu este listat sub **Gestionare domeniu**, vedeți “Adăugarea unui domeniu EIM la folderul Gestionare domeniu” la pagina 86.
  - Dacă nu sunteți conectat curent la domeniul EIM în care vreți să lucrați, vedeți Conectarea la controlerul de domeniu EIM.
3. Expandați domeniul EIM la care sunteți conectat acum.
4. Faceți clic pe **Registreele de utilizatori** pentru a afișa o listă cu definiții de registru din domeniu.

**Notă:** Dacă aveți Administrator pentru controlul accesului registrelor selectate, lista conține doar acele definiții de registru pentru care sunteți autorizat.

5. Faceți clic dreapta pe o definiție registru și selectați **Proprietăți**.
6. Selectați pagina **Alias**.
7. Selectați un alias pe care vreți să-l înlăturați și apăsați **Înlăturare**.
8. Apăsați **OK** pentru a salva modificările.

## Adăugarea unui membru la o definiție de registru grup

Pentru a adăuga un membru la o definiție registru grup, trebuie să fiți conectat la domeniul EIM în care doriți să lucrați și trebuie să aveți control de acces EIM ca administrator EIM, Administrator registru, Administrator pentru registrele selectate (pentru ambele definiții registru de grup la care vreți să adăugați membrul și la membrul individual pe care vreți să îl adăugați).

Pentru a adăuga un membru definiției pentru registrul grup, completați acești pași:

1. **Expandare rețea → EIM (Enterprise Identity Mapping) → Gestionare domeniu.**
2. Selectați domeniul EIM în care vreți să lucrați.
  - a. Dacă domeniul EIM cu care doriți să lucrați nu este menționat sub Gestionare domeniu, vedeți Adăugarea unui domeniu EIM la Gestionare domeniu.
  - b. Dacă nu sunteți conectat curent la domeniul EIM în care vreți să lucrați, vedeți Conectarea la controlerul de domeniu EIM.
3. Expandați domeniul EIM la care sunteți conectat acum.
4. Faceți clic pe **Registre de utilizatori** pentru a afișa lista de definiții pentru registrele din domeniu.
5. Faceți clic dreapta pe definiția pentru registru de grup la care vreți să adăugați un membru și selectați **Proprietăți**.
6. Selectați pagina **Membri** și faceți clic pe **Adăugare**.
7. În dialogul **Adăugare membri la registru grup EIM**, selectați una sau mai multe definiții pentru registru și faceți clic pe **OK**. Conținutul listei variază în funcție de tipul de control acces EIM pe care îl aveți și este restricționat pentru definițiile pentru registru cu aceeași sensibilitate la majuscule ca ceilalți membri ai grupului.
8. Faceți clic pe **OK** pentru a ieși.

## Gestionarea identificatorilor EIM

Utilizați aceste informații pentru a afla cum să creați și să gestionați identificatorii EIM (Enterprise Identity Mapping) pentru un domeniu.

Crearea și utilizarea identificatorilor EIM care reprezintă utilizatorii din rețeaua dumneavoastră pot fi foarte folositori pentru a vă ajuta să urmăriți care persoană deține o identitate utilizator particulară. Utilizatorii din întreprindere se schimbă tot timpul, unii vin, alții pleacă și alții se mută între diferite zone din întreprindere. Aceste schimbări se adaugă la problema administrativă continuă a urmării identității utilizatorilor și a parolilor pentru sisteme și aplicații în rețea. În plus, gestiunea parolilor necesită mult timp pentru o întreprindere. Prin crearea identificatorilor EIM și asocierea lor cu identitățile utilizatorului pentru fiecare utilizator, puteți urmări cine deține o identitate a utilizatorului specifică. În acest fel, gestiunea parolei devine mult mai facilă.

Implementarea unui mediu de semnare unică face procesul de gestionare a identităților utilizator mai ușor și pentru utilizatori de asemenea, în special când se mută la alt departament sau zonă din întreprindere. Activarea semnării unice poate elimina cerința pentru acești utilizatori să țină minte noile nume utilizator și parole pentru sisteme noi.

**Notă:** Cum să creați și să folosiți identificatorii EIM depinde de nevoile organizației dumneavoastră. Pentru a afla mai multe, consultați “Dezvoltarea unui plan de numire identificatori EIM” la pagina 63.

Puteți gestiona identificatorii EIM pentru orice domeniu care este disponibil sub folderul **Gestiunea domeniului** Puteți realiza oricare dintre următoarele operații pentru a gestiona identificatorii EIM într-un domeniu EIM

### Informații înrudite

Semnare unică

## Crearea unui identificator EIM

Pentru a crea un identificator EIM, trebuie să fiți conectat la domeniul EIM (Enterprise Identity Mapping) în care vreți să lucrați și trebuie să aveți control acces EIM ca și administrator identificator administrator sau administrator EIM.

Pentru a crea un identificator EIM pentru o persoană sau pentru o entitate din întreprinderea dumneavoastră, efectuați acești pași:

1. Expandați **Rețea > EIM (Enterprise Identity Mapping) > Gestionare domeniu**.
2. Selectați domeniul EIM în care doriți să lucrați.
  - Dacă domeniul EIM cu care vreți să lucrați nu este listat sub **Gestionare domeniu**, vedeți “Adăugarea unui domeniu EIM la folderul Gestionare domeniu” la pagina 86.
  - Dacă nu sunteți conectat momentan la domeniul EIM în care vreți să lucrați, vedeți “Conectarea la domeniul EIM” la pagina 86.
3. Expandați domeniul EIM la care sunteți conectat acum.
4. Faceți clic dreapta pe **Identificatori** și selectați **Identificator nou**.
5. În fereastra de dialog **Identificator nou EIM**, primiți informații despre identificatorul EIM, după cum urmează:
  - a. Un nume pentru identificator.
  - b. Pentru ca sistemul să genereze un nume unic, dacă este necesar.
  - c. O descriere a identificatorului.
  - d. Unul sau mai multe alias-uri pentru identificator, dacă este necesar.
6. Faceți clic pe **Ajutor**, dacă este necesar, pentru a determina ce informații să specificați pentru fiecare câmp.
7. După ce introduceți informațiile necesare, apăsați **OK** pentru a crea identificatorul EIM.

**Notă:** Dacă creați un număr mare de identificatori, asta ia uneori mult timp înainte ca lista afișării identificatorilor când expandați folderul **Identificatori**. Pentru a îmbunătăți performanța când aveți un număr mare de identificatori EIM, consultați “Personalizarea vizualizării de identificatori EIM” la pagina 100.

## Adăugarea unui alias la un identificator EIM

S-ar putea să vreți să creați un alias pentru a furniza informații distinctive suplimentare pentru un identificator EIM. Aliasurile pot ajuta în localizarea unui anumit identificator EIM când realizați o operație de căutare EIM. De exemplu, aliasurile pot fi de ajutor în situații unde numele legal al cuiva este diferit de numele persoanei sub care este cunoscut.

Numele de identificatori EIM trebuie să fie unice în cadrul unui domeniu EIM. Alias-urile pot ajuta în situațiile de adresare unde utilizarea de nume de identificatori unice poate fi dificilă. De exemplu, persoane diferite din cadrul unei întreprinderi pot împărtăși același nume, ceea ce poate fi confuz dacă utilizați numele proprii ca identificatori EIM. De exemplu, dacă aveți doi utilizatori numiți John J. Johnson, ați putea crea un alias al lui John Joseph Johnson și un alias al lui John Jeffrey Johnson pentru a face mai ușoară deosebirea între identitățile fiecărui utilizator. De exemplu, alias-urile suplimentare pot conține numărul de angajat, numărul departamentului, profesia fiecărui utilizator sau un alt atribut distinctiv.

Pentru a adăuga un alias la un identificator EIM, trebuie să fiți conectat la un domeniu EIM în care doriți să lucrați și trebuie să aveți “Controlul accesului în EIM” la pagina 38 unul din următoarele niveluri:

- Administrator EIM.
- Administrator identificator.

Pentru a adăuga un alias la un identificator EIM, efectuați acești pași.

1. Expandați **Rețea > EIM (Enterprise Identity Mapping) > Gestionare domeniu**.
2. Selectați domeniul EIM în care doriți să lucrați.
  - Dacă domeniul EIM cu care vreți să lucrați nu este listat sub **Gestionare domeniu**, vedeți “Adăugarea unui domeniu EIM la folderul Gestionare domeniu” la pagina 86.
  - Dacă nu sunteți conectat momentan la domeniul EIM în care vreți să lucrați, vedeți “Conectarea la domeniul EIM” la pagina 86.
3. Expandați domeniul EIM la care sunteți conectat acum.
4. Faceți clic pe **Identificatori** pentru a afișa, în panoul din dreapta, o listă de identificatori EIM disponibili în domeniu.



**Notă:** Uneori când doriți să expandați folderul **Identificatori** , acesta poate lua mult timp înainte ca lista identificatorilor să fie afișată. Pentru a îmbunătăți performanța când aveți un număr mare de identificatori EIM în domeniu, consultați “Personalizarea vizualizării de identificatori EIM” la pagina 100.

5. Faceți clic dreapta pe identificatorul EIM pentru care doriți să adăugați un alias și selectați **Proprietăți**.
6. În câmpul **Alias** , specificați numele aliasului pe care doriți să îl adăugați la acest identificator EIM și apăsați **Adăugare**.
7. Faceți clic pe **OK** pentru a salva modificările identificatorului dumneavoastră EIM.

## Înlăturarea unui alias din identificatorul EIM

Pentru a înlătura un alias de la un identificator EIM (Enterprise Identity Mapping), trebuie să fiți conectat la domeniul EIM în care vreți să lucrați și trebuie să aveți control acces EIM ca și administrator identificator sau administrator EIM.

Pentru a șterge un alias dintr-un identificator EIM, efectuați acești pași:

1. Expandați **Rețea > EIM (Enterprise Identity Mapping) > Gestionare domeniu**.
2. Selectați domeniul EIM în care doriți să lucrați.
  - Dacă domeniul EIM cu care vreți să lucrați nu este listat sub **Gestionare domeniu**, vedeți “Adăugarea unui domeniu EIM la folderul Gestionare domeniu” la pagina 86.
  - Dacă nu sunteți conectat momentan la domeniul EIM în care vreți să lucrați, vedeți “Conectarea la domeniul EIM” la pagina 86.
3. Expandați domeniul EIM la care sunteți conectat acum.
4. Faceți clic pe **Identificatori** pentru a afișa, în panoul din dreapta, o listă de identificatori EIM disponibili în domeniu.

**Notă:** Uneori când doriți să expandați folderul **Identificatori** , acesta poate lua mult timp înainte ca lista identificatorilor să fie afișată. Pentru a îmbunătăți performanța când aveți un număr mare de identificatori EIM în domeniu, consultați “Personalizarea vizualizării de identificatori EIM” la pagina 100.

5. Faceți clic dreapta pe identificatorul EIM pentru care doriți să adăugați un alias și selectați **Proprietăți**.
6. Selectați un alias pe care vreți să-l înlăturați și apăsați **Înlăturare**.
7. Faceți clic **OK** pentru a vă salva modificările.

## Ștergerea unui identificator EIM

Pentru a șterge un identificator EIM, trebuie să fiți conectat la EIM (Enterprise Identity Mapping) în care vreți să lucrați și trebuie să aveți control acces administrator EIM.

Pentru a șterge un identificator EIM, efectuați acești pași:

1. Expandați **Rețea > EIM (Enterprise Identity Mapping) > Gestionare domeniu**.
2. Selectați domeniul EIM în care vreți să lucrați.
  - Dacă domeniul EIM cu care vreți să lucrați nu este listat sub **Gestionare domeniu**, vedeți “Adăugarea unui domeniu EIM la folderul Gestionare domeniu” la pagina 86.
  - Dacă nu sunteți conectat curent la domeniul EIM în care vreți să lucrați, vedeți Conectarea la controlerul de domeniu EIM.
3. Expandați domeniul EIM la care sunteți conectat acum.
4. Apăsați **Identificatori**.

**Notă:** Uneori când doriți să expandați folderul **Identificatori** , acesta poate lua mult timp înainte ca lista identificatorilor să fie afișată. Pentru a îmbunătăți performanța când aveți un număr mare de identificatori EIM în acest domeniu, puteți să “Personalizarea vizualizării de identificatori EIM” la pagina 100.

5. Selectați identificatorul EIM pe care doriți să îl ștergeți. Pentru a șterge identificatori multipli, apăsați tasta **Ctrl** atunci când selectați identificator EIM.
6. Faceți clic dreapta pe identificatorii EIM selectați și selectați **Ștergere** .

7. În fereastra dialog **Confirmarea ștergerii**, apăsați **Da** pentru a șterge identificatorul EIM selectat.

## Personalizarea vizualizării de identificatori EIM

Câteodată când încercați să expandați folderul Identificatori, ar putea să dureze mult până lista de identificatori se afișează. Pentru a îmbunătăți performanța când aveți un număr mare de identificatori EIM (Enterprise Identity Mapping) în domeniu, puteți personaliza vizualizarea folderului Identificatori.

Pentru a personaliza vederea folderului **Identificatori**, urmați acești pași:

1. Expandați **Rețea** → **EIM (Enterprise Identity Mapping)** → **Gestionare domeniu**.
2. Selectați domeniul EIM în care doriți să lucrați.
  - Dacă domeniul EIM cu care vreți să lucrați nu este listat sub **Gestionare domeniu**, vedeți “Adăugarea unui domeniu EIM la folderul Gestionare domeniu” la pagina 86.
  - Dacă nu sunteți conectat momentan la domeniul EIM în care vreți să lucrați, vedeți “Conectarea la domeniul EIM” la pagina 86.
3. Faceți clic dreapta pe folderul **Identificatori** și selectați **Personalizarea aceste vizualizări**.
4. Specificați criteriul pe care doriți îl folosiți pentru a afișa identificatori EIM în domeniu. Pentru a limita numărul de identificatori EIM, specificați caracterele pe care doriți să le folosiți pentru sortarea identificatorilor. Puteți specifica unul sau mai multe caractere de înlocuire (\*) în numele identificator. De exemplu, ați putea introduce \*JOHNSON\* ca și criteriu de căutare în câmpul **Identificatori**. Rezultatele vor întoarce toți identificatorii EIM unde șirul de caractere JOHNSON este definit ca parte numelui identificator EIM și va întoarce de asemenea identificatori EIM unde șirul de caractere JOHNSON este definit ca parte a aliasului pentru un identificator EIM.
5. Apăsați clic pe **OK** pentru a vă salva modificările.

