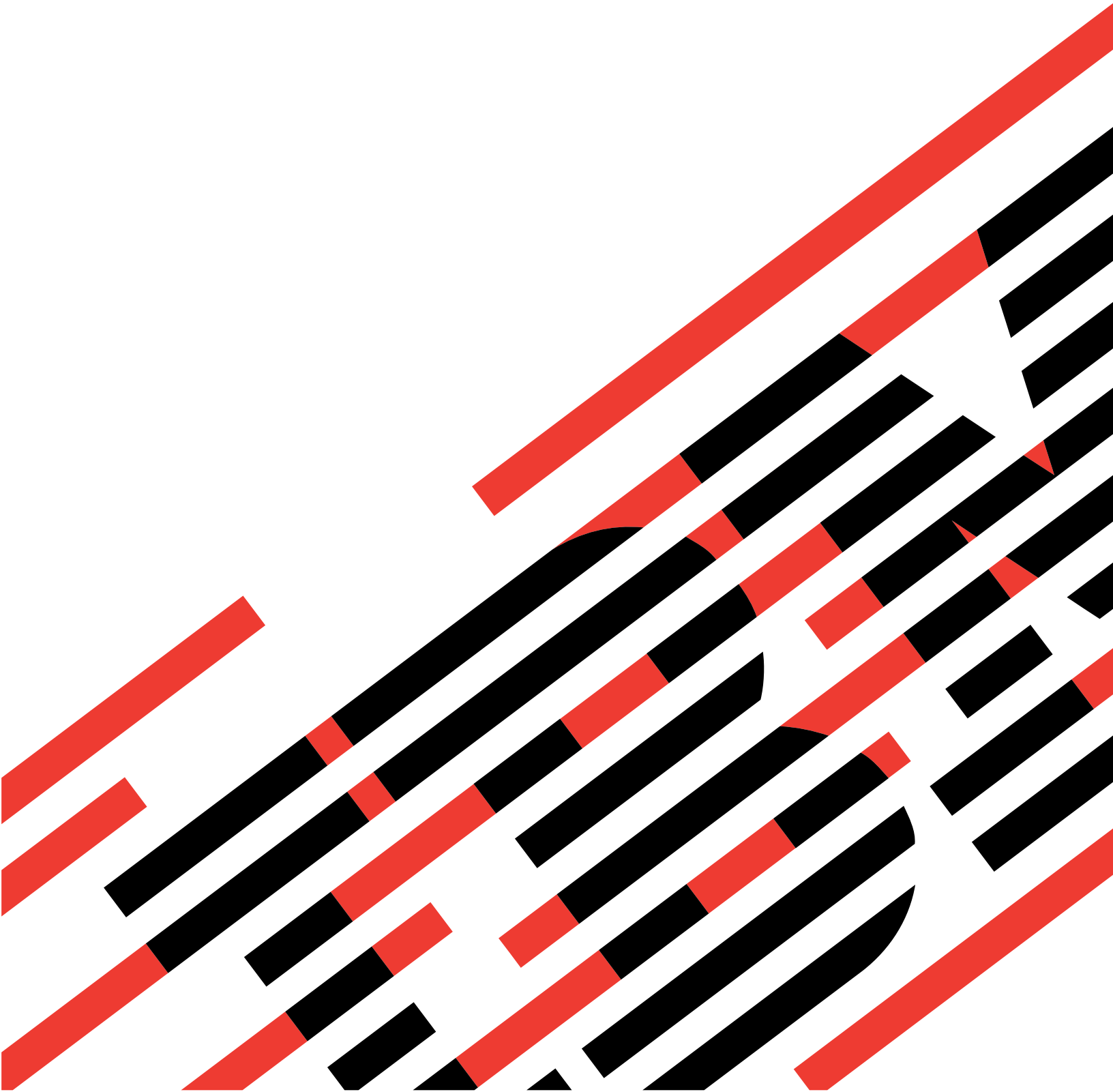
IBM

eserver

iSeries

Mapiranje identiteta u poduzeću (EIM)

Verzija 5 Izdanje 3



IBM

@server

iSeries

Mapiranje identiteta u poduzeću (EIM)

Verzija 5 Izdanje 3

Napomena

Prije korištenja ovih informacija i proizvoda koji podržavaju, pročitajte informacije u “Napomene”, na stranici 113.

Četvrto izdanje (kolovoz, 2005)

Ovo izdanje se primjenjuje na verziju 5, izdanje 3, modifikacija 0 od IBM Operating System/400 (broj proizvoda 5722–SS1) i na sva naredna izdanja i modifikacije, sve dok se drukčije ne naznači u novim izdanjima. Ova verzija ne radi na svim modelima računala smanjenog seta instrukcija (RISC), niti ne radi na CISC modelima.

Sadržaj

Mapiranje identiteta u poduze⌂u (EIM) . . 1

| ⌂to je novo u V5R3 2
Ispis ovog poglavlja 2
Pregled Mapiranja identiteta u poduze⌂u (EIM) 3
| Scenariji Mapiranja identiteta u poduze⌂u 5
Koncepti Mapiranja identiteta u poduze⌂u 5
Kontroler EIM domene. 7
EIM domena 7
EIM identifikator 9
Definicije EIM registra 12
EIM asocijacije 16
Operacije pregledavanja Mapiranja identiteta u poduze⌂u 25
| Mapiranje identiteta u poduze⌂u: podr⌂ka i
| omogu⌂avanja politike mapiranja 32
EIM kontrola pristupa. 33
LDAP koncepti za EIM 39
| iSeries koncepti za Mapiranje identiteta u poduze⌂u. . 41
Planiranje Mapiranja identiteta u poduze⌂u 43
| Planiranje Mapiranja identiteta u poduze⌂u za eServer 44
| Planiranje Mapiranje identiteta u poduze⌂u za OS/400 58
Konfiguriranje Mapiranja identiteta u poduze⌂u 61
Kreiranje i spajanje nove lokalne domene 62
| Kreiranje i spajanje nove udaljene domene 66
Pristup postoje⌂oj domeni 72
Konfiguriranje sigurne veze s EIM kontrolerom domene 76
Upravljanje Mapiranjem identiteta u poduze⌂u 77
Upravljanje domenama Mapiranja identiteta u poduze⌂u 77
Upravljanje definicijama registra Mapiranja identiteta u poduze⌂u 82
Upravljanje identifikatorima Mapiranja identiteta u poduze⌂u 87
Upravljanje asocijacijama 90
Upravljanje EIM kontrolom korisni⌂kog pristupa . . 104
Upravljanje svojstvima EIM konfiguracije 104
API-ji Mapiranja identiteta u poduze⌂u 105
Rje⌂avanje problema Mapiranja identiteta u poduze⌂u 106
Rje⌂avanje problema s povezivanjem kontrolera domene 106
Rje⌂avanje op⌂enitih EIM konfiguracijskih problema i problema domene 107
Rje⌂avanje problema Mapiranja identiteta u poduze⌂u: problemi mapiranja. 109
Sli⌂ne informacije za Mapiranje identiteta u poduze⌂u 111
Termini i uvjeti za spu⌂tanje i ispis informacija. . . . 111

Dodatak. Napomene 113

Zaštitni znaci 115
Termini i uvjeti za spu⌂tanje i ispis informacija. . . . 115

Mapiranje identiteta u poduze⌂u (EIM)

Mapiranje identiteta u poduze⌂u (EIM) za iSeries je OS/400 implementacija IBM @server infrastrukture koja administratorima i razvija⌂ima aplikacija dozvoljava rje⌂avanje problema upravljanja vi⌂estrukim korisni⌂kim registrima kroz ⌂itavo poduze⌂e. Mnoga mre⌂na poduze⌂a suo⌂avaju se s problemom vi⌂estrukih korisni⌂kih registara, ⌂to zahtijeva da svaka osoba ili cjelina unutar poduze⌂a ima korisni⌂ki identitet u svakom registru. Potreba za vi⌂estrukim korisni⌂kim registrima brzo raste u veliki administrativni problem koji utje⌂e na korisnike, administratore i razvija⌂e aplikacija. Mapiranje identiteta u poduze⌂u (EIM) omogu⌂uje jeftino rje⌂enje za lak⌂e upravljanje vi⌂estrukim korisni⌂kim registrima i korisni⌂kim identitetima u va⌂em poduze⌂u.

