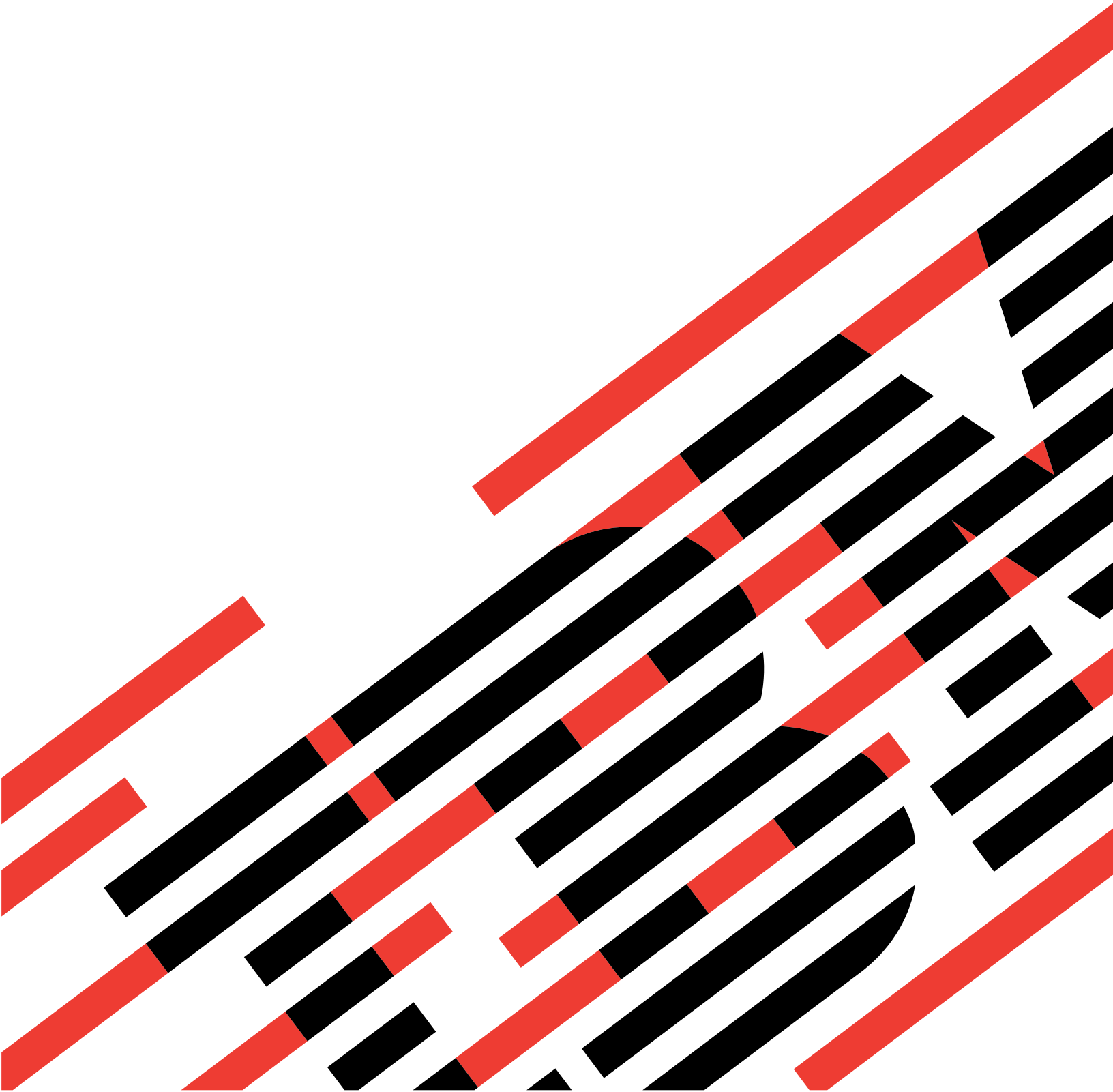
IBM

eserver

iSeries

Enterprise Identity Mapping



IBM

@server

iSeries

Enterprise Identity Mapping

Sadržaj

Mapiranje identiteta u poduzeću (EIM)

Mnoga mrežna poduzeća suočavaju se s problemom višestrukih korisničkih registara, što zahtijeva da svaka osoba ili cjelina unutar poduzeća ima korisnički identitet u svakom registru. Potreba za višestrukim korisničkim registrima brzo raste u veliki administrativni problem koji utječe na korisnike, administratore i razvijače aplikacija. Mapiranje identiteta u poduzeću (EIM) omogućuje jeftino rješenje za lakše upravljanje višestrukim korisničkim registrima i korisničkim identitetima u vašem poduzeću.

EIM je mehanizam za mapiranje (udruživanje) osobe ili cjeline u prikladni korisnički identitet u različitim registrima kroz poduzeće. EIM osigurava API-je za kreiranje i upravljanje ovim odnosima mapiranja identiteta, ako i API-je koje aplikacija koristi za upit ove informacije. U dodatku, OS/400(R) koristi EIM i Kerberos mogućnosti za dobavljanje okruženja jednostruke prijave.

iSeries Navigator, iSeries grafičko korisničko sučelje, dobavlja čarobnjake za konfiguriranje i upravljanje EIM-om. U dodatku, administratori mogu upravljati EIM odnosima za korisničke profile kroz iSeries Navigator.

iSeries(TM) poslužitelj koristi EIM za omogućavanje OS/400 sučelja kod provjere autentičnosti korisnika u smislu mrežne usluge provjere autentičnosti. Aplikacije, kao i OS/400, mogu prihvatiti Kerberos ulaznice i koristiti EIM za pronalaženje korisničkog profila koji predstavlja istu osobu koju Kerberos ulaznica predstavlja.

Sljedeća poglavlja osiguravaju specifične informacije o EIM-u:

Ispis ovog poglavlja
Ispis PDF-a ovog EIM poglavlja i drugih srodnih poglavlja.

Pregled Mapiranja identiteta u poduzeću
Naučite o problemima koje vam EIM pomaže riješiti, trenutne industrijske pristupe ovim problemima i zašto je EIM pristup bolje rješenje.

EIM koncepti
Naučite o EIM konceptima koje morate razumjeti za uspješno implementiranje EIM-a.

LDAP koncepti za EIM
Naučite o Lightweight Directory Access Protocol (LDAP) konceptima koje morate razumjeti za uspješno implementiranje EIM-a.

Omogućenje jednostruke prijave
Pročitajte o koristi koju EIM osigurava pojednostavljenjem prijave korisnika.

Plan za EIM
Budite uvjereni da imate konfigurirane sve potrebne usluge i aplikacije prije konfiguriranja EIM-a.

Konfiguracija EIM-a
Koristite Čarobnjaka konfiguracije Mapiranja identiteta u poduzeću (dalje u tekstu kao EIM Konfiguracijski čarobnjak) za početak s EIM-om.

Upravljanje EIM-om
Upravljajte EIM svojstvima, korisničkim registrima, EIM korisničkim ovlaštenjima i mnogo više.

API-ji za EIM
Koristite EIM API-je u vašim aplikacijama i mreži.

Uklanjanje pogrešaka EIM-a
Pronađite rješenja zajedničkih problema i grešaka koje se mogu desiti kod korištenja EIM-a u vašoj mreži.

Srodne informacije za EIM
Veza na srodne informacije o EIM-u.

Ispis teme na pisač

Za pregled ili spuštanje PDF verzije, odaberite Mapiranje identiteta u poduzeću

(oko 390 KB ili 50 stranica).

Ostale informacije

Možete pregledati ili spustiti srodna poglavlja:

- Mrežna usluga provjere autentičnosti (oko 199 KB ili 60 stranica) sadrži informacije o tome kako konfigurirati mrežnu uslugu provjere autentičnosti zajedno s EIM-om za kreiranje okruženja jednostruke prijave.
- Usluge Direktorija (LDAP) (oko 323 KB ili 66 stranica) sadrži informacije o tome kako konfigurirati LDAP poslužitelj, kojeg možete koristiti kao kontroler EIM domene, zajedno s informacijama o naprednoj LDAP konfiguraciji.

Spremanje PDF datoteka

Da spremite PDF na vašu radnu stanicu za gledanje ili ispis:

1. Otvorite PDF u vašem pretražitelju (kliknite na vezu iznad).
2. U izborniku vašeg pretražitelja, kliknite **File**.
3. Kliknite **Spremi kao...**
4. Izaberite direktorij u koji želite spremiti PDF datoteku.
5. Kliknite **Save**.

Spuštanje Adobe Acrobat Reader-a

Ako trebate Adobe Acrobat Reader za pregled ili ispis ovih PDF-ova, možete spustiti kopiju s Adobe Web stranice (www.adobe.com/prodindex/acrobat/readstep.html)

.

Pregled Mapiranja identiteta u poduzeću

Današnje mrežno okruženje napravljeno je od kompleksne grupe sistema i aplikacija, rezultirajući potrebom za upravljanjem s više korisničkih registara. Bavljenje s višestrukim korisničkim registrima brzo raste u veliki administrativni problem koji utječe na korisnike, administratore i razvijače aplikacija. Prema tome, mnoge tvrtke se bore za sigurno upravljanje provjerom autentičnosti i autorizacije za sisteme i aplikacije. Mapiranje identiteta u poduzeću (EIM) je tehnologija infrastrukture IBM

koja dozvoljava administratorima i razvijačima aplikacija da adresiraju ovaj problem lakše i jeftinije nego što je prije bilo moguće.

Sljedeće informacije opisuju probleme, izdvajaju trenutne industrijske pristupe i objašnjavaju zašto je EIM pristup bolji.

Problem upravljanja višestrukim korisničkim registrima

Mnogi administratori upravljaju mrežama koje uključuju različite sisteme i poslužitelje, svaki s jedinstvenim načinom upravljanja korisnicima kroz različite korisničke registre. U ovim kompleksnim mrežama, administratori su odgovorni za upravljanje svakim korisničkim identitetom i lozinkom kroz višestruke sisteme. Dodatno, administratori često moraju sinkronizirati ove identitete i lozinke, a korisnici su opterećeni s pamćenjem višestrukih identiteta i lozinki i njihovim usklađivanjem. Opterećenost korisnika i administratora u ovom okruženju je pretjerana. Isto tako, administratori često troše vrijedno vrijeme u ispravljanju pogrešaka neuspjelih pokušaja prijava te resetiranjem zaboravljenih lozinki umjesto upravljanjem poduzeća.

Problem upravljanja višestrukih korisničkih registara također utječe na razvijače aplikacije koji žele osigurati višestruko povezane ili heterogene aplikacije. Ovi razvijači razumiju da korisnici imaju važnih poslovnih podataka raspršenih kroz mnoge različite tipove sistema, gdje svaki sistem posjeduje svoje vlastite korisničke registre. Nadalje, razvijači moraju kreirati vlasničke korisničke registre i udružene sigurnosne semantike za njihove aplikacije. Iako ovo rješava problem za razvijača aplikacije, također i povećeva opterećenje za korisnike i administratore.

Trenutni pristupi

Dostupno je nekoliko trenutnih industrijskih prilaza rješavanju problema upravljanja višestrukim korisničkim registrima, ali svi oni dobavljaju nepotpuna rješenje. Na primjer, Lightweight Directory Access Protocol (LDAP) osigurava rješenje distribuiranog korisničkog registra. Međutim, korištenje LDAP-a (ili drugih popularnih rješenja kao što je Microsoft Passport) znači da administratori moraju upravljati još jednim korisničkim registrom i semantikama sigurnosti ili moraju zamijeniti postojeće aplikacije koje su izgrađene za korištenje tih registara.

Korištenjem ovog tipa rješenja, administratori moraju upravljati višestrukim sigurnosnim mehanizmima za individualne resurse, čime se povećava administrativno opterećenje i potencijalno se povećava mogućnost sigurnosnog izlaganja. Kada višestruki mehanizmi podržavaju jedan resurs, šanse mijenjanja ovlaštenja kroz jedan mehanizam i zaboravljanja promjene ovlaštenja za jedan ili više drugih mehanizama, mnogo su veće. Na primjer, sigurnosno izlaganje može rezultirati kada je korisniku prikladno odbijen pristup kroz jedno sučelje, ali dozvoljen je pristup kroz jedan ili više drugih sučelja.

Nakon dovršenja ovog posla, administratori pronalaze da nisu u potpunosti riješili problem. Općenito, poduzeća su investirala previše novca u trenutne korisničke registre i u njihove udružene sigurnosne semantike kako bi korištenje ovog tipa rješenja bilo praktično. Kreiranje drugog korisničkog registra i udružene sigurnosne semantike rješava problem za dobavljača aplikacije, ali ne i probleme za korisnike i administratore.

Drugo moguće rješenje je korištenje pristupa jednostruke prijave. Dostupno je nekoliko proizvoda koji dozvoljavaju administratorima da upravljaju datotekama koje sadrže sve korisničke identitete i lozinke. Međutim, ovaj pristup ima nekoliko slabosti:

- Adresira samo jedan od problema s kojim se korisnici suočavaju. Iako dozvoljava prijavu korisnika na višestruke sisteme dobavljajući identitet i lozinku, ono ne eliminira potrebu korisnika da ima lozinku na drugim sistemima ili potrebu za upravljanjem ovim lozinkama.
- Predstavlja novi problem kreiranjem sigurnosnih izlaganja, jer su čisti tekst ili lozinke s mogućnošću dešifriranja spremljeni u ovim datotekama. Lozinke nikad ne bi trebale biti spremljene u datotekama čistog teksta ili biti lako dostupne bilo kome, uključujući i administratorima.
- To ne rješava probleme razvijača aplikacije treće strane, koji dobavljaju heterogene, višestruko povezane aplikacije. Oni još uvijek moraju dobaviti vlasničke korisničke registre za njihove aplikacije.

Usprkos slabostima, neka poduzeća odabrala su prihvaćanje ovakvih pristupa, jer osiguravaju neko olakšanje za probleme višestrukog korisničkog registra.

EIM pristup

EIM nudi novi pristup za omogućavanje jeftinih rješenja u lakom upravljanju korisničkim registrima i korisničkim identitetima u poduzeću. EIM je arhitektura za opisivanje odnosa između pojedinaca ili cjelina (kao poslužitelji datoteka i poslužitelji ispisa) u poduzeću i mnogih identiteta koji ih predstavljaju unutar poduzeća. U dodatku, EIM osigurava skup API-ja koji dozvoljavaju aplikacijama da postavljaju pitanja o ovim odnosima.

Na primjer, danim korisničkim identitetom u jednom korisničkom registru, možete odrediti koji korisnički identitet u drugom korisničkom registru predstavlja istu osobu. Ako je korisniku provjerena autentičnost s jednim korisničkim identitetom i možete mapirati taj korisnički identitet u prikladni identitet drugog korisničkog registra, tada korisnik ne treba osiguravati vjerodostojnost kod ponovne provjere autentičnosti. Znate tko je korisnik i samo trebate znati koji korisnički identitet predstavlja tog korisnika u drugom korisničkom registru. Zbog toga, EIM osigurava generaliziranu funkciju mapiranja identiteta za poduzeće.

Mogućnost mapiranja između korisničkih identiteta u različitim korisničkim registrima osigurava mnoge koristi. Primarno, to znači da aplikacije mogu imati fleksibilnost korištenja jednog korisničkog registra za provjeru autentičnosti dok koriste potpuno drugačiji korisnički registar za autorizaciju. Na primjer, administrator bi mogao mapirati SAP identitet (ili još bolje, SAP bi mogao sam napraviti mapiranje) za pristup SAP resursima.

Upotreba mapiranja identiteta zahtijeva da administratori učine sljedeće:

1. Kreiraju EIM identifikatore koji predstavljaju ljude ili cjeline u njihovom poduzeću.
2. Kreiraju definicije EIM registra koje opisuju postojeće korisničke registre u njihovom poduzeću.
3. Definiraju odnos između korisničkih identiteta u onim registrima EIM identifikatora gdje su kreirani.

Nisu potrebne promjene kodne stranice za postojeće korisničke registre. Administrator ne treba imati mapiranja za sve identitete u korisničkom registru. EIM dozvoljava jedno-u-mnoga mapiranja (drugim riječima, jedan korisnik s više od jednog korisničkog identiteta u jednom korisničkom registru). EIM također dozvoljava mnoga-u-jedno mapiranja (drugim riječima, višestruki korisnici koji dijele identitet u jednom korisničkom registru, što, iako podržano, nije preporučljivo). Administrator može predstavljati bilo koji korisnički registar bilo kojeg tipa u EIM-u.

EIM je otvorena arhitektura koje administratori mogu koristiti za predstavljanje odnosa mapiranja identiteta za bilo koji registar. Ne zahtijeva kopiranje postojećih podataka u novo spremište i pokušava održati obje kopije sinkroniziranim. Jedini novi podaci koje EIM predstavlja su informacije odnosa. Administratori upravljaju ovim podacima u LDAP direktoriju, koji dobavlja fleksibilnost upravljanja podacima na jednom mjestu i postojanost kopija gdje god se informacije koriste. Konačno, EIM daje poduzećima i razvijačima aplikacija fleksibilnost za lagani rad u širokom rasponu okruženja s manje troška nego što je to moguće bez ove podrške.

EIM koncepti

Konceptualno razumijevanje o tome kako radi Mapiranje identiteta u poduzeću (EIM) potrebno je za potpuno razumijevanje kako možete koristiti EIM u vašem poduzeću. Iako se konfiguracija i implementacija EIM API-ja može razlikovati među platformama poslužitelja, EIM koncepti su zajednički kroz platforme

.