## Gestionarea asocierilor EIM

EIM vă permite să creați și gestiona două feluri de asocieri, care definesc direct sau indirect relații între identități utilizator: asocieri identificator și asocieri de politică. EIM vă permite să creați și să gestionați asocieri identificator între identificatorii EIM și identitățile lor utilizator, ce vă permit să definiți indirect, dar specific, relații individuale între identități utilizator.

EIM vă permite de asemenea să creați asocieri de politică pentru a descrie o relație între identități utilizator multiple în unul sau mai multe registre și o identitate utilizator destinație individuală în alt registru. Asocierile de politică folosesc suport pentru politica de mapare EIM pentru a crea mapări multe-la-una între identități utilizator fără a invoca un identificator EIM. Deoarece ambele tipuri de asocieri definesc legături între identități utilizator dintr-o întreprindere, gestionarea asocierilor este un element important în gestiunea EIM.

Gestionarea asocierilor într-un domeniu este cheia pentru a simplifica task-urile administrative necesare pentru a păstra urma la care utilizatori au conturi și sisteme variate în rețea. Trebuie să țineți asocierile identificator și asocierile de politică curente când implementați o semnare rețea unică sigură.

Puteți executa următoarele operații de management pentru asocieri:

### Crearea asocierilor EIM

Sunt două tipuri de asocieri EIM pe care le puteți crea. Puteți crea fie o asociere identificator sau o asociere de politică.

Puteți crea o asociere identificator pentru a defini o relație între două identități de utilizator pe care un singur utilizator le utilizează. O asociere identificator descrie o relație între un identificator EIM și o identitate utilizator într-un registru de utilizatori. Asocierile identificator vă permit să creați mapări una la una între un identificator EIM și fiecare din identitățile utilizator diverse ce sunt înrudite cu utilizatorul care identificatorul EIM îl reprezintă.

Puteți crea o asociere de politică pentru a defini direct o relație între identități multiple de utilizator într-un registru sau mai mulți și o identitate utilizator individuală în alt registru. Asocierile de politică folosesc suport pentru politica de mapare EIM pentru a crea mapări multe-la-una între identități utilizator fără a invoca un identificator EIM. Asocierile de politică vă permit să creați rapid un mare număr de mapări între identitățile utilizator înrudite în registrele de utilizatori diferite.

Dacă ați ales să creați asocieri de identificator, creați asocieri de politică sau folosiți o legătură între cele două metode în funcție de nevoile de implementare EIM.

#### **Concepte înrudite**

“Dezvoltarea unui plan de mapare identități” la pagina 60

O parte critică a procesului de planificare a implementării EIM (Enterprise Identity Mapping) cere să determinați cum vreți să folosiți maparea identității în întreprinderea dumneavoastră.

“Crearea unei asocieri de politică” la pagina 102

O asociere de politică furnizează un mod de a defini o relație dintre mai multe identități de utilizatori din unul sau mai multe registre și o identitate de utilizator unică în alt registru.

#### **Operații înrudite**

“Crearea unei asocieri de identificator EIM”

Asocierile de identificator definesc o relație într-un identificator EIM (Enterprise Identity Mapping) și o identitate de utilizator în întreprinderea dumneavoastră pentru persoana sau entitatea la care identificatorul EIM se referă.

#### **Crearea unei asocieri de identificator EIM:**

Asocierile de identificator definesc o relație într-un identificator EIM (Enterprise Identity Mapping) și o identitate de utilizator în întreprinderea dumneavoastră pentru persoana sau entitatea la care identificatorul EIM se referă.

Puteți crea trei tipuri de asocieri de identificatori: destinație, sursă și administrativ. Pentru a preveni problemele potențiale cu asocierile și cum mapează ele identitățile, vedeți “Dezvoltarea unui plan de mapare identități” la pagina 60.

Pentru a crea o asociere de identificator, trebuie să fiți conectat la domeniul EIM în care vreți să lucrați și trebuie să aveți controlul de acces EIM cerut de tipurile de asocieri pe care vreți să le creați.

Pentru a crea o asociere sursă sau administrativă, trebuie să aveți control de acces la EIM la unul din următoarele niveluri:

- Administrator de identificatori.
- Administrator EIM.

Pentru a crea o asociere destinație, trebuie să aveți control de acces la EIM la unul din următoarele niveluri:

- Administrator de registru
- Administrator pentru registrele selectate (pentru definiția de registru care se referă la registrul de utilizatori care conține identitatea de utilizator destinație)
- Administrator EIM.

Pentru a crea o asociere de identificator, realizați acești pași:

1. Expandați **Rețea > EIM (Enterprise Identity Mapping) > Gestionare domeniu**.
2. Selectați domeniul EIM în care vreți să lucrați.
  - Dacă domeniul EIM cu care vreți să lucrați nu este listat sub **Gestionare domeniu**, vedeți “Adăugarea unui domeniu EIM la folderul Gestionare domeniu” la pagina 86.
  - Dacă nu sunteți conectat momentan la domeniul EIM în care vreți să lucrați, vedeți “Conectarea la domeniul EIM” la pagina 86.
3. Expandați domeniul EIM la care sunteți conectat acum.
4. Faceți clic pe **Identificatori** pentru a afișa lista de identificatori EIM pentru domeniu.

**Notă:** Uneori când încercați să expandați folderul **Identificatori**, poate trece un timp mai îndelungat până se afișează lista cu identificatori. Pentru a îmbunătăți performanța când aveți un număr mare de identificatori EIM în domeniu, consultați “Personalizarea vizualizării de identificatori EIM” la pagina 100.

5. Faceți clic dreapta pe identificatorul EIM pentru care vreți să creați o asociere și selectați **Proprietăți...**
6. Selectați pagina **Asocieri** și faceți clic pe **Adăugare...**

7. În pagina **Adăugare asociere**, furnizați informații pentru a defini asocierea, după cum urmează:
  - Numele registrului care conține identitatea de utilizator pe care vreți să o asociați cu identificatorul EIM. Specificați numele exact al unei definiții de registru existente sau răsfoiți pentru a selecta una.
  - Numele identității de utilizator pe care vreți să o asociați cu identificatorul EIM.
  - Tipul asocierii. Puteți crea trei tipuri diferite de asocieri.
    - Administrativă
    - Sursă
    - Destinație
8. Faceți clic pe **Ajutor** pentru a determina ce informații să specificați pentru fiecare câmp.
9. Opțional. Pentru asocierea destinație, faceți clic pe **Avansat...** pentru a afișa dialogul **Adăugare asociere - Avansat**. Specificați informațiile de căutare pentru identitatea de utilizator destinație și faceți clic pe **OK** pentru a vă întoarce la dialogul **Adăugare asociere**.
10. După ce ați furnizat informațiile necesare, faceți clic pe **OK** pentru a crea asocierea.

#### **Concepte înrudite**

“Crearea asocierilor EIM” la pagina 100

Sunt două tipuri de asocieri EIM pe care le puteți crea. Puteți crea fie o asociere identificator sau o asociere de politică.

#### **Crearea unei asocieri de politică:**

O asociere de politică furnizează un mod de a defini o relație dintre mai multe identități de utilizatori din unul sau mai multe registre și o identitate de utilizator unică în alt registru.

Asocierile de politică utilizează suportul politică de mapare EIM (Enterprise Identity Mapping) pentru a crea mapări multe-la-unu între identitățile utilizator fără să implice un identificator EIM. Deoarece puteți utiliza asocierile de politică într-o varietate de moduri de suprapunere, trebuie să aveți o înțelegere bună a suportului politicii de mapare EIM înainte să creați și să utilizați asocierile de politică. De asemenea, pentru a împiedica problemele potențiale cu asocieri și cum mapează identități, trebuie să dezvoltați un plan de mapare identitate general pentru întreprinderea dumneavoastră înainte să începeți să definiți asocieri.

Dacă alegeți să creați asocieri de identificatori, să creați asocieri de politică sau să folosiți un amestec din amândouă metodele, totul depinde de nevoile dumneavoastră de implementare EIM.

Cum creați o asociere de politică depinde de tipul de asociere de politică. Pentru a afla mai multe despre cum să creați o asociere de politică, vedeți:

#### **Concepte înrudite**

“Gestionarea definițiilor de registre EIM” la pagina 91

Pentru ca registrele de utilizatori și identitățile utilizator pe care le conțin să participe într-un domeniu EIM trebuie să creați definiții registru pentru ele. Puteți gestiona modul în care registrele de utilizator și identitățile lor de utilizator participă în EIM prin gestionarea acestor definiții de registru EIM.

“Crearea asocierilor EIM” la pagina 100

Sunt două tipuri de asocieri EIM pe care le puteți crea. Puteți crea fie o asociere identificator sau o asociere de politică.

“Suportul pentru politica EIM și activarea” la pagina 37

Suportul politicii de mapare EIM (Enterprise Identity Mapping) vă permite să folosiți asocieri de politică precum și asocieri identificator specifice într-un domeniu EIM. Puteți folosi asocierile de politică în locul sau în combinație cu asocierile identificator.

“Dezvoltarea unui plan de mapare identități” la pagina 60

O parte critică a procesului de planificare a implementării EIM (Enterprise Identity Mapping) cere să determinați cum vreți să folosiți maparea identității în întreprinderea dumneavoastră.

*Crearea unei asocieri politice de domeniu implicită:*

Pentru a crea o asociere politică domeniu implicită, trebuie să fiți conectat la domeniul EIM (Enterprise Identity Mapping) în care vreți să lucrați și trebuie să aveți control acces EIM la fie administrator EIM sau administrator registru.

O asociere de politică descrie o relație între mai multe identități de utilizatori și o singură identitate de utilizator destinație într-un registru de utilizatori destinație. Puteți folosi o asociere de politică pentru a descrie o relație între un set de mai multe identități de utilizatori sursă și o singură identitate de utilizator destinație într-un registru de utilizatori destinație specificat. Asocierile de politică folosesc suport pentru politica de mapare EIM pentru a crea mapări multe-la-una între identități utilizator fără a invoca un identificator EIM.

**Notă:** Deoarece puteți folosi asocieri de politică într-o varietate de moduri care se suprapun, aveți nevoie de o înțelegere temeinică a suportului politicii de mapare EIM, înainte de a crea și folosi asocierile de politică. De asemenea, pentru a preveni apariția problemelor legate de asocieri și de modul în care acestea mapează identitățile, trebuie să elaborați un plan general de mapare a identităților din întreprinderea dumneavoastră înainte de a începe să definiți asocierile.

Într-o asociere de politică domeniu implicită, toți utilizatorii din domeniu sunt sursa asocierii de politică și sunt mapați la un singur registru destinație și la un singur utilizator destinație. Puteți defini o asociere de politică domeniu implicită pentru fiecare registru din domeniu. Dacă două sau mai multe asocieri de politică domeniu se referă la același registru destinație, puteți să definiți informații de căutare unice pentru fiecare dintre ele pentru a vă asigura că operațiile de căutare mapare pot distinge între ele. Altfel, operațiile de căutare mapare pot returna identități utilizator destinație multiple. Ca răspuns la aceste rezultate ambigue, aplicațiile care se bazează pe EIM s-ar putea să nu fie capabile să determine identitatea destinație exactă care va fi folosită.

Pentru a crea o asociere de politică domeniu implicită, realizați acești pași:

1. Expandați **Rețea > EIM (Enterprise Identity Mapping) > Gestionare domeniu**.
2. Faceți clic dreapta pe domeniul EIM în care vreți să lucrați și selectați **Politică mapare**
  - Dacă domeniul EIM cu care vreți să lucrați nu este listat sub **Gestionare domeniu**, vedeți “Adăugarea unui domeniu EIM la folderul Gestionare domeniu” la pagina 86.
  - Dacă nu sunteți conectat curent la domeniul EIM în care vreți să lucrați, vedeți Conectarea la controlerul de domeniu EIM.
3. Selectați **Activare căutare mapări folosind asocierile de politică pentru domeniu** pe pagina General.
4. Selectați pagina **Domeniu** și faceți clic pe **Adăugare**.
5. În dialogul **Adăugare asociere de politică domeniu implicită**, specificați următoarele informații necesare:
  - Numele definiției de registru pentru **Registru destinație** pentru asocierea de politică.
  - Numele identității utilizatorului pentru **Utilizator destinație** pentru asocierea de politică.
6. Faceți clic pe **Ajutor**, dacă este nevoie, pentru mai multe detalii despre cum să completați acest dialog și dialogurile următoare.
7. Opțional. Faceți clic pe **Avansat** pentru a afișa dialogul **Adăugare asociere - Avansat**. Specificați **Informații de căutare** pentru asocierea de politică și faceți clic pe **OK** pentru a vă întoarce la dialogul **Adăugare asociere de politică domeniu implicită**.

**Notă:** Dacă două sau mai multe asocieri de politică domeniu implicite se referă la același registru destinație, trebuie să definiți informații de căutare unice pentru fiecare identitate de utilizator destinație în aceste asocieri de politică. Definind informații de căutare pentru fiecare identitate de utilizator destinație, în această situație, vă asigurați că o operație de căutare mapări poate distinge între ele. Altfel, operațiile de căutare mapare pot returna identități utilizator destinație multiple. Ca răspuns la aceste rezultate ambigue, aplicațiile care se bazează pe EIM s-ar putea să nu fie capabile să determine identitatea destinație exactă care va fi folosită.

8. Faceți clic pe **OK** pentru a crea asocierea de politică nouă și să vă întoarceți la pagina **Domeniu**. Noua asociere de politică se afișează în tabelul **Asocierile de politică implicite**.
9. Verificați că noua asociere de politică este activată pentru registrul destinație.