EIM vam omogu⌂uje kreiranje sistema mapiranja identiteta, koji se zovu asocijacije, izme⌂u razli⌂itih korisni⌂kih identiteta u razli⌂itim korisni⌂kim registrima za osobu u va⌂em poduze⌂u. EIM tako⌂er omogu⌂uje zajedni⌂ki skup API-ja koji se mogu koristiti na svim platformama za razvoj aplikacija koje mogu koristiti mapiranje identiteta koje kreirate za gledanje odnosa me⌂u korisni⌂kim identitetima. U dodatku, mo⌂ete koristiti EIM konjunkciju s uslugom mre⌂ne provjere autenti⌂nosti OS/400 implementacije Kerberosa, za pru⌂anje okoline jednostruke prijave.

Mo⌂ete konfigurirati i upravljati EIM-om kroz iSeries Navigator, iSeries grafi⌂ko korisni⌂ko su⌂elje. iSeries poslu⌂itelj koristi EIM za omogu⌂avanje OS/400 su⌂elja za provjeru autenti⌂nosti korisnika upotrebom mre⌂ne usluge provjere autenti⌂nosti. Aplikacije kao i OS/400, mogu prihvatiti Kerberos ulaznice i koristiti EIM za pronalazak korisni⌂kog profila koji predstavlja istu osobu koju predstavlja Kerberos ulaznica.

Da nau⌂ite vi⌂e o tome kako EIM radi, o EIM konceptima i kako mo⌂ete koristiti EIM u poduze⌂u pogledajte sljede⌂e:

Ispis ovog poglavlja
Ispi⌂ite PDF ovog poglavlja i bilo koje ostalo sli⌂no poglavlje.

⌂to je novo u V5R3
Nau⌂ite o novim funkcijama za EIM ovog izdanja.

Pregled mapiranja identiteta u poduze⌂u
Nau⌂ite o problemima koje vam EIM poma⌂e rije⌂iti, trenutne industrijske pristupe ovim problemima i za⌂to je EIM pristup bolje rje⌂enje.

EIM koncepti
Nau⌂ite o va⌂nim EIM konceptima koji su vam potrebni za razumijevanje da uspje⌂no implementirate EIM.

Planiranje EIM-a
Nau⌂ite kako razviti plan implementacije EIM-a da osigurate da ste uspje⌂no konfigurirali EIM za iSeries ili za okru⌂enja mje⌂ovitih platformi.

Konfiguriranje EIM-a
Nau⌂ite kako koristiti ⌂arobnjaka za konfiguriranje mapiranja identiteta poduze⌂a za konfiguriranje EIM-a za va⌂e iSeries poslu⌂itelje.

Upravljanje EIM-om
Nau⌂ite kako upravljati EIM domenom i podacima domene, uklju⌂uju⌂i upravljanje EIM domenama, identifikatorima, asocijacijama, definicijama registra, EIM kontrolama pristupa i vi⌂e.

EIM API-ji
Nau⌂ite o EIM API-jima i kako ih mo⌂ete koristiti u va⌂im aplikacijama i mre⌂i.

Uklanjanje pogre⌂aka EIM-a
Nau⌂ite o ⌂estim problemima i pogre⌂kama na koje mo⌂ete nai⌂i kada konfigurirate i koristite EIM kao i mogu⌂a rje⌂enja za te probleme i pogre⌂ke.

Srodne informacije za EIM
Nau⌂ite o drugim resursima i informacijama koje se odnose na kori⌂tenje EIM-a.

⌂to je novo u V5R3

V5R3 Mapiranje identiteta u poduze⌂u (EIM) za iSeries pobolj⌂anja i sli⌂na OS/400 pobolj⌂anja uklju⌂uju:

Nova ili pobolj⌂ana funkcija za EIM

- ⌂**arobnjak funkcija Sinkronizacije**. Mo⌂ete koristiti ⌂arobnjaka **Funkcija Sinkronizacije** u iSeries Navigatoru za ⌂irenje usluge mre⌂ne provjere autenti⌂nosti i EIM konfiguracija na grupu V5R3 sistema. ⌂arobnjak udvostru⌂uje konfiguracije na sistemu modela i kopira ih na ostale sisteme u grupi. Vrijeme ⌂tedite jednim konfiguriranjem i ⌂irenjem te konfiguracije na vi⌂estruke sisteme umjesto konfiguriranja svakog sistema zasebno. Za tehni⌂ke i konfiguracijske detalje pogledajte scenarij: ⌂irenje usluge mre⌂ne provjere autenti⌂nosti i EIM-a preko vi⌂estrukih sistemskih scenarija.
- **Podr⌂ka politike mapiranja**. EIM podr⌂ka politike mapiranja omogu⌂uje vam kori⌂tenje asocijacija politike kao i specifi⌂nih asocijacija identifikatora u EIM domeni. Mo⌂ete kreirati i koristiti asocijacije politike za definiranje izravnih odnosa izme⌂u korisni⌂kih identiteta iz razli⌂itih korisni⌂kih registara. Asocijacija politike je sredstvo za kreiranje mapiranja s vi⌂e na jedan izme⌂u izvornog skupa vi⌂estrukih korisni⌂kih identiteta u jednom korisni⌂kom registru i jednostrukog ciljnog korisni⌂kog identiteta u odre⌂enom ciljnom korisni⌂kom registru. Asocijacije politika mo⌂ete koristiti umjesto ili u kombinaciji s asocijacijama identifikatora.
- **Pobolj⌂anje naredbi korisni⌂kog profila**. Dodatni parametar, zvan EIMASSOC, dodan je naredbi Kreiranje korisni⌂kog profila (CRTUSRPRF) i naredbi Promjena korisni⌂kog profila (CHGUSRPRF). Parametar EIMASSOC vam omogu⌂ava definiranje EIM asocijacija identifikatora za navedeni korisni⌂ki profil lokalnog registra. Za kori⌂tenje ovog parametra trebate navesti EIM identifikator, opciju akcije za asocijaciju, upisati asocijaciju identifikatora i da li kreirati navedeni EIM identifikator ako ve⌂ ne postoji. Za vi⌂e informacija o tom novom parametru pogledajte “Razmatranja OS/400 korisni⌂kog profila za Mapiranje identiteta u poduze⌂u” na stranici 42.

Pobolj⌂anja EIM informacija

Za ovo izdanje postoji jako pro⌂irena sekcija planiranja koja pokriva sva planiranja koja su potrebna za implementaciju EIM-a za bilo koju @server platformu kao i specifi⌂ne informacije planiranja za implementaciju EIM-a za OS/400.

Dodatno, poglavlje Jednostruka prijava dodano je Informacijskom Centru za omogu⌂avanje iscrpne dokumentacije o implementaciji EIM-a kao dijela okoline jednostruke prijave za smanjenje upravljanja lozinkom. Ovo poglavlje daje mno⌂tvo detaljnih scenarija uobi⌂ajenih situacija jednostruke prijave s detaljnim uputama za konfiguraciju za njihovu implementaciju.

Kako vidjeti ⌂to je novo ili promijenjeno

Da bi vam pomogle vidjeti gdje su u⌂injene tehni⌂ke promjene, ove informacije koriste:

- Sliku » za ozna⌂avanje gdje zapo⌂inju nove ili promijenjene informacije.
- Sliku « za ozna⌂avanje gdje nove ili promijenjene informacije zavr⌂avaju.

Za prona⌂ene ostale informacije o tome ⌂to je novo ili promijenjeno u ovom izdanju, pogledajte Memorandum korisnicima.

Ispis ovog poglavlja

Za pregled ili spu⌂tanje PDF verzije, izaberite Mapiranje identiteta u poduze⌂u (oko 1389 Kb).

Ostale informacije

Mo⌂ete pregledati ili spustiti srodna poglavlja:

- Usluge mre⌂ne provjere autenti⌂nosti (oko 1398 Kb) sadr⌂e informacije o tome kako s EIM-om konfigurirati uslugu mre⌂ne provjere autenti⌂nosti za kreiranje okoline jednostruke prijave.