Slika 1 osigurava primjer EIM implementacije u poduzeću. Tri poslužitelja ponašaju se kao EIM-omogućene aplikacije koje zahtijevaju EIM podatke korištenjem operacije EIM pregledavanja

6

. Kontroler domene

1

sprema informacije o EIM domeni

2

, što uključuje EIM identifikator

3

, udruženja

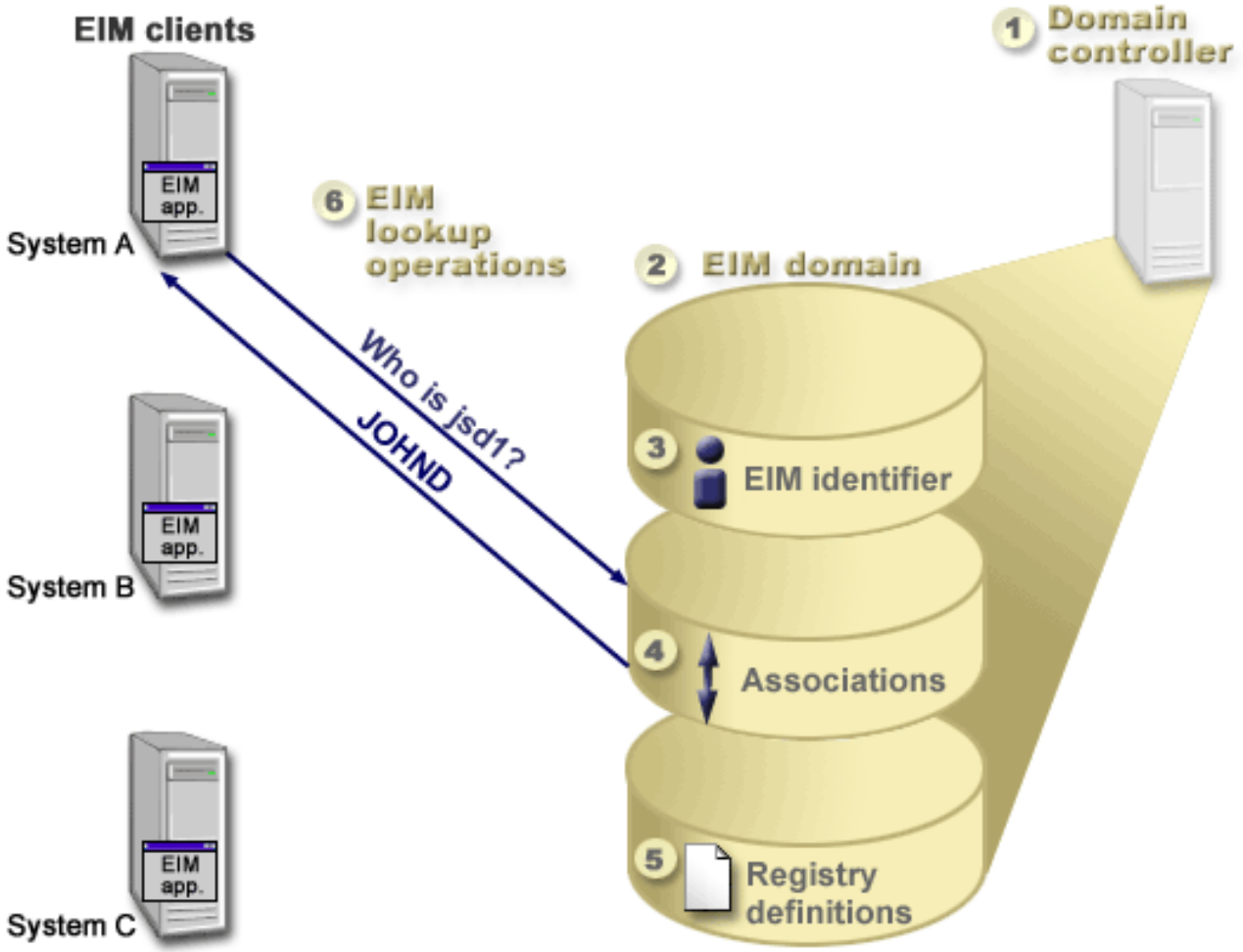
4

između ovih EIM identifikatora i korisničkih identiteta i definicije EIM registra

5

.

Slika 1: Primjer EIM implementacije



Pregledajte sljedeće informacije da naučite više o ovim EIM konceptima:

- Kontroler EIM domene
- EIM domena
- EIM identifikator
- Definicije EIM registra
- EIM udruženja
- Operacija EIM pregledavanja
- EIM ovlaštenja

Kontroler EIM domene

Kontroler EIM domene je poslužitelj Lightweight Directory Access Protokola (LDAP), konfiguriran za upravljanja s bar jednom EIM domenom. *EIM domena* je LDAP direktorij koji se sastoji od svih EIM identifikatora, EIM udruženja i korisničkih registara koji su definirani u toj domeni. Sistemi (EIM klijenti) sudjeluju u EIM domeni korištenjem podataka domene za operacije EIM pregledavanja. Mora postojati najmanje jedan kontroler EIM domene u poduzeću.

Trenutno možete konfigurirati neke IBM platforme

da se ponašaju kao kontroler EIM domene. Svaki sistem koji podržava EIM API-je može sudjelovati kao klijent u domeni. Ovi klijent sistemi koriste EIM API-je za kontaktiranje kontrolera EIM domene radi izvođenja EIM operacija pregledavanja.

Lokacija EIM klijenta određuje da li je kontroler EIM domene lokalni ili udaljeni sistem. Kontroler domene je *lokalni* ako se EIM klijent izvodi na istom sistemu kao i kontroler domene. Kontroler domene je *udaljeni* ako se EIM klijent izvodi na odvojenom sistemu od kontrolera domene.

EIM domena

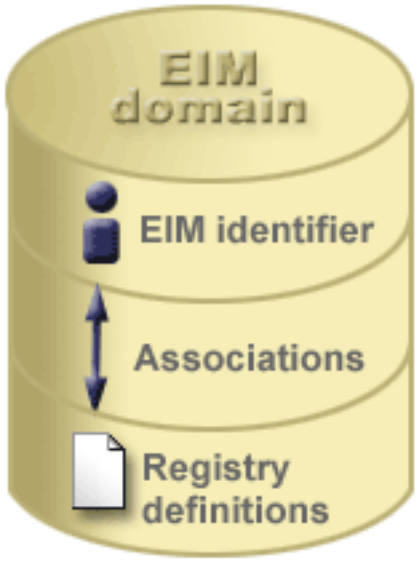
EIM domena je direktorij unutar poslužitelja Lightweight Directory Access Protokola (LDAP) koji sadrži EIM podatke za poduzeće. EIM domena je skup svih EIM identifikatora, EIM udruženja i korisničkih registara koji su definirani u toj domeni. Sistemi (EIM klijenti) sudjeluju u domeni korištenjem domenskih podataka za EIM operacije pregledavanja.

EIM domena se razlikuje od korisničkog registra. Korisnički registar definira skup korisničkih identiteta poznatih i provjerenih od pojedinačne instance operativnog sistema ili aplikacije. Korisnički registar također sadrži informacije potrebne za provjeru autentičnosti korisnika identiteta. Dodatno, korisnički registar često sadrži druge atribute kao što su korisničke preference, sistemske privilegije ili osobne informacije za taj identitet.

Nasuprot tomu, EIM domena *odnosi* se na korisničke identitete, definirane u korisničkim registrima. EIM domena sadrži informacije o *odnosima* između identiteta u različitim korisničkim registrima (korisničko ime, tip registra i instanca registra) i stvarne ljude ili cjeline koje ovi identiteti predstavljaju. Budući da EIM prati samo informacije odnosa, nema se što sinkronizirati između korisničkih registara i EIM-a.

Slika 2 prikazuje podatke spremljene unutar EIM domene. Ovi podaci uključuju EIM identifikatore, definicije EIM registra i EIM udruženja. EIM podaci definiraju odnos između korisničkih identiteta i ljudi ili cjelina koje ovi identiteti predstavljaju u poduzeću.

Slika 2: EIM domena i podaci spremljeni unutar domene



EIM podaci uključuju:

- **EIM identifikatore.** Svaki EIM identifikator koji kreirate predstavlja osobu ili cjelinu (kao što je poslužitelj ispisa ili poslužitelj datoteka) unutar poduzeća. Pogledajte EIM identifikator za više informacija.

- **Definicije EIM registra.** Svaka definicija EIM registra koju kreirate predstavlja stvarni korisnički registar (i informacije korisničkog identiteta koje sadrži) koji postoji na sistemu unutar poduzeća. Jednom kada ste definirali specifični korisnički registar u EIM-u, taj korisnički registar može sudjelovati u EIM domeni. Pogledajte Definicije EIM registra za više informacija.
- **EIM udruženja.** Svako EIM udruženje koje kreirate predstavlja odnos između EIM identifikatora i udruženog identiteta unutar poduzeća. Vi kreirate adruženja za identitete u korisničkim registrima koji sudjeluju u EIM domeni. Udruženja osiguravaju informacije koja vežu EIM identifikator sa specifičnim korisničkim identitetom u specifičnom korisničkom registru. Prema tome, udruženja moraju biti definirana tako da EIM klijenti mogu koristiti EIM API-je za izvođenje EIM operacija pregledavanja. Ove EIM operacije pregledavanja pretražuju EIM domenu za definirana udruženja između EIM identifikatora i korisničkih identiteta u prepoznatim korisničkim registrima. Pogledajte EIM operacije pregledavanja za više informacija.

Kada jednom kreirate vaše EIM identifikatore, definicije registra i udruženja, možete započeti s korištenjem EIM-a da lakše organizirate posao s korisničkim identitetima unutar vašeg poduzeća.

EIM identifikator

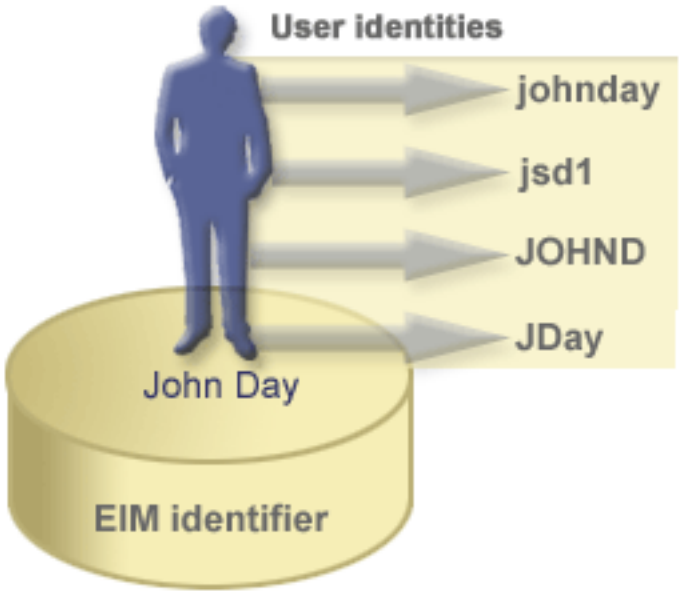
EIM identifikator predstavlja osobu ili cjelinu u poduzeću. Tipična mreža sastoji se od različitih hardverskih platformi i aplikacija i njihovih udruženih korisničkih registara. Mnoge platforme i mnoge aplikacije koriste platformski specifične ili aplikacijski specifične korisničke registre. Ovi korisnički registri sadrže sve informacije identifikacije korisnika za korisnike koji rade s ovim poslužiteljima ili aplikacijama.

Kada kreirate EIM identifikator i udružite ga s različitim korisničkim identitetima za osobu ili cjelinu, tada postaje lakše izgraditi heterogene, višestruko povezane aplikacije, na primjer, okruženje jednostruke prijave. Kada kreirate EIM identifikator i udruženja, također postaje lakše izgraditi i koristiti alate koji pojednostavljuju administraciju uključenu u upravljanje svakim korisničkim identitetom koje osoba ili cjelina ima unutar poduzeća.

EIM identifikator koji predstavlja osobu

Slika 3 prikazuje primjer EIM identifikatora koji predstavlja osobu *John Day* i ima različite korisničke identitete u poduzeću. U ovom primjeru, osoba *John Day* ima četiri korisnička identiteta u četiri različita korisnička registra: johnday, jsd1, JOHND i JDay.

Slika 3: Odnos između EIM identifikatora za *John Day* i njegovi različiti korisnički identiteti

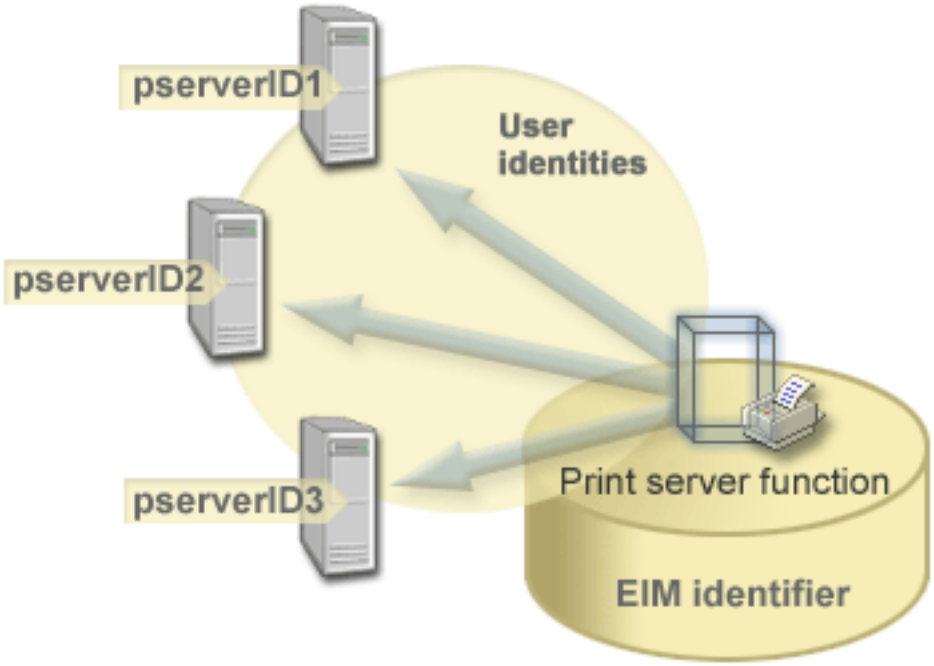


U EIM-u možete kreirati udruženja koja definiraju odnose između John Day identifikatora i svakog od različitih korisničkih identiteta za *John Day*. Kreiranjem ovih udruženja za definiranje ovih odnosa, vi i drugi možete pisati aplikacije koje koriste EIM API-je za traženje potrebnog, ali nepoznatog korisničkog identiteta na osnovu poznatog korisničkog identiteta.

EIM identifikator koji predstavlja cjelinu

U dodatku predstavljanja korisnika, EIM identifikatori mogu predstavljati cjeline unutar poduzeća kao što to prikazuje slika 4. Na primjer, često se funkcija poslužitelja ispisa u poduzeću izvodi na mnogim sistemima. Na slici 4, funkcija poslužitelj ispisa u poduzeću, izvodi se na tri različita sistema pod tri različita korisnička identiteta pserverID1, pserverID2 i pserverID3.

Slika 4: Odnos između EIM identifikatora koji predstavlja funkciju poslužitelja ispisa i različiti korisnički identiteti za tu funkciju.



S EIM-om možete kreirati pojedinačni identifikator koji predstavlja funkciju poslužitelja ispisa unutar poduzeća. U ovom primjeru, EIM identifikator funkcije poslužitelja ispisa predstavlja stvarnu cjelinu poslužitelj ispisa u poduzeću. Udruženja su kreirana za definiranje odnosa između EIM identifikatora (funkcija poslužitelja ispisa) i svakog od korisničkih identiteta za ovu funkciju (pserverID1, pserverID2, i pserverID3). Ove aplikacije dozvoljavaju razvijačima aplikacije da koriste EIM operacije pregledavanja za pronalaženje specifične funkcije poslužitelja ispisa. Dobavljači aplikacije mogu tada lakše pisati distribuirane aplikacije koje upravljaju funkcijom poslužitelja kroz poduzeće.

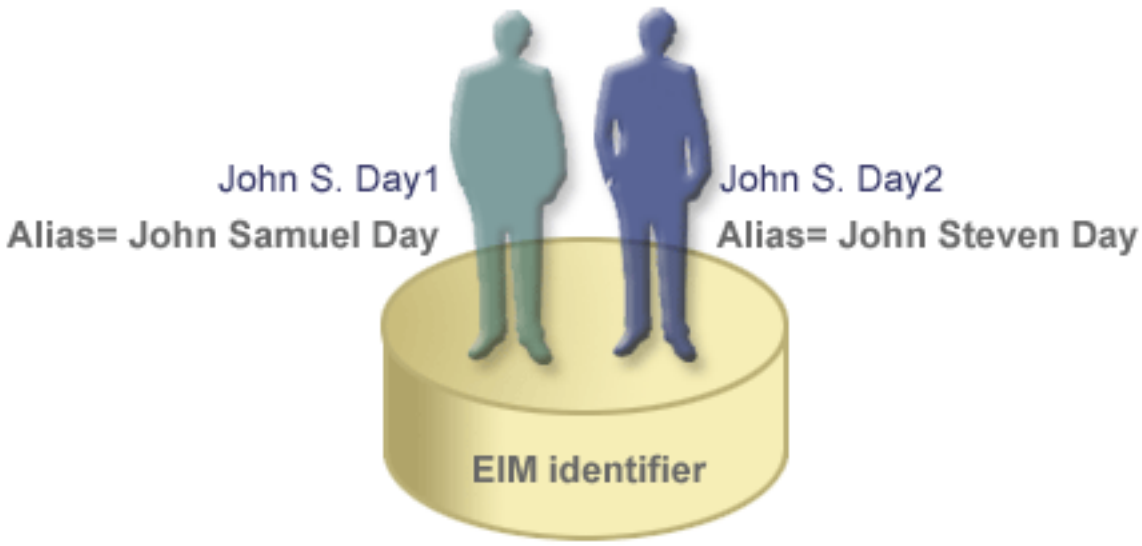
EIM identifikatori i zamjensko ime

Također možete kreirati zamjenska imena za EIM.identifikatore. Zamjenska imena mogu pomoći u lociranju specifičnog EIM identifikatora kod izvođenja EIM operacije pregledavanja. Na primjer, zamjenska imena mogu biti korisna u situacijama gdje je nečije zakonito ime drugačije od imena pod kojim je ta osoba poznata.

Imena EIM identifikatora moraju biti jedinstvena u EIM domeni. Zamjenska imena mogu pomoći u adresiranju situacija gdje korištenje jedinstvenih imena identifikatora može biti teško. Na primjer, različite individue unutar poduzeća mogu dijeliti isto ime, što može biti zbunjujuće ako koristite prava imena kao EIM identifikatore.

Slika 5 prikazuje primjer gdje poduzeće ima dva korisnika s imenom *John S. Day*. EIM administrator kreira dva različita EIM identifikatora da napravi razliku među njima: John S. Day1 i John S. Day2. Međutim, koji *John S. Day* je predstavljen s bilo kojim od ovih identifikatora nije odmah vidljivo.

Slika 5: Zamjenska imena za sva EIM identifikatora na osnovu dijeljenog pravog imena *John S. Day*



Korištenjem zamjenskih imena, EIM administrator može dobaviti dodatne informacije o pojedincu za svaki EIM identifikator. Ove informacije također se mogu koristiti u operaciji EIM pregledavanja za razlikovanje korisnika koje identifikator predstavlja. Na primjer, zamjensko ime za John S. Day1 može biti John Samuel Day i zamjensko ime za John S. Day2 može biti John Steven Day.

Svaki EIM identifikator može imati višestruka zamjenska imena za identificiranje kojeg *John S. Daya* EIM identifikator predstavlja. EIM administrator može dodati drugo zamjensko ime svakom od EIM identifikatora za dva pojedinca kako bi ih još više razlikovao. Na primjer, dodatna zamjenska imena mogu sadržavati korisnikov broj posla, broj odjela, naslov posla ili druge razlikovne atribute.

Definicije EIM registra

Definicija EIM registra predstavlja stvarni korisnički registar koji postoji na sistemu unutar poduzeća. Korisnički registar djeluje kao direktorij i sadrži listu važećih korisničkih identiteta za pojedinačni sistem ili aplikaciju. Osnovni korisnički registar sadrži korisničke identitete i njihove lozinke. Jedan primjer korisničkog registra je z/OS Security Server Resource Access Control Facility (RACF(R)) registar. Korisnički registri mogu sadržavati i druge informacije. Na primjer, Lightweight Directory Access Protocol (LDAP) direktorij sadrži vezana razlikovna imena, lozinke i kontrole pristupa podacima koji su spremljeni u LDAP-u. Drugi primjeri zajedničkih korisničkih registara su Kerberos centar distribucije ključa (KDC) i registar OS/400 korisničkih profila.