10. Apăsați **OK** pentru a vă salva modificările și să vă întoarceți la dialogul **Politică de mapare**.

**Notă:** Verificați dacă sunt activate corespunzător suportul de politică mapare și utilizarea asocierilor de politică pentru registrul de utilizator destinație. Dacă nu sunt activate, asocierea de politică nu poate să aibă efect.

*Crearea unei asocieri de politică registru implicită:*

Pentru a crea o asociere de politică registru implicită, trebuie să fiți conectat la domeniul EIM (Enterprise Identity Mapping) în care vreți să lucrați și trebuie să aveți control acces EIM ca și administrator registru sau administrator EIM.

O asociere de politică descrie o relație dintre mai multe identități de utilizator și o unică identitate de utilizator dintr-un registru de utilizatori destinație. Puteți folosi o asociere de politică pentru a descrie o relație între un set sursă de identități și o unică identitate destinație de utilizator dintr-un registru de utilizatori destinație, specificat. Asocierile de politică folosesc suportul de politică mapare EIM pentru a crea mapări multe-la-una între identități de utilizator fără a implica un identificator EIM.

**Notă:** Deoarece puteți folosi asocierile de politică într-o varietate de modalități care se suprapun, trebuie să înțelegeți pe deplin suportul de politică mapare EIM înainte de a crea și folosi asocierile de politică. De asemenea, pentru a împiedica problemele potențiale cu asocieri și cum mapează identități, trebuie să dezvoltați un plan de mapare identitate general pentru întreprinderea dumneavoastră înainte să începeți să definiți asocieri.

Într-o asociere de politică registru implicită, toți utilizatorii dintr-un singur registru sunt sursa asocierii de politică și sunt mapați la un singur registru destinație și utilizator destinație. Atunci când activați asocierea de politică registru implicită pentru un registru destinație, asocierea de politică asigură faptul că toți toate aceste identități de utilizator sursă pot fi mapate la un singur registru destinație, specificat și un utilizator sursă.

Pentru a crea o asociere de politică registru implicită, parcurgeți pașii următori:

1. Expandați **Rețea > EIM (Enterprise Identity Mapping) > Gestionare domeniu**.
2. Selectați domeniul EIM în care doriți să lucrați.
  - Dacă domeniul EIM cu care vreți să lucrați nu este listat sub **Gestionare domeniu**, vedeți “Adăugarea unui domeniu EIM la folderul Gestionare domeniu” la pagina 86.
  - Dacă nu sunteți conectat curent la domeniul EIM în care vreți să lucrați, vedeți Conectarea la controlerul de domeniu EIM.
3. Selectați **Activare căutări mapare folosind asocieri de politică pentru domeniu** în pagina General.
4. Selectați **Activare căutări mapare folosind asocieri de politică pentru domeniu** în pagina General.
5. În dialogul **Adăugare asociere de politică registru implicită**, specificați următoarele informații necesare:
  - Numele definiției de registru al **Registrului sursă** pentru asocierea de politică.
  - Numele definiției de registru al **Registrului destinație** pentru asocierea de politică.
  - Numele identității de utilizator a **Utilizatorului destinație** pentru asocierea de politică.
6. Faceți clic pe **Ajutor**, dacă este nevoie, pentru detalii suplimentare privind completarea acestui dialog și a celor următoare.
7. Opțional. Faceți clic pe **Avansat** pentru a afișa dialogul **Adăugare asociere - Avansat**. Specificați **informații căutare** pentru asocierea de politică și faceți clic pe **OK** pentru a reveni la dialogul **Adăugare asociere de politică registru implicită**. Dacă două sau mai multe asocieri de politică cu același registru sursă se referă la același registru destinație, trebuie să definiți informații de căutare unice pentru fiecare dintre identitățile de utilizator destinație din aceste asocieri de politică. Dacă într-o astfel de situație definiți informații de căutare pentru fiecare identitate de utilizator destinație, vă asigurați că operațiile de căutare mapare pot face deosebirea între ele. Altfel, operațiile de căutare mapare pot returna mai multe identități de utilizator destinație. În urma unor astfel de rezultate ambigue, este posibil ca aplicațiile care se bazează pe EIM să nu fie capabile să determine identitatea destinație exactă care urmează să fie folosită.
8. Faceți clic pe **OK** pentru a crea noua asociere de politică și pentru a reveni în pagina **Registru**. Noua asociere de politică registru implicită este afișată în **Asocierile de politică implicite**.

9. Verificați dacă noua asociere de politică este activată pentru registrul destinație.
10. Faceți clic pe **OK** pentru a salva modificările și a ieși din dialogul **Politică mapare**.

**Notă:** Verificați dacă sunt activate corespunzător suportul de politică mapare și utilizarea asocierilor de politică pentru registrul de utilizator destinație. Dacă nu sunt activate, asocierea de politică nu devine efectivă.

*Creare unei asocieri politică de filtru de certificate:*

Pentru a crea o asociere politică filtru de certificate, trebuie să fiți conectat la EIM (Enterprise Identity Mapping) în care vreți să lucrați și să aveți control acces EIM fie ca administrator registru sau administrator EIM.

O asociere de politică descrie o relație între un set de mai multe identități de utilizatori sursă și o singură identitate de utilizator destinație într-un registru de utilizatori destinație specificat. Asocierile de politică folosesc suport pentru politica de mapare EIM pentru a crea mapări multe-la-una între identități utilizator fără a invoca un identificator EIM.

**Notă:** Deoarece puteți folosi asocieri de politică într-o varietate de moduri care se suprapun, aveți nevoie de o înțelegere temeinică a suportului politicii de mapare EIM, înainte de a crea și folosi asocierile de politică. De asemenea, pentru a preveni problemele potențiale cu asocieri și cum mapează identități, trebuie să dezvoltați un plan general de mapare identități pentru întreprinderea dumneavoastră înainte să începeți definirea asocierilor.

Într-o asociere de politică de filtrare certificate, specificați un set de certificate într-un singur registru X.509 ca sursă a asocierii. Aceste certificate sunt mapate pe un singur registru destinație și utilizator destinație pe care îi specificați. Spre deosebire de o asociere a politicii de registre implicită în care toți utilizatorii dintr-un singur registru sunt sursa asocierii, scopul unei asocieri de politică de filtrare certificate este mai flexibil. Puteți specifica un subset de certificate în registru ca sursă. Filtrul de certificate pe care îl specificați pentru asocierea de politică îi determină domeniul.

**Notă:** Creați și folosiți o asociere de politică implicită a registrelor, când vreți să mapați toate certificatele dintr-un registru de utilizatori X.509 la o singură identitate utilizator destinație.

Filtru de certificate controlează cum o asociere de politică filtru certificate mapează un set de identități utilizator sursă, în acest caz certificate digitale, la o identitate de utilizator destinație specifică. De aceea, filtru de certificate pe care vreți să-l folosiți trebuie să existe înainte de a putea crea o asociere de politică filtru certificate.

Înainte de a crea o asociere de politică filtru de certificate, trebuie mai întâi să creați un filtru de certificate de folosit ca bază pentru asocierea de politică.

Pentru a crea o asociere de politică filtru de certificate, realizați acești pași:

1. Expandați **Rețea > EIM (Enterprise Identity Mapping) > Gestionare domeniu**.
2. Faceți clic dreapta pe domeniul EIM în care vreți să lucrați și selectați **Politică mapare**
  - Dacă domeniul EIM cu care vreți să lucrați nu este listat sub **Gestionare domeniu**, vedeți “Adăugarea unui domeniu EIM la folderul Gestionare domeniu” la pagina 86.
  - Dacă nu sunteți conectat curent la domeniul EIM în care vreți să lucrați, vedeți Conectarea la controlerul de domeniu EIM.
3. Selectați **Activare căutare mapări folosind asocierile de politică pentru domeniu** pe pagina General.
4. Selectați pagina **Filtru de certificate** și faceți clic pe **Adăugare** pentru a afișa dialogul **Adăugare asocieri politică filtru de certificate**.
5. Faceți clic pe **Ajutor**, dacă este nevoie, pentru mai multe detalii despre cum să completați acest dialog și dialogurile următoare.
6. Specificați următoarele informații necesare pentru a defini asocierea de politică.
  - a. Introduceți numele definiției de registru pentru un registru de utilizatori X.509 pentru a-l folosi ca **Registru X.509 sursă** pentru asocierea de politică. Sau, faceți clic pe **Răsfoire** pentru a selecta o definiție registru din listă pentru domeniu

- b. Faceți clic pe **Selectare** pentru a afișa dialogul **Selectare filtru de certificate** și selectați un filtru de certificate existent pentru a-l folosi ca bază pentru noua asociere de politică filtru certificate.

**Notă:** **Trebuie** să folosiți un filtru de certificate existent. Dacă filtrul de certificate pe care vreți să îl utilizați nu e menționat, faceți clic pe **Adăugare** pentru a crea un nou filtru de certificate.

- c. Specificați numele definiției registru a **Registrului destinație** sau faceți clic pe **Răsfoire** pentru a selecta unul dintr-o listă de definiții registre existente pentru domeniu.
- d. Specificați numele **Utilizator destinație** la care să se mapeze toate certificatele din **Registru X.509 sursă** care se potrivesc cu filtru de certificate. Sau, faceți clic pe **Răsfoire** pentru a selecta una din lista de utilizatori cunoscuți domeniului.
- e. Opțional. Faceți clic pe **Avansat** pentru a afișa dialogul **Adăugare asociere - Avansat**. Specificați **Informații de căutare** pentru identitatea de utilizator destinație și clic **OK** pentru a vă întoarce la dialogul **Adăugare asociere de politică filtru certificate**.

**Notă:** Dacă două sau mai multe asocieri de politică cu același registru X.509 sursă și cu aceleași criterii de filtrare certificate se referă la același registru destinație, trebuie să definiți informații de căutare unice pentru identitățile de utilizatori destinație în fiecare dintre aceste asocieri de politică. Definind informații de căutare pentru fiecare identitate de utilizator destinație, în această situație, vă asigurați că o operație de căutare mapări poate distinge între ele. Altfel, operațiile de căutare mapare pot returna identități utilizator destinație multiple. Ca răspuns la aceste rezultate ambigue, aplicațiile care se bazează pe EIM s-ar putea să nu fie capabile să determine identitatea destinație exactă care va fi folosită.

7. Faceți clic pe **OK** pentru a crea asocierea de politică filtru de certificate și să vă întoarceți la pagina **Filtru de certificate**. Noua asociere de politică apare acum în listă.
8. Verificați că noua asociere de politică este activată pentru registrul destinație.
9. Apăsați **OK** pentru a vă salva modificările și să vă întoarceți la dialogul **Politică de mapare**.

**Notă:** Verificați dacă sunt activate corespunzător suportul de politică mapare și utilizarea asocierilor de politică pentru registrul de utilizator destinație. Dacă nu sunt activate, asocierea de politică nu poate să aibă efect.

#### *Crearea unui filtru de certificate:*

Un filtru de certificate definește un set de atribute nume distinctive similare pentru un grup de certificate într-un registru de utilizatori sursă X.509. Puteți folosi filtrul de certificate ca baza unei asocieri de politică de filtrare certificate.

Filtrul de certificate într-o asociere de politică determină care certificate din registrul sursă X.509 specificat să fie mapate la utilizatorul destinație specificat. Acele certificate care au informațiile DN subiect și DN emitent care satisfac criteriile filtrelor sunt mapate la utilizatorul destinație specificat în timpul operațiilor de căutare mapare EIM (Enterprise Identity Mapping).

Pentru a crea un filtru de certificate, trebuie să fiți conectat la un domeniu EIM în care vreți să lucrați și trebuie să aveți "Controlul accesului în EIM" la pagina 38 la unul din următoarele niveluri:

- Administrator EIM
- Administrator de registru
- Administrator pentru registrele selectate (pentru definiția de registru care se referă la registrul de utilizatori X.509 pentru care vreți să creați filtru de certificate).

Crează un filtru de certificate bazat pe informațiile unui nume distinctiv (DN) specific dintr-un certificat digital. Informațiile DN pe care le specificați pot fi nume distinctiv subiect, care desemnează proprietarul certificatului sau nume distinctiv emitent, care desemnează emitentul certificatului. Pentru un filtru de certificate, puteți specifica fie informații complete, fie informații parțiale DN.

Când adăugați filtru de certificate la asociere de politică filtru certificate, filtru de certificate determină care certificate dintr-un registru X.509 sunt mapate la identitatea de utilizator destinație specificată de asocierea de politică. Când un



certificat digital este identitatea utilizator sursă într-o operație de căutare mapare EIM (după ce aplicația solicitantă folosește API-ul EIM `eimFormatUserIdentity()` pentru a formata numele identitate utilizator) și se aplică asocierea de politică filtru certificate, EIM compară informațiile DN din certificat cu informațiile DN sau DN parțial specificate în filtru. Dacă informația din DN din certificat se potrivește cu filtrul, EIM returnează identitatea utilizator destinație pe care a specificat-o asocierea de politică filtru certificate.

Când creați filtru de certificate puteți furniza informațiile de nume distinctiv cerute, într-unul din următoarele trei moduri:

- Puteți introduce DN-uri complete sau parțiale ale unui certificat specific pentru **DN subiect**, **DN emitent** sau pentru amândouă.
- Puteți copia informația dintr-un certificat anume în clipboard și să o folosiți pentru a genera lista de candidați pentru filtru de certificate bazată pe informațiile de nume distinctiv din certificat. Apoi puteți selecta ce DN-uri veți folosi pentru filtru de certificate.

**Notă:** Dacă doriți să generați informațiile de nume distinctiv necesare pentru a crea un filtru de certificate, trebuie să copiați, înainte de realizarea acestei operații, informațiile certificatului într-un clipboard. De asemenea, certificatul trebuie să fie în format codat bază64. Pentru informații mai detaliate despre metodele de obținere a unui certificat în formatul corespunzător, vedeți Filtru certificate.

- Puteți genera o listă de candidați filtru de certificate bazată pe informațiile de nume distinctiv dintr-un certificat digital, pentru care există o asociere sursă cu un identificator EIM. Apoi puteți selecta ce DN-uri veți folosi pentru filtru de certificate.