- Posluˆitelj direktorija (LDAP) (oko 1700 KB) sadrˆi informacije o tome kako konfigurirati LDAP posluˆitelj, kojeg zajedno s informacijama o LDAP konfiguraciji moˆete koristiti kao EIM kontroler domene.

Spremanje PDF datoteka

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

1. Otvorite PDF u vaˆem pretraˆitelju (kliknite na vezu iznad).
2. U izborniku vaˆeg pretraˆitelja, kliknite **Datoteka**.
3. Kliknite **Spremi kao...**
4. Otiˆite u direktorij u koji ˆelite spremiti PDF.
5. Kliknite **Spremi**.

Spuˆtanje Adobe Acrobat Readera

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

Pregled Mapiranja identiteta u poduzeˆu (EIM)

Danaˆnje mreˆno okruˆenje napravljeno je od kompleksne grupe sistema i aplikacija, rezultirajuˆi iz potrebe za upravljanjem s viˆe korisniˆkih registara. Bavljenje s viˆestrukim korisniˆkim registrima brzo raste u veliki administrativni problem koji utjeˆe na korisnike, administratore i razvijaˆe aplikacija. Prema tome, mnoge tvrtke se bore za sigurno upravljanje provjerom autentiˆnosti i autorizacije za sisteme i aplikacije. Mapiranje identiteta u poduzeˆu (EIM) je tehnologija infrastrukture IBM @server koja omoguˆuje administratorima i razvijaˆima aplikacija da se posvete ovom problemu na jednostavniji i jeftiniji naˆin nego ˆto je to bilo prethodno moguˆe.

Sljedeˆe informacije opisuju probleme, izdvajaju trenutne industrijske pristupe i objaˆnjavaju zaˆto je EIM pristup bolji.

Problem upravljanja viˆestrukim korisniˆkim registrima

Mnogi administratori upravljaju mreˆama koje ukljuˆuju razliˆite sisteme i posluˆitelje, svaki s jedinstvenim naˆinom upravljanja korisnicima kroz razliˆite korisniˆke registre. U ovim kompleksnim mreˆama, administratori su odgovorni za upravljanje svakim korisniˆkim identitetom i lozinkom kroz viˆestruke sisteme. Dodatno, administratori ˆesto moraju sinkronizirati ove identitete i lozinke, a korisnici su optereˆeni s pamˆenjem viˆestrukih identiteta i lozinki i njihovim usklaˆivanjem. Optereˆenost korisnika i administratora u ovom okruˆenju je pretjerana. Prema tome, administratori ˆesto utroˆe vrijedno vrijeme rjeˆavajuˆi problem neuspjelih pokuˆaja prijave i ponovnom postavljanju zaboravljenih lozinki umjesto upravljajuˆi poduzeˆem.

Problem upravljanja viˆestrukim korisniˆkim registrima takoˆer utjeˆe na razvijaˆe aplikacije koji ˆele osigurati viˆestruko povezane ili heterogene aplikacije. Ovi razvijaˆi razumiju da korisnici imaju vaˆne poslovne podatke rasprˆene kroz mnoge razliˆite tipove sistema, gdje svaki sistem posjeduje svoje vlastite korisniˆke registre. Nadalje, razvijaˆi moraju kreirati vlasniˆke korisniˆke registre i udruˆene sigurnosne semantike za njihove aplikacije. Iako ovo rjeˆava problem za razvijaˆa aplikacije, takoˆer i poveˆava optereˆenje za korisnike i administratore.

Trenutni pristupi

Dostupno je nekoliko trenutnih industrijskih pristupa rjeˆavanju problema upravljanja viˆestrukim korisniˆkim registrima, ali svi oni dobavljaju nepotpuna rjeˆenja. Na primjer, Lightweight Directory Access Protocol (LDAP) osigurava rjeˆenje distribuiranog korisniˆkog registra. Meˆutim koriˆtenje LDAP-a (ili ostalih popularnih rjeˆenja kao ˆto su Microsoft Passport) znaˆi da administratori moraju upravljati joˆ jednim korisniˆkim registrom i semantikom sigurnosti ili moraju zamijeniti postojeˆe aplikacije koje su izgraˆene za koriˆtenje tih registara.

Kori⌂tenjem ovog tipa rje⌂enja, administratori moraju upravljati vi⌂estrukim sigurnosnim mehanizmima za individualne resurse, ⌂ime se pove⌂ava administrativno optere⌂enje i potencijalno se pove⌂ava mogu⌂nost sigurnosnog izlaganja. Kada vi⌂estruki mehanizmi podr⌂avaju jedan resurs, ⌂anse mijenjanja ovla⌂tenja kroz jedan mehanizam i zaboravljanja promjene ovla⌂tenja za jedan ili vi⌂e drugih mehanizama, mnogo su ve⌂e. Na primjer, sigurnosno izlaganje mo⌂e rezultirati kada je korisniku prikladno odbijen pristup kroz jedno su⌂elje, ali dozvoljen je pristup kroz jedan ili vi⌂e drugih su⌂elja.

Nakon dovr⌂enja ovog posla, administratori pronalaze da nisu u potpunosti rije⌂ili problem. Op⌂enito, poduze⌂a su investirala previ⌂e novca u trenutne korisni⌂ke registre i u njihove udru⌂ene sigurnosne semantike kako bi kori⌂tenje ovog tipa rje⌂enja bilo prakti⌂no. Kreiranje drugog korisni⌂kog registra i udru⌂ene sigurnosne semantike rje⌂ava problem za dobavlja⌂a aplikacije, ali ne i probleme za korisnike i administratore.

Jedno drugo mogu⌂e rje⌂enje je kori⌂tenje pristupa jednostruke prijave. Dostupno je nekoliko proizvoda koji dozvoljavaju administratorima da upravljaju datotekama koje sadr⌂e sve korisni⌂ke identitete i lozinke. Me⌂utim, ovaj pristup ima nekoliko slabosti:

- Adresira samo jedan od problema s kojim se korisnici suo⌂avaju. Iako dozvoljava prijavu korisnika na vi⌂estruke sisteme dobavljaju⌂i 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 ⌂isti tekst ili lozinke s mogu⌂no⌂⌂u de⌂ifriranja spremljeni u ovim datotekama. Lozinke nikad ne bi trebale biti spremljene u datotekama ⌂istog teksta ili biti lako dostupne bilo kome, uklju⌂uju⌂i i administratorima.
- To ne rje⌂ava probleme razvija⌂a aplikacije tre⌂e strane, koji dobavljaju heterogene, vi⌂estruko povezane aplikacije. Oni jo⌂ uvijek moraju dobaviti vlasni⌂ke korisni⌂ke registre za njihove aplikacije.

Usprkos slabostima, neka poduze⌂a izabrala su prihva⌂anje ovakvih pristupa, jer osiguravaju neko olak⌂anje za probleme vi⌂estrukog korisni⌂kog registra.

EIM pristup

EIM nudi novi pristup za jeftina rje⌂enja izgradnje za jednostavnije upravljanje vi⌂estrukim korisni⌂kim registrima i korisni⌂kim identitetima u heterogenoj okolini aplikacija s vi⌂estrukim razinama. EIM je arhitektura za opisivanje odnosa izme⌂u individualaca ili cjelina (poput poslu⌂itelja datoteka i poslu⌂itelja ispisa) u poduze⌂u i mnogih identiteta koji ih u tom poduze⌂u predstavljaju. U dodatku, EIM osigurava skup API-ja koji dozvoljavaju aplikacijama da postavljaju pitanja o ovim odnosima.

Na primjer, danim korisni⌂kim identitetom u jednom korisni⌂kom registru, mo⌂ete odrediti koji korisni⌂ki identitet u drugom korisni⌂kom registru predstavlja istu osobu. Ako je korisniku provjerena autenti⌂nost s jednim korisni⌂kim identitetom i mo⌂ete mapirati taj korisni⌂ki identitet u prikladni identitet drugog korisni⌂kog registra, tada korisnik ne treba osiguravati vjerodostojnost kod ponovne provjere autenti⌂nosti. Znate tko je korisnik i samo trebate znati koji korisni⌂ki identitet predstavlja tog korisnika u drugom korisni⌂kom registru. Zbog toga, EIM osigurava generaliziranu funkciju mapiranja identiteta za poduze⌂e.