Definicije EIM registra osiguravaju informacije koje se odnose na korisničke registre u poduzeću. Administrator definira ove registre u EIM-u dobavljanjem sljedećih informacija:

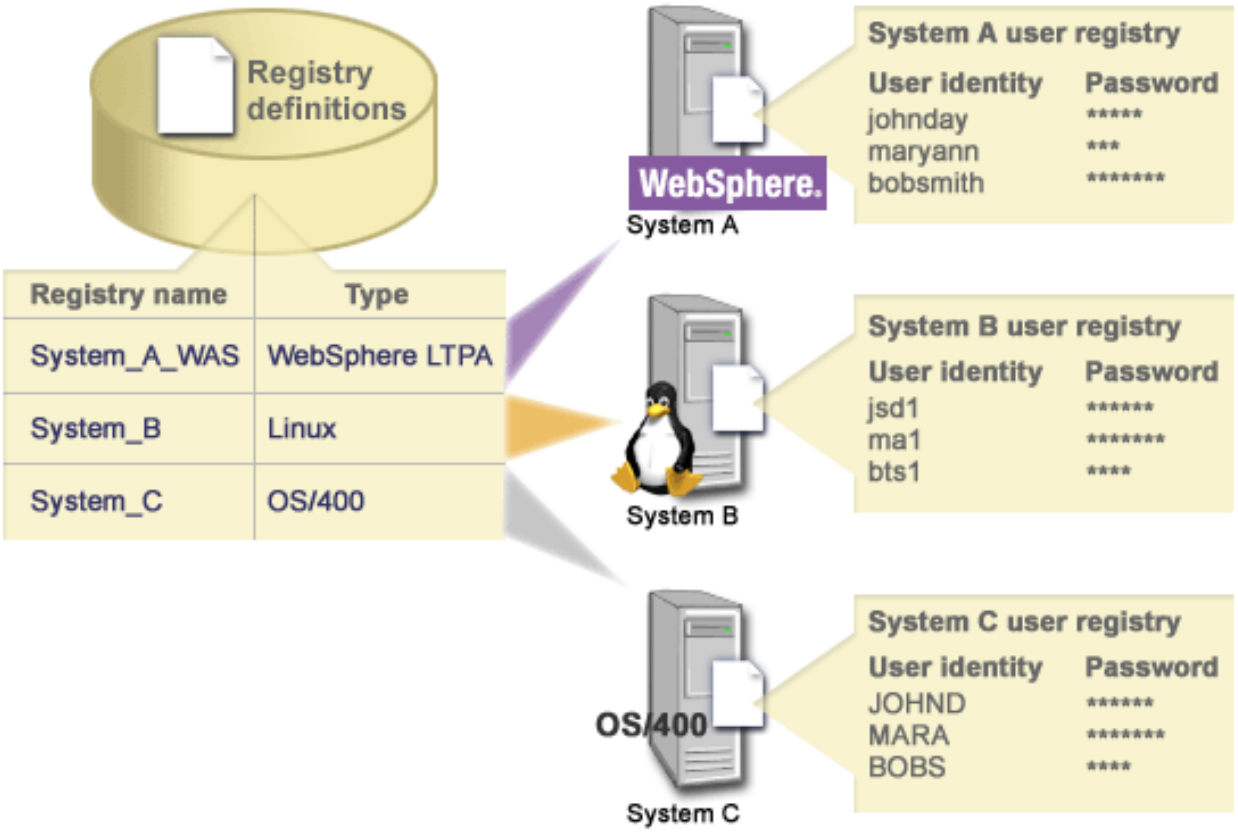
- Jedinstveno, proizvoljno ime EIM registra
- Tip korisničkog registra

Svaka definicija registra predstavlja specifičnu instancu korisničkog registra. Prema tome, trebali biste odabrati ime definicije EIM registra koje vam pomaže u identificiranju pojedinačne instance korisničkog registra. Na primjer, mogli bi odabrati TCP/IP ime hosta za sistemski korisnički registar, ili ime hosta kombinirano s imenom aplikacije za aplikacijski korisnički registar. Možete koristiti bilo koju kombinaciju alfanumeričkih znakova, različite veličine slova i razmake za kreiranje jedinstvenih imena definicije EIM registra.

Na slici 6, administrator je kreirao definicije EIM registra za korisničke registre koji predstavljaju Sistem A, Sistem B i Sistem C. Na primjer, Sistem A sadrži korisnički registar za WebSphere Lightweight Third-Party Authentication (LTPA). Ime definicije registra kojeg administrator koristi, pomaže u identificiranju specifičnih

pojavljivanja tipa korisničkog registra. Na primjer, IP adresa ili ime hosta često je dovoljno za mnoge tipove korisničkih registara. U ovom primjeru, administrator identificira specifičnu instancu korisničkog registra korištenjem System_A_WAS za ime definicije registra. U dodatku imenu, administrator također osigurava tip registra kao WebSphere LTPA.

Slika 6: Definicije EIM registra za tri korisnička registra u poduzeću



Također možete definirati korisničke registre koji postoje unutar drugih korisničkih registara. Na primjer, z/OS Security Server (RACF) registar može sadržavati specifične korisničke registre koji su podskup korisnika unutar ukupnog RACF korisničkog registra. Za detaljniji primjer o tome kako ovo radi, pogledajte Definicije sistemskog i aplikacijskog registra.

Definicije EIM registra i zamjensko ime

Također možete kreirati zamjenska imena za definicije EIM registra. Možete koristiti predefinirane tipove zamjenskog imena ili možete sami definirati tipove zamjenskog imena za korištenje. Predefinirani tipovi zamjenskog imena uključuju:

- Sistem imena domene (DNS) ime hosta
- Kerberos područje
- Razlikovno ime izdavača (DN)
- Korijensko razlikovno ime (DN)
- TCP/IP adresa
- LDAP DNS ime hosta

Ova podrška zamjenskog imena dozvoljava programerima da pišu aplikacije bez unaprijed poznavanja proizvoljnog imena EIM registra odabranog od administratora koji razvija aplikaciju. Dokumentaciju aplikacije može dobaviti EIM administrator sa zamjenskim imenom kojeg aplikacija koristi. Korištenjem ove informacije, EIM administrator može dodijeliti ovo zamjensko ime definiciji EIM registra koja predstavlja stvarni korisnički registar za kojeg administrator želi da ga aplikacija koristi.

Kada administrator doda zamjensko ime definiciji EIM registra, aplikacija može izvesti pretraživanje zamjenskog imena da pronađe ime EIM registra i inicijalizaciju. Pregledavanje po zamjenskom imenu dozvoljava aplikaciji da odredi ime ili imena EIM registra za korištenje kao ulaza u API-je koji izvode EIM operaciju pregledavanja.

Definicije sistemskog i aplikacijskog registra

Neke aplikacije koriste podskup korisničkih identiteta unutar jedne instance korisničkog registra. EIM dozvoljava administratorima da oblikuju scenario dobavljanjem dviju vrsta definicija EIM registra: sistemske i aplikacijske.

Definicija sistemskog registra predstavlja određeni registar unutar radne stanice ili poslužitelja. Možete kreirati definiciju sistemskog registra kada registar u poduzeću ima jedno od sljedećih obilježja:

- Registar je dobavljen od operativnog sistema, kao što je AIX(R), OS/400(R), ili proizvod sigurnosnog upravljanja kao što je z/OS Security Server Resource Access Control Facility (RACF(R)).
- Registar sadrži korisničke identitete koji su jedinstveni za specifičnu aplikaciju, kao što je Lotus Notes(R).
- Registar sadrži distribuirane korisničke identitete kao što su Kerberos principali ili Lightweight Directory Access Protocol (LDAP) razlikovna imena.

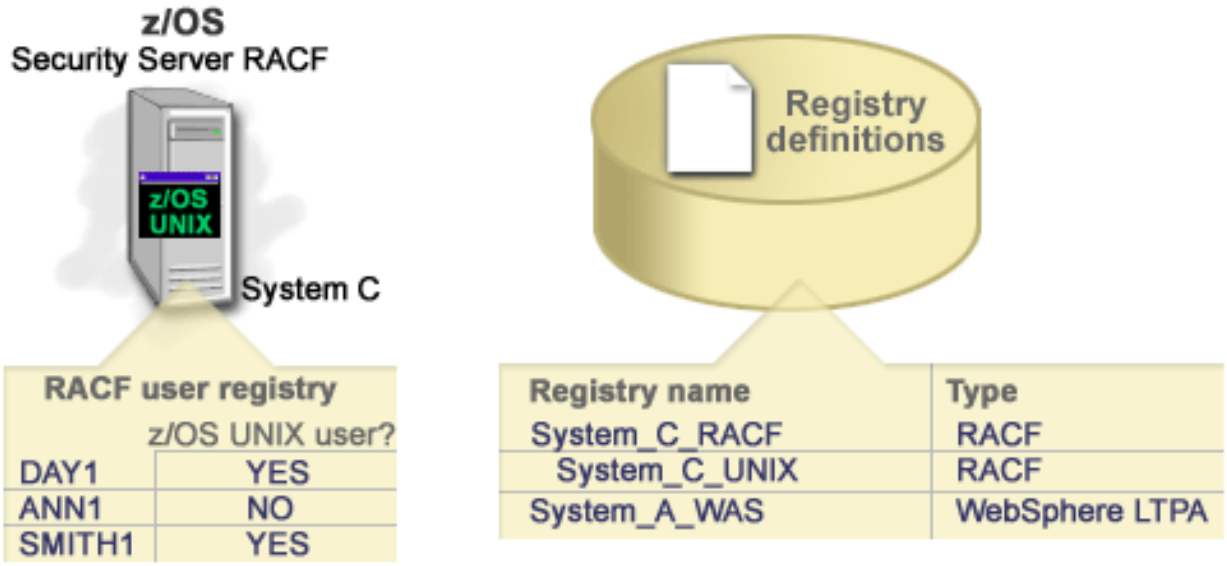
Definicija aplikacijskog registra predstavlja podskup korisničkih identiteta koji su definirani u sistemskom registru. Ovi korisnički identiteti dijele zajednički skup atributa ili karakteristika koje im dozvoljavaju korištenje pojedinačne aplikacije ili skupa aplikacija. Možete kreirati definiciju aplikacijskog registra kada korisnički identiteti imaju sljedeća obilježja:

- Korisnički identiteti za aplikaciju ili skup aplikacija nisu spremljeni u korisničkom registru specifičnim za aplikaciju ili skup aplikacija.
- Korisnički identiteti za aplikaciju ili skup aplikaciju su spremljeni u sistemskom registru koji sadrži korisničke identitete za druge aplikacije.

EIM operacije pregledavanja izvode se ispravno bez obzira definira li EIM administrator registar kao sistemski ili aplikacijski. Međutim, odvojene definicije registra dozvoljavaju da mapiranje podataka bude upravljano na aplikacijskoj osnovi. Odgovornost upravljanja aplikacijski specifičnih mapiranja može biti dodijeljeno administratoru za specifični registar.

Na primjer, Slika 7 prikazuje kako je EIM administrator kreirao definiciju sistemskog registra za predstavljanje z/OS Security Server RACF registra. Administrator je također kreirao definiciju aplikacijskog registra za predstavljanje korisnički identiteta unutar RACF registra koji koriste z/OS UNIX Sistemske usluge (z/OS UNIX). Sistem C sadrži RACF korisnički registar koji sadrži informacije za tri korisnička identiteta DAY1, ANN1 i SMITH1. Dva ova korisnička identiteta DAY1 i SMITH1) pristupaju z/OS UNIX na Sistemu C. Ovi korisnički identiteti su u stvari RACF korisnici s jedinstvenim atributima koji ih definiraju kao z/OS UNIX korisnike. Unutar definicija EIM registra, EIM administrator definirao je System_C_RACF za predstavljanje ukupnog RACF korisničkog registra. Administrator je također definirao System_C_UNIX za predstavljanje korisničkih identiteta koji imaju z/OS UNIX atribute.

Slika 7: Definicije EIM registra za RACF korisnički registar i za korisnike z/OS UNIX-a



EIM udruženja

EIM udruženje je odnos između EIM identifikatora koji predstavlja specifičnu osobu i jednog korisničkog identiteta u korisničkom registru koji također predstavlja tu osobu. Kada kreirate udruženja između EIM identifikatora i svih korisničkih identiteta osobe ili cjeline, tada osiguravate jedno, potpuno razumijevanje o tome kako ta osoba ili cjelina koristi resurse u poduzeću. EIM osigurava API-je koji dozvoljavaju aplikacijama da pronađu nepoznati korisnički identitet u specifičnom (ciljnom) korisničkom registru dobavljanjem poznatog korisničkog identiteta u nekom drugom (izvornom) korisničkom registru. Ova obrada se naziva *mapiranje identiteta*.

Prije nego možete kreirati udruženje, prvo morate kreirati prikladni EIM identifikator i prikladnu definiciju EIM registra za korisnički registar koji sadrži udruženi korisnički identitet. Udruženje definira vezu između EIM identifikatora i korisnički identitet korištenjem sljedećih informacija:

- Ime EIM identifikatora
- Ime korisničkog identiteta
- EIM Ime definicije EIM registra
- Tip udruženja

Administrator može kreirati različite tipove udruženja između EIM identifikatora i korisničkog identiteta na temelju toga kako se koristi korisnički identitet. Korisnički identiteti mogu se koristiti za provjeru autentičnosti, autorizaciju ili oboje.

Provjera autentičnosti je obrada provjeravanja da cjelina ili osoba koja dobavlja korisnički identitet ima pravo na pretpostavku tog identiteta. Provjera se često postiže prisiljavanjem osobe koja šelje korisnički identitet za dobavljanje tajnih ili privatnih informacija udruženih s korisničkim identitetom, kao što je lozinka.

Autorizacija je obrada osiguravanja da ispravno ovlašteni korisnički identitet može izvoditi samo funkcije ili pristupati resursima za koje su identitetu dane povlastice. U prošlosti, skoro sve aplikacije su bile prisiljene na korištenje korisničkih identiteta u jednom korisničkom registru za provjeru autentičnosti i autorizaciju. Korištenjem Operacija EIM pregledavanja aplikacije sada mogu koristiti korisničke identitete u jednom korisničkom registru za provjeru autentičnosti za vrijeme korištenja korisničkih identiteta u različitim korisničkim registrima kod provjere autentičnosti.

U EIM-u postoje tri tipa udruženja koje administrator može definirati između EIM identifikatora i korisničkog identiteta. Ovi tipovi su izvor, cilj i administrativna udruženja.

Izvorno udruženje

Kada se koristi korisnički identitet za *provjeru autentičnosti*, taj korisnički identitet bi trebao imati izvorno udruženje s EIM identifikatorom. Izvorno udruženje dozvoljava korištenje korisničkog identiteta kao izvor u operaciji EIM pregledavanja za pronalaženje korisničkog identiteta koji je udružen s istim EIM identifikatorom. Ako se korisnički identitet sa samo izvornim udruženjem koristi kao ciljni identitet u operaciji EIM pregledavanja, tada nisu vraćeni udruženi korisnički identiteti.

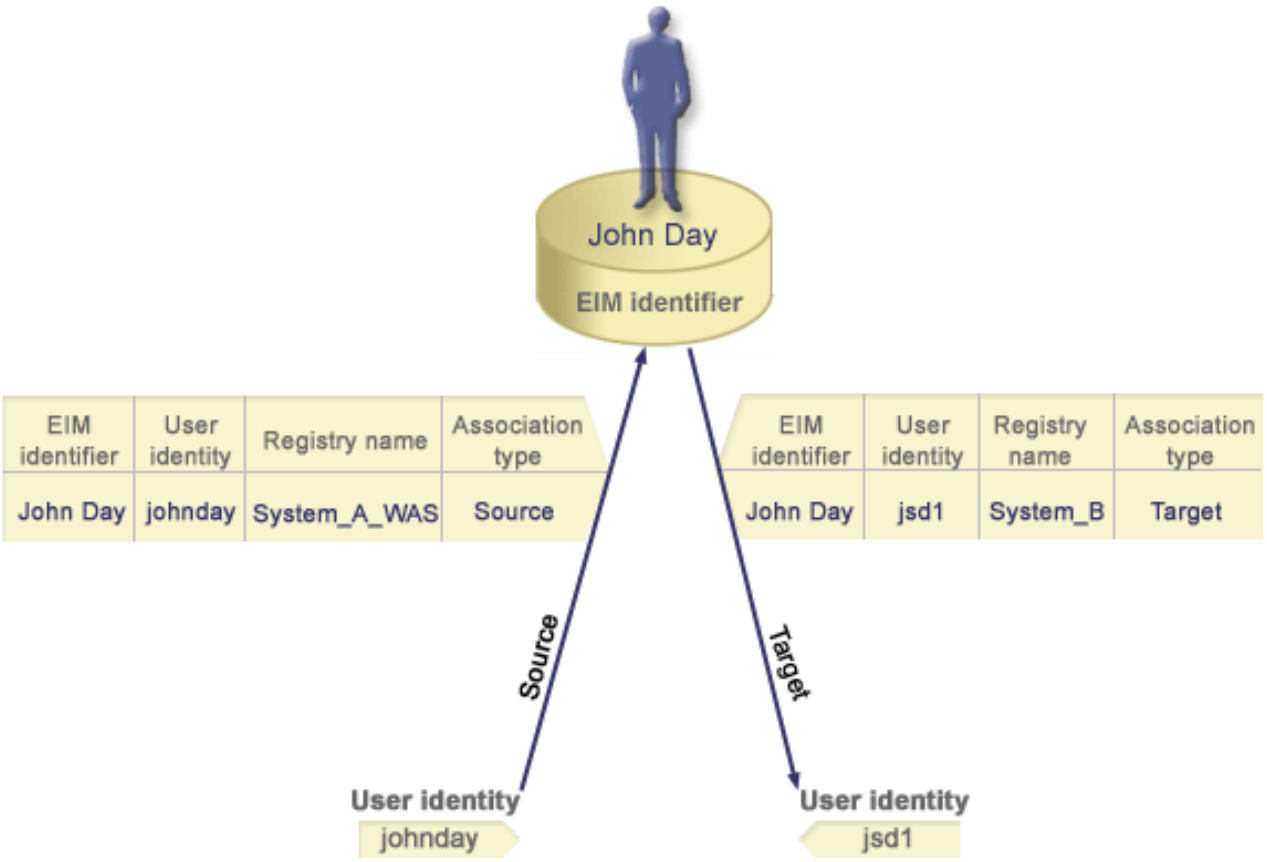
Ciljno udruženje

Kada se korisnički identitet koristi za *autorizaciju* radije nego za provjeru autentičnosti, tada bi taj korisnički identitet trebao imati ciljno udruženje s EIM identifikatorom. Ciljno udruženje dozvoljava vraćanje korisničkog identiteta kao rezultat operacije EIM pregledavanja. Ako se korisnički identitet sa samo ciljnim udruženjem koristi kao izvorni identitet u operaciji EIM pregledavanja, tada nema vraćenih udruženih korisničkih identiteta.

Možda će biti potrebno kreirati i ciljno i izvorno udruženje za jedan korisnički identitet. Ovo je potrebno kada pojedinac koristi jedan sistem kao klijent i kao poslužitelj ili za pojedince koji se ponašaju kao administratori. Na primjer, korisnik normalno provjeri autentičnost na Windows platformi i izvodi aplikacije koje pristupaju AIX poslužitelju. Zbog odgovornosti korisnikovog posla, korisnik se također mora povremeno prijaviti direktno na AIX poslužitelj. U ovoj situaciji možete kreirati i izvorna i ciljna udruženja između AIX korisničkog identiteta i EIM identifikatora osobe. Korisnički identiteti koji predstavljaju krajnje korisnike normalno trebaju samo ciljno udruženje.

Slika 6 prikazuje primjer izvornog i ciljnog udruženja. U ovom primjeru, administrator je kreirao dva udruženja za EIM identifikator John Day za definiranje veza između ovog identifikatora i dva udružena korisnička identiteta. Administrator je kreirao izvorno udruženje za johnday, WebSphere Lightweight Third-Party Authentication (LTPA) korisnički identitet u System_A_WAS korisničkom registru. Administrator je također kreirao ciljna udruženja za jsd1, OS/400 korisnički profil u System B korisničkom registru. Ova udruženja imaju značenje kod aplikacija za dobavljanje nepoznatog korisničkog identiteta (ciljni, jsd1) na osnovu poznatog korisničkog identiteta (izvorni, johnday) kao dijela operacije EIM pregledavanja.