Pentru a crea un filtru de certificate de folosit ca bază pentru o asociere de politică filtru certificate, realizați acești pași:

1. Expandati **Rețea > EIM (Enterprise Identity Mapping) > Gestionare domeniu**.
2. Faceți clic dreapta pe domeniul EIM în care vreți să lucrați și selectați **Politică mapare**
  - Dacă domeniul EIM cu care vreți să lucrați nu este listat sub **Gestionare domeniu**, vedeți “Adăugarea unui domeniu EIM la folderul Gestionare domeniu” la pagina 86.
  - Dacă nu sunteți conectat curent la domeniul EIM în care vreți să lucrați, vedeți Conectarea la controlerul de domeniu EIM.
3. Selectați pagina **Filtru de certificate** și faceți clic pe **Filtru de certificate** pentru a afișa dialogul **Filtre certificate**.

**Notă:** Dacă faceți clic pe **Filtre de certificate** fără a selecta o asociere de politică, apoi dialogul **Răsfoire registre EIM** apare. Acest dialog vă permite să selectați un registru X.509 dintr-o listă de definiții de registre X.509 din domeniul pentru care doriți să vedeți filtrele de certificate. Conținutul listei variază cu tipul de control al accesului la EIM pe care îl aveți:

4. Faceți clic pe **Adăugare** pentru a afișa dialogul **Adăugare filtru de certificate**.
5. În dialogul **Adăugare filtru de certificate**, trebuie să selectați dacă să adăugați un singur filtru de certificate sau să generați un filtru de certificate bazat pe un certificat digital specific. Faceți clic pe **Ajutor**, dacă este nevoie, pentru mai multe detalii despre cum să completați acest dialog și dialogurile următoare.
  - a. Dacă selectați **Adăugarea unui singur filtru de certificate**, puteți introduce anumite informații complete sau parțiale **DN subiect**, informații complete sau parțiale **DN emitent** sau amândouă. Faceți clic pe **OK** pentru a crea filtru de certificate și să vă întoarceți la dialogul **Filtru de certificate**. Filtrul apare acum în listă.
  - b. Dacă selectați **Generare filtru de certificate dintr-un certificat digital**, faceți clic pe **OK** pentru a afișa dialogul **Generare filtre de certificate**.
    - 1) Lipiți (paste) versiunea codificată bază64 a informațiilor certificat pe care le-ați copiat mai devreme în clipboard în câmpul **Informații certificat**.
    - 2) Faceți clic pe **OK** pentru a genera o listă de filtre de certificate potențiale bazată pe **DN subiect** și **DN emitent** ale certificatului.
    - 3) Din dialogul **Răsfoire filtre de certificate**, selectați unul sau mai multe din aceste filtre de certificate. Faceți clic pe **OK** pentru a vă întoarce la dialogul **Selectare filtre de certificate** unde sunt afișate acum și filtrele de certificate selectate.

- c. Dacă selectați **Generare filtru de certificate de la o asociere sursă pentru un utilizator X.509**, faceți clic pe **OK** pentru a afișa dialogul **Generare filtre de certificate**. Acest dialog afișează o listă de identități utilizator X.509 care au o asociere sursă cu un identificator EIM în domeniu.
- 1) Selectați identitatea de utilizator X.509 a cărui certificat digital vreți să-l folosiți, pentru a genera unul sau mai mulți candidați de filtre certificate și faceți clic pe **OK**.
  - 2) Faceți clic pe **OK** pentru a genera o listă de filtre de certificate potențiale bazată pe **DN subiect** și **DN emitent** ale certificatului.
  - 3) Din dialogul **Răspunde filtre de certificate**, selectați unul sau mai multe din aceste filtre de certificate potențiale. Faceți clic pe **OK** pentru a vă întoarce la dialogul **Selectare filtre de certificate** unde sunt afișate acum și filtrele de certificate selectate.

Puteți folosi acum noul filtru de certificate ca bază pentru crearea unei asocieri de politică de filtrare certificate.

## Adăugarea de informații de căutare la o identitate de utilizator destinație

Informațiile de căutare sunt date de identificare unice pentru identitatea utilizator unică definită într-o asociere. Această asociere poate să fie o asociere destinație identificator sau o asociere de politică.

Informațiile de căutare sunt necesare doar când o operație de căutare mapare poate întoarce mai mult de o identitate de utilizator destinație. Această situație poate crea probleme pentru aplicațiile permise EIM (Enterprise Identity Mapping), inclusiv pentru aplicațiile și produsele iOS care nu sunt proiectate să trateze aceste rezultate ambigue.

Atunci când este necesar, puteți adăuga informații de căutare unice pentru fiecare identitate utilizator destinație pentru a furniza mai multe informații de identificare detaliate pentru a descrie mai departe fiecare identitate utilizator destinație. Dacă definiți informații de căutare pentru o identitate utilizator destinație, aceste informații de căutare trebuie să fie furnizate la operația de căutare de mapare pentru a asigura că operația poate returna o identitate utilizator destinație unică. Altfel, aplicațiile care se bazează pe EIM s-ar putea să nu poată determina identitatea destinație exactă de folosit.

**Notă:** Dacă nu doriți operații de căutare EIM capabile să întoarcă mai mult de o identitate utilizator destinație, atunci ar trebui să corectați configurația asocierilor EIM în locul folosirii informației de căutare pentru a rezolva situația. Pentru informații mai detaliate, consultați “Depanarea problemelor de mapare EIM” la pagina 119.

Cum adăugați informații de căutare pentru a defini mai departe o identitate utilizator destinație ce variază dacă identitatea utilizator destinație este definită într-o asociere identificator sau o asociere destinație. În ciuda metodei pe care o folosiți pentru a adăuga informații de căutare, informațiile pe care le specificați sunt legate de identitatea utilizator destinație, nu de asocierile de identificatori sau asocierile de politică în care se găsește identitatea utilizatorului.

### Adăugarea informațiilor de căutare la o identitate utilizator destinație într-o asociere identificator:

Pentru a adăuga informații de căutare la identitatea utilizator destinație într-o asociere identificator, trebuie să fiți conectat la domeniul EIM în care doriți să lucrați și trebuie să aveți “Controlul accesului în EIM” la pagina 38 la unul din aceste niveluri:

- Administrator registru.
- Administrator pentru registrele selectate (pentru definiția de registru care se referă la registrul de utilizatori care conține identitatea de utilizator destinație).
- Administrator EIM.

Pentru a adăuga informațiile de căutare pentru identitatea de utilizator destinație dintr-o asociere identificator, completați acești pași:

1. Expandați **Rețea > EIM (Enterprise Identity Mapping) > Gestionare domeniu**.
2. Selectați domeniul EIM în care vreți să lucrați.
  - Dacă domeniul EIM cu care vreți să lucrați nu este listat sub **Gestionare domeniu**, vedeți “Adăugarea unui domeniu EIM la folderul Gestionare domeniu” la pagina 86.

- Dacă nu sunteți conectat curent la domeniul EIM în care vreți să lucrați, vedeți Conectarea la controlerul de domeniu EIM.
3. Expandați domeniul EIM la care sunteți conectat.
  4. Faceți clic pe **Identificatori** pentru a afișa lista de identificatori EIM pentru domeniu.

**Notă:** Uneori când încercați să expandați folderul **Identificatori**, poate trece un timp mai îndelungat până se afișează lista cu identificatori. Pentru a îmbunătăți performanța când aveți un număr mare de identificatori EIM în domeniu, puteți personaliza vizualizarea folderului **Identificatori** restricționând valoarea de căutare utilizată pentru afișarea identificatorilor. Faceți clic dreapta pe **Identificatori**, selectați **Personalizare această vizualizare > Includere** și specificați criteriile de afișare de folosit pentru generarea listei identificatorilor EIM de inclus în această vizualizare.

5. Faceți clic dreapta pe un identificator EIM și selectați **Proprietăți**.
6. Selectați pagina **Asocieri**, selectați asocierea destinație la care vreți să adăugați informațiile de căutare și faceți clic pe **Detalii**. Faceți clic pe **Ajutor** pentru a determina ce informații să specificați pentru fiecare câmp din dialog.
7. În dialogul **Asociere - Detalii**, specificați **Informațiile de căutare** pe care doriți să le folosiți în identitatea utilizator destinație din această asociere și faceți clic pe **Adăugare**.
8. Repetați acest pas pentru fiecare intrare informații de căutare pe care doriți să le adăugați la asociere.
9. Apăsați **OK** pentru a salva modificările și să vă întoarceți la dialogul **Asociere - Detalii**.
10. Faceți clic pe **OK** pentru a ieși.

#### **Adăugarea informațiilor de căutare la o identitate utilizator destinație dintr-o asociere politică:**

Pentru a adăuga informații de căutare la identitatea utilizator destinație, trebuie să fiți conectat la domeniul EIM în care doriți să lucrați și trebuie să aveți “Controlul accesului în EIM” la pagina 38 la unul din aceste niveluri:

- Administrator registru.
- Administrator pentru registrele selectate (pentru definiția de registru care se referă la registrul de utilizatori care conține identitatea de utilizator destinație (ID)).
- Administrator EIM.

Pentru a adăuga informații de căutare la identitatea utilizator destinație dintr-o asociere politică, completați acești pași:

1. Expandați **Rețea > EIM (Enterprise Identity Mapping) > Gestionare domeniu**.
2. Selectați domeniul EIM în care vreți să lucrați.
  - Dacă domeniul EIM cu care vreți să lucrați nu este listat sub **Gestionare domeniu**, vedeți “Adăugarea unui domeniu EIM la folderul Gestionare domeniu” la pagina 86.
  - Dacă nu sunteți conectat curent la domeniul EIM în care vreți să lucrați, vedeți Conectarea la controlerul de domeniu EIM.
3. În dialogul **Mapare politică**, folosiți paginile pentru vizualizarea asocierilor de politică pentru domeniu.
4. Găsiți și selectați asocierea politică pentru registrul destinație care conține identitatea de utilizator destinație pentru care doriți să adăugați informațiile de căutare.
5. Faceți clic pe **Detalii** pentru a afișa dialogul corespunzător **Asocieri de politică - Detalii** pentru tipul de asociere de politică pe care l-ați selectat. Faceți clic pe **Ajutor** pentru a determina ce informații să specificați pentru fiecare câmp din dialog.
6. Specificați **Informații de căutare** pe care doriți să utilizați pentru a identifica în continuare identitatea utilizatorului destinație în această asociere de politică și faceți clic pe **Adăugare**. Repetați acest pas pentru fiecare intrare informații de căutare pe care doriți să le adăugați la asociere.
7. Apăsați **OK** pentru a salva modificările și să vă întoarceți la dialogul **Asociere politică - Detalii**.
8. Faceți clic pe **OK** pentru a ieși.

## Înlăturarea informațiilor de căutare de la o identitate utilizator destinație

Informațiile de căutare sunt date de identificare unice opționale pentru identitatea utilizator destinație definită în asociere. Această asociere poate să fie o asociere destinație identificator sau o asociere de politică.

Informațiile de căutare sunt necesare doar când o operație de căutare mapare poate întoarce mai mult de o identitate de utilizator destinație. Această situație poate crea probleme pentru aplicațiile permise EIM (Enterprise Identity Mapping), inclusiv pentru aplicațiile și produsele i5/OS care nu sunt proiectate să trateze aceste rezultate ambigue.

Aceste informații de căutare trebuie furnizate operației de căutare mapări pentru a vă asigura că operația întoarce o identitate unică de utilizator destinație. Dar, dacă informațiile de căutare definite anterior nu mai sunt necesare, puteți dori să le înlăturați ca să nu mai fie oferite operațiilor de căutare.

Cum înlăturați informațiile de căutare dintr-o identitate de utilizator destinație depinde dacă identitatea de utilizator destinație este definită într-o asociere identificator sau o asociere destinație. Informațiile de căutare sunt legate de identitatea de utilizator destinație, nu la asocierile de identificatori sau asocierile de politică în care se găsește identitatea utilizatorului. În consecință, când ștergeți ultima asociere identificator utilizator sau politică, care definește identitatea utilizator destinație, atât identitatea utilizatorului, cât și informațiile de căutare sunt șterse din domeniul EIM.

### Înlăturarea informațiilor de căutare pentru o identitate utilizator destinație dintr-o asociere identificator.:

Pentru a înlătura informațiile de căutare pentru identitatea de utilizator destinație dintr-o asociere identificator, trebuie să fiți conectat la un domeniu EIM în care vreți să lucrați și trebuie să aveți “Controlul accesului în EIM” la pagina 38 la unul din următoarele niveluri:

- Administrator de registru
- Administrator pentru registrele selectate (pentru definiția de registru care se referă la registrul de utilizatori care conține identitatea de utilizator destinație).
- Administrator EIM.

Pentru a șterge informațiile de căutare pentru identitatea de utilizator destinație dintr-o asociere identificator, completați acești pași:

1. Expandați **Rețea > EIM (Enterprise Identity Mapping) > Gestionare domeniu**.
2. Selectați domeniul EIM în care vreți să lucrați.
  - Dacă domeniul EIM cu care vreți să lucrați nu este listat sub **Gestionare domeniu**, vedeți “Adăugarea unui domeniu EIM la folderul Gestionare domeniu” la pagina 86.
  - Dacă nu sunteți conectat curent la domeniul EIM în care vreți să lucrați, vedeți Conectarea la controlerul de domeniu EIM.
3. Expandați domeniul EIM la care sunteți conectat acum.
4. Faceți clic pe **Identificatori** pentru a afișa lista de identificatori EIM pentru domeniu.

**Notă:** Uneori când încercați să expandați folderul **Identificatori**, poate trece un timp mai îndelungat până se afișează lista cu identificatori. Pentru a îmbunătăți performanța când aveți un număr mare de identificatori EIM în domeniu, puteți personaliza vizualizarea folderului **Identificatori** restricționând valoarea de căutare utilizată pentru afișarea identificatorilor. Faceți clic dreapta pe **Identificatori**, selectați **Personalizare această vizualizare > Includere** și specificați criteriile de afișare de folosi t pentru generarea listei identificatorilor EIM de inclus în această vizualizare.