EIM dozvoljava jedan-prema-vi⌂e mapiranja (drugim rije⌂ima, jedan korisnik s vi⌂e od jednog korisni⌂kog identiteta u jednom korisni⌂kom registru). Me⌂utim, administrator ne mora imati specifi⌂na pojedina⌂na mapiranja za sve korisni⌂ke identitete u korisni⌂kom registru. EIM tako⌂er omogu⌂uje mapiranja vi⌂e-na-jedan (drugim rije⌂ima, vi⌂estruki korisnici mapirani u jednostruki korisni⌂ki identitet u jednostrukom korisni⌂kom registru).

Mogu⌂nost mapiranja izme⌂u korisni⌂kih identiteta u razli⌂itim korisni⌂kim registrima osigurava mnoge koristi. Primarno, to zna⌂i da aplikacije mogu imati fleksibilnost kori⌂tenja jednog korisni⌂kog registra za provjeru autenti⌂nosti dok koriste potpuno druga⌂iji korisni⌂ki registar za autorizaciju. Na primjer, administrator je mogao mapirati identitet Windows korisnika u Kerberos registru na neki OS/400 korisni⌂ki profil u druk⌂ijem korisni⌂kom registru radi pristupa do OS/400 resursa za koje je OS/400 korisni⌂ki profil ovla⌂ten.

EIM je otvorena arhitektura koju administratori mogu koristiti za predstavljanje odnosa mapiranja identiteta za bilo koji registar. Ne zahtijeva kopiranje postoje⌂ih podataka u novo spremi⌂te i poku⌂ava odr⌂ati obje kopije sinkroniziranim.

Jedini novi podaci koje EIM predstavlja su informacije odnosa. EIM te podatke pohranjuje u LDAP direktorij, koji na jednom mjestu omogu⌂uje fleksibilnost pri upravljanju podacima i sadr⌂i kopije kada se program koristi. Kona⌂no, EIM daje poduze⌂ima i razvija⌂ima aplikacija fleksibilnost za lagani rad u ⌂irokom rasponu okru⌂enja s manje tro⌂ka nego ⌂to je to mogu⌂e bez ove podr⌂ke.

EIM, kori⌂ten zajedno s uslugama mre⌂ne provjere autenti⌂nosti i OS/400 implementacija Kerberosa osiguravaju rje⌂enje jednostruke prijave. Aplikacije mogu biti napisane tako da koriste GSS API-je i EIM za prihva⌂anje Kerberos karata i da se mapiraju na drugi, pridru⌂eni korisni⌂ki identitet u nekom drugom korisni⌂kom registru. Asocijacija izme⌂u korisni⌂kih identiteta koji omogu⌂uju mapiranje ovog identiteta mo⌂e se posti⌂i kreiranjem asocijacija identifikatora koji indirektno pridru⌂uju jedan korisni⌂ki identitet drugom kroz EIM identifikator ili kreiranjem asocijacija politika koje direktno pridru⌂uju jedan korisni⌂ki identitet grupe s jednostrukim specifi⌂nim korisni⌂kim identitetom.

Upotreba mapiranja identiteta zahtijeva da administratori u⌂ine sljede⌂e:

1. Konfigurirajte EIM domenu u mre⌂i. Mo⌂ete koristiti ⌂arobnjaka iSeries EIM Konfiguracije za kreiranje kontrolera domene za domenu i konfigurirate pristup na domenu. Kada koristite ⌂arobnjaka mo⌂ete izabrati kreirati novu EIM domenu i kreirati kontroler domene na lokalnom sistemu ili udaljenom sistemu. Ili, ako EIM domena ve⌂ postoji, mo⌂ete izabrati sudjelovati u postoje⌂oj EIM domeni.
2. Odredite kojim je korisnicima koji su definirani za poslu⌂itelj direktorija na kojem je smje⌂ten EIM kontroler domene dozvoljeno upravljanje ili pristup specifi⌂nim informacijama u EIM domeni i pridru⌂ite ih odgovaraju⌂im grupama EIM kontrole pristupa.
3. Kreirajte EIM definicije registra za one korisnike registra koji ⌂e sudjelovati u domeni. Iako mo⌂ete definirati sve korisni⌂ke registre za EIM domenu, morate definirati korisni⌂ke registre za one aplikacije i operativne sisteme koji su EIM-omogu⌂eni.
4. Ovisno o potrebama EIM implementacije, odredite koje od sljede⌂ih zadataka treba izvesti za zavr⌂avanje EIM konfiguracije:
   - Kreirajte EIM identifikator za svakog jedinstvenog korisnika u domeni i kreirajte asocijacije identifikatora za njih.
   - Kreirajte asocijacije politika.
   - Kreirajte kombinaciju istih.

Da nau⌂ite vi⌂e o konfiguriranju i kori⌂tenju EIM-a za kreiranje okoline jednostruke prijave za maksimiziranje koristi smanjenog upravljanja lozinkom pogledajte Jednostruka prijava u iSeries Informacijskom Centru.

Scenariji Mapiranja identiteta u poduze⌂u

Mapiranje identiteta u poduze⌂u (EIM) je tehnologija IBM infrastrukture koja vam omogu⌂uje pra⌂enje i upravljanje korisni⌂kim identitetima u cijelom poduze⌂u. Tipi⌂no koristite EIM s nekom tehnologijom provjere autenti⌂nosti, poput usluge mre⌂ne provjere autenti⌂nosti za implementaciju okoline jednostruke prijave.

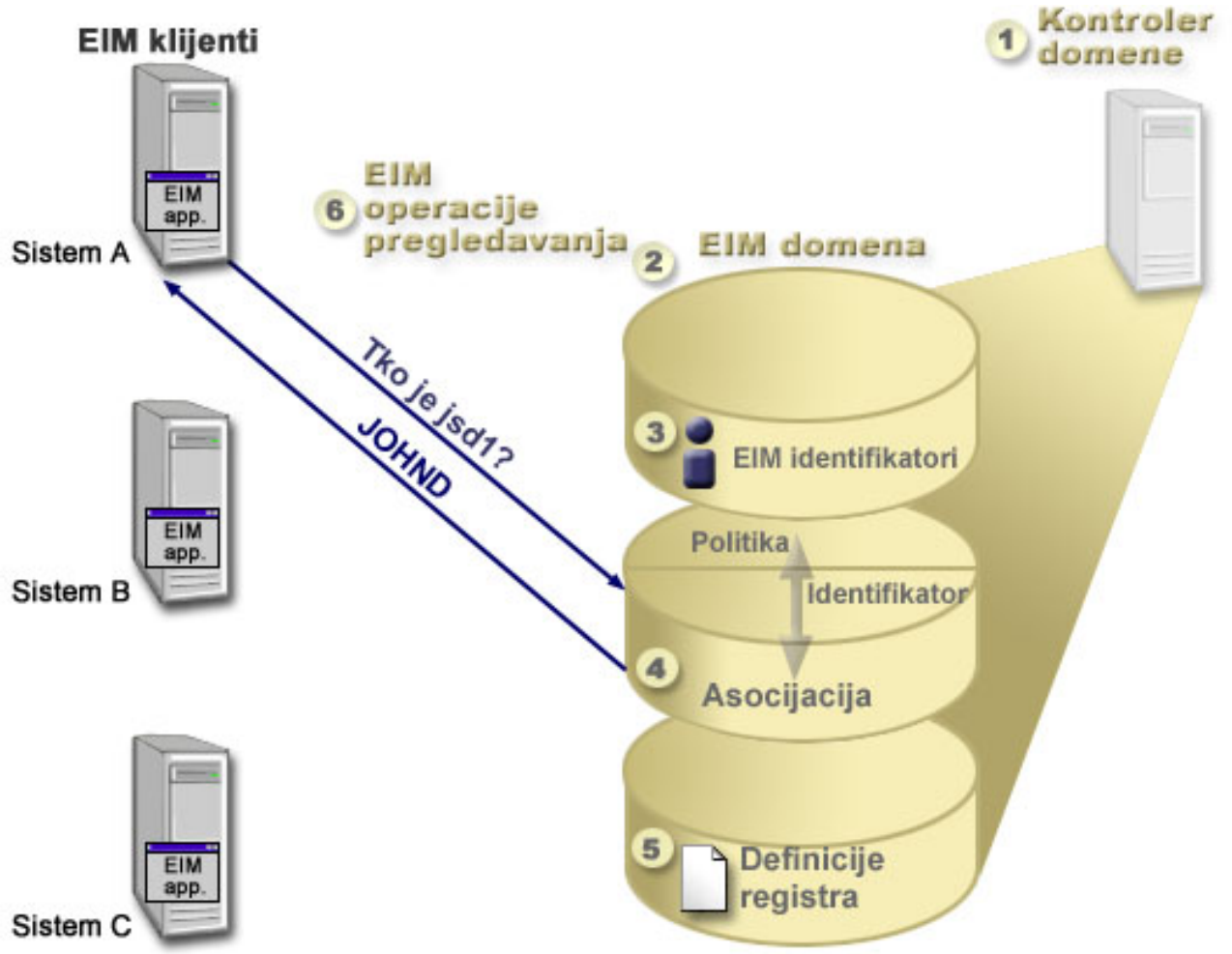
Prema tome, ako ste zainteresirani za ovu ⌂iru upotrebu EIM-a, morate pogledati Scenarije u poglavlju Informacijski Centar za Jednostruku Prijavu.