Slika 6: EIM ciljna i izvorna udruženja za EIM identifikator John Day



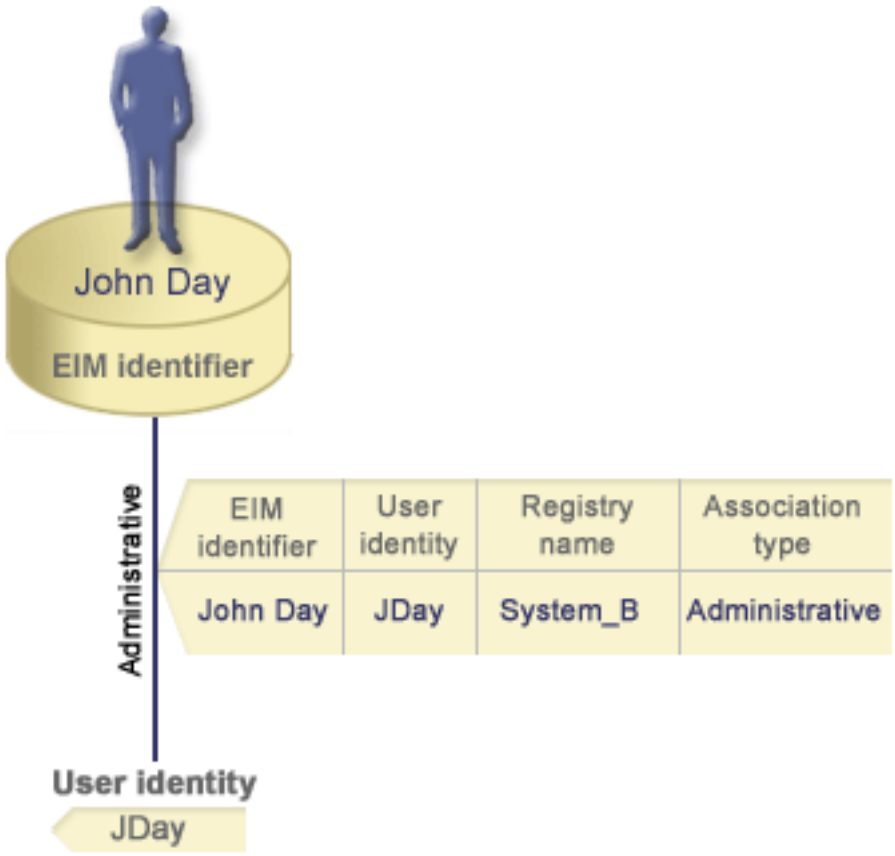
Administrativno udruženje

Adminstrativno udruženje za EIM identifikator tipično se koristi za prikaz da osoba ili cjelina predstavljena EIM identifikatorom posjeduje korisnički identitet koji zahtijeva specijalna razmatranja kod specificiranog sistema. Ovaj tip udruženja može se koristiti, na primjer, s visoko osjetljivim korisničkim registrima.

Zbog prirode predstavljanja administrativnog udruženja, operacija EIM pregledavanja, koja dobavlja izvorni korisnički identitet s administrativnim udruženjem, ne vraća rezultate. Slično, korisnički identitet s administrativnim udruženjem nikad se ne vraća kao rezultat operacije EIM pregledavanja.

Slika 7 prikazuje primjer administrativnog udruženja. U ovom primjeru, John Day ima jedan korisnički identitet na Sistemu A i drugi korisnički identitet na Sistemu B, što je visoko osigurani sistem. Sistemski administrator želi osigurati provjeru autentičnosti korisnika na Sistemu B korištenjem samo lokalnog korisničkog registra ovog sistema. Administrator ne želi dozvoliti da aplikacija provjeri autentičnost John Daya na sistemu koristeći neke strane mehanizme provjere autentičnosti. Korištenjem administrativnog udruženja za JDay korisnički identitet na Sistemu B, EIM administrator može vidjeti da John Day posjeduje račun na Sistemu B, ali EIM ne vraća informacije o JDay identitetu kod operacije EIM pregledavanja. Čak i ako aplikacije postoje na ovom sistemu koji koristi operacije EIM pregledavanja, one ne mogu pronaći korisničke identitete koji imaju administrativna udruženja.

Slika 7: EIM administrativno udruženje za EIM identifikator John Day



EIM operacije pregledavanja

EIM operacija pregledavanja je obrada kroz koju aplikacija ili operativni sistem pronalazi nepoznati korisnički identitet u specifičnom ciljnom registru dobavljanjem poznate i provjerene informacije. Aplikacije koje koriste EIM API-je mogu izvoditi ove EIM operacije pregledavanja na informacijama samo ako su te informacije spremljene u EIM domeni. Aplikacija može izvesti jedan od dva tipa EIM operacija pregledavanja na osnovu tipa informacije kojeg aplikacija dobavlja kao izvor EIM operacije pregledavanja: korisnički identitet ili EIM identifikator.

Kada aplikacija dobavi *korisnički identitet kao izvor*, ona također mora dobaviti ime definicije EIM registra za izvor korisničkog identiteta i ime definicije EIM registra koje je cilj EIM operacije pregledavanja. Da bi se koristio kao izvor u EIM operaciji pregledavanja, korisnički identitet mora imati definirano izvorno udruženje za njega.

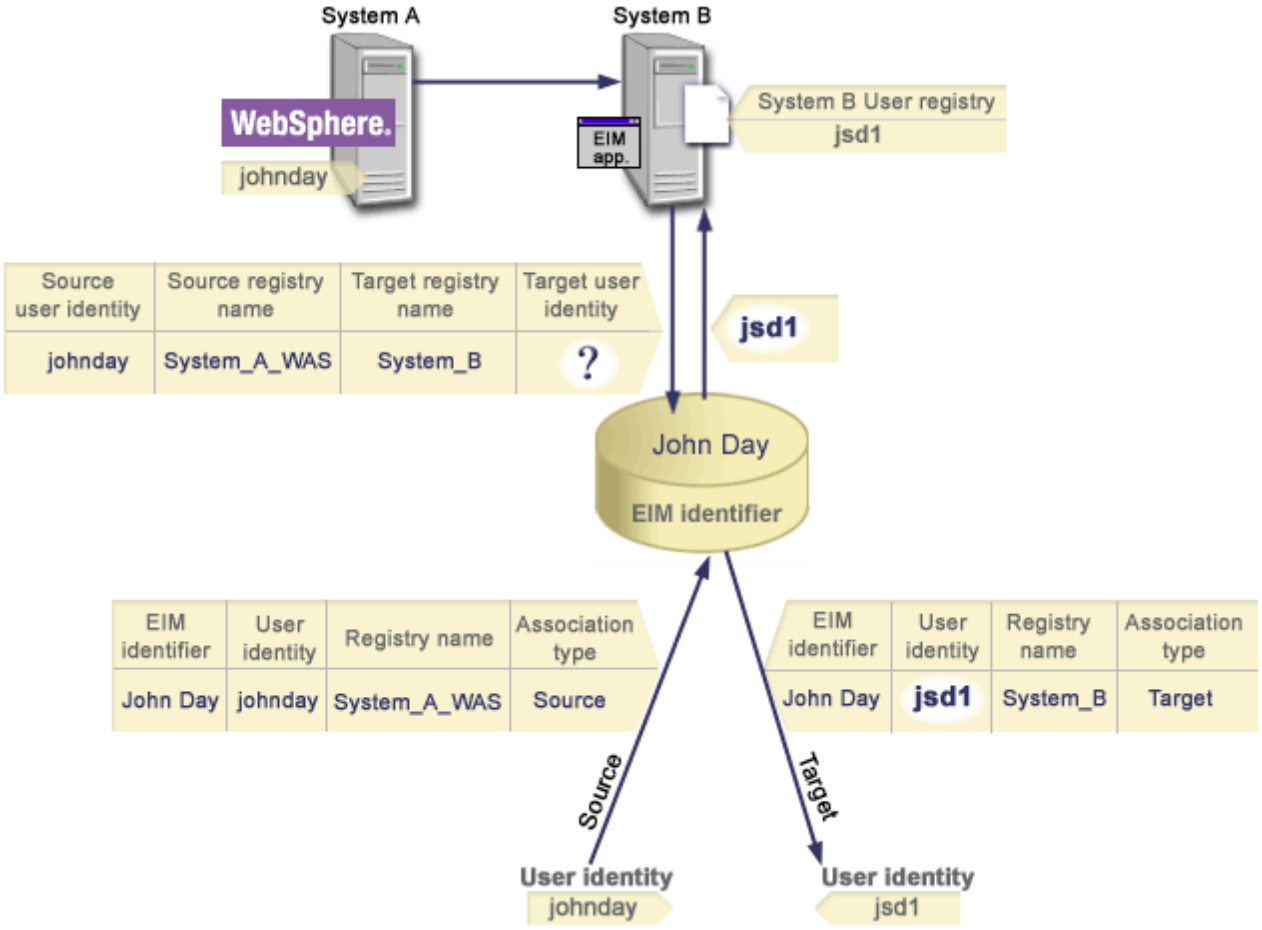
Kada aplikacija dobavi *EIM identifikator kao izvor* EIM operacije pregledavanja, ona također mora dobaviti ime definicije EIM registra što je cilj EIM operacije pregledavanja. Da bi korisnički identitet bio vraćen kao cilj bilo kojeg tipa EIM operacije pregledavanja, korisnički identitet mora za njega imati definirano ciljno udruženje.

Dobavljena informacije proslijeđena je kontroleru EIM domene gdje su spremljene sve EIM informacije i EIM operacija pregledavanja traži izvorno udruženje koje odgovara dobavljenoj informaciji. Na osnovu EIM identifikatora (dobavljenog API-ju ili određenog iz informacije izvornog udruženja), EIM operacija pregledavanja tada traži ciljno udruženje za taj identifikator koji odgovara ciljnom imenu definicije EIM registra.

Na slici 10, provjerava se autentičnost korisničkog identiteta johnday na Websphere poslužitelju aplikacije korištenjem Lightweight Third-Party Authentication (LPTA) na Sistemu A. Websphere poslužitelj aplikacija na

Sistemu A poziva domaći program na Sistemu B za pristup podacima na Sistemu B. Domaći program koristi EIM API za izvođenje EIM operacija pregledavanja na osnovu korisničkog identiteta na Sistemu A kao izvor operacije. Aplikacija dobavlja sljedeće informacije za izvođenje operacije: johnday kao izvorni korisnički identitet, System_A_WAS kao izvorno ime definicije EIM registra i System_B kao ciljno ime definicije EIM registra. Ove informacije izvora proslijeđene su kontroleru EIM domene i EIM operacija pregledavanja pronalazi izvorno udruženje koje odgovara informacijama. Korištenjem imena EIM identifikatora, EIM operacija pregledavanja traži ciljno udruženje za John Day identifikator koji odgovara ciljnom imenu definicije EIM registra za System_B. Kada je odgovarajuće ciljno udruženje pronađeno, EIM operacija pregledavanja vraća jsd1 korisnički identitet aplikaciji.

Slika 10: EIM operacija pregledavanja na osnovu poznatog korisničkog identiteta johnday



EIM ovlaštenja

EIM ovlaštenje dozvoljavaju korisniku izvođenje specifičnih administrativnih zadataka ili EIM operacija pregledavanja. Samo je korisnicima s EIM ovlaštenjem administratora dozvoljeno dodjeljivanje ili opozivanje ovlaštenja za druge korisnike. EIM ovlaštenja su dozvoljena samo korisničkim identitetima koja su poznata kontroleru EIM domene.

Slijede kratki opisi funkcija koje svaka EIM grupa ovlaštenja može izvoditi:

- **Lightweight Directory Access Protocol (LDAP) administrator.** Ovo ovlaštenje dozvoljava korisniku da konfigurira novu EIM domenu. Korisnik s ovim ovlaštenjem može izvoditi sljedeće funkcije:
  - Kreiranje domene

  - Brisanje domene
  - Kreiranje i uklanjanje EIM identifikatora
  - Kreiranje i uklanjanje definicije EIM registra
  - Kreiranje i uklanjanje izvornih, ciljnih i administrativnih udruženja
  - Izvođenje EIM operacija pregledavanja
  - Dohvaćanje udruženja, EIM identifikatora i definicija EIM registra
  - Dodavanje, uklanjanje i ispis informacija EIM ovlaštenja
- **EIM administrator.** Ovo ovlaštenje dozvoljava korisniku da upravlja svim EIM podacima unutar ove EIM domene. Korisnik s ovim ovlaštenjem može izvoditi sljedeće funkcije:
  - Brisanje domene
  - Kreiranje i uklanjanje EIM identifikatora
  - Kreiranje i uklanjanje definicije EIM registra
  - Kreiranje i uklanjanje izvornih, ciljnih i administrativnih udruženja
  - Izvođenje EIM operacija pregledavanja
  - Dohvaćanje udruženja, EIM identifikatora i definicija EIM registra
  - Dodavanje, uklanjanje i ispis informacija EIM ovlaštenja
- **Administrator EIM identifikatora.** Ovo ovlaštenje dozvoljava korisnicima da dodaju i mijenjaju EIM identifikatore i upravljaju izvornim i ciljnim udruženjima. Korisnik s ovim ovlaštenjem može izvoditi sljedeće funkcije:
  - Kreiranje EIM identifikatora
  - Dodavanje i uklanjanje izvornih udruženja
  - Dodavanje i uklanjanje administrativnih udruženja
  - Izvođenje EIM operacija pregledavanja
  - Dohvaćanje udruženja, EIM identifikatora i definicija EIM registra
- **EIM pregledavanje mapiranja.** Ovo ovlaštenje dozvoljava korisniku provođenje EIM operacija pregledavanja. Korisnik s ovim ovlaštenjem može izvoditi sljedeće funkcije:
  - Izvođenje EIM operacija pregledavanja
  - Dohvaćanje udruženja, EIM identifikatora i definicija EIM registra
- **Administrator EIM registara.** Ovo ovlaštenje dozvoljava korisniku da upravlja definicijama EIM registara. Korisnik s ovim ovlaštenjem može izvoditi sljedeće funkcije:
  - Dodavanje i uklanjanje ciljnih udruženja
  - Izvođenje EIM operacija pregledavanja
  - Dohvaćanje udruženja, EIM identifikatora i definicija EIM registra
- **Administrator EIM registra X.** Ovo ovlaštenje dozvoljava korisniku da upravlja specifičnom definicijom EIM registra. Ovo ovlaštenje dozvoljava korisniku:
  - Dodavanje i uklanjanje ciljnih udruženja za definicije EIM registra
  - Izvođenje EIM operacija pregledavanja
  - Dohvaćanje udruženja, EIM identifikatora i definicija EIM registra

Svaka od sljedećih tablica je organizirana s EIM zadatkom koje izvodi API. Svaka tablica prikazuje EIM API, različita EIM ovlaštenja i pristup koje svako od ovih ovlaštenja ima za određene EIM funkcije.

Tablica 1: Rad s domenama

EIM API	LDAP administrator	EIM administrator	Administrator EIM identifikatora	EIM pregledavanje mapiranja	Administrator EIM registara	Administrator EIM registra X
eimChangeDomain	X	X	-	-	-	-

EIM API	LDAP administrator	EIM administrator	Administrator EIM identifikatora	EIM pregledavanje mapiranja	Administrator EIM registara	Administrator EIM registra X
eimCreateDomain	X	-	-	-	-	-
eimDeleteDomain	X	X	-	-	-	-
eimListDomains	X	X	-	-	-	-

Tablica 2: Rad s identifikatorima

EIM API	LDAP administrator	EIM administrator	Administrator EIM identifikatora	EIM pregledavanje mapiranja	Administrator EIM registara	Administrator EIM registra X
eimAddIdentifier	X	X	X	-	-	-
eimChangeIdentifier	X	X	X	-	-	-
eimListIdentifiers	X	X	X	X	X	X
eimRemoveIdentifier	X	X	-	-	-	-

Tablica 3: Rad s registrima

EIM API	LDAP administrator	EIM administrator	Administrator EIM identifikatora	EIM pregledavanje mapiranja	Administrator EIM registara	Administrator EIM registra X
eimAddApplicationRegistry	X	X	-	-	-	-
eimAddSystemRegistry	X	X	-	-	-	-
eimChangeRegistry	X	X	-	-	X	X
eimChangeRegistryUser	X	X	-	-	X	X
eimChgRegistryAlias	X	X	-	-	X	X
eimGetRegistryFromAlias	X	X	X	X	X	X
eimListRegistries	X	X	X	X	X	X
eimListRegistryAliases	X	X	X	X	X	X
eimListRegistryUsers	X	X	X	X	X	X
eimRemoveRegistry	X	X	-	-	-	-

Tablica 4: Rad s udruženjima

Za eimAddAssociation() i eimRemoveAssociation() API-je postoje četiri parametra koji određuju tip udruženja koji se ili dodaje ili uklanja. Ovlaštenje za ove API-je se razlikuje na osnovu tipa udruženja specificiranog u ovim parametrima. U sljedećoj tablici uključen je tip udruženja za svaki od ovih API-ja.

EIM API	LDAP administrator	EIM administrator	Administrator EIM identifikatora	EIM pregledavanje mapiranja	Administrator EIM registara	Administrator EIM registra X
eimAddAssociation (administrativan)	X	X	X	-	-	-
eimAddAssociation (izvorni)	X	X	X	-	-	-
eimAddAssociation (izvorni i ciljni)	X	X	X	-	X	X
eimAddAssociation (ciljni)	X	X	-	-	X	X
eimListAssociations	X	X	X	X	X	X
eimRemoveAssociation (administrativan)	X	X	X	-	-	-
eimRemoveAssociation (izvorni)	X	X	X	-	-	-
eimRemoveAssociation (izvorni i ciljni)	X	X	X	-	X	X
eimRemoveAssociation (ciljni)	X	X	-	-	X	X

Tablica 5: Rad s mapiranjima

EIM API	LDAP administrator	EIM administrator	Administrator EIM identifikatora	EIM pregledavanje mapiranja	Administrator EIM registara	Administrator EIM registra X
eimGetAssociatedIdentifier	X	X	X	X	X	X
eimGetTargetFromIdentifier	X	X	X	X	X	X
eimGetTargetFromSource	X	X	X	X	X	X

Tablica 6: Rad s pristupom

EIM API	LDAP administrator	EIM administrator	Administrator EIM identifikatora	EIM pregledavanje mapiranja	Administrator EIM registara	Administrator EIM registra X
eimAddAccess	X	X	-	-	-	-
eimListAccess	X	X	-	-	-	-
eimListUserAccess	X	X	-	-	-	-
eimQueryAccess	X	X	-	-	-	-
eimRemoveAccess	X	X	-	-	-	-

LDAP koncepti za EIM

Mapiranje identiteta u poduzeću (EIM) koristi Lightweight Directory Access Protocol (LDAP) poslužitelj kao kontroler EIM domene za spremanje EIM podataka. Možete koristiti LDAP razlikovna imena kod konfiguriranja EIM-a za vaš iSeries poslužitelj i kao sredstvo provjeravanja autentičnosti na kontroleru EIM domene.