5. Faceți clic dreapta pe un identificator EIM și selectați **Proprietăți**.
6. Selectați pagina **Asocieri**, selectați asocierea destinație pentru identitatea utilizatorului pentru care vreți să înlăturați informațiile de căutare și faceți clic pe **Detalii**.
7. În dialogul **Asociere - Detalii**, selectați informațiile de căutare pe care vreți să le înlăturați din identitatea de utilizator destinație și faceți clic **Înlăturare**.

**Notă:** Nu există prompt pentru confirmare când apăsați **Înlăturare**.

8. Apăsați **OK** pentru a salva modificările și să vă întoarceți la dialogul **Asociere - Detalii**.
9. Faceți clic pe **OK** pentru a ieși.

*Înlăturarea informațiilor de căutare pentru o identitate utilizator destinație dintr-o asociere politică.:*

Pentru a înlătura informațiile de căutare pentru identitatea de utilizator destinație dintr-o asociere politică, trebuie să fiți conectat la un domeniu EIM în care vreți să lucrați și trebuie să aveți “Controlul accesului în EIM” la pagina 38 la unul din următoarele niveluri:

- Administrator de registru
- Administrator pentru registrele selectate (pentru definiția de registru care se referă la registrul de utilizatori care conține identitatea de utilizator destinație (ID)).
- Administrator EIM.

Pentru a șterge informațiile de căutare pentru identitatea de utilizator destinație dintr-o asociere politică, completați acești pași:

1. Expandați **Rețea > EIM (Enterprise Identity Mapping) > Gestionare domeniu**.
2. Selectați domeniul EIM în care vreți să lucrați.
  - Dacă domeniul EIM cu care vreți să lucrați nu este listat sub **Gestionare domeniu**, vedeți “Adăugarea unui domeniu EIM la folderul Gestionare domeniu” la pagina 86.
  - Dacă nu sunteți conectat curent la domeniul EIM în care vreți să lucrați, vedeți Conectarea la controlerul de domeniu EIM.
3. În dialogul **Mapare politică**, folosiți paginile pentru vizualizarea asocierilor de politică pentru domeniu.
4. Găsiți și selectați asocierile de politică pentru registrul de destinație care conține identitatea de utilizator destinație pentru care doriți să înlăturați informațiile de căutare.
5. Faceți clic pe **Detalii** pentru a afișa dialogul corespunzător **Asocieri de politică - Detalii** pentru tipul de asociere de politică pe care l-ați selectat.
6. Selectați informațiile de căutare pe care vreți să le înlăturați din identitatea de utilizatori destinație și faceți clic pe **Înlăturare**.

**Notă:** Nu există prompt pentru confirmare când apăsați **Înlăturare**.

7. Apăsați **OK** pentru a salva modificările și să vă întoarceți la dialogul **Asociere politică - Detalii**.
8. Faceți clic pe **OK** pentru a ieși.

## **Afișarea tuturor asocierilor de identificator pentru un identificator EIM**

Pentru a afișa toate asocierile pentru un identificator EIM (Enterprise Identity Mapping) trebuie să fiți conectat la domeniul EIM în care vreți să lucrați și să aveți un nivel de control acces EIM pentru a realiza acest task.

Puteți vizualiza toate asocierile cu orice nivel de control al accesului cu excepția controlului de acces Administrator pentru registre selectate. Acest nivel de control al accesului vă permite să listați și să vizualizați numai asocierile pentru registrele pentru care aveți autorizare explicită, cu excepția cazului în care aveți și controlul de acces Operații căutare mapare EIM.

Pentru a afișa toate asocierile dintre un identificator EIM și identitățile de utilizator (ID-urile) pentru care au fost definite asocieri cu identificatorul EIM, parcurgeți pașii următori:

Pentru a afișa asocierile pentru un identificator, parcurgeți pașii următori:

1. Expandați **Rețea > EIM (Enterprise Identity Mapping) > Gestionare domeniu**.
2. Selectați domeniul EIM în care vreți să lucrați.
  - Dacă domeniul EIM cu care vreți să lucrați nu este listat sub **Gestionare domeniu**, vedeți “Adăugarea unui domeniu EIM la folderul Gestionare domeniu” la pagina 86.
  - Dacă nu sunteți conectat curent la domeniul EIM în care vreți să lucrați, vedeți Conectarea la controlerul de domeniu EIM.

3. Expandați domeniul EIM la care sunteți conectat acum.
4. Faceți clic pe **Identificatori** pentru a afișa lista de identificatori EIM pentru domeniu.

**Notă:** Uneori, când încercați să expandați folderul **Identificatori** poate trece un timp mai îndelungat până se afișează lista cu identificatori. Pentru a îmbunătăți performanța când aveți un număr mare de identificatori EIM în domeniu, puteți personaliza vizualizarea folderului **Identificatori** restricționând valoarea de căutare utilizată pentru afișarea identificatorilor. Faceți clic dreapta pe **Identificatori**, selectați **Personalizare această vizualizare > Includere** și specificați criteriile de afișare de folosi t pentru generarea listei identificatorilor EIM de inclus în această vizualizare.

5. Selectați un identificator EIM, faceți clic dreapta pe identificatorul EIM și selectați **Proprietăți**.
6. Selectați pagina **Asocieri** pentru a afișa lista cu identitățile de utilizator asociate pentru identificatorul EIM selectat.
7. Faceți clic pe **OK** pentru a termina.

## Afișarea tuturor asocierilor de politică pentru un domeniu

Pentru a afișa toate asocierile de politică definite pentru un domeniu, trebuie să fiți conectat la domeniul (Enterprise Identity Mapping) în care vreți să lucrați și trebuie să aveți control de acces EIM pentru a realiza acest task.

Puteți vizualiza toate asocierile de politică cu orice nivel de control al accesului cu excepția controlului de acces Administrator pentru registre selectate. Acest nivel de control al accesului vă permite să listați și să vizualizați numai asocierile pentru registrele pentru care aveți autorizare explicită. Ca urmare, cu acest control al accesului nu puteți lista sau vizualiza asocierile de politică domeniu implicite, cu excepția cazului în care aveți și controlul de acces Operații căutare mapare EIM.

Pentru a afișa toate asocierile de politică pentru un domeniu, parcurgeți pașii următori:

1. Expandați **Rețea > EIM (Enterprise Identity Mapping) > Gestionare domeniu**.
2. Faceți clic dreapta pe domeniul EIM în care vreți să lucrați și selectați **Politică mapare**
  - Dacă domeniul EIM cu care vreți să lucrați nu este listat sub **Gestionare domeniu**, vedeți “Adăugarea unui domeniu EIM la folderul Gestionare domeniu” la pagina 86.
  - Dacă nu sunteți conectat curent la domeniul EIM în care vreți să lucrați, vedeți Conectarea la controlerul de domeniu EIM.
3. Selectați o pagină pentru a afișa asocierile de politică definite pentru domeniu, după cum urmează:
  - a. Selectați pagina **Domeniu** pentru a vedea asocierile de politică domeniu implicite definite pentru domeniu și dacă o asociere de politică este activată la nivel de registru.
  - b. Selectați pagina **Registru** pentru a vedea asocierile de politică registru implicite definite pentru domeniu. De asemenea, puteți vedea ce registre sursă și destinație afectează asocierile de politică.
  - c. Selectați pagina **Filtru certificat** pentru a vedea asocierile de politică filtru certificat definite și activate la nivel de registru.
4. Faceți clic pe **OK** pentru a termina.

## Afișarea tuturor asocierilor de politică pentru o definiție de registru

Pentru a afișa toate asocierile de politică definite pentru un registru specific, trebuie să fiți conectat la domeniul(Enterprise Identity Mapping) în care vreți să lucrați și trebuie să aveți un anume nivel de control acces EIM pentru a realiza acest task.

Puteți vizualiza toate asocierile de politică cu orice nivel de control al accesului cu excepția controlului de acces Administrator pentru registre selectate. Acest nivel de control al accesului vă permite să listați și să vizualizați numai asocierile pentru registrele pentru care aveți autorizare explicită. Ca urmare, cu acest control al accesului nu puteți lista sau vizualiza asocierile de politică domeniu implicite, cu excepția cazului în care aveți și controlul de acces Operații căutare mapare EIM.

Pentru a afișa toate asocierile de politică pentru o definiție de registru, parcurgeți pașii următori:

1. Expandați **Rețea > EIM (Enterprise Identity Mapping) > Gestionare domeniu**.

2. Selectați domeniul EIM în care vreți să lucrați.
  - Dacă domeniul EIM cu care vreți să lucrați nu este listat sub **Gestionare domeniu**, vedeți “Adăugarea unui domeniu EIM la folderul Gestionare domeniu” la pagina 86.
  - Dacă nu sunteți conectat curent la domeniul EIM în care vreți să lucrați, vedeți Conectarea la controlerul de domeniu EIM.
3. Faceți clic dreapta pe definiția registru cu care vreți să lucrați și selectați **Politică mapare**.
4. Selectați o pagină pentru a afișa asocierile de politică definite pentru definiția de registru specificată, după cum urmează:
  - Selectați pagina **Domeniu** pentru a vedea asocierile de politică domeniu implicite definite pentru registru.
  - Selectați pagina **Registru** pentru a vedea asocierile de politică registru implicite definite și activate pentru registru.
  - Selectați pagina **Filtru certificat** pentru a vedea asocierile de politică filtru certificat definite și activate pentru registru.
5. Faceți clic pe **OK** pentru a termina.

## Ștergerea unei asocieri de identificator

Pentru a șterge o asociere identificator, trebuie să fiți conectat la domeniul EIM (Enterprise Identity Mapping) în care vreți să lucrați și să aveți control de acces EIM cerut de tipul asocierii pe care vreți să o ștergeți.

Pentru a șterge o sursă sau o asociere administrativă, trebuie să aveți control de acces EIM la unul din aceste niveluri:

- Administrator identificator.
- Administrator EIM.

Pentru a șterge o asociere destinație, trebuie să aveți control de acces EIM la unul din aceste niveluri:

- Administrator registru.
- Administrator pentru registrele selectate (pentru definiția de registru care se referă la registrul de utilizatori care conține identitatea de utilizator destinație).
- Administrator EIM.

Pentru a șterge un domeniu identificator, efectuați pașii următori.

1. Expandați **Rețea > EIM (Enterprise Identity Mapping) > Gestionare domeniu**.
2. Selectați domeniul EIM în care vreți să lucrați.
  - Dacă domeniul EIM cu care vreți să lucrați nu este listat sub **Gestionare domeniu**, vedeți “Adăugarea unui domeniu EIM la folderul Gestionare domeniu” la pagina 86.
  - Dacă nu sunteți conectat curent la domeniul EIM în care vreți să lucrați, vedeți Conectarea la controlerul de domeniu EIM.
3. Expandați domeniul EIM la care sunteți conectat acum.
4. Faceți clic pe **Identificatori** pentru a afișa lista de identificatori EIM pentru domeniu.

**Notă:** Uneori când încercați să expandați folderul **Identificatori**, poate trece un timp mai îndelungat până se afișează lista cu identificatori. Pentru a îmbunătăți performanța când aveți un număr mare de identificatori în domeniu, puteți personalizavizualizarea folderului **Identificatori** restricționând criteriile de căutare utilizate pentru afișarea identificatorilor. Faceți clic dreapta pe **Identificatori**, selectați **Personalizare această vizualizare > Includere** și specificați criteriile de afișare de folosi t pentru generarea listei identificatorilor EIM de inclus în această vizualizare.

5. Selectați un identificator EIM, faceți clic dreapta pe identificatorul EIM și selectați **Proprietăți**.
6. Selectați pagina **Asocieri** pentru a afișa lista cu identitățile de utilizator asociate pentru identificatorul EIM selectat.
7. Selectați asocierea pe care doriți să o ștergeți și apăsați clic pe **Înlăturare** pentru a șterge asocierea.

**Notă:** Nu este nici un prompt de confirmare atunci când apăsați pe **Înlăturare**.

8. Apăsați clic pe **OK** pentru a vă salva modificările.

**Notă:** Atunci când ștergeți o asociere destinație, orice mapări operații de căutare la registrul destinație ce se bazează pe utilizarea asocierii șterse poate eșua dacă alte asocieri (fie asocieri de politică fie asocieri identificator) nu există pentru registrul destinație afectat.

Singura cale pentru a defini o identitate utilizator la EIM este atunci când specificați identitatea utilizator ca parte a creării unei asocieri, fie o asociere identificator sau o asociere politică. În mod consecvent, atunci când ștergeți ultima asociere destinație pentru o identitate utilizator (dacă prin înlăturarea unei asocieri destinație individuală sau prin înlăturarea unei asocieri politică), acea identitate utilizator nu mai este definită în EIM. În mod consecvent, numele identității utilizator și orice informații de căutare pentru acea identitate utilizator este pierdută.

## Ștergerea unei asocieri de politică

Pentru a șterge o asociere de politică, trebuie să fiți conectat la domeniul EIM (Enterprise Identity Mapping) în care vreți să lucrați și trebuie să aveți control acces EIM pentru fie administrator registru sau administrator EIM.

Pentru a șterge o asociere de politică, parcurgeți pașii următori:

1. Expandați **Rețea > EIM (Enterprise Identity Mapping) > Gestionare domeniu**.
2. Selectați domeniul EIM în care vreți să lucrați.
  - Dacă domeniul EIM cu care vreți să lucrați nu este listat sub **Gestionare domeniu**, vedeți “Adăugarea unui domeniu EIM la folderul Gestionare domeniu” la pagina 86.
  - Dacă nu sunteți conectat curent la domeniul EIM în care vreți să lucrați, vedeți Conectarea la controlerul de domeniu EIM.
3. Selectați pagina corespunzătoare pentru asocierea de politică pe care doriți să o ștergeți.
4. În pagina respectivă, selectați asocierea de politică corespunzătoare și faceți clic pe **Înlăturare**.