Koncepti Mapiranja identiteta u poduze⌂u

Konceptualno razumijevanje o tome kako radi Mapiranje identiteta u poduze⌂u (EIM) potrebno je za potpuno razumijevanje kako mo⌂ete koristiti EIM u va⌂em poduze⌂u. Iako se konfiguracija i implementacija EIM API-ja mo⌂e razlikovati me⌂u platformama poslu⌂itelja, EIM koncepti su jednaki na svim IBM @server platformama.

Slika 1 osigurava primjer EIM implementacije u poduze⌂u. Tri poslu⌂itelja pona⌂aju se kao EIM-omogu⌂ene aplikacije koje zahtijevaju EIM podatke kori⌂tenjem operacija EIM pregledavanja 6 . Kontroler domene 1 sprema

informacije o EIM domeni 2 , ∆to uklju∆uje EIM identifikator 3 , asocijacije 4 izme∆u ovih EIM identifikatora i korisni∆kih identiteta i definicije EIM registra 5 .



Slika 1. Primjer EIM implementacije

Pogledajte sljede∆e informacije da nau∆ite vi∆e o ovim EIM @server konceptima:

- “Kontroler EIM domene” na stranici 7
- “EIM domena” na stranici 7
- “EIM identifikator” na stranici 9
- “Definicije EIM registra” na stranici 12
- “EIM asocijacije” na stranici 16
- “Operacije pregledavanja Mapiranja identiteta u poduze∆u” na stranici 25
- “Mapiranje identiteta u poduze∆u: podr∆ka i omogu∆avanja politike mapiranja” na stranici 32
- “EIM kontrola pristupa” na stranici 33

Pogledajte sljede∆e informacije da nau∆ite vi∆e o ostalim sli∆nim konceptima koji su va∆ni za razumijevanje upotrebe EIM-a:

- “LDAP koncepti za EIM” na stranici 39
- “iSeries koncepti za Mapiranje identiteta u poduze∆u” na stranici 41

Kontroler EIM domene

Kontroler EIM domene je jednostavno Lightweight Directory Access Protocol (LDAP) poslu⌂itelj koji je konfiguriran tako da upravlja s jednom ili vi⌂e EIM domenama. *EIM domena* je LDAP direktorij koji se sastoji od svih EIM identifikatora, EIM asocijacija i korisni⌂kih registara koji su definirani u toj domeni. Sistemi (EIM klijenti) sudjeluju u EIM domeni kori⌂tenjem podataka domene za operacije EIM pregledavanja.

Trenutno mo⌂ete konfigurirati IBM Poslu⌂itelj direktorija na nekim IBM @server platformama tako da djeluje kao kontroler EIM domene. Svaki sistem koji podr⌂ava EIM API-je mo⌂e sudjelovati kao klijent u domeni. Ovi klijent sistemi koriste EIM API-je za kontaktiranje kontrolora EIM domene za izvo⌂enje “Operacije pregledavanja Mapiranja identiteta u poduze⌂u” na stranici 25. Lokacija EIM klijenta odre⌂uje 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.

Opaska: Ako planirate konfigurirati poslu⌂itelj direktorija na udaljenom sistemu, poslu⌂itelj direktorija mora omogu⌂iti EIM podr⌂ku. EIM zahtijeva da je kontroler domene smje⌂ten na poslu⌂itelju direktorija koji podr⌂ava verziju 3 Lightweight Directory Access Protocola (LDAP). Dodatno, proizvod poslu⌂itelja direktorija mora biti konfiguriran tako da prihva⌂a EIM shemu. IBM Poslu⌂itelj direktorija za iSeries i IBM Poslu⌂itelj direktorija V5.1 omogu⌂ava tu podr⌂ku.

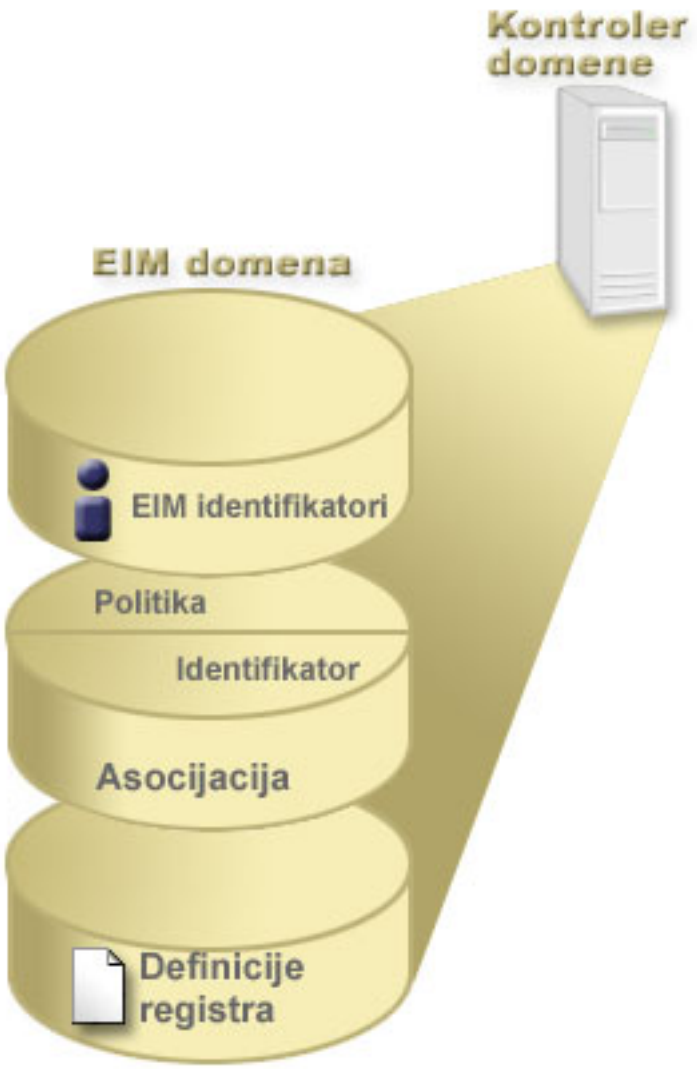
EIM domena

EIM domena je direktorij unutar poslu⌂itelja Lightweight Directory Access Protokola (LDAP) koji sadr⌂i EIM podatke za poduze⌂e. EIM domena je zbirka svih EIM identifikatora, EIM asocijacija i korisni⌂kih registara koji su u toj domeni definirani kao i kontrole pristupa nad podacima. Sistemi (EIM klijenti) sudjeluju u domeni kori⌂tenjem domenskih podataka za EIM operacije pregledavanja.