Da bi koristili LDAP razlikovno ime kod konfiguriranja i administriranja EIM-a, trebali biste razumjeti sljedeće LDAP koncepte:

- LDAP razlikovno ime
- LDAP nadređeno razlikovno ime

LDAP razlikovno ime

LDAP razlikovno ime (DN) je Lightweight Directory Access Protocol (LDAP) ulaz koji identificira i poisuje ovlaštenog korisnika za LDAP poslužitelj. Vi koristite EIM Čarobnjak konfiguracije za konfiguriranje LDAP poslužitelja i spremanje informacija EIM domene. Možete koristiti LDAP razlikovna imena kao sredstvo pristupanja i dohvaćanja EIM podataka tako da vaš iSeries poslužitelj može sudjelovati u okruženju jednostruke prijave.

Razlikovna imena sastoje se od samog imena ulaza kao i od imena, u poretku dolje prema gore, objekata iznad njega u LDAP direktoriju. Primjer potpunog LDAP razlikovnog imena može biti cn=Tim Jones, o=IBM, c=US. Svaki upis ima barem jedan atribut koji se koristi za imenovanje upisa. Ovaj atribut imenovanja se naziva relativno razlikovno ime (RDN) ulaza. Ulaz iznad danog RDN-a naziva se njegovim LDAP nadređenim razlikovnim imenom. U ovom primjeru, cn=Tim Jones imenuje ulaz, tako da je RDN. o=IBM, c=US je nadređeni DN zacn=Tim Jones. Pogledajte LDAP nadređeno razlikovno ime da naučite više o tome kako ih EIM koristi.

Budući da EIM koristi LDAP poslužitelj za spremanje EIM podataka, možete koristiti LDAP razlikovna imena u svrhu provjere autentičnosti na kontroleru EIM domene. Također možete koristiti LDAP razlikovna imena kod konfiguriranja EIM-a za vaš iSeries poslužitelj. Na primjer, možete koristiti LDAP razlikovna imena kada:

- Konfigurirate LDAP poslužitelj da se ponaša kao kontroler EIM domene. To činite kreiranje i korištenjem LDAP razlikovnog imena koje identificira LDAP administratora za LDAP poslužitelj. Ako LDAP poslužitelj nije bio prethodno konfiguriran, možete ga konfigurirati kada koristite EIM Čarobnjaka konfiguracije za kreiranje i pristupanje novoj domeni.
- Koristite EIM Čarobnjaka konfiguracije za odabir tipa korisničkog identiteta kojeg bi čarobnjak trebao koristiti u povezivanju na kontroler EIM domene. Razlikovno ime je jedno od korisničkih tipova koje odaberete. LDAP razlikovno ime mora predstavljati korisnika koji je ovlašten za kreiranje objekata u lokalnom imenskom prostoru LDAP poslužitelja.
- Koristite EIM Čarobnjaka konfiguracije za odabir tipa korisnika za izvođenje EIM operacija u korist funkcija operativnog sistema. Ove operacije uključuju pregledavanja mapiranja i brisanje udruženja kod brisanja lokalnog OS/400 korisničkog profila. Razlikovno ime je jedno od korisničkih tipova koje odaberete.
- Povezivanja na kontroler domene za administraciju EIM-a, na primjer, za upravljanje registrima i identifikatorima te za izvođenje operacija pregledavanja mapiranja.

Da naučite više o razlikovnim imenima i kako ih LDAP koristi, pogledajte LDAP osnove.

LDAP nadređeno razlikovno ime

LDAP nadređeno razlikovno ime (DN) je ulaz u Lightweight Directory Access Protocol (LDAP) imenskom prostoru poslužitelj direktorija. Ulazi LDAP poslužitelja svrstani su u hijerarhijskoj strukturi koja može odražavati političke, geografske, organizacijske ili domenske granice. Razlikovnim imenom smatra se nadređeni DN kada je DN na najvišoj razini imenskog prostora LDAP poslužitelja.

Primjer potpunog LDAP razlikovnog imena može biti cn=Tim Jones, o=IBM, c=US. Svaki upis ima barem jedan atribut koji se koristi za imenovanje upisa. Ovaj atribut imenovanja se naziva relativno razlikovno ime (RDN) ulaza. Ulaz iznad danog RDN-a naziva se njegovim nadređenim razlikovnim imenom. U ovom primjeru, cn=Tim Jones imenuje ulaz, tako da je RDN. o=IBM, c=US je nadređeni DN zacn=Tim Jones.

Budući da EIM koristi LDAP poslužitelj za spremanje EIM podataka, možete koristiti LDAP razlikovna imena u svrhu provjere autentičnosti na kontroleru EIM domene. Također možete koristiti LDAP razlikovna imena i nadređena razlikovna imena kod konfiguriranja EIM-a za vaš iSeries poslužitelj. Na primjer, kada koristite

EIM Čarobnjaka konfiguracije za kreiranje i pristupanje novoj domeni, možete odabrati specificiranje nadređenog DN-a za domenu koju kreirate. Korištenjem nadređenog DN-a, možete specificirati gdje trebaju prebivati EIM podaci u lokalnom LDAP imenskom prostoru za domenu. Kada ne trebate specificirati nadređeni DN, EIM podaci prebivaju u svom vlastitom sufiksu u imenskom prostoru.

Da naučite više o razlikovnim imenima i kako ih se koristi, pogledajte LDAP osnove.

Omogućenje jednostruke prijave kroz EIM

EIM dobavlja jeftin mehanizam za omogućenje jednostruke prijave kroz poduzeće. OS/400 implementacija EIM-a i Kerberosa osigurava pravo, višepovezano, heterogeno okruženje jednostruke prijave. Korist za korisnike, administratore i razvijače aplikacije kada je okruženje jednostruke prijave omogućeno u poduzeću slijedi:

Korist za korisnike
U okruženju jednostruke prijave, provjera autentičnosti dešava se kad god korisnik pokuša pristupiti novom sistemu; međutim, od njih neće biti zatražena lozinka. EIM smanjuje potrebu korisnika da prate i upravljaju višestrukim korisničkim imenima i lozinkama za pristup drugim sistemima u mreži. Jednom kad je korisniku provjerena autentičnost u mreži, korisnik može pristupiti uslugama i aplikacijama u poduzeću bez potrebe za višestrukim lozinkama ovih različitih sistema.

Korist za administratore
Za administratora, jednostruka prijava pojednostavljuje ukupno sigurnosno upravljanje poduzeća. Bez jednostruke prijave, korisnici i aplikacije mogu stavljati lozinke u predmemoriju na različitim sistema, što može ugroziti sigurnost cijele mreže. Administratori troše vrijeme i novac na rješenja za izbjegavanje ovakvih rizika. Jednostruka prijava smanjuje administrativno opterećenje u upravljanju provjerom autentičnosti dok održava cijelu mrežu sigurnom. Dodatno, jednostruka prijava smanjuje administrativne troškove resetiranja zaboravljenih lozinki.

Korist za razvijače aplikacija
Za razvijače aplikacija koje se moraju izvoditi u heterogenim mrežama, EIM osigurava infrastrukturu za razvoj aplikacija koje rade na raznim platformama. Korištenjem EIM API-ja, programeri mogu pisati aplikacije koje koriste najprikladniji postojeći korisnički registar za provjeru autentičnosti, a drugi korisnički registar za autorizaciju. RAzvijači aplikacija ne trebaju podršku korisničkog registra specifične platforme unutar aplikacije koju kreiraju, jer EIM dobavlja infrastrukturu za kreiranje aplikacija koje mapiraju korisničke identitete unutar tih korisničkih registara u jedan EIM identifikator. U dodatku, EIM dozvoljava programerima da održavaju te aplikacije bez mijenjanja pridružene sigurnosne semantike, a sigurnost razine aplikacije značajno smanjuje trošak implementiranja višestruko povezanih, platformskih aplikacija.

iSeries omogućavanje jednostruke prijave
Da bi omogućio okruženje jednostruke prijave, IBM koristi dvije tehnologije koje rade zajedno: EIM i usluga mrežne provjere autentičnosti, što je IBM implementacija Kerberosa i GSS API-ja. Konfiguriranje ovih dviju tehnologija, administrator može omogućiti okruženje jednostruke prijave. Windows 2000, XP, AIX, i zSeries koriste Kerberos protokol za provjeru autentičnosti korisnika na mreži. Kerberos uključuje upotrebu centra distribucije ključa, mrežno baziranog i sigurnog koji provjerava autentičnost principala (Kerberos korisnika)) u mreži. Korisnik dobiva Kerberos ulaznicu iz centraliziranog centra distribucije ključa. Ova ulaznica provjerava autentičnost korisnika za druge usluge u poduzeću. Ulaznica može biti proslijeđena od korisnika na uslugu koja prihvaća ulaznice. Usluga koja prihvaća ulaznicu koristi je za određivanje tko je korisnik (unutar Kerberos korisničkog registra i područja) i da su to u stvari oni koji tvrde da jesu.

Dok usluga mrežne provjere autentičnosti dozvoljava iSeries poslužitelju da sudjeluje u Kerberos području, EIM dobavlja mehanizam za pridruživanje ovih Kerberos principala u jednostruki EIM identifikator koji predstavlja tog korisnika unutar cijelog poduzeća. Drugi korisnički identiteti, kao što je OS/400 korisničko ime, također mogu biti pridruženi s ovim EIM identifikatorom. Na osnovu ovih udruženja, EIM dobavlja mehanizam za OS/400 i aplikacije kako bi odredio koji OS/400 korisnički profil predstavlja osobu ili cjelinu

predstavljenu Kerberos principalom. Možete zamisliti informacije u EIM-u kao stablo s EIM identifikatorom kao korijenom, i listom korisničkih identiteta pridruženih s EIM identifikatorom kao granama.

Korištenjem donje slike kao primjera, zamislite da se korisnik, kao što je John Smith, prijavi na mrežu kroz svoj Windows PC i pristupi instanci OS/400 za pristup Kerberos-omogućenim aplikacijama. John nije upitan za njegovo OS/400 korisničko ime. Ove aplikacije mogu potražiti udruženje s Johnovim EIM identifikatorom za pronalaženje OS/400 korisničkog imena. John Smith više ne treba lozinku u svom OS/400 korisničkom profilu, jer se korisnički profil ne koristi za provjeru autentičnosti; koristi se samo za autorizaciju.

Slika 1. Okruženje jednostruke prijave

Poglavlje, Scenario: Omogućavanje jednostruke prijave, osigurava primjer kako administrator konfigurira uslugu mrežne provjere autentičnosti i EIM za omogućavanje jednostruke prijave.

Sljedećim se aplikacijama može pristupiti kroz jednostruku prijavu:

- iSeries Navigator
- PC5250 Emulator
- Arhitektura distribuirane relacijske baze podataka (TM)(DRDA)(R)
- NetServer
- QFileSvr.400

Planiranje EIM-a

Postoje višestruke tehnologije i usluge koje EIM okružuje na iSeries poslužitelju. Prije konfiguriranja EIM-a na vašem poslužitelju trebali bi odlučiti o funkcionalnosti koju želite implementirati koristeći EIM i sposobnosti jednostruke prijave.

Prije implementiranje EIM-a trebali biste odlučiti o osnovnim sigurnosnim zahtjevima za vašu mrežu i implementirati te sigurnosne mjere. EIM osigurava administratorima i korisnicima lakše upravljanje identitetom kroz poduzeće. Kada se koristi s mrežnom uslugom provjere autentičnosti, EIM osigurava sposobnosti jednostruke prijave za vaše poduzeće.

Sljedeća radna tablica planiranja identificira usluge koje bi trebali instalirati prije konfiguriranja EIM-a.

Radna tablica planiranja	**Odgovori**
Je li vaš OS/400 V5R2 (5722-SS1) ili kasniji?	
Je li instaliran Dobavljač kriptografičkog pristupa (5722-AC3) na vašem iSeries poslužitelju?	
Je li iSeries Access za Windows (5722-XE1) instaliran na prikladnim PC-ima u vašoj mreži (Pc-i korišteni za rad s iSeries poslužiteljima) i na vašim iSeries poslužiteljima?	
Je li Mrežna podkomponenta iSeries Navigatora instalirana na svim PC-ima u vašoj mreži i na vašim iSeries sistemima?	
Ako je LDAP poslužitelj trenutno konfiguriran i želite ga koristiti kao kontroler EIM domene, znate li razlikovno ime (DN) LDAP administratora i lozinku?	
Ako je LDAP poslužitelj trenutno konfiguriran, može li biti privremeno zaustavljen? (Ovo će biti potrebno za dovršavanje EIM konfiguracijske obrade.)	
Imate li *SECADM, *ALLOBJ i *IOSYSCFG specijalna ovlaštenja?	
Jeste li primijenili najkasnije privremene popravke programa (PTF-ove)?	

Ako planirate koristiti Kerberos za provjeru autentičnosti korisnika, također bi trebali konfigurirati mrežnu uslugu provjere autentičnosti. Pogledajte Planiranje mrežne usluge provjere autentičnosti za potpunu radnu tablicu kod planiranja mrežne usluge provjere autentičnosti.

Ako konfigurirate mrežnu uslugu provjere autentičnosti i EIM za omogućavanje jednostruke prijave, pogeldajte Scenario: Omogućavanje jednostruke prijave koji pokazuje je tvrtka konfigurirala oba ova proizvoda.

Instalacija potrebnih opcija iSeries Navigatora

Da omogućite okruženje jednostruke prijave s EIM-om i mrežnom uslugom provjere autentičnosti, morate instalirati obje opcije, Mrežnu i Sigurnosnu, iSeries Navigatora. EIM je smješten unutar Mrežne opcije, a mrežna usluga provjere autentičnosti je unutar Sigurnosne opcije. Ako ne planirate koristiti mrežnu uslugu provjere autentičnosti u vašoj mreži, tada ne morate instalira Sigurnosnu opciju iSeries Navigatora.

Da instalirate Mrežnu opciju iSeries Navigatora ili da provjerite imate li trenutno instaliranu ovu opciju, osigurajte da je iSeries Access za Windows instaliran na PC-u kojeg koristite za rad s iSeries poslužiteljem.

Za instaliranje Mrežne opcije:

1. Kliknite **Start —> Programs —> IBM iSeries Access za Windows —> Selektivan postav**.
2. Pratite instrukcije u dijalogu. U dijalogu **Odabir komponente** proširite **iSeries Navigator** i zatim odaberite opciju **Mreža**.
   Ako planirate koristiti mrežnu uslugu provjere autentičnosti, također bi trebali odabrati opciju **Sigurnost**.
3. Nastavite kroz ostatak Selektivnog postava.

Konfiguriranje mrežne usluge provjere autentičnosti

Mrežna usluga provjere autentičnosti omogućuje vam korištenje Kerberos provjere autentičnosti na vašem iSeries poslužitelju. Ova usluga nije preduvjet za korištenje EIM-a na vašem poslužitelju; međutim, mnoge su koristi u korištenju Kerberos provjere autentičnosti za sigurnost u vašoj mreži.

Mrežna usluga provjere autentičnosti,kada se koristi u spoju s EIM-om, osigurava vas sa sredstvima za omogućavanje okruženja jednostruke prijave. Okruženje jednostruke prijeva je korisno za korisnike i administratore. Korisnici imaju manje korisničkih imena i lozinki za upravljanje, a administratori imaju manje informacija za svakog korisnika. Budući da omogućenje jednostruke prijave također pomaže u premošćenju manjka među platformama i različitim sistemima koji mogu biti unutar vaše mreže, razvoj aplikacije i općeniti administrativni troškovi mogu biti smanjeni.

Ako trenutno nemate konfiguriranu mrežnu uslugu provjere autentičnosti na vašem iSeries poslužitelju ili na svim poslužiteljima u vašoj mreži, pogledajte Planiranje mrežne usluge provjere autentičnosti za informacije planiranja koje će vam pomoći u početku. Ako ste upoznati s mrežnom uslugom provjere autentičnosti, pogledajte Konfiguriranje mrežne usluge provjere autentičnosti za početak s konfiguracijskom obradom.

Konfiguriranje EIM-a

Da omogućite okruženje jednostruke prijave kroz višestruke platforme bez potrebe za promjenom politika sigurnosti, morate konfigurirati EIM kao i uslugu provjere autentičnosti mreže. Međutim, konfiguriranje i korištenje usluge provjere autentičnosti mreže nije preduvjet ili zahtjev za konfiguriranje i korišten je EIM-a.

Za početak obrade konfiguriranja EIM-a da iSeries poslužitelj sudjeluje u okruženju jednostruke prijave, koristite EIM čarobnjaka konfiguracije. Ovisno o vašim konfiguracijskim potrebama, možete koristiti čarobnjaka za pristup postojećoj domeni ili za kreiranje i pristup novoj domeni.

EIM čarobnjak konfiguracije dozvoljava vam lako dovršavanje potpune osnovne EIM konfiguracije. Na primjer, ako još nemate konfiguriran LDAP poslužitelj ili ako niste konfigurirali uslugu provjere autentičnosti mreže, tada vam čarobnjak EIM konfiguracije pomaže u obavljanju ovih zadataka.

Nakon što ste upotrijebili čarobnjaka za obavljanje osnovne EIM konfiguracije, morate izvesti dodatne konfiguracijske korake prije nego možete koristiti okruženje jednostruke prijave. Pogledajte Scenario: Omogući jednostruku prijavu za primjer koji pokazuje kako je izmišljena tvrtka konfigurirala okruženje jednostruke prijave koristeći uslugu provjere autentičnosti mreže i EIM.

Prije nego upotrijebite EIM Čarobnjaka konfiguracije, trebali biste imati dovršene sve korake planiranja da točno odredite kako ćete koristiti i EIM i uslugu provjere autentičnosti mreže za omogućavanje okruženja jednostruke prijave. Kada je planiranje dovršeno, možete koristiti čarobnjaka za konfiguriranje EIM-a vašeg iSeries poslužitelja na jedan od dva načina: kreiranje novih domena ili pristupanje postojećim domenama. Sljedeća poglavlja osiguravaju upute za konfiguriranje EIM-a:

Kreiranje i pristupanje novoj domeni
Odaberite ovaj zadatak za kreiranje EIM domene vaše mreže i za konfiguriranje iSeries poslužitelja koji će u njoj sudjelovati. Čarobnjak kreira novu domenu i konfigurira lokalni LDAP poslužitelj tako da bude kontroler EIM domene za novu domenu. Također, ako Kerberos trenutno nije konfiguriran na iSeries poslužitelju, čarobnjak će vas upitati za lansiranje Čarobnjaka konfiguracije usluge provjere autentičnosti mreže. Nakon dovršenja ovog zadatka možete konfigurirati druge iSeries poslužitelje da sudjeluju u domeni. Da konfigurirate druge poslužitelje za sudjelovanje u domeni, povežite se na svaki od njih i upotrijebite EIM Konfiguracijskog čarobnjaka u konfiguriranje poslužitelja za pristup postojećoj EIM domeni.

Pristup postojećoj domeni
Kada jednom koristite EIM Konfiguracijskog čarobnjaka za konfiguriranje kontrolera domene i EIM domene, odaberite ovaj zadatak za konfiguriranje drugih iSeries poslužitelja da sudjeluju u domeni.

Morate dovršiti ovaj zadataka za svaki iSeries poslužitelj u mreži koji će koristiti EIM. Nakon što ste dovršili čarobnjaka, morate dobaviti informacije o domeni kojoj se pristupa, uključujući uključujući informacije povezivanja (kao što je broj porta i treba li se koristiti sloj Sigurnog prijenosa (TLS)/Sloj sigurnih utičnica (SSL) u kontroleru EIM domene. Ako Kerberos trenutno nije konfiguriran na iSeries poslužitelju, čarobnjak će vas upitati za lansiranje Čarobnjaka konfiguracije usluge provjere autentičnosti mreže.