**Notă:** Nu există prompt pentru confirmare când apăsați **Înlăturare**.

5. Faceți clic pe **OK** pentru a ieși din dialogul **Politică mapare** și a salva modificările.

**Notă:** Atunci când înlăturați o asociere de politică destinație, operațiile de căutare mapare pentru registrul destinație care se bazează pe utilizarea asocierii de politică șterse pot eșua dacă nu există alte asocieri (asocieri de politică sau asocieri de identificator) pentru registrul destinație afectat.

Singura posibilitate de a defini un identificator de utilizator în EIM este la specificarea identității ca parte a creării unei asocieri, de identificator sau de politică. Ca urmare, atunci când ștergeți ultima asociere destinație pentru o identitate de utilizator (prin înlăturarea unei asocieri destinație individuale sau prin înlăturarea unei asocieri de politică), acea identitate de utilizator nu mai este definită în EIM. În consecință, numele identității de utilizator și informațiile de căutare pentru identitatea de utilizator respectivă se pierd.

### Concepte înrudite

“Gestionarea definițiilor de registre EIM” la pagina 91

Pentru ca registrele de utilizatori și identitățile utilizator pe care le conțin să participe într-un domeniu EIM trebuie să creați definiții registru pentru ele. Puteți gestiona modul în care registrele de utilizator și identitățile lor de utilizator participă în EIM prin gestionarea acestor definiții de registru EIM.

## Gestionarea controlului de acces al utilizatorului EIM

Un utilizator EIM (Enterprise Identity Mapping) este un utilizator care posedă control acces EIM bazat pe apartenența la grupuri utilizator predefinite LDAP (Lightweight Directory Access Protocol). Specificarea controlului de acces EIM pentru un utilizator îl adaugă pe acel utilizator la un grup de utilizatori LDAP specific.

Fiecare grup LDAP are autoritate să realizeze diverse operații administrative EIM într-un domeniu. Care și ce tip de operații administrative, incluzând operații de căutare, un utilizator EIM le poate realiza este determinat de grupul de control acces de care utilizatorul EIM aparține.



Doar utilizatorii cu control acces administrator LDAP sau cu control acces administrator EIM pot să adauge alți utilizatori la un grup de control acces sau să schimbe setările de control acces pentru alți utilizatori. Înainte ca un utilizator să devină un membru al unui grup de control acces EIM, acest utilizator trebuie să aibă o intrare în serverul de director care acționează ca un controler de domeniu EIM. De asemenea, doar tipurile specifice de utilizatori pot fi făcute membri ai grupului de control acces EIM: principali Kerberos, nume distinctive și profiluri utilizator i5/OS.

**Notă:** Pentru a avea tipul utilizator Kerberos principal disponibil în EIM, serviciul de autentificare în rețea trebuie configurat pe sistem. Pentru a avea tipul profilului utilizator i5/OS disponibil în EIM, trebuie să configurați un sufix obiect de sistem pe serverul de director. Aceasta permite serverului de director să facă referință la obiectele de sistem i5/OS, precum profilurile utilizator i5/OS.

Pentru a gestiona controlul acces pentru un utilizator director server sau pentru a adăuga un utilizator director existent la un grup de control acces, efectuați acești pași:

1. Expandați **Rețea > EIM (Enterprise Identity Mapping) > Gestionare domeniu**.
2. Selectați domeniul EIM în care vreți să lucrați.
  - Dacă domeniul EIM cu care vreți să lucrați nu este listat sub **Gestionare domeniu**, vedeți “Adăugarea unui domeniu EIM la folderul Gestionare domeniu” la pagina 86.
  - Dacă nu sunteți conectat curent la domeniul EIM în care vreți să lucrați, vedeți Conectarea la controlerul de domeniu EIM.
3. Faceți clic pe domeniul EIM la care sunteți conectat și selectați **Control acces**.
4. În fereastra **Editare Control acces EIM**, selectați **Tipul utilizatorului** pentru a afișa câmpurile necesare pentru a furniza informații de identificare pentru utilizator.
5. Introduceți informațiile utilizator necesare pentru a identifica utilizatorul pentru care doriți să gestionați controlul acces EIM și apăsați **OK** pentru a afișa panoul **Editare Control acces EIM**. Faceți clic pe **Ajutor**, dacă este necesar, pentru a determina ce informații să specificați pentru fiecare câmp.
6. Selectați unul sau mai multe grupuri de **Control acces** pentru utilizator și apăsați **OK** pentru a adăuga utilizatorul la grupuri selectate. Faceți clic pe **Ajutor** pentru detalii suplimentare despre ce autorizare are fiecare grup și să învățați despre anumite cerințe speciale.
7. După ce furnizați informațiile necesare, apăsați **OK** pentru a salva modificările.

#### Concepte înrudite

“Controlul accesului în EIM” la pagina 38

Un utilizator EIM (Enterprise Identity Mapping) este un utilizator care are control acces EIM bazat pe calitatea sa de membru într-un grup de utilizatori predefinit LDAP (Lightweight Directory Access Protocol) pentru un domeniu specific.

#### Informații înrudite

Network authentication service

## Gestionarea proprietăților de configurare EIM

Puteți controla mai multe proprietăți de configurare EIM pentru serverul. Tipic, acest lucru nu este necesar să-l faceți des.

Dar, sunt situații care necesită să faceți modificări la proprietățile configurației. De exemplu, dacă sistemul pică și aveți nevoie să re-creați proprietățile configurației dumneavoastră EIM puteți relua rularea vrăjitorului Configurare EIM sau modifica aici proprietățile. Un alt exemplu este când nu alegeți să creați definițiile de registru pentru registrele locale când rulați vrăjitorul Configurare EIM, puteți actualiza informațiile de definiții registru aici.

Proprietățile pe care le puteți modifica includ:

- Domeniul EIM în care participă serverul.
- Informațiile de conectare pentru controlerul de domeniu EIM.
- Identitatea pe care sistemul o folosește pentru a realiza operații EIM din partea funcțiilor sistemului de operare.

- Numele definițiilor de registru care se referă la registrele de utilizatori reale pe care sistemul le poate folosi când realizează operații EIM din partea funcțiilor sistemului de operare. aceste nume de definiții registru se referă la registrele de utilizatori locale pe care le puteți crea când rulați vrăjitorul Configurare EIM.

**Notă:** Dacă ați ales să nu creați numele de definiții registre locale când ați rulat vrăjitorul de configurare EIM, fie din cauză că registrele erau deja definite în domeniul EIM, fie pentru că ați ales să le definiți la domeniu mai târziu, trebuie să actualizați aici proprietățile configurației sistemului cu aceste nume de definiții registru. Sistemul are nevoie de aceste informații definiții registru pentru a realiza operații EIM din partea funcțiilor sistemului de operare.

Pentru a modifica proprietățile configurației EIM, trebuie să aveți aceste autorizări speciale:

- Administrator securitate (\*SECADM).
- Toate obiectele (\*ALLOBJ).

Pentru a modifica proprietățile de modificare EIM pentru platforma dumneavoastră System i, finalizați acești pași:

1. Expandați **Rețea >Mapare identitate în întreprindere**.
2. Faceți clic dreapta **Configurare** și selectați **Proprietăți**.
3. Faceți modificările la informațiile de configurare EIM.
4. Faceți clic pe **Ajutor** pentru a determina ce informații să specificați pentru fiecare câmp din dialog.
5. Faceți clic pe **Verificare configurație** să vă asigurați că toate informațiile specificate permit sistemului să stabilească cu succes o conexiune la controlerul de domeniu EIM.
6. Faceți clic **OK** pentru a vă salva modificările.

**Notă:** Dacă nu ați folosit vrăjitorul de configurare EIM pentru a crea sau a vă alătura unui domeniu, nu încercați să creați o configurație EIM specificând manual proprietățile configurației. Folosind vrăjitorul ca să creați configurația de bază EIM, puteți preveni probleme potențiale de configurare deoarece vrăjitorul face mai multe decât configurarea acestor proprietăți.

---

## Depanarea EIM (Enterprise Identity Mapping)

Utilizați următoarele metode de depanare pentru a rezolva unele din problemele de bază pe care ați putea trece cât timp configurați și utilizați EIM (Enterprise Identity Mapping).

EIM este compus din tehnologii multiple și multe aplicații și funcții. Prin urmare, problemele pot apărea în multe zone. Informațiile următoare descriu unele probleme și erori obișnuite pe care le puteți întâlni când folosiți EIM și ceva sugestii de cum să corectați aceste erori și probleme.

### Informații înrudite

Depanare configurație semnare unică

## Depanarea problemelor conexiunii la controlerul de domeniu

La problemele de conectare când încercați să vă conectați la controlerul de domeniu pot contribui un număr de factori. Examinați următoarea tabelă pentru a determina cum să rezolvați problemele de conexiune la controlerul de domeniu

Tabela 27. Problemele obișnuite la conectarea la controlerul de domeniu EIM și soluții

Problema posibilă	Soluțiile posibile
<p>Nu vă puteți conecta la controlerul de domeniu când utilizați Navigator System i pentru a gestiona EIM.</p>	<p>Informațiile de conectare la controlerul de domeniu pot fi specificate incorect pentru domeniul pe care vreți să-l gestionați. Terminați acești pași pentru a verifica informațiile de conectare la domeniu:</p> <ul style="list-style-type: none"> <li>• Expandați <b>Rețea--&gt;EIM (Enterprise Identity Mapping)--&gt;Rețea-&gt;Gestionare domeniu</b>. Faceți clic-dreapta pe domeniul pe care vreți să-l gestionați și selectați <b>Proprietăți</b>.</li> <li>• Verificați că numele <b>Controler de domeniu</b> este corect și că <b>DN părinte</b>, dacă este specificat, este și el corect.</li> <li>• Verificați că informațiile <b>Conexiune</b> pentru controlerul de domeniu sunt corecte. Asigurați-vă că numărul de <b>Port</b> este corect. Dacă este selectată <b>Folosirea conexiunii securizate (SSL sau TLS)</b>, serverul de director trebuie configurat să folosească SSL. Faceți clic pe <b>Verificare conexiune</b> pentru a verifica dacă puteți folosi informațiile specificate pentru a stabili o conexiune cu succes la controlerul de domeniu.</li> <li>• Verificați că informațiile de utilizator din panoul <b>Conectare la controlerul de domeniu</b> sunt corecte.</li> </ul>
<p>Sistemul de operare și aplicațiile nu se pot conecta la controlerul de domeniu pentru a accesa datele EIM. De exemplu, operațiile de căutare mapări EIM realizate în numele sistemului eșuează. Aceasta se poate întâmpla deoarece configurația EIM este incorectă pe sistem sau pe sisteme.</p>	<p>Verificați configurația EIM. Expandați <b>Rețea--&gt;EIM (Enterprise Identity Mapping)--&gt;Configurare</b> pe sistemul pe care încercați să îl autentificați. Faceți clic pe folderul <b>Configurare</b>, selectați <b>Proprietăți</b> și verificați următoarele:</p> <ul style="list-style-type: none"> <li>• Pagina <b>Domeniu</b> : <ul style="list-style-type: none"> <li>– Numele controlerului de domeniu și numerele porturilor sunt corecte.</li> <li>– Faceți <b>Verificare configurație</b> pentru a verifica dacă este activ controlerul de domeniu.</li> <li>– Numele de registru local este specificat corect</li> <li>– Numele de registru Kerberos este specificat corect</li> <li>– Verificați că <b>Activare operații EIM pentru sistem</b> este selectat.</li> </ul> </li> <li>• Pagina <b>Utilizator sistem</b>: <ul style="list-style-type: none"> <li>– Utilizatorul specificat are control de acces EIM suficient pentru a realiza o căutare de mapare și parola este validă pentru utilizator. Vedeți ajutorul online să aflați mai multe despre diferitele tipuri de acreditări utilizator.</li> <li><b>Notă:</b> Dacă ați schimbat parola pentru utilizatorul sistem specificat în serverul de director, trebuie să modificați parola și aici. Dacă aceste parole nu se potrivesc, atunci utilizatorul sistem nu poate realiza funcțiile EIM pentru sistemul de operare și operațiile de căutare mapare eșuează.</li> <li>– Faceți clic pe <b>Verificare conexiune</b> pentru a confirma că informațiile de utilizator specificate sunt corecte.</li> </ul> </li> </ul>

Tabela 27. Problemele obișnuite la conectarea la controlerul de domeniu EIM și soluții (continuare)

Problema posibilă	Soluțiile posibile
Informațiile de conectare par a fi corecte, dar nu vă puteți conecta la controlerul de domeniu.	<ul style="list-style-type: none"> <li>Asigurați-vă că serverul de director care acționează ca și controler de domeniu EIM este activ. Dacă controlerul de domeniu este o platformă System i, puteți utiliza Navigator System i și urmați acești pași: <ol style="list-style-type: none"> <li>1. Expandați <b>rețea &gt; Servere &gt; TCP/IP</b>.</li> <li>2. Verificați că serverul de director are starea <b>Pornit</b>. Dacă serverul este oprit, faceți clic dreapta pe <b>Serverul de director</b> și selectați <b>Pornire</b></li> </ol> </li> </ul>

După ce ați verificat informațiile de conexiune și serverul de director este activ, încercați să vă conectați la controlerul de domeniu urmând acești pași:

1. Expandați **Rețea > EIM (Enterprise Identity Mapping) > Gestionare domeniu**.
2. Faceți clic dreapta pe domeniul EIM la care vreți să vă conectați și selectați **Conectare**.
3. Specificați tipul de utilizator și informațiile despre utilizator necesare care trebuie utilizate pentru conectarea la controlerul de domeniu EIM.
4. Selectați **OK**.

## Depanarea probleme generale legate de domeniu și de configurația EIM

Există un număr de probleme generale pe care le puteți întâlni când configurați EIM pentru sistemul dumneavoastră sau puteți întâlni probleme când accesați un domeniu EIM. Examinați următoarea tabelă pentru a învăța mai multe despre unele probleme obișnuite și soluțiile potențiale pe care le puteți utiliza pentru a rezolva aceste probleme.