EIM domena se razlikuje od korisni⌂kog registra. Korisni⌂ki registar definira skup korisni⌂kih identiteta poznatih i provjerenih od pojedina⌂ne instance operativnog sistema ili aplikacije. Korisni⌂ki registar tako⌂er sadr⌂i informacije potrebne za provjeru autenti⌂nosti korisnika identiteta. Dodatno, korisni⌂ki registar ⌂esto sadr⌂i druge atribute kao ⌂to su korisni⌂ke preference, sistemske privilegije ili osobne informacije za taj identitet.

Nasuprot tomu, EIM domena *odnosi* se na korisni⌂ke identitete, definirane u korisni⌂kim registrima. EIM domena sadr⌂i informacije o *odnosima* izme⌂u identiteta u razli⌂itim korisni⌂kim registrima (korisni⌂ko ime, tip registra i instanca registra) i stvarne ljude ili cjeline koje ovi identiteti predstavljaju.

Slika 2 prikazuje podatke spremljene unutar EIM domene. Ovi podaci uklju⌂uju EIM identifikatore, definicije EIM registra i EIM asocijacije. EIM podaci definiraju odnos izme⌂u korisni⌂kih identiteta i ljudi ili cjelina koje ovi identiteti predstavljaju u poduze⌂u.



Slika 2. EIM domena i podaci koji su spremljeni unutar domene

EIM podaci uklju⌂uju:

- **Definicije EIM registra.** Svaka definicija EIM registra koju kreirate predstavlja stvarni korisni⌂ki registar (i informacije korisni⌂kog identiteta koje sadr⌂i) koji postoji na sistemu unutar poduze⌂a. Jednom kada ste definirali specifi⌂ni korisni⌂ki registar u EIM-u, taj korisni⌂ki registar mo⌂e sudjelovati u EIM domeni. Mo⌂ete kreirati dva tipa definicija registra, jedan tip se odnosi na korisni⌂ke registre sistema, a drugi se tip odnosi na korisni⌂ke registre aplikacija. Pogledajte “Definicije EIM registra” na stranici 12 za vi⌂e informacija.
- **EIM identifikatori.** Svaki EIM identifikator koji kreirate jednozna⌂no predstavlja osobu ili cjelinu (poput posluⲟitelja pisa⌂a ili posluⲟitelja datoteka) unutar poduze⌂a. Mo⌂ete kreirati EIM identifikator kada ⌂elite imati mapiranje s jednog na jedan me⌂u korisni⌂kim identitetima koji pripadaju osobi ili cjelini kojoj odgovara EIM identifikator. Pogledajte “EIM identifikator” na stranici 9 za vi⌂e informacija.
- **EIM asocijacije.** EIM asocijacije koje kreirate predstavljaju odnos me⌂u korisni⌂kim identitetima. Asocijacije morate definirati tako da EIM klijenti mogu koristiti EIM API-je za uspje⌂no izvo⌂enje EIM operacija pregledavanja. Ove EIM operacije pregledavanja tra⌂e definirane asocijacije na EIM domeni. Za vi⌂e informacija pogledajte “Operacije pregledavanja Mapiranja identiteta u poduze⌂u” na stranici 25. Postoje dva razli⌂ita tipa asocijacija koje mo⌂ete kreirati:
  - **Asocijacije identifikatora.** Asocijacije identifikatora vam omogu⌂uju definiranje odnosa jedan na jedan me⌂u korisni⌂kim identitetima pomo⌂u EIM identifikatora koji je definiran za pojedinca. Svaka EIM asocijacija

identifikatora koju kreirate predstavlja jednostruki, specifi⌂ni odnos izme⌂u EIM identifikatora i pridru⌂enog korisni⌂kog identiteta unutar poduze⌂a. Asocijacije identifikatora omogu⌂uju informacije koje ve⌂u EIM identifikator za jedan odre⌂eni korisni⌂ki identitet u specifi⌂nom korisni⌂kom registru i za korisnika vam omogu⌂uju kreiranje mapiranja identiteta jedan na jedan. Asocijacije identiteta su posebno korisne kada pojedinci imaju korisni⌂ki identitet s posebnim ovla⌂tenjima i ostalim privilegijama koje ⌂elite posebno kontrolirati kreiranjem mapiranja jedan na jedan izme⌂u njihovih korisni⌂kih identiteta.

- **Asocijacije politika.** Asocijacije politika omogu⌂uju vam definiranje odnosa izme⌂u grupe korisni⌂kih identiteta u jednom ili vi⌂e registara i individualnog korisni⌂kog identiteta u nekom drugom korisni⌂kom registru. Svaka EIM asocijacija politike koju kreirate rezultira u mapiranju s vi⌂e na jedan izme⌂u izvorne grupe korisni⌂kog identiteta u jednom korisni⌂kom registru i jednostrukog ciljnog korisni⌂kog identiteta. Tipi⌂no, kreirate asocijacije politika za mapiranje grupe korisnika od kojih svi zahtijevaju istu razinu ovla⌂tenja nad jednostrukim korisni⌂kim identitetom s tom razinom ovla⌂tenja.

Kada kreirate EIM identifikatore, definicije registra i razne asocijacije, mo⌂ete zapo⌂eti s kori⌂tenjem EIM-a da bi lak⌂e organizirali rad s korisni⌂kim identitetima unutar va⌂eg poduze⌂a.

EIM identifikator

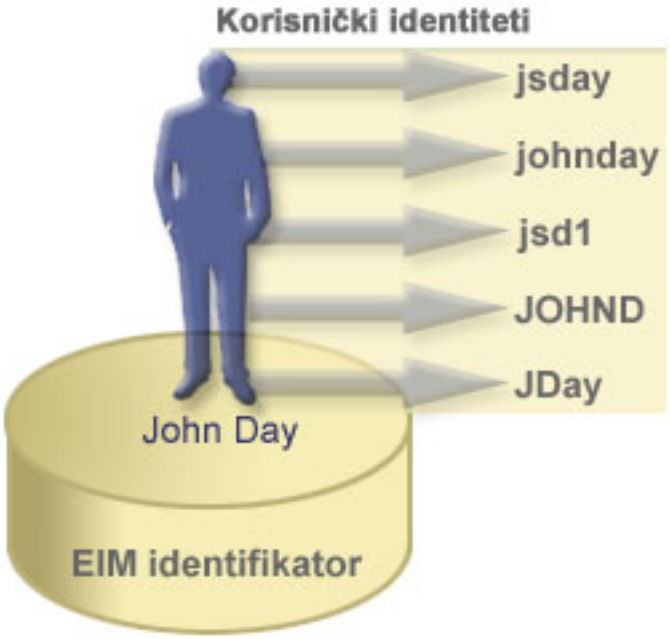
EIM identifikator predstavlja osobu ili cjelinu u poduze⌂u. Tipi⌂na mre⌂a sastoji se od razli⌂itih hardverskih platformi i aplikacija i njihovih udru⌂enih korisni⌂kih registara. Mnoge platforme i mnoge aplikacije koriste platformski specifi⌂ne ili aplikacijski specifi⌂ne korisni⌂ke registre. Ovi korisni⌂ki registri sadr⌂e sve informacije korisni⌂ke identifikacije za korisnike koji rade s ovim poslu⌂iteljima ili aplikacijama.

EIM mo⌂ete koristiti za kreiranje jedinstvenih EIM identifikatora za ljude ili cjeline u va⌂em poduze⌂u. Zatim mo⌂ete kreirati asocijacije identifikatora ili mapirati identitete s jedan na jedan izme⌂u EIM identifikatora i razli⌂itih korisni⌂kih identiteta za osobe ili cjeline koje EIM identitet predstavlja. Ovaj proces olak⌂ava izgradnju heterogenih aplikacija na vi⌂e razina. Tako⌂er postaje jednostavnija izgradnja i upotreba alata koji pojednostavljuju administraciju uklju⌂enu u upravljanje korisni⌂kim identitetom koji osoba ili cjelina ima unutar poduze⌂a.