Kako pristupiti EIM Konfiguracijskom čarobnjaku

Za pristup EIM Konfiguracijskom čarobnjaku, pratite ove korake:

1. Pokrenite iSeries Navigator.
2. Prijavite se na iSeries poslužitelj za kojeg želite konfigurirati EIM.
   Ako konfigurirate EIM za više od jednog iSeries poslužitelja, počnite od onog na kojem želite konfigurirati kontroler domene za EIM.
3. Proširite **Mreža —> Mapiranje identiteta u poduzeću**.
4. Desno kliknite **Konfiguracija** i odaberite **Konfiguriraj...** za lansiranje EIM konfiguracijskog čarobnjaka.
5. Odaberite ili stazu **Pristup postojećoj domeni** ili **Kreiraj i pristupi novoj domeni**.

Nakon što ste završili s korištenjem EIM konfiguracijskog čarobnjaka za kreiranje kontrolera domene i za konfiguriranje vaših iSeries poslužitelja koji će sudjelovati u domeni, morate dovršiti ove zadatke za dovršavanje vaše EIM konfiguracije:

1. Dodaj EIM registre u EIM domenu za ne-iSeries poslužitelje i aplikacije za koje želite da sudjeluju u EIM domeni.
2. Kreiraj EIM identifikatore u domeni za svakog jedinstvenog korisnika ili cjelinu sistema koji sudjeluju u domeni.
3. Kreiraj udruženja između različitih korisničkih identiteta osobe ili cjeline prema ovim EIM identifikatorima.

Kreiranje i pristupanje novoj domeni

Možete koristiti EIM Konfiguracijskog čarobnjaka za konfiguriranje LDAP poslužitelja na iSeries poslužitelju da bude kontroler EIM domene za novu domenu. Ako je potrebno, EIM konfiguracijski čarobnjak osigurava da dobavite osnovne konfiguracijske informacije LDAP poslužitelja.

Također, ako Kerberos trenutno nije konfiguriran na iSeries poslužitelju, čarobnjak će vas upitati za lansiranje Čarobnjaka konfiguracije usluge provjere autentičnosti mreže. Kada završite s ovim čarobnjakom, konfigurirana je nova EIM domena, vaš iSeries sistem je konfiguriran za pristup novoj domeni i korisnički registri koje ste specificirali, dodani su domeni.

Da bi koristili čarobnjaka za dovršavanje ovog zadatka, morate imati specijalna ovlaštenja Administratora sigurnosti (*SECADM), Svih objekata (*ALLOBJ), i Sistemske konfiguracije (*IOSYSCFG).

Da pokrenete i koristite EIM Konfiguracijskog čarobnjaka za kreiranje i pristupanje novoj EIM domeni, dovršite ove korake unutar iSeries Navigatora:

Opaska: Ovaj čarobnjak također konfigurira lokalni LDAP poslužitelj kao novi kontroler EIM domene.

1. Proširite **Mreža** —> **Mapiranje identiteta u poduzeću**.
2. Desno kliknite **Konfiguracija** i odaberite **Konfiguriraj...** za lansiranje EIM Konfiguracijskog čarobnjaka.
3. Na stranici čarobnjaka **Dobro došli!**, odaberite **Kreiraj i pristupi novoj domeni** i kliknite **Sljedeće**.
4. Ako usluga provjere autentičnosti mreže trenutno nije konfigurirana na iSeries poslužitelju, prikazuje se dijalog **Konfiguracija usluge provjere autentičnosti mreže**. Ovaj dijalog postavlja upit želite li konfigurirati uslugu provjere autentičnosti mreže. Ako odaberete **Da**, lansira se Čarobnjak konfiguracije usluge provjere autentičnosti mreže. Kada dovršite konfiguraciju usluge provjere autentičnosti mreže, nastavlja se EIM Konfiguracijski čarobnjak.

5. Ako lokalni LDAP poslužitelj trenutno nije konfiguriran, prikazuje se dijalog **Konfiguracija poslužitelja direktorija**.Osigurajte sljedeće informacije u dijalogu za konfiguraciju lokalnog LDAP poslužitelja:
   - U polju **Port**, prihvatite defaultni broj porta **389** ili unesite drugi broj porta za upotrebu kod nesigurnih EIM komunikacija s poslužiteljem direktorija.
   - U polju **Razlikovno ime**, unesite LDAP razlikovno ime (DN) koje identificira LDAP administratora za LDAP poslužitelj. EIM Konfiguracijski čarobnjak kreira ovaj LDAP administratorski DN i koristi ga za konfiguraciju LDAP poslužitelja kao kontrolera domene koju kreirate.
   - U polju **Lozinka** unesite lozinku za LDAP administratora.
   - U polju **Potvrda lozinke** ponovno unesite lozinku.
   - Kliknite **Sljedeće**.
6. U dijalogu **Specificiraj kontroler domene** dobavite sljedeće informacije:
   - U polju **Domena** specificirajte ime EIM domene koju želite kreirati. Prihvatite defaultno ime **EIM** ili upotrijebite bilo koji niz znakova koji vam imaju smisla. Međutim, ne možete koristiti specijalne znakove kao što su = + < > , # ; \ i *.
   - U polju **Opis** unesite tekst za opis domene.
   - Kliknite **Sljedeće**.
7. U dijalogu **Specificiranje nadređenog DN-a domene** odaberite treba li se specificirati nadređeni DN domene koju kreirate. Specificiranjem nadređenog DN-a, možete specificirati gdje trebaju prebivati EIM podaci u lokalnom LDAP imenskom prostoru. Kada ne trebate specificirati nadređeni DN, EIM podaci prebivaju u svom vlastitom sufiksu u imenskom prostoru. Ako odaberete **Da**, koristite kućicu s popisom u odabiru lokalnog LDAP sufiksa za upotrebu kao nadređenog DN-a, ili unesite tekst za kreiranje i imenovanje novog nadređenog DN-a. Nije potrebno specificirati nadređeni DN nove domene.
8. U dijalogu **Specificiranje korisnika za povezivanje** odaberite **korisnički tip** za povezivanje. Možete odabrati jedan od sljedećih tipova korisnika: Razlikovno ime i lozinka, Kerberos keytab datoteka i principal, ili Kerberos principal i lozinka. Dva Kerberos korisnička tipa dostupna su samo ako je usluga provjere autentičnosti mreže konfigurirana za lokalni iSeries sistem. Korisnički tip koji odaberete određuje druge informacije koje morate dobaviti za dovršavanje dijaloga kako slijedi:
   - Ako odaberete **Razlikovno ime i lozinka**, osigurajte sljedeće informacije:
     - U polju **Razlikovno ime**, unesite LDAP razlikovno ime (DN) koje identificira korisnika koji je ovlašten za kreiranje objekata u lokalnom imenskom prostoru LDAP poslužitelja. Ako ste koristili ovog čarobnjaka za konfiguriranje LDAP poslužitelja u ranijem koraku, tada biste trebali unijeti Razlikovno ime LDAP administratora kojeg ste kreirali u ovom koraku.
     - U polju **Lozinka** unesite lozinku za korisnika.
     - U polju **Potvrda lozinke** ponovno unesite lozinku.
   - Ako odaberete **Kerberos keytab datoteka i principal**, osigurajte sljedeće informacije:
     - U polju **Keytab datoteka**, unesite keytab datoteke na iSeries poslužitelju koje identificira korisnika ovlaštenog za kreiranje objekata u lokalnom imenskom prostoru LDAP poslužitelja. Ili, možete kliknuti **Pregčed** za odabir keytab datoteke.
     - U polju **Principal** unesite ime Kerberos principala za korištenje u identifikaciji korisnika.
     - U polju **Područje** unesite ime Kerberos područja za principal. Ime principala i područja jedinstveno identificira Kerberos korisnike u keytab datoteci. Na primjer, principal jsmith u području ordept.myco.com, predstavljeno je u keytab datoteci kao jsmith@ordept.myco.com.
   - Ako odaberete **Kerberos principal i lozinka**, osigurajte sljedeće informacije:
     - U polju **Principal**, unesite ime Kerberos principala koje identificira korisnika ovlaštenog za kreiranje objekata u lokalnom imenskom prostoru LDAP poslužitelja.
     - U polju **Područje** unesite ime Kerberos područja za principal.
     - U polju **Lozinka** unesite lozinku za korisnika.
     - U polju **Potvrda lozinke** ponovno unesite lozinku.Ime principala i područja jedinstveno identificira Kerberos korisnike u keytab datoteci. Na primjer, principal jsmith u području ordept.myco.com predstavljeno je u keytab datoteci kao jsmith@ordept.myco.com.

- Kliknite **Provjeri povezivanje** za testiranje vaših korisničkih konfiguracijskih informacija kod povezivanja na kontroler domene.
- Kliknite **Sljedeće**.

9. U dijalogu **Informacije registra** odaberite tip korisničkih registara koje želite dodati u EIM domenu. Odaberite jedno ili oboje od ovih tipova korisničkog registra:
   - Odaberite **OS400** za dodavanje korisničkog registra koji predstavlja lokalni registar u EIM domeni. U dobavljenom polju upišite ime registra koji treba biti kreiran u domeni. Ime EIM registra je proizvoljan niz znakova koji predstavlja tip registra i specifičnu instancu tog registra.
   - Odaberite **Kerberos** za dodavanje Kerberos korisničkog registra u EIM domenu. U dobavljenom polju, upišite ime registra koji treba biti kreiran u domeni i odaberite **Kerberos korisnički identiteti su osjetljivi na velika i mala slova**, ako je potrebno.
   - Kliknite **Sljedeće**.
10. U dijalogu **Specificiraj EIM sistemskog korisnika**, odaberite tip korisnika za kojeg želite da ga sistem koristi kod izvođenja EIM operacija u korist funkcija operativnog sistema. Ove operacije uključuju pregledavanja mapiranja i brisanje udruženja kod brisanja lokalnog OS/400 korisničkog profila. Možete odabrati jedan od sljedećih tipova korisnika: Razlikovno ime i lozinka, Kerberos keytab datoteka i principal, ili Kerberos principal i lozinka. Korisnički tip koji odaberete određuje druge informacije koje morate dobaviti za dovršavanje dijaloga kako slijedi:

Opaska: Korisnik kojeg specificira mora imati povlastice na minimumu za izvođenje pregledavanja mapiranja i administracije registra za lokalni korisnički registar. Ako korisnik kojeg specificirate nema te povlastice, tada se određene funkcije operativnog sistema odnose na jednostruku prijavu i brisanje korisničkih profila može biti neuspješno.

11. Ako odaberete **Razlikovno ime i lozinka**, osigurajte sljedeće informacije:
    - U polju **Razlikovno ime**, unesite LDAP razlikovno ime (DN) koje identificira korisnika za OS/400 koji će se koristiti u kontaktiranju kontrolera EIM domene.
    - U polju **Lozinka** unesite lozinku za korisnika.
    - U polju **Potvrda lozinke** ponovno unesite lozinku.
12. Ako odaberete **Kerberos principal i lozinka**, osigurajte sljedeće informacije:
    - U polju **Principal**, unesite ime Kerberos principala koje identificira korisnika za OS/400 koji će se koristiti u kontaktiranju kontrolera EIM domene.
    - U polju **Područje** unesite ime Kerberos područja za principal.
    - U polju **Lozinka** unesite lozinku za korisnika.
    - U polju **Potvrda lozinke** ponovno unesite lozinku.Ime principala i područja jedinstveno identificira Kerberos korisnike u keytab datoteci. Na primjer, principal jsmith u području ordept.myco.com predstavljeno je u keytab datoteci kao jsmith@ordept.myco.com.
13. Ako odaberete **Kerberos keytab datoteka i principal**, osigurajte sljedeće informacije:
    - U polju **Keytab datoteka**, unesite ime keytab datoteke na iSeries poslužitelju koje identificira korisnika za OS/400 koji će se koristiti u kontaktiranju kontrolera EIM domene. Ili, možete kliknuti **Pregčed** za odabir keytab datoteke.
    - U polju **Principal** unesite ime Kerberos principala za korištenje u identifikaciji korisnika.
    - U polju **Područje** unesite ime Kerberos područja za principal. Ime principala i područja jedinstveno identificira Kerberos korisnike u keytab datoteci. Na primjer, principal jsmith u području ordept.myco.com predstavljeno je u keytab datoteci kao jsmith@ordept.myco.com.
14. Kliknite **Provjeri povezivanje** za testiranje povezivanja na kontroler domene za sistemskog korisnika kojeg ste upravo kreirali.
15. Kliknite **Sljedeće**.
16. Na panelu **Sažetak** pregledajte konfiguracijske informacije koje ste dobavili. AKo su sve informacije točne, kliknite **Završetak**.

Kada se čarobnjak dovrši, završili ste vašu osnovnu EIM konfiguraciju. Međutim, morate dovršiti ove zadatke da dovršite vašu EIM konfiguraciju ovog poslužitelja:

1. Dodajte domenu koju ste kreirali u folder Upravljanje EIM domenom.
2. Dodajte EIM registre u EIM domenu za druge poslužitelje i aplikacije za koje želite da sudjeluju u EIM domeni.
3. Kreiraj EIM identifikatore u domeni za svakog jedinstvenog korisnika ili cjelinu sistema koji sudjeluju u domeni.
4. Kreiraj udruženja između različitih korisničkih identiteta osobe ili cjeline prema ovim EIM identifikatorima.

Dodatno, možete htjeti koristiti Sloj sigurnih utičnica (SSL) ili Sloj sigurnog prijenosa (TLS) za konfiguriranje sigurnog povezivanja na kontroler domene.

Konfiguriranje sigurnog povezivanja na kontroler EIM domene

Kada ste koristili čarobnjaka za kreiranje i pristupanje novoj domeni, možda ćete htjeti koristiti Sloj sigurnih utičnica (SSL) ili Protokol sigurnosti sloja prijenosa (TLS) za uspostavljanje sigurnog povezivanja na kontroler EIM domene. Da konfigurirate SSL ili TLS za EIM, morate dovršiti sljedeće zadatke:

1. Omogućite SSL za kontroler domene LDAP poslužitelja.
2. Koristite Upravitelja digitalnih certifikata (DCM) za kreiranje certifikata koje LDAP poslužitelj treba kod upotrebe za SSL.
3. Koristite DCM za dodjelu certifikata LDAP poslužitelju.
4. Ažurirajte svojstva EIM Konfiguracije za specificiranje da iSeries poslužitelj koristi sigurno SSL povezivanje.
5. Ažurirajte svojstva EIM domene za svaku EIM domenu radi specificiranja da EIM koristi SSL povezivanje kod upravljanja kroz iSeries Navigator.

Pristupanje postojećoj domeni

Možete koristiti EIM Konfiguracijskog čarobnjaka za pristupanje postojećoj EIM domeni. Koristite ovu opciju u EIM Konfiguracijskom čarobnjaku kada su EIM domena i kontroler domene već konfigurirani u mreži. Kako radite kroz čarobnjaka, morate dobaviti informacije o domeni, uključujući informacije povezivanja na EIM kontroler domene. Čarobnjak sprema ove informacije na iSeries poslužitelj i zatim ih koristi za povezivanje na EIM kontroler domene. Čarobnjak također kreira EIM korisnički registar koji predstavlja OS/400 korisnički profil registra na ovom iSeries poslužitelju.

Da bi koristili čarobnjaka za dovršavanje ovog zadatka, morate imati specijalna ovlaštenja Administratora sigurnosti (*SECADM), Svih objekata (*ALLOBJ).

Da pokrenete i koristite EIM Konfiguracijskog čarobnjaka za pristupanje postojećoj EIM domeni, dovršite ove korake koristeći iSeries Navigator:

1. Proširite **Mreža —> Mapiranje identiteta u poduzeću**.
2. Desno kliknite **Konfiguracija** i odaberite **Konfiguriraj...** za lansiranje EIM Konfiguracijskog čarobnjaka. Kada se čarobnjak pokrene, osigurajte sljedeće informacije kako radite kroz dijaloge.
3. U dijalogu čarobnjaka **Dobro došli!** odaberite **Pristupanje postojećoj domeni** i kliknite **Sljedeće**.
4. Ako usluga provjere autentičnosti mreže trenutno nije konfigurirana na iSeries poslužitelju, prikazuje se dijalog **Konfiguracija usluge provjere autentičnosti mreže**. Ovaj dijalog vas pita želite li konfigurirati uslugu provjere autentičnosti mreže. Ako odaberete **Da**, lansira se Čarobnjak konfiguracije usluge provjere autentičnosti mreže. Kada dovršite konfiguraciju usluge provjere autentičnosti mreže, nastavlja se EIM Konfiguracijski čarobnjak.
5. Kada se prikaže dijalog **Specificiranje kontrolera domene** osigurajte sljedeće informacije:
   - U polju **Ime kontrolera domene** specificirajte ime sistema koji se koristi kao kontroler domene za EIM domenu na koju želite iSeries poslužitelj pristupi.
   - Kliknite **Koristi Sloj sigurnih utičnica (SSL)** ako želite da dohvaćanje EIM informacija iz kontrolera domene koristi SSL kao zaštitu prijenosa EIM podataka.

- Kliknite **Provjeri povezivanje** za testiranje vaših konfiguracijskih informacija kontrolera domene.

Opaska: Ako ste specificirali korištenje SSL-a i primili ste poruku o greški, poruka može označavati da LDAP poslužitelj nije bio konfiguriran za korištenje SSL-a.

- Kliknite **Sljedeće**.