Tabela 28. Problemele obișnuite legate de domeniu și de configurația EIM și soluțiile lor

Problema posibilă	Soluțiile posibile
Vrăjitorul de configurare EIM pare că este agățat la procesarea <b>Sfârșit</b> .	Vrăjitorul poate aștepta după controlerul de domeniu să pornească. Verificați că nu există erori în timpul pornirii serverului director. Pentru platforme System i, verificați istoricul jobului pentru jobul QDIRSRV în subsistemul QSYSWRK. Pentru a verifica istoricul de job, urmați acești pași: <ol style="list-style-type: none"> <li>1. În Navigator System i, expandați <b>Control funcționare &gt; Sub sisteme &gt; Qsyswrk</b>.</li> <li>2. Faceți clic dreapta pe <b>Qdirsrv</b> și selectați <b>Istoric job</b>.</li> </ol>
Când folosiți vrăjitorul de configurare EIM pentru a crea un domeniu pe un sistem de la distanță, ați primit următorul mesaj de eroare: "Numele distinctiv (DN) părinte pe care l-ați introdus nu este valid. DN trebuie să existe pe serverul de director de la distanță. Specificați sau selectați un DN nou sau existent."	DN părinte specificat pentru domeniul de la distanță nu există. Vedeți "Crearea și alăturarea la un nou domeniu la distanță" la pagina 75 pentru a afla mai multe despre cum să folosiți vrăjitorul de configurare EIM. De asemenea, vedeți ajutorul online pentru informații detaliate despre specificarea unui DN părinte la crearea domeniului.
Primiți un mesaj indicând că domeniul EIM nu există.	Dacă nu ați creat un domeniu EIM, folosiți vrăjitorul de configurare EIM. Acest vrăjitor creează un domeniu EIM pentru dumneavoastră sau vă permite să configurați un domeniu existent. Dacă ați creat un domeniu EIM, asigurați-vă că utilizatorul specificat este un membru al unui grup "Controlul accesului în EIM" la pagina 38 cu autorizare suficientă pentru accesarea lui.
Primiți un mesaj indicând că nu a fost găsit un obiect EIM (identificator, registru, asociere, asociere politică sau filtru certificate) sau că nu sunteți autorizat la datele EIM.	Verificați că obiectul EIM există și dacă utilizatorul specificat este membru al grupului "Controlul accesului în EIM" la pagina 38 cu autorizare suficientă pentru accesarea lui.

Tabela 28. Problemele obișnuite legate de domeniu și de configurația EIM și soluțiile lor (continuare)

Problema posibilă	Soluțiile posibile
<p>Când expandați folderul <b>Identificatori</b>, trece un timp mai îndelungat până se afișează lista cu identificatori.</p>	<p>Acest lucru se poate întâmpla dacă există în domeniu un număr mare de identificatori EIM. Pentru a rezolva aceasta, puteți personaliza folderul <b>Identificatori</b> prin restricționarea criteriului de căutare folosit pentru afișarea identificatorilor. Pentru a personaliza vizualizarea pentru identitățile EIM, urmați acești pași:</p> <ol style="list-style-type: none"> <li>1. În Navigator System i, expandați <b>Rețea &gt;EIM (Enterprise Identity Mapping) &gt; Gestionare domeniu</b>.</li> <li>2. Expandați domeniul din care doriți să afișați identificatorii EIM.</li> <li>3. Faceți clic dreapta pe <b>Identificatori</b> și selectați <b>Personalizare această vizualizare &gt; Includere</b>.</li> <li>4. Specificați criteriile de afișare de folosit pentru generarea listei de identificatori EIM de inclus în această vizualizare. <b>Notă:</b> Puteți folosi asteriscul (*) ca și un caracter de înlocuire.</li> <li>5. Selectați <b>OK</b>.</li> </ol> <p>Data următoare când faceți clic pe <b>Identificatori</b>, se afișează numai acei indicatori EIM care se potrivesc cu criteriul de căutare specificat.</p>
<p>Cât timp gestionați EIM prin Navigator System i, primiți o eroare care indică faptul că manipularea EIM nu mai este validă.</p>	<p>Conexiunea la controlerul de domeniu s-a pierdut. Pentru a realiza reconectarea la controlerul de domeniu, urmați acești pași:</p> <ol style="list-style-type: none"> <li>1. În Navigator System i, expandați <b>Rețea &gt;EIM (Enterprise Identity Mapping) &gt; Gestionare domeniu</b>.</li> <li>2. Faceți clic dreapta pe domeniul cu care vreți să lucrați și selectați <b>Reconectare</b>.</li> <li>3. Specificați informațiile de conexiune.</li> <li>4. Selectați <b>OK</b>.</li> </ol>
<p>Când folosiți protocolul Kerberos pentru autentificarea la EIM, mesajul de diagnostică CPD3E3F este scris în istoricul jobului.</p>	<p>Acest mesaj este generat de fiecare dată când eșuează autentificarea sau operația de mapare a identității. Mesajul de diagnostic conține ambele coduri de stare major și 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, consultați informațiile de ajutor asociate cu mesajul de diagnosticare. Deasemenea ați putea găsi de ajutor trecerea în revistă Depanare configurație semnare unică.</p>

## Depanarea problemelor de mapare EIM

Există un număr de probleme obișnuite care pot duce la nefuncționarea tuturor mapărilor EIM sau la funcționarea lor necorespunzătoare. Revedeți următoarea tabelă pentru a găsi informații despre ce problemă ar putea cauza o mapare EIM să eșueze și soluțiile potențiale pentru acea problemă. Dacă mapările EIM eșuează, s-ar putea să fie nevoie să vedeți fiecare soluție din tabelă pentru a găsi și rezolva problema sau problemele care au dus la eșuarea mapărilor.

Tabela 29. Problemele obișnuite de mapare EIM și soluțiile lor

Probleme posibile	Soluții posibile
<p>Informațiile de conectare pentru controlerul de domeniu pot fi incorecte sau controlerul de domeniu nu este activ.</p>	<p>Consultați Probleme conexiune controler de domeniu pentru a învăța cum să verificați informațiile conexiunii pentru controlerul de domeniu și cum să verificați că acel controler de domeniu este activ.</p>
<p>Operațiile de căutare mapări EIM realizate în numele sistemului au eșuat. Aceasta se poate întâmpla deoarece configurația EIM este incorectă pe sistem sau pe sisteme.</p>	<p>Verificați configurația EIM. Expandați <b>Rețea--&gt;EIM (Enterprise Identity Mapping)--&gt;Configurare</b> pe sistemul pe care încercați să îl autentificați. Faceți clic pe folderul <b>Configurare</b>, selectați <b>Proprietăți</b> și verificați următoarele:</p> <ul style="list-style-type: none"> <li>• Pagina <b>Domeniu</b> : <ul style="list-style-type: none"> <li>– Numele controlerului de domeniu și numerele porturilor sunt corecte.</li> <li>– Faceți <b>Verificare configurație</b> pentru a verifica dacă este activ controlerul de domeniu.</li> <li>– Numele de registru local este specificat corect</li> <li>– Numele de registru Kerberos este specificat corect</li> <li>– Verificați că <b>Activare operații EIM pentru sistem</b> este selectată.</li> </ul> </li> <li>• Pagina <b>Utilizator sistem</b>: <ul style="list-style-type: none"> <li>– Utilizatorul specificat are control de acces EIM suficient pentru a realiza o căutare de mapare și parola este validă pentru utilizator. Consultați ajutorul online pentru a afla mai multe despre diferitele tipuri de acreditări utilizator.</li> <li><b>Notă:</b> Dacă ați schimbat parola pentru utilizatorul sistem specificat în serverul de director, trebuie să modificați parola și aici. Dacă aceste parole nu se potrivesc, atunci utilizatorul sistem nu poate realiza funcțiile EIM pentru sistemul de operare și operațiile de căutare mapare eșuează.</li> <li>– Faceți clic pe <b>Verificare conexiune</b> pentru a confirma că informațiile de utilizator specificate sunt corecte.</li> </ul> </li> </ul>

Tabela 29. Problemele obișnuite de mapare EIM și soluțiile lor (continuare)

Probleme posibile	Soluții posibile
<p>O operație de căutare mapare poate să întoarcă mai multe identități de utilizator destinație. Aceasta se poate întâmpla când există una sau mai multe din situațiile următoare:</p> <ul style="list-style-type: none"> <li>• Un identificator EIM are mai multe asocieri destinație individuale la același registru destinație.</li> <li>• Mai mult de un identificator EIM are aceeași identitate utilizator specificată într-o asociere sursă și fiecare din acești identificatori EIM are o asociere destinație la același registru destinație, deși identitatea utilizator specificată pentru fiecare asociere destinație poate fi diferită.</li> <li>• Mai mult de o asociere politică domeniu implicită specifică același registru destinație.</li> <li>• Mai mult de o asociere politică registru implicită specifică același registru sursă și același registru destinație.</li> <li>• Mai mult de o asociere politică filtru certificate specifică aceleași registru sursă X.509, filtru de certificate și registru destinație.</li> </ul>	<p>Utilizați funcția Testare mapare EIM pentru a verifica că o identitate sursă specifică mapează corect la identitatea utilizator destinație corectă. Cum corecți problema depinde de ce rezultate obțineți de la test, după cum urmează:</p> <ul style="list-style-type: none"> <li>• Testul returnează identități multiple nedorite din unul din următoarele motive: <ul style="list-style-type: none"> <li>– Configurarea de asociere pentru domeniu, ar putea fi arătat, nu este corectă, datorită unui din motivele următoare: <ul style="list-style-type: none"> <li>- O asociere destinație sau sursă pentru un identificator EIM nu este configurată corect. De exemplu, nu există nici o asociere sursă pentru principalul Kerberos (sau utilizatorul Windows) sau este incorectă. Sau, asocierea destinație specifică o identitate de utilizator incorectă. Afișați toate asocierile de identificatori pentru un identificator EIM pentru a verifica asocierile pentru un identificator specific.</li> <li>- O asociere politică nu este configurată corect. Afișați toate asocierile politică pentru un domeniu pentru a verifica informațiile sursă și destinație pentru toate asocierile de politică definite în domeniu.</li> </ul> </li> <li>– Aceasta ar putea indica că definițiile pentru registrul grup care conțin membrii obișnuiți sunt registre sursă sau destinație pentru asocieri de identificatori EIM sau pentru asocieri de politică. Utilizați detaliile furnizate de operația de căutare mapare de test pentru a determina dacă registrele sursă sau destinație sunt definiții pentru registrul grup. Dacă sunt, verificați proprietățile definiției pentru registrul grup pentru a determina dacă definițiile pentru registrul grup conțin membrii comuni.</li> <li>– Testul întoarce mai multe identități destinație și aceste rezultate sunt corespunzătoare pentru modul cum sunt configurate asocierile. Dacă aceasta este situația, aveți nevoie mai departe să specificați informații de căutare pentru fiecare identitate de utilizator destinație pentru a vă asigura că fiecare operație de căutare întoarce o singură identitate de utilizator destinație, mai degrabă decât toate identitățile posibile de utilizator destinație. Consultați Adăugarea de informații de căutare pentru o identitate utilizator destinație.</li> </ul> </li> </ul> <p><b>Notă:</b> Această abordare funcționează doar dacă aplicația este activată să folosească informațiile de căutare. Totuși, aplicațiile de bază i5/OS ca System i Access pentru Windows nu pot folosi informațiile de căutare pentru a distinge între identități utilizator multiple returnate de o operație de căutare. În consecință, ați putea considera redefinirea asocierilor pentru domeniu pentru a vă asigura că o operație de căutare de mapare poate returna o singură identitate utilizator destinație pentru a se asigura că aplicațiile i5/OS de bază pot realiza operații de căutare și mapare de identități cu succes.</p>

Tabela 29. Problemele obișnuite de mapare EIM și soluțiile lor (continuare)

Probleme posibile	Soluții posibile
Operațiile de căutare EIM nu întorc nici un rezultat și asocierile sunt configurate pentru domeniu.	<p>Utilizați funcția Testare mapare EIM pentru a verifica că o identitate sursă specifică mapează corect la identitatea utilizator destinație corectă. Verificați că ați furnizat informații corecte pentru test. Dacă informațiile sunt corecte și testul nu întoarce nici un rezultat, atunci problema poate fi cauzată de una din următoarele:</p> <ul style="list-style-type: none"> <li>• Configurația asocierilor este incorectă. Verificați configurația asocierilor folosind informațiile de rezolvare a problemei oferite în intrarea anterioară.</li> <li>• Suportul de asocieri politică nu este activat la nivelul domeniului. S-ar putea să fie nevoie să activați asocierile de politică pentru un domeniu.</li> <li>• Suportul de căutare mapări sau suportul de asocieri politică nu este activat la nivelul de registru individual. S-ar putea să fie nevoie să activați suportul de căutare mapări și folosirea de asocieri politică pentru registrul destinație</li> <li>• Definiția de registru și identitățile de utilizator nu se potrivesc datorită sensibilității la majuscule. Puteți șterge și recrea registrul sau șterge și recrea asocierea cu respectarea literelor mari și mici.</li> </ul>

### Operații înrudite

“Testarea mapărilor EIM” la pagina 88

Testare mapare EIM (Enterprise Identity Mapping) vă permite să emiteți operații de căutare EIM împotriva configurației EIM. Puteți folosi testul pentru a verifica că o identitate specifică de utilizator sursă se mapează corect la identitatea de utilizator destinație. Testarea asigură că operațiile de căutare mapare EIM pot returna identitatea utilizator destinație corectă bazată pe informațiile specificate.

## API-urile EIM

EIM furnizează mecanismul pentru gestionarea identității utilizatorului pe mai multe platforme. EIM are mai multe API-uri care pot fi folosite de către aplicații pentru a realiza operații EIM în numele aplicației sau în numele unui utilizator de aplicație.

Puteți folosi aceste API-uri pentru a realiza operații de căutare mapare, diferite gestionări EIM și funcții de configurare precum și modificări de informații și capabilități de interogare. Fiecare dintre aceste API-uri sunt susținute pe platformele IBM.