EIM identifikator koji predstavlja osobu

Slika 3 prikazuje primjer EIM identifikatora koji predstavlja osobu *John Day* i ima razli⌂ite korisni⌂ke identitete u poduze⌂u. U ovom primjeru, osoba *John Day* ima pet korisni⌂kih identiteta u ⌂etiri razli⌂ita korisni⌂ka registra: johnday, jsd1, JOHND, jsday i JDay.

Slika 3: Odnos izme⌂u EIM identifikatora za *John Day* i njegovi razli⌂iti korisni⌂ki identiteti

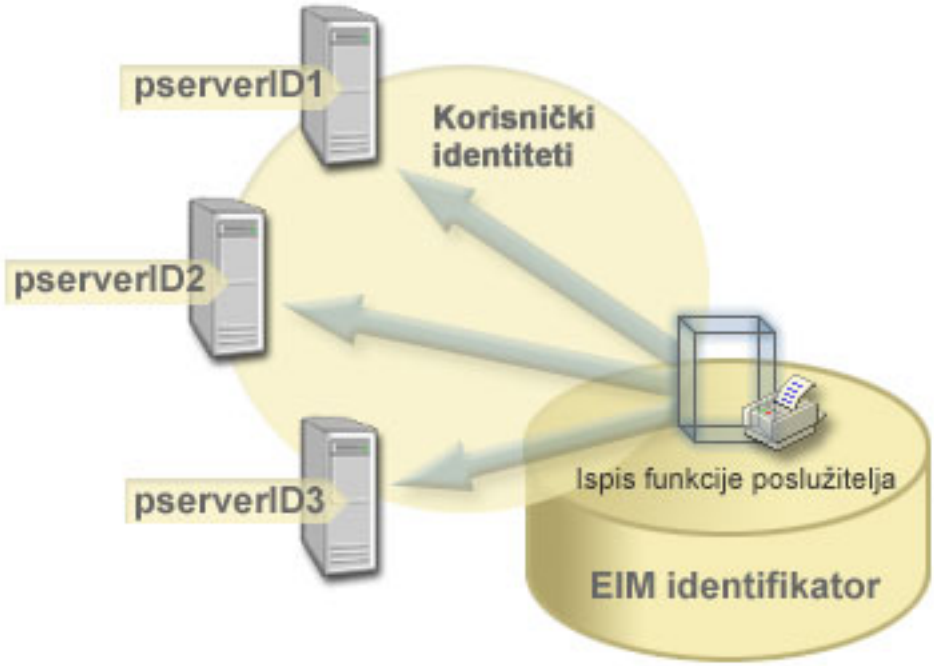


U EIM-u mo⌂ete kreirati asocijacije koje definiraju odnose izme⌂u John Day identifikatora i svakog od razli⌂itih korisni⌂kih identiteta za *John Day*. Kreiranjem ovih asocijacija za definiranje ovih odnosa, vi i drugi mo⌂ete pisati aplikacije koje koriste EIM API-je za tra⌂enje potrebnog, ali nepoznatog korisni⌂kog identiteta na osnovu poznatog korisni⌂kog identiteta.

EIM identifikator koji predstavlja cjelinu

U dodatku predstavljanja korisnika, EIM identifikatori mogu predstavljati cjeline unutar poduze⌂a kao ⌂to to prikazuje slika 4. Na primjer, ⌂esto se poslu⌂iteljska funkcija ispisa u poduze⌂u izvodi na mnogim sistemima. Na slici 4, poslu⌂iteljska funkcija ispisa u poduze⌂u, izvodi se na tri razli⌂ita sistema pod tri razli⌂ita korisni⌂ka identiteta pserverID1, pserverID2 i pserverID3.

Slika 4: Odnos izme⌂u EIM identifikatora koji predstavlja poslu⌂iteljsku funkciju ispisa i razli⌂itih korisni⌂kih identiteta za tu funkciju.



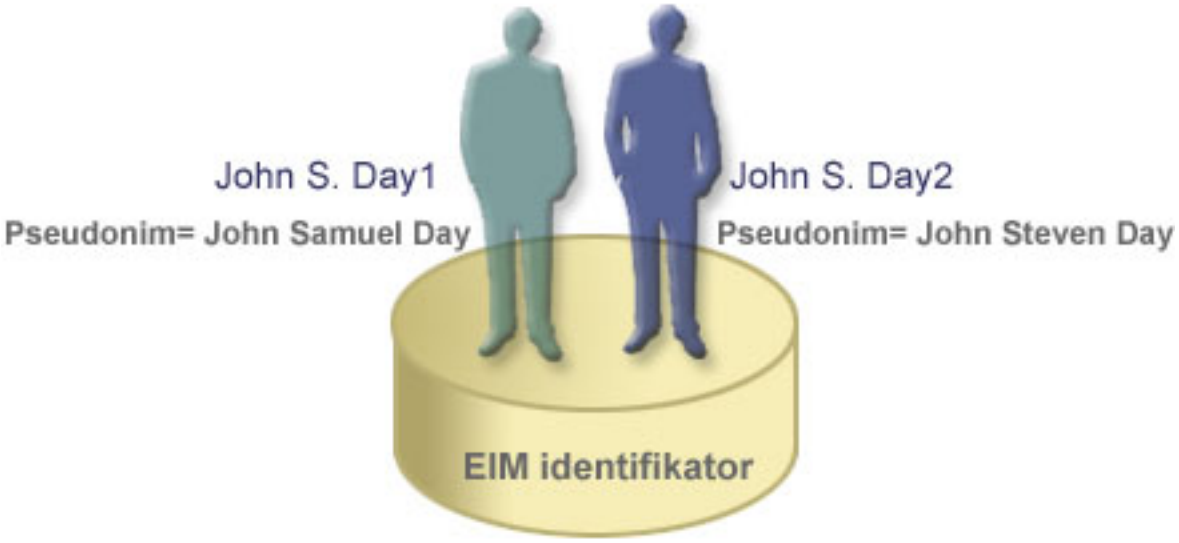
S EIM-om mo⌂ete kreirati pojedina⌂ni identifikator koji predstavlja poslu⌂iteljsku funkciju ispisa unutar poduze⌂a. Kao ⌂to primjer pokazuje, EIM identifikator Poslu⌂iteljska funkcija ispisa predstavlja stvarnu cjelinu poslu⌂iteljske funkcije ispisa u poduze⌂u. Asocijacije su kreirane za definiranje odnosa izme⌂u EIM identifikatora (Poslu⌂iteljska funkcija ispisa) i svakog od korisni⌂kih identiteta za tu funkciju (pserverID1, pserverID2 i pserverID3). Ove aplikacije dozvoljavaju razvija⌂ima aplikacije da koriste EIM operacije pregledavanja za pronala⌂enje specifi⌂ne poslu⌂iteljske funkcije ispisa. Dobavlja⌂i aplikacije mogu tada lak⌂e pisati distribuirane aplikacije koje upravljaju poslu⌂iteljskom funkcijom ispisa unutar poduze⌂a.

EIM identifikatori i zamjensko ime

Imena EIM identifikatora moraju biti jedinstvena u EIM domeni. Zamjenska imena mogu pomo⌂i u adresiranju situacija gdje kori⌂tenje jedinstvenih imena identifikatora mo⌂e biti te⌂ko. Primjer korisnosti zamjenskih imena EIM identifikatora je u situaciji kada je ne⌂ije legalno ime razli⌂ito od imena pod kojim je ta osoba poznata. Na primjer, razli⌂iti pojedinci unutar poduze⌂a mogu dijeliti isto ime, ⌂to mo⌂e biti zbunjuju⌂e ako koristite prava imena kao EIM identifikatore.

Slika 5 prikazuje primjer gdje poduze⌂e ima dva korisnika s imenom *John S. Day*. EIM administrator kreira dva razli⌂ita EIM identifikatora da napravi razliku me⌂u njima: John S. Day1 i John S. Day2. Me⌂utim, koji *John S. Day* je predstavljen s bilo kojim od ovih identifikatora nije odmah vidljivo.