6. U dijalogu **Specificiranje korisnika za povezivanje** odaberite **korisnički tip** za povezivanje. Možete odabrati jedan od sljedećih tipova korisnika: Razlikovno ime i lozinka, Kerberos keytab datoteka i principal, ili Kerberos principal i lozinka. Dva Kerberos korisnička tipa dostupna su samo ako je usluga provjere autentičnosti mreže konfigurirana za lokalni iSeries sistem. Korisnički tip koji odaberete određuje druge informacije koje morate osigurati za dovršavanje dijaloga kako slijedi:
   - Ako odaberete **Razlikovno ime i lozinka**, osigurajte sljedeće informacije:
     - U polju **Razlikovno ime**, unesite LDAP razlikovno ime (DN) koje identificira korisnika koji je ovlašten za kreiranje objekata u lokalnom imenskom prostoru LDAP poslužitelja.
     - U polju **Lozinka** unesite lozinku za korisnika.
     - U polju **Potvrda lozinke** ponovno unesite lozinku.
   - Ako odaberete **Kerberos keytab datoteka i principal**, osigurajte sljedeće informacije:
     - U polju **Keytab datoteka**, unesite keytab datoteke na iSeries poslužitelju koje identificira korisnika ovlaštenog za kreiranje objekata u lokalnom imenskom prostoru LDAP poslužitelja. Ili, možete kliknuti **Pregčed** za odabir keytab datoteke.
     - U polju **Principal** unesite ime Kerberos principala za korištenje u identifikaciji korisnika.
     - U polju **Područje** unesite ime Kerberos područja za principal. Ime principala i područja jedinstveno identificira Kerberos korisnike u keytab datoteci. Na primjer, principal jsmith u području ordept.myco.com predstavljeno je u keytab datoteci kao jsmith@ordept.myco.com.
   - Ako odaberete **Kerberos principal i lozinka**, osigurajte sljedeće informacije:
     - U polju **Principal**, unesite ime Kerberos principala koje identificira korisnika ovlaštenog za kreiranje objekata l lokalnom imenskom prostoru LDAP poslužitelja.
     - U polju **Područje** unesite ime Kerberos područja za principal.
     - U polju **Lozinka** unesite lozinku za korisnika.
     - U polju **Potvrda lozinke** ponovno unesite lozinku.Ime principala i područja jedinstveno identificira Kerberos korisnike u keytab datoteci. Na primjer, principal jsmith u području ordept.myco.com predstavljeno je u keytab datoteci kao jsmith@ordept.myco.com.
   - Kliknite **Provjeri povezivanje** za testiranje vaših korisničkih konfiguracijskih informacija kod povezivanja na kontroler domene.
   - Kliknite **Sljedeće**.
7. Na stranici **Specificiranje domene** odaberite ime domene kojoj želite pristupiti i kliknite **Sljedeće**.
8. Na stranici **Informacije registra** odaberite tip korisničkih registara koje želite dodati u EIM domenu. Odaberite jedno ili oboje od ovih tipova korisničkog registra:
   - Odaberite **OS400** za dodavanje korisničkog registra koji predstavlja lokalni registar u EIM domeni. U dobavljenom polju upišite ime registra koji treba biti kreiran u domeni. Ime EIM registra je proizvoljan niz znakova koji predstavlja tip registra i specifičnu instancu tog registra.
   - Odaberite **Kerberos** za dodavanje Kerberos korisničkog registra u EIM domenu. U dobavljenom polju, upišite ime registra koji treba biti kreiran u domeni i odaberite **Kerberos korisnički identiteti su osjetljivi na velika i mala slova**, ako je potrebno. Možete prihvatiti defaultnu vrijednost; Kerberos ime registra je isto kao i ime područja. Korištenjem Kerberos registarskog imena kao imena područja, možete povećati izvedbu u dohvaćanju informacija iz registra. Za više informacija o tome kako mogu biti definirani korisnički registri unutar EIM-a, pogledajte Definicije EIM registra.
   - Kliknite **Sljedeće**.
9. U dijalogu **Specificiraj EIM sistemskog korisnika**, odaberite tip korisnika za kojeg želite da ga sistem koristi kod izvođenja EIM operacija u korist funkcija operativnog sistema. Ove operacije uključuju pregledavanja mapiranja i brisanje udruženja kod brisanja lokalnog OS/400 korisničkog profila. Možete

odabrati jedan od sljedećih tipova korisnika: Razlikovno ime i lozinka, Kerberos keytab datoteka i principal, ili Kerberos principal i lozinka. Korisnički tip koji odaberete određuje druge informacije koje morate dobaviti za dovršavanje dijaloga kako slijedi:

- Ako odaberete **Razlikovno ime i lozinka**, osigurajte sljedeće informacije:
  - U polju **Razlikovno ime**, unesite LDAP razlikovno ime (DN) koje identificira korisnika za OS/400 koji će se koristiti u kontaktiranju kontrolera EIM domene.
  - U polju **Lozinka** unesite lozinku za korisnika.
  - U polju **Potvrda lozinke** ponovno unesite lozinku.
- Ako odaberete **Kerberos principal i lozinka**, osigurajte sljedeće informacije:
  - U polju **Principal**, unesite ime Kerberos principala koje identificira korisnika za OS/400 koji će se koristiti u kontaktiranju kontrolera EIM domene.
  - U polju **Područje** unesite ime Kerberos područja za principal.
  - U polju **Lozinka** unesite lozinku za korisnika.
  - U polju **Potvrda lozinke** ponovno unesite lozinku.Ime principala i područja jedinstveno identificira Kerberos korisnike u keytab datoteci. Na primjer, principal jsmith u području ordept.myco.com predstavljeno je u keytab datoteci kao jsmith@ordept.myco.com.
- Ako odaberete **Kerberos keytab datoteka i principal**, osigurajte sljedeće informacije:
  - U polju **Keytab datoteka**, unesite ime keytab datoteke na iSeries poslužitelju koje identificira korisnika za OS/400 koji će se koristiti u kontaktiranju kontrolera EIM domene. Ili, možete kliknuti **Pregčed** za odabir keytab datoteke.
  - U polju **Principal** unesite ime Kerberos principala za korištenje u identifikaciji korisnika.
  - U polju **Područje** unesite ime Kerberos područja za principal.
- Kliknite **Provjeri povezivanje** za testiranje povezivanja sistemskog korisnika kojeg ste upravo kreirali.
- Kliknite **Sljedeće**.

10. Na panelu **Sažetak** pregledajte konfiguracijske informacije koje ste dobavili. AKo su sve informacije točne, kliknite **Završetak**.

Kada se čarobnjak dovrši, završili ste vašu osnovnu EIM konfiguraciju. Međutim, morate dovršiti ove zadatke da dovršite vašu EIM konfiguraciju ovog poslužitelja:

1. Dodajte domenu koju ste pristupili u folder Upravljanje EIM domenom.
2. Dodaj EIM registre u EIM domenu za ne-iSeries poslužitelje i aplikacije za koje želite da sudjeluju u EIM domeni.
3. Kreiraj EIM identifikatore u domeni za svakog jedinstvenog korisnika ili cjelinu sistema koji sudjeluju u domeni.
4. Kreiraj udruženja između različitih korisničkih identiteta osobe ili cjeline prema ovim EIM identifikatorima.

Također, da omogućite okruženje jednostruke prijave, morate konfigurirati uslugu provjere autentičnosti mreže za iSeries poslužitelj.

Upravljanje EIM-om

Kada ste konfigurirali EIM na vašem iSeries poslužitelju, postoje još mnogi zadaci koje trebate izvesti za upravljanje vašom EIM domenom i informacijama. Sljedeća poglavlja raspravljaju o specifičnim zadacima korištenim za upravljanje EIM-om na vašem iSeries poslužitelju i unutar vašeg mrežnog poduzeća.

Upravljanje EIM domenama
Rad s EIM informacijama sadržanim u vašoj EIM domeni i svojstvima EIM domene.

Upravljanje udruženjima
Održavajte udruženja korisničkih identiteta prema EIM identifikatorima za sve korisnike unutar poduzeća.

Upravljanje EIM identifikatorima
Održavajte EIM identifikatore pridružene korisnicima u poduzeću.

Upravljanje EIM korisničkim ovlaštenjima
Održavajte sigurnost vaših EIM informacija radeći s EIM ovlaštenjima radi kontrole EIM funkcija i operacija koje korisnik može obavljati.

Upravljanje korisničkim registrima
Rad s korisničkim registrima koje ste dodali u vašu EIM domenu.

Upravljanje EIM domenama

Možete koristiti iSeries Navigator za upravljanje svim vašim EIM domenama. Da bi upravljali EIM domenom, domena mora biti ispisana, ili je morate dodati, u folder Upravljanje domenom pod folderom Upravljanje domenom u iSeries Navigatoru. Nakon što kreirate i konfigurirate novu EIM domenu, morate je dodati u folder Upravljanje domenom da bi upravljali informacijama u domeni.

Možete koristiti bilo koje iSeries povezivanje za upravljanje EIM domenom koja prebiva bilo gdje u mreži. iSeries koji je povezan na iSeries Navigator ne treba sudjelovati u domeni kako bi upravljao tom domenom.

Možete dovršiti sljedeće zadatke za upravljanje vašim EIM domenama:

- Dodavanje domene u upravljanje domenom
- Povezivanje na domenu
- Brisanje domene
- Uklanjanje domene iz Upravljanja domenom

Dodavanje domene u upravljanje domenom

Da dodate domenu, morate imati *SECADM specijalno ovlaštenje. Da dodate postojeću EIM domenu u upravljanje domenom, dovršite sljedeće korake.

1. Proširite **Mreža —> Mapiranje identiteta u poduzeću**.
2. Desno kliknite na **Upravljanje domenom** i odaberite **Dodaj domenu...**.
3. Specificirajte potrebne informacije domene i povezivanja.
4. Kliknite **OK** za dodavanje domene.

Povezivanje na domenu

Ako trenutno niste povezani na EIM domenu u kojoj želite raditi, prvo se morate povezati na domenu. Možete se povezati na EIM domenu iako vaš iSeries poslužitelj nije trenutno konfiguriran za sudjelovanje u ovoj domeni.

Da se povežete na EIM domenu, dovršite sljedeće korake:

1. Proširite **Mreža —> Mapiranje identiteta u poduzeću —> Upravljanje domenom**.
2. Odaberite domenu na koju se želite povezati. Ako domena s kojom želite raditi nije ispisana, morate Dodati EIM domenu u upravljanje domenom.
3. Desno kliknite na EIM domenu na koju se želite povezati i odaberite **Povezivanje...**.
4. Specificirajte korisnički tip i potrebne korisničke informacije koje bi se trebale koristiti za povezivanje na kontroler EIM domene.
5. Kliknite**OK**.

Brisanje domene
Da dovršite ovaj zadatak, morate imati ili ovlaštenje LDAP administratora ili EIM administratora. Prije brisanja EIM domene morate prvo ukloniti sve registre i informacije EIM identifikatora iz domene.

Za brisanje EIM domene dovršite sljedeće korake.

1. Proširite **Mreža —> Mapiranje identiteta u poduzeću —> Upravljanje domenom**.
2. Uklonite sve korisničke registre iz EIM domene.
3. Izbrišite sve EIM identifikatore iz EIM domene.
4. Desno kliknite na domenu koju želite izbrisati i odaberite **Izbriši...**.
5. Kliknite **Da** u dijalogu **Potvrda brisanja**.

Uklanjanje domene iz upravljanja domenom
Iako nije potrebno, možete ukloniti EIM domenu iz foldera Upravljanje domenom kada ste završili s promjenama.

Da uklonite domenu, dovršite sljedeće korake:

1. Proširite **Mreža —> Mapiranje identiteta u poduzeću**.
2. Desno kliknite **Upravljanje domenom** i odaberite **Ukloni domenu...**.
3. Odaberite EIM domenu koju želite ukloniti iz upravljanja domenom.
4. Kliknite **OK** za uklanjanje domene.

Upravljanje udruženjima
Udruženje definira odnos između EIM identifikatora i korisničkog identiteta unutar registra. Na primjer, možete kreirati udruženje između OS/400 korisničkog profila ili Kerberos principala i EIM identifikatora. Ovo udruženje se tada može koristiti za određivanje EIM identifikatora koji odgovara lokalnom iSeries korisničkom profilu ili Kerberos principalu.

Održavanje udruženja korisničkih identiteta s prikladnim EIM identifikatorima je ključ pojednostavljenja administrativnih zadataka potrebnih za praćenje koji korisnici imaju račune na različitim sistemima u mreži.

Upravljanje ovim udruženjima također vam osigurava prednost u omogućavanju jednostruke prijave u vašoj mreži. Morate održavati udruženja trenutnim kada implementirate mrežu jednostruke prijave.

Postoje tri tipa udruženja koje možete kreirati: izvorno, ciljno i administrativno. Da kreirate ili održavate udruženja među korisničkim identitetima s prikladnim EIM identifikatorima, možete izvesti jedan od sljedećih zadataka:

- Kreiranje udruženja
- Brisanje udruženja

Kreiranje udruženja
Da omogućite okolinu jednostruke prijave, morate kreirati udruženja između različitih korisničkih identiteta osobe ili cjeline s jednim EIM identifikatorom za tu osobu ili cjelinu. Možete kreirati tri tipa udruženja: ciljno, izvorno i administrativno.

Za kreiranje izvornog ili administrativnog udruženja morate imati ili ovlaštenje administratora identifikatora ili EIM ovlaštenje administratora. Za kreiranje ciljnog udruženja morate imati ovlaštenje administratora registra za sve registre, administratora registra za specifični registar ili EIM ovlaštenje administratora.

Za kreiranje udruženja EIM identifikatora, dovršite sljedeće korake:

1. Proširite **Mreža —> Mapiranje identiteta u poduzeću —> Upravljanje domenom**.
2. Morate biti povezani na EIM domenu u kojoj želite raditi.

- Ako EIM domena s kojom želite raditi nije ispisana u folderu Upravljanje domenom, pogledajte Dodavanje EIM domene u Upravljanje domenom.
- Ako trenutno niste povezani na EIM domenu u kojoj želite raditi, pogledajte Povezivanje na kontroler EIM domene.

3. Proširite EIM domenu na koju ste sada povezani.
4. Kliknite **Identifikatori** za prikaz liste EIM identifikatora.
5. Desno kliknite na prikladni EIM identifikator i odaberite **Svojstva...**.
6. Kliknite na karticu **Udruženja**.
7. Kliknite **Dodaj...** za prikaz dijaloga **Dodavanje udruženja**.
8. Kliknite **Pomoć** ako trebate više informacija za dovršavanje polja.
9. Kada ste specificirali potrebne informacije, kliknite **OK**.

Brisanje udruženja

Za brisanje administrativnog ili izvornog udruženja, morate imati ovlaštenje administratora identifikatora ili EIM ovlaštenje administratora. Za brisanje ciljnog udruženja morate imati ovlaštenje administratora za odabrane registre (uključujući registar s kojim želite raditi), ovlaštenje administratora registra ili EIM ovlaštenje administratora.

Za brisanje udruženja dovršite sljedeće korake.

1. Proširite **Mreža —> Mapiranje identiteta u poduzeću —> Upravljanje domenom**.
2. Morate biti povezani na EIM domenu u kojoj želite raditi:
   - Ako EIM domena s kojom želite raditi nije ispisana u Upravljanje domenom, pogledajte Dodavanje EIM domene u upravljanje domenom.
   - Ako trenutno niste povezani na EIM domenu u kojoj želite raditi, pogledajte Povezivanje na EIM domenu.
3. Proširite EIM domenu na koju ste sada povezani.
4. Kliknite **Identifikatori**.
5. Desno kliknite na EIM identifikator kojeg želite i odaberite **Svojstva...** .
6. Kliknite na karticu **Udruženja** za prikaz trenutnih udruženja EIM identifikatora.
7. Odaberite udruženje koje želite ukloniti.
8. Kliknite **Ukloni** za uklanjanje udruženja.
9. Kliknite **OK**.

Upravljanje EIM identifikatorima

Održavanje EIM identifikatora koji predstavljaju korisnike u vašoj mreži, važno je iz sigurnosnih razloga. Korisnici unutar poduzeća se skoro stalno mijenjaju, neki dolaze, neki odlaze, a neki se premještaju među područjima. Zajedno s ovim promjenama dolazi potreba za praćenjem korisničkih računa i njihovih pristupa sistemima unutar mreže. Kreiranje EIM identifikatora i njihovo pridruživanje korisničkim identitetima za svakog korisnika, čini ovaj zadatak praćenja lakšim.

Omogućavanje jednostruke prijave čini zadatak za korisnike puno lakšim i kada se oni premještaju u drugi odjel ili područje unutar poduzeća. Također se mogu promijeniti njihove potrebe potvrde sigurnosti i pristupa sistemu. Omogućavanje jednostruke prijave eliminira potrebnu da korisnici pamte nova korisnička imena i lozinke za nove sisteme.

Upravljanje EIM identifikatorima za vaše korisnike unutar poduzeća uključuje mnoge zadatke koju mogu biti rutinirani. Možete koristiti sljedeće zadatke za upravljanje EIM identifikatorima u vašoj mreži i domenama:

- Kreiranje EIM identifikatora
- Dodavanje zamjenskog imena EIM identifikatoru
- Brisanje EIM identifikatora

Za informacije o upravljanju udruženjima, pogledajte poglavlje Upravljanje udruženjima.

Kreiranje EIM identifikatora

Da kreirate EIM identifikator morate imati ili ovlaštenje administratora identifikatora ili ovlaštenje EIM administratora.

Za kreiranje EIM identifikatora osobe ili cjeline, dovršite ove korake:

1. Proširite **Mreža —> Mapiranje identiteta u poduzeću —> Upravljanje domenom**.
2. Morate biti povezani na EIM domenu u kojoj želite raditi:
   - Ako EIM domena s kojom želite raditi nije ispisana pod **Upravljanje domenom**, pogledajte Dodavanje domene u Upravljanje domenom.
   - Ako trenutno niste povezani na EIM domenu u kojoj želite raditi, pogledajte Povezivanje na domenu.
3. Proširite EIM domenu na koju ste sada povezani.
4. Desno kliknite na **Identifikatori** i odaberite **Nov identifikator...**.
5. Kliknite **Pomoć** ako trebate više informacija o bilo kojim poljima.
6. Kada ste specificirali potrebne informacije, kliknite **OK**.

Dodavanje zamjenskog imena EIM identifikatoru

Možda ćete htjeti kreirati zamjensko ime za osiguravanje dodatnih razlikovnih informacija EIM identifikatora. Vi, ili drugi, možete tada koristiti zamjensko ime za razlikovanje EIM identifikatora. Na primjer, ako imate dva korisnika s imenom Ivan I. Ivanić, mogli biste kreirati zamjensko ime Ivan Ivo Ivanić za jednog i Ivan Ivica Ivanić za drugog kako bi lakše razlikovali identitet svakog korisnika.

Da dodate zamjensko ime identifikatoru, morate imati ili ovlaštenje administratora identifikatora ili ovlaštenje EIM administratora.

Da dodate zamjensko ime EIM identifikatoru, dovršite ove korake.

1. Proširite **Mreža —> Mapiranje identiteta u poduzeću —> Upravljanje domenom**.
2. Morate biti povezani na EIM domenu u kojoj želite raditi:
   - Ako EIM domena s kojom želite raditi nije ispisana pod Upravljanjem domene, pogledajte Dodavanje EIM domene u Upravljanje domenom.
   - Ako trenutno niste povezani na EIM domenu u kojoj želite raditi, pogledajte Povezivanje na kontroler EIM domene.
3. Proširite EIM domenu na koju ste povezani.
4. Desno kliknite na EIM identifikator kojeg želite i odaberite **Svojstva**. Ako ne postoje EIM identifikatori, pogledajte Kreiranje EIM identifikatora.
5. Specificirajte ime zamjenskog imena kojeg želite dodati ovom EIM identifikatoru i kliknite **Dodaj**.
6. Kliknite **OK** za spremanje promjena.

Brisanje EIM identifikatora

Za brisanje EIM identifikatora morate imati ovlaštenje EIM administratora.

Za brisanje EIM identifikatora dovršite ove korake:

1. Proširite **Mreža —> Mapiranje identiteta u poduzeću —> Upravljanje domenom**.
2. Morate biti povezani na EIM domenu u kojoj želite raditi:
   - Ako EIM domena s kojom želite raditi nije ispisana pod Upravljanjem domene, pogledajte Dodavanje EIM domene u Upravljanje domenom.
   - Ako trenutno niste povezani na EIM domenu u kojoj želite raditi, pogledajte Povezivanje na kontroler EIM domene.
3. Proširite EIM domenu na koju ste sada povezani.
4. Kliknite **Identifikatori**.

5. Odaberite jedan ili više EIM identifikatora za brisanje.
6. Desno kliknite na odabrane EIM identifikatore i odaberite **Izbriši**.
7. Kliknite **Da** u dijalogu **Potvrda brisanja** za uklanjanje odabranih EIM identifikatora.

Upravljanje EIM ovlaštenjima korisnika

EIM definira različita EIM ovlaštenja koja su potrebna za izvođenje različitih operacija unutar domene. Ovo uključuje funkcije upravljanja domenom kao što je kreiranje identifikatora, ispis registara, te izvođenje operacija pregledavanja mapiranja. Samo je korisnicima s EIM ovlaštenjem administratora dozvoljeno dodjeljivanje ili opozivanje ovlaštenja za druge korisnike.

Pogledajte EIM ovlaštenja za sažete definicije svake grupe ovlaštenja i detalje o specifičnom pristupu EIM funkcijama kojeg ova ovlaštenja imaju.