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

- Operații de manipulare și conectare EIM
- Administrare de domeniu EIM
- Operații registru
- Operații cu identificatori EIM
- Gestiunea asocierilor EIM
- Operații de căutare mapare EIM
- Gestiunea autorizărilor EIM

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

1. Obținere mâner EIM



2. Conectare la un domeniu EIM
3. Procesare normală a aplicației.
4. Folosirea unei API pentru operație de căutare mapare identitate EIM sau administrare EIM
5. Procesare normală a aplicației.
6. Înainte de terminare, distrugerea mânerului EIM

#### Concepte înrudite

“Planificarea pentru dezvoltarea aplicațiilor de mapare EIM (Enterprise Identity Mapping)” la pagina 66  
Pentru ca o aplicație să folosească EIM (Enterprise Identity Mapping) și să participe într-un domeniu, ea trebuie să fie capabilă să folosească API-urile EIM.

#### Informații înrudite


Enterprise Identity Mapping (EIM) APIs

---

## Informații legate de EIM (Enterprise Identity Mapping)

Publicațiile IBM Redbooks și alte colecții de subiecte din Centrul de informare conțin informații ce se înrudesc cu colecția de subiect EIM (Enterprise Identity Mapping). Puteți vizualiza sau tipări oricare dintre aceste fișiere PDF.

### IBM Redbooks

- Windows-based Single Signon and the EIM Framework on the IBM eServer iSeries Server 
- iSeries Access for Windows V5R2 Hot Topics: Tailored Images, Application Administration, SSL, and Kerberos



### Alte informații

- Single signon
- Network authentication service
- IBM Tivoli Directory Server for i5/OS (LDAP)

---

## Termenii și condițiile

Permisunile pentru utilizarea acestor publicații sunt acordate în conformitate cu următorii termeni și condiții.

**Utilizare personală:** Puteți reproduce aceste publicații pentru utilizarea personală, necomercială, cu condiția ca toate anunțurile de proprietate să fie păstrate. Nu puteți distribui, afișa sau realiza obiecte derivate din aceste publicații sau dintr-o porțiune a lor fără consimțământul explicit al IBM.

**Utilizare comercială:** Puteți reproduce, distribui și afișa aceste publicații doar în cadrul întreprinderii dumneavoastră, cu condiția ca toate anunțurile de proprietate să fie păstrate. Nu puteți să realizați lucrări derivate din aceste informații, nici să reproduceți, să distribuiți sau să afișați aceste informații sau o porțiune a lor în afara întreprinderii dumneavoastră fără consimțământul explicit al IBM.

Cu excepția a ceea ce este acordat explicit prin această permisiune, nu sunt acordate alte permisiuni, licențe sau drepturi, explicit sau implicit, pentru Publicații sau alte informații, date, software sau altă proprietate intelectuală conțină în acestea.

IBM își rezervă dreptul de a retrace permisiunile acordate aici oricând consideră că folosirea publicațiilor este în detrimentul intereselor sale sau când personalul IBM constată că instrucțiunile de mai sus nu sunt urmate corespunzător.

Nu puteți descărca, exporta sau reexporta aceste informații decât în deplină conformitate cu legile și regulamentele aplicabile, inclusiv toate legile și regulamentele de export ale Statelor Unite.

IBM NU ACORDĂ NICI O GARANȚIE PENTRU CONȚINUTUL ACESTOR PUBLICAȚII. ACESTE PUBLICAȚII SUNT FURNIZATE "CA ATARE", FĂRĂ NICI UN FEL DE GARANȚIE, EXPLICITĂ SAU IMPLICITĂ, INCLUZÂND, DAR FĂRĂ A SE LIMITA LA ELE, GARANȚIILE IMPLICITE DE VANDABILITATE, DE NEÎNCĂLCARE A UNOR DREPTURI SAU NORME ȘI DE POTRIVIRE PENTRU UN ANUMIT SCOP.

---

## Anexa. Observații

Aceste informații au fost elaborate pentru produse și servicii oferite în S.U.A.

Este posibil ca IBM să nu ofere în alte țări produsele, serviciile sau caracteristicile discutate în acest document. Luați legătura cu reprezentanța IBM locală pentru a obține informații cu privire la produsele și serviciile disponibile în zona dumneavoastră. Referirea la un produs, program sau serviciu IBM nu înseamnă că se afirmă sau că se sugerează faptul că poate fi folosit numai acel produs, program sau serviciu IBM. Poate fi folosit în loc orice produs, program sau serviciu care este echivalent din punct de vedere funcțional și care nu încalcă dreptul de proprietate intelectuală al IBM. Însă evaluarea și verificarea modului în care funcționează un produs, program sau serviciu non-IBM ține de responsabilitatea utilizatorului.

IBM poate avea brevete sau aplicații în curs de brevetare care să acopere subiectele descrise în acest document. Faptul că vi se furnizează acest document nu înseamnă că vi se acordă licența pentru aceste brevete. Puteți trimite întrebări cu privire la licențe, în scris, la:

IBM Director of Licensing  
IBM Corporation  
North Castle Drive  
Armonk, NY 10504-1785  
U.S.A.

Pentru întrebări privind licența pentru informațiile DBCS (double-byte), contactați departamentul de Proprietate intelectuală IBM din țara dumneavoastră sau trimiteți întrebările în scris la:

IBM World Trade Asia Corporation  
Licensing  
2-31 Roppongi 3-chome, Minato-ku  
Tokyo 106-0032, Japan

**Următorul paragraf nu se aplică în cazul Marii Britanii sau al altor țări unde asemenea prevederi sunt incompatibile cu legile locale:** INTERNATIONAL BUSINESS MACHINES CORPORATION OFERĂ ACEASTĂ PUBLICAȚIE “CA ATARE”, FĂRĂ NICI UN FEL DE GARANȚIE EXPLICITĂ SAU IMPLICITĂ, INCLUZÂND, DAR FĂRĂ A SE LIMITA LA GARANȚIILE IMPLICITE DE NEÎNCĂLCARE A UNOR DREPTURI SAU NORME, DE VANDABILITATE SAU DE POTRIVIRE CU UN ANUMIT SCOP. Unele state nu permit declinarea responsabilității pentru garanțiile exprese sau implicite în anumite tranzacții și de aceea este posibil ca aceste clauze să nu fie valabile în cazul dumneavoastră.

Aceste informații pot conține greșeli tehnice sau erori de tipar. Se efectuează modificări periodice la informațiile incluse aici; aceste modificări vor fi încorporate în noi ediții ale publicației. IBM poate aduce îmbunătățiri și/sau modificări produsului (produselor) și/sau programului (programelor) descrise în această publicație în orice moment, fără notificare.

Orice fel de referințe din aceste informații către situri Web non-IBM sunt furnizate doar pentru conveniență și nu servește în nici un caz ca aprobare a acelor situri Web. Materialele de pe siturile Web respective nu fac parte din materialele pentru acest produs IBM, iar utilizarea acestor situri Web se face pe propriul risc.

IBM poate utiliza sau distribui oricare dintre informațiile pe care le furnizați, în orice mod considerat adecvat, fără ca aceasta să implice vreo obligație față de dumneavoastră.

Posesorii de licențe pentru acest program care doresc să obțină informații despre el în scopul de a permite: (I) schimbul de informații între programe create independent și alte programe (inclusiv acesta) și (II) utilizarea mutuală a informațiilor care au fost schimbate, vor contacta:

IBM Corporation

Software Interoperability Coordinator, Department 49XA  
3605 Highway 52 N  
Rochester, MN 55901  
U.S.A.

Aceste informații pot fi disponibile cu condiția respectării termenilor și condițiilor, iar în unele cazuri cu plata unor taxe.

- | Programul cu licență descris în acest document și toate materialele cu licență disponibile pentru acesta sunt furnizate de către IBM conform termenilor din IBM Customer Agreement, IBM International Program License Agreement, IBM License Agreement for Machine Code sau orice contract echivalent dintre noi.

Toate datele de performanță conținute aici au fost determinate într-un mediu controlat. Prin urmare, rezultatele obținute în alte medii de operare pot varia semnificativ. Este posibil ca unele măsurători să fi fost realizate pe sisteme de nivel evoluat și nu există nici o garanție că aceste măsurători vor fi identice pe sisteme general disponibile. Mai mult, este posibil ca anumite măsurători să fi fost estimate prin extrapolare. Rezultatele reale pot varia. Utilizatorii acestui document ar trebui să verifice datele aplicabile pentru mediul lor specific.

Informațiile în legătură cu produsele non-IBM au fost obținute de la furnizorii acelor produse, din anunțurile publicate de aceștia sau din alte surse publice disponibile. IBM nu a testat acele produse și nu poate confirma acuratețea performanței, compatibilitatea sau orice alte pretenții legate de produse non-IBM. Întrebările privind capacitățile produselor non-IBM se pot adresa furnizorilor acelor produse.

Toate declarațiile privind orientarea viitoare sau intențiile IBM sunt supuse modificării sau retractării fără o înștiințare prealabilă și reprezintă doar ținte și obiective.

Toate prețurile IBM arătate sunt prețurile cu amănuntul sugerate de IBM, sunt curente și pot fi modificate fără notificare. Prețurile dealer-ului pot fi diferite.

Aceste informații sunt doar în scop de planificare. Informațiile menționate aici se pot modifica înainte ca produsele descrise să devină disponibile pe piață.

Aceste informații conțin exemple de date și rapoarte folosite în operații de afaceri zilnice. Pentru a fi cât mai complete, exemplele includ nume de persoane, de companii, de mărci și de produse. Toate aceste nume sunt fictive și orice asemănare cu nume și adrese utilizate de o întreprindere reală este pur întâmplătoare.

#### LICENȚĂ DE COPYRIGHT:

Aceste informații cuprind exemple de programe de aplicație în limbaj sursă, care ilustrează tehnici de programare pe diverse platforme de operare. Puteți copia, modifica și distribui aceste programe-eșantion în orice formă fără necesitatea unei plăți către IBM, în scopul dezvoltării, utilizării, marketingului sau distribuirii programelor de aplicație în concordanță cu interfața de programare a aplicației pentru platforma de operare pentru care sunt scrise programele-eșantion. Aceste exemple nu au fost testate complet în toate condițiile. Prin urmare, IBM nu poate garanta sau sugera că aceste programe vor fi fiabile, practice sau funcționale.

Fiecare copie sau orice porțiune din aceste exemple de program sau orice lucrare derivată din acestea trebuie să includă un anunț de copyright de genul următor:

© (numele companiei dumneavoastră) (anul). Porțiuni din acest cod sunt derivate din Programe eșantion ale IBM Corp.  
© Copyright IBM Corp. \_introduceți anul sau anii\_. Toate drepturile rezervate.

Dacă vedeți aceste informații folosind o copie electronică, fotografiile și ilustrațiile color s-ar putea să nu apară.

---

## Mărci comerciale

Următorii termeni sunt mărci comerciale deținute de International Business Machines Corporation în Statele Unite, în alte țări sau ambele:

AIX  
Distributed Relational Database Architecture  
Domino  
DRDA  
eServer  
i5/OS  
IBM  
iSeries  
Lotus Notes  
NetServer  
OS/400  
pSeries  
RACF  
RDN  
System i  
Tivoli  
WebSphere  
xSeries  
z/OS

- | Adobe, logo-ul Adobe, PostScript și logo-ul PostScript sunt fie mărci comerciale înregistrate sau mărci comerciale
- | Adobe Systems Incorporated în Statele Unite și/sau alte țări.
  
- | Linux este o marcă comercială înregistrată a Linus Torvalds în Statele Unite, alte țări sau ambele.

Microsoft, Windows, Windows NT și logo-ul Windows sunt mărci comerciale ale corporației Microsoft din Statele Unite, din alte țări sau ambele.

UNIX este o marcă comercială înregistrată a The Open Group din Statele Unite și din alte țări.

Alte nume de companii, produse sau servicii pot fi mărci comerciale sau mărci de serviciu ale altora.

---

## Termenii și condițiile

Permisunile pentru utilizarea acestor publicații sunt acordate în conformitate cu următorii termeni și condiții.

**Utilizare personală:** Puteți reproduce aceste publicații pentru utilizarea personală, necomercială, cu condiția ca toate anunțurile de proprietate să fie păstrate. Nu puteți distribui, afișa sau realiza obiecte derivate din aceste publicații sau dintr-o porțiune a lor fără consimțământul explicit al IBM.

**Utilizare comercială:** Puteți reproduce, distribui și afișa aceste publicații doar în cadrul întreprinderii dumneavoastră, cu condiția ca toate anunțurile de proprietate să fie păstrate. Nu puteți să realizați lucrări derivate din aceste informații, nici să reproduceți, să distribuiți sau să afișați aceste informații sau o porțiune a lor în afara întreprinderii dumneavoastră fără consimțământul explicit al IBM.

Cu excepția a ceea ce este acordat explicit prin această permisiune, nu sunt acordate alte permisiuni, licențe sau drepturi, explicit sau implicit, pentru Publicații sau alte informații, date, software sau altă proprietate intelectuală conținută în acestea.

IBM își rezervă dreptul de a retrage permisiunile acordate aici oricând consideră că folosirea publicațiilor este în detrimentul intereselor sale sau când personalul IBM constată că instrucțiunile de mai sus nu sunt urmate corespunzător.

Nu puteți descărca, exporta sau reexporta aceste informații decât în deplină conformitate cu legile și regulamentele aplicabile, inclusiv toate legile și regulamentele de export ale Statelor Unite.

IBM NU ACORDĂ NICI O GARANȚIE PENTRU CONȚINUTUL ACESTOR PUBLICAȚII. ACESTE PUBLICAȚII SUNT FURNIZATE "CA ATARE", FĂRĂ NICI UN FEL DE GARANȚIE, EXPLICITĂ SAU IMPLICITĂ, INCLUZÂND, DAR FĂRĂ A SE LIMITA LA ELE, GARANȚIILE IMPLICITE DE VANDABILITATE, DE NEÎNCĂLCARE A UNOR DREPTURI SAU NORME ȘI DE POTRIVIRE PENTRU UN ANUMIT SCOP.





Tipărit în S.U.A.