Da promijenite EIM ovlaštenja za korisnika, pratite ove korake:

1. U iSeries Navigator, proširite **Mreža —> Mapiranje identiteta u poduzeću —> Upravljanje domenom**.
2. Proširite EIM domenu u kojoj želite raditi. Ako trenutno niste povezani na ovu domenu, bit ćete upitani za povezivanje. Osigurajte da se povežete na domenu s ovlaštenjem korisnika koji ima EIM ovlaštenje administratora.
3. Desno kliknite na EIM domenu i odaberite **Ovlaštenje...**.
4. U dijalogu **Uređivanje EIM ovlaštenja** specificirajte korisnika za kojeg mijenjate EIM ovlaštenja.
5. Kliknite**OK**.
6. U dijalogu **Uređivanje EIM ovlaštenja** napravite potrebne promjene u ovlaštenjima za korisnika.
7. Kada ste završili, kliknite **OK** za spremanje promjena u ovlaštenjima.

Upravljanje korisničkim registrima

Prije nego možete kreirati udruženja među identitetima sadržanim u korisničkim registrima i prikladne EIM identifikatore, morate prvo definirati korisnički registar u EIM domeni:

Sljedeći zadaci su dio upravljanja korisničkim registrima unutar EIM domene.

- Dodavanje korisničkog registra
- Dodavanje pseudonima u korisnički registar
- Definiranje privatnog tipa korisničkog registra u EIM-u
- Uklanjanje korisničkog registra
- Uklanjanje zamjenskog imena iz korisničkog registra

Dodavanje korisničkog registra

Da dodate korisnički registar morate imati EIM ovlaštenje administratora. Za detalje o ovom ovlaštenju i čemu korisnik s ovim ovlaštenjem može pristupiti, pogledajte EIM ovlaštenja.

Da dodate korisnički registar u EIM domenu, dovršite ove korake.

1. Proširite **Mreža —> Mapiranje identiteta u poduzeću —> Upravljanje domenom**.
2. Povežite se na EIM domenu s korisnikom koji ima EIM ovlaštenje administratora.
   - Ako EIM domena s kojom želite raditi nije ispisana u folderu Upravljanje domenom, pogledajte Dodavanje EIM domene u upravljanje domenom.
   - Ako trenutno niste povezani na EIM domenu u kojoj želite raditi, pogledajte Povezivanje na kontroler EIM domene.
3. Proširite EIM domenu na koju ste sada povezani.
4. Desno kliknite na **Korisnički registri** i odaberite **Dodavanje registra...**.
5. Specificirajte potrebne informacije korisničkog registra. Također možete specificirati informacije zamjenskog imena za korisnički registar.

6. Kliknite **OK** za spremanje informacija i dodavanje korisničkog registra u EIM domenu.

Dodavanje pseudonima u korisnički registar

Vi, ili razvijač aplikacija, možete poželjeti kreirati pseudonim za osiguravanje razlikovnih informacija korisničkog registra. Vi, ili drugi, tada možete koristiti pseudonim za razlikovanje jednog korisničkog registra od drugog. Na primjer, razvijači aplikacija i administratori koriste pseudonim na korisničkom registru za dogovor koje bi EIM registre aplikacija trebala koristiti. Za informacije o korištenju pseudonima s korisničkim registrima, pogledajte Definicije EIM registra.

Da dodate pseudonim u korisnički registar, morate koristiti jedno od sljedećih ovlaštenja: EIM administrator, administrator registra za sve registre, ili administrator registra za specifičan registar nad kojim obavljate ovaj zadatak.

Da dodate pseudonim korisničkom registru unutar EIM domene, dovršite ove korake:

1. Proširite **Mreža —> Mapiranje identiteta u poduzeću —> Upravljanje domenom**.
2. Morate biti povezani na EIM domenu u kojoj želite raditi:
   - Ako EIM domena s kojom želite raditi nije ispisana u folderu Upravljanje domenom, pogledajte Dodavanje EIM domene u upravljanje domenom.
   - Ako trenutno niste povezani na EIM domenu u kojoj želite raditi, pogledajte Povezivanje na kontroler EIM domene.
3. Proširite EIM domenu na koju ste sada povezani.
4. Kliknite **Korisnički registri** za prikaz liste registara unutar domene.
5. Desno kliknite na korisnički registar u kojeg dodajete pseudonim i odaberite **Svojstva...**.
6. Kliknite na karticu **Zamjensko ime** u dijalogu **Svojstva**.
7. Specificirajte ime i tip zamjenskog imena kojeg želite dodati. Možete specificirati tip zamjenskog imena koji nije uključen u listi tipova.
8. Kliknite **Dodaj**.
9. Kliknite **OK** za spremanje promjena.

Definiranje privatnog tipa korisničkog registra u EIM-u

Da definirate tip korisničkog registra za kojeg EIM nije predodređen da ga prepozna, morate specificirati tip registra u obliku **ObjectIdentifier-normalization**, gdje je **ObjectIdentifier** identifikator objekta s decimalnom točkom kao što je 1.2.3.4.5.6.7, a **normalization** je ili vrijednost **caseExact** ili vrijednost **caseIgnore**. Na primjer, identifikator objekta (OID) za OS/400 je 1.3.18.0.2.33.2-caseIgnore.

Trebali biste pribaviti sve OID-e koje trebate od legitimnih OID ovlaštenja registracije za osiguranje da kreirate i koristite jedinstvene OID-e. Jedinstveni OID-i pomažu vam u izbjegavanju mogućih sukoba s OID-ima kreiranim od drugih organizacija ili aplikacija.

Postoje dva načina dobavljanja OID-a:

- **Registriranje objekata s ovlaštenjem**.
  Ova metoda je dobar izbor kada trebate manji broj čvrstih OID-a za predstavljanje informacija. Na primjer, ovi OID-ovi mogu predstavljati police certifikata za korisnike u vašem poduzeću.
- **Postizanje dodjele luka iz ovlaštenja registracije i dodjeljivanje vaših vlastitih OID-a prema potrebi**.
  Ova metoda, dodjela raspona identifikatora objekta s decimalnom točkom, dobar je izbor ako trebate velik broj OID-a ili ako su vaše dodjele OID-a podložne promjeni. Dodjela luka sastoji se od početnih brojeva s decimalnom točkom iz kojih morate zasnovati vaš **ObjectIdentifier**. Na primjer, dodjela luka mogla bi biti 1.2.3.4.5.. Tada možete kreirati OID-e dodavanjem u ovaj osnovni luk. Na primjer, mogli bi kreirati OID-e u obliku 1.2.3.4.5.x.x.x).

Možete naučiti više o registriranju vaših OID-a s ovlaštenjem registracije, pregledavanjem ovih Internet resursa:

- American National Standards Institute (ANSI) je ovlaštenje registracije Sjedinjenih država za imena organizacija pod globalnom registracijskom obradom uspostavljenom od International Standards Organization (ISO) i International Telecommunication Union (ITU). List papira s činjenicama s vezama na formu aplikacije, smješten je na ANSI Web stranici http://web.ansi.org/public/services/reg_org.html

  . ANSI OID luk za organizacije je 2.16.840.1. ANSI naplaćuje pristojbu za dodjele OID luka. Potrebno je otprilike dva tjedna za primanje dodijeljenog OID luka iz ANSI-a. ANSI će dodijeliti broj (NEWNUM), kreiranjem novog OID luka: 2.16.840.1.NEWNUM.
- U većini zemalja ili regija, udruženje nacionalnih standarda održava OID registar. Kao i s ANSI lukom, to su uglavnom lukovi dodijeljeni pod OID-om 2.16. Može biti potrebno malo istraživanje da se pronađe OID ovlaštenje za određenu zemlju ili regiju. Adresa za ISO nacionalne članove tijela može se pronaći na http://www.iso.ch/addresse/membodies.html

  . Informacije uključuju poštansku adresu i elektroničku poštu. U mnogim slučajevima specificirana je i Web stranica.
- Druga moguća početna točka je Internacionalni registar ISO DCC NSAP shema. NSAP označava Network Service Access Point i koristi se u različitim internacionalnim standardima. Registar za sheme može se dobiti na http://www.fei.org.uk pod zaglavljem ISO DCC NSAP

  . Web stranica trenutno ispisuje informacije kontakta za 13 imenovanih ovlaštenja, od kojih će neka također dodijeliti OID-e.
- Internet Assigned Numbers Authority (IANA) dodjeljuje brojeve privatnih poduzeća, što su OID-i, u luku 1.3.6.1.4.1. IANA je dodijelila lukove više od 7500 tvrtki do danas. Aplikacijska stranica smještena je na http://www.iana.org/cgi-bin/enterprise.pl

  , pod Brojevima privatnih poduzeća. IANA obično traje oko jedan tjedan. OID od IANA-e je besplatan. IANA će dodijeliti broj (NEWNUM) tako da će novi OID luk biti 1.3.6.1.4.1.NEWNUM.
- Federalna vlada Sjedinjenih država održava Computer Security Objects Registry (CSOR). CSOR je ovlaštenje imenovanja za luk 2.16.840.1.101.3, i trenutno registrira objekte za sigurnosne oznake, , kriptografičke algoritme i politike certifikata. OID-i politike certifikata definirani su u luku 2.16.840.1.101.3.2.1. CSOR osigurava politiku OID-a za agencije Vlade Sjedinjenih država. Za više informacija o CSOR-u, pogledajte http://csrc.nist.gov/csor/

  .

Za više informacija o OID-ima za politike certifikata, pogledajtehttp://csrc.nist.gov/csor/pkireg.htm

.

Uklanjanje korisničkog registra

Uklanjanje korisničkog registra iz EIM domene uzrokuje gubitak svih udruženja EIM identifikatora za korisničke identitete unutar korisničkog registra. Dodavanje korisničkog registra natrag u EIM domenu nakon uklanjanja ne vraća veze udruženja.

Da uklonite korisnički registar morate imati EIM ovlaštenje administratora.

Da uklonite korisnički registar, dovršite sljedeće korake:

1. Proširite **Mreža —> Mapiranje identiteta u poduzeću —> Upravljanje domenom**.
2. Morate biti povezani na EIM domenu u kojoj želite raditi.
   - Ako EIM domena s kojom želite raditi nije ispisana u folderu Upravljanje domenom, pogledajte Dodavanje EIM domene u upravljanje domenom.
   - Ako trenutno niste povezani na EIM domenu u kojoj želite raditi, pogledajte Povezivanje na kontroler EIM domene.
3. Proširite EIM domenu na koju ste sada povezani.
4. Kliknite **Korisnički registri** za prikaz liste korisničkih registara u domeni.
5. Desno kliknite na korisnički registar kojeg želite ukloniti i odaberite **Izbriši...**.
6. Kliknite **Da** u dijalogu **Potvrda** za brisanje korisničkog registra.

Uklanjanje zamjenskog imena iz korisničkog registra

Da uklonite zamjensko ime iz korisničkog registra, morate imati administratorsko ovlaštenje registra i administratorsko ovlaštenje za odabrane registre (uključujući registre s kojima želite raditi), ili EIM administratorsko ovlaštenje.

Da uklonite zamjensko ime iz korisničkog registra unutar EIM domene, dovršite sljedeće korake:

1. Proširite **Mreža —> Mapiranje identiteta u poduzeću —> Upravljanje domenom**.
2. Morate biti povezani na EIM domenu u kojoj želite raditi:
   - Ako EIM domena s kojom želite raditi nije ispisana u folderu Upravljanje domenom, pogledajte Dodavanje EIM domene u upravljanje domenom.
   - Ako trenutno niste povezani na EIM domenu u kojoj želite raditi, pogledajte Povezivanje na kontroler EIM domene.
3. Proširite EIM domenu na koju ste sada povezani.
4. Kliknite **Korisnički registri** za prikaz liste registara unutar domene.
5. Desno kliknite na korisnički registar za kojeg uklanjate zamjensko ime i odaberite **Svojstva**.
6. Kliknite na karticu **Zamjensko ime** u dijalogu **Svojstva**.
7. Odaberite zamjensko ime koje želite ukloniti i kliknite **Ukloni**.
8. Kliknite **OK** za spremanje promjena.

API-ji za EIM

EIM ima višestruka sučelja aplikativnog programiranja (API-je) koje aplikacija može koristiti za vođenje EIM operacija u koristi aplikacije ili aplikacijskog korisnika. Možete koristiti ove API-je za vođenje operacija pregledavanja mapiranja identiteta, vođenje različitih EIM funkcija upravljanja i konfiguracije, kao i promjene informacija i sposobnosti upita.

EIM API-ji spadaju u više kategorija kako slijedi:

- Operacije EIM rukovanja i povezivanja
- Administracija EIM domene
- Operacije registra
- Operacije EIM identifikatora
- Upravljanje EIM udruženjem
- Operacije EIM pregledavanja mapiranja
- Upravljanje EIM ovlaštenjem

Aplikacije koje koriste ove API-je za upravljanje ili upotrebu EIM informacija u EIM domeni tipično se odnose na sljedećei programerski model:

1. Dohvati EIM hvatište
2. Poveži se na EIM domenu

3. Normalna obrada podataka
4. Koristi API EIM administracije ili EIM operacije pregleda mapiranja identiteta
5. Normalna obrada podataka
6. Prije završetka, uništi EIM hvatište

Za detaljnije informacije i kompletnu listu EIM API-ja dostupnih za iSeries poslužitelj, pogledajte poglavlje API-ji Mapiranja identiteta u poduzeću (EIM).

Uklanjanje pogreške EIM-a

EIM je sastavljen od više tehnologija te mnogih aplikacija i funkcija. Budući da ima mnogo putova koji se mogu izabrati u rješavanju problema, sljedeće poglavlje sadrži detaljne informacije i instrukcije o tome kako ukloniti greške ili ispraviti neke učestale greške na koje možete naići, kao što su:

- Nemogućnost povezivanja na kontroler domene
- Ispis EIM identifikatora traje dugo
- EIM Čarobnjak konfiguracije ostaje visjeti za vrijeme obrađivanja završetka
- EIM hvatište više nije važeće
- Kerberos provjera autentičnosti i dijagnostičke poruke

Nemogućnost povezivanja na kontroler domene

Velik broj faktora može pridonijeti problemima povezivanja kod pokušaja povezivanja na kontroler domene. Provjerite sljedeće stavke kao pomoć u pronalaženju uzroka problema:

- Provjerite ispravnost specificiranih informacija za sljedeće stavke:
  - Ime kontrolera domene
  - Specificirani port
  - Korisnički ID i lozinka
- Provjerite je li kontroler domene aktivan. Ako je kontroler domene iSeries poslužitelj, možete koristiti iSeries Navigator i pratite sljedeće korake:
  1. Proširite **Mreža —> Poslužitelji —> TCP/IP**.
  2. Provjerite da Usluge direktorija imaju stanje **Pokrenuto**. Ako je poslužitelj zaustavljen, desno kliknite na **Usluge direktorija** i odaberite **Pokreni...**

Kad je kontroler domene jednom aktivan, pokušajte se ponovno povezati na domenu.

1. Proširite **Mreža —> Mapiranje identiteta u poduzeću —> Upravljanje domenom**.
2. Odaberite domenu na koju se želite povezati. Ako nema ispisanih EIM domena ili EIM domena s kojom želite raditi nije ispisana u folderu Upravljanje domenom, pogledajte dodavanje EIM domene u upravljanje domenom.
3. Desno kliknite na EIM domenu na koju se želite povezati i odaberite **Povezivanje...**.
4. Specificirajte korisnički tip i potrebne korisničke informacije koje bi se trebale koristiti za povezivanje na kontroler EIM domene.
5. Kliknite**OK**.

Ispis EIM identifikatora traje dugo

Otvaranje foldera Identifikatora i iSeries Navigatoru može potrajati duže dok se ne generira lista identifikatora. Možda ćete htjeti suziti kriterij pretraživanja u prikazu liste EIM identifikatora ako imate veći broj EIM identifikatora u vašoj domeni.

Da prilagodite pregled EIM identifikatora, pratite ove korake:

1. U iSeries Navigator, proširite **Mreža —> Mapiranje identiteta u poduzeću —> Upravljanje domenom**.

2. Proširite EIM domenu u kojoj želite prikazati EIM identifikatore.
3. Desno kliknite na **Identifikatori** i odaberite **Prilagodi ovaj pogled —> Uključi...**.
4. Specificirajte kriterij prikaza kojeg želite. Znak zvjezdice (*) može se koristiti kao zamjenski znak.
5. Kliknite OK.

Sljedeći put kad kliknete na **Identifikatori**, EIM identifikatori prikazani su samo s odgovarajućim kriterijem kojeg ste specificirali. Ako želite pogledati sve EIM identifikatore, koristite korake iznad i odaberite **Svi identifikatori** kao vašu prilagođenu opciju.

EIM Čarobnjak konfiguracije ostaje visjeti za vrijeme obrađivanja završetka

Ako se čini da je čarobnjak ostao visjeti za vrijeme obrađivanja završetka, možda čeka pokretanje kontrolera domene. Provjerite da se nisu desile nikakve greške za vrijeme pokretanja LDAP poslužitelja. Za iSeries poslužitelje, provjerite dnevnik posla za QDIRSRV posao u QSYSWRK podsistemu.

Da provjerite dnevnik posla, pratite ove korake:

1. U iSeries Navigatoru proširite **Upravljanje poslom —> Podsistemi —> Qsyswrk**.
2. Desno kliknite na **Qdirsrv** i odaberite **Dnevnik posla**.

EIM hvatište više nije važeće

Za vrijeme upravljanja EIM-om kroz iSeries Navigator, ako korisnik primi grešku koja označava da EIM hvatište više nije važeće, tada je izgubljeno povezivanje na kontroler domene.

Da se ponovno povežete na kontroler domene, pratite ove korake:

1. U iSeries Navigator, proširite **Mreža —> Mapiranje identiteta u poduzeću —> Upravljanje domenom**.
2. Desno kliknite domenu s kojom želite raditi i odaberite **Ponovno spajanje...**.
3. Specificirajte informacije povezivanja.
4. Kliknite**OK**.

Kerberos provjera autentičnosti i dijagnostičke poruke

Kod korištenja Kerberos protokola za provjeru autentičnosti s EIM-om, dijagnostička poruka CPD3E3F se zapisuje u dnevnik posla kad god nije uspjela provjera autentičnosti ili operacija mapiranja identiteta. Dijagnostičke poruke sadrže glavne i manje važne kodove stanja za označavanje gdje se desio problem. Najčešće greške su dokumentirane u poruci zajedno s obnavljanjem.

Pogledajte informacije pomoći pridružene dijagnostičkoj poruci za pokretanje ispravljanja grešaka u problemu.

Srodne informacije za EIM

Možda ćete htjeti naučiti o drugim tehnologijama vezanim uz EIM. Sljedeća poglavlja Informacijskog Centra pomažu vam u razumijevanju ovih srodnih tehnologija:

- **Usluga provjere autentičnosti mreže**
  Ovo poglavlje osigurava informacije o konfiguriranju usluge provjere autentičnosti mreže na iSeries. Usluga mrežne provjere autentičnosti dozvoljava iSeries da sudjeluje u postojećoj Kerberos mreži. Kada se koristi s EIM-om, usluga mrežne provjere autentičnosti osigurava jednostruku prijavu za mrežu.
- **Usluge direktorija (LDAP)**
  Ovo poglavlje osigurava konfiguraciju i konceptualne informacije za Usluge Direktorija (LDAP). EIM koristi LDAP poslužitelj za spremanje EIM podataka i mapiranje udruženja.

Tiskano u Hrvatskoj