Slika 5: Zamjenska imena za dva EIM identifikatora zasnovana na dijeljenom vlastitom imenu *John S. Day*



Kori⌂tenjem zamjenskih imena, EIM administrator mo⌂e dobaviti dodatne informacije o pojedincu za svaki EIM identifikator. Svaki EIM identifikator mo⌂e imati vi⌂estruka zamjenska imena za identificiranje kojeg *John S. Daya* EIM identifikator predstavlja. Na primjer, dodatna zamjenska imena mogu sadr⌂avati korisnikov broj posla, broj odjela, naziv posla ili druge razlikovne atribute. U ovom primjeru zamjensko ime za John S. Day1 mo⌂e biti John Samuel Day, a zamjensko ime za John S. Day2 mo⌂e biti John Steven Day.

Informacije o zamjenskom imenu mo⌂ete koristiti za pomo⌂ prilikom lociranja odre⌂enog EIM identifikatora. Na primjer, aplikacija koja koristi EIM mo⌂e navesti zamjensko ime koje koristi za pronalazak odgovaraju⌂eg EIM identifikatora za aplikaciju. Administrator mo⌂e to zamjensko ime dodati u EIM identifikator tako da aplikacija za EIM operacije mo⌂e koristiti zamjensko ime umjesto jedinstvenog imena identifikatora. Aplikacija mo⌂e ove informacije navesti prilikom kori⌂tenja API-ja Dohvat EIM ciljnih identiteta iz identifikatora (eimGetTargetFromIdentifier()) za izvedbu EIM operacije pregledavanja za pronalazak odgovaraju⌂ih korisni⌂kih identiteta koji su mu potrebni.

Definicije EIM registra

EIM definicija registra je unos unutar EIM-a koji kreirate za predstavljanje stvarnog korisni⌂kog registra koji postoji na sistemu unutar poduze⌂a. Korisni⌂ki registar djeluje kao direktorij i sadr⌂i listu va⌂e⌂ih korisni⌂kih identiteta za pojedina⌂ni sistem ili aplikaciju. Osnovni korisni⌂ki registar sadr⌂i korisni⌂ke identitete i njihove lozinke. Jedan primjer korisni⌂kog registra je z/OS Security Server Resource Access Control Facility (RACF) registar. Korisni⌂ki registri mogu sadr⌂avati i druge informacije. Na primjer, Lightweight Directory Access Protocol (LDAP) direktorij sadr⌂i vezana razlikovna imena, lozinke i kontrole pristupa podacima koji su spremljeni u LDAP-u. Ostali primjeri uobi⌂ajenih korisni⌂kih registara su principali u Kerberos podru⌂ju ili korisni⌂ki identiteti u Windows Active Directory domeni i OS/400 registru korisni⌂kog profila.

Tako⌂er mo⌂ete definirati korisni⌂ke registre koji postoje unutar drugih korisni⌂kih registara. Neke aplikacije koriste podskup korisni⌂kih identiteta unutar jedne instance korisni⌂kog registra. Na primjer, registar z/OS Poslu⌂itelja Sigurnosti (RACF) mo⌂e sadr⌂avati specifi⌂ne korisni⌂ke registre koji su podskup korisnika unutar svih RACF korisni⌂kih registara. Za modeliranje ovakvog pona⌂anja, EIM dopu⌂ta administratoru kreiranje dvije vrste EIM definicije registra:

- Definicije registra sistema
- Definicije registra aplikacije

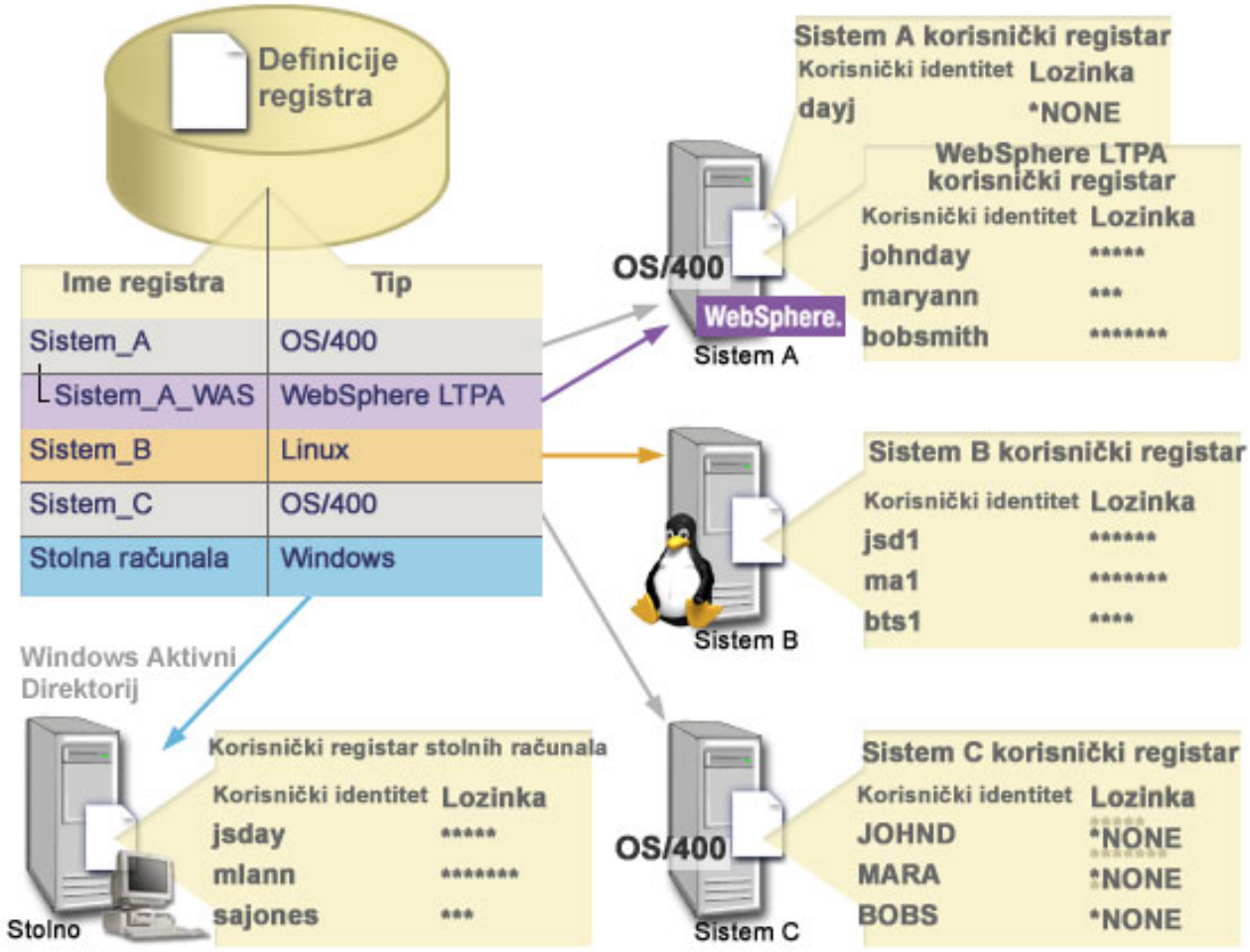
Definicije EIM registra osiguravaju informacije koje se odnose na korisni⌂ke registre u poduze⌂u. Administrator definira ove registre u EIM-u dobavljanjem sljede⌂ih informacija:

- Jedinstveno, arbitrarno EIM ime registra. Svaka definicija registra predstavlja specifi⌂nu instancu korisni⌂kog registra. Prema tome, trebali biste izabrati ime definicije EIM registra koje vam poma⌂e u identificiranju pojedina⌂ne instance korisni⌂kog registra. Na primjer, mogli bi izabrati TCP/IP ime hosta za sistemski korisni⌂ki registar ili ime hosta kombinirano s imenom aplikacije za aplikacijski korisni⌂ki registar. Mo⌂ete koristiti bilo koju kombinaciju alfanumeri⌂kih znakova, naizmjeni⌂no koristiti velika i mala slova i prazna mjesta za kreiranje jedinstvenog imena EIM definicije registra.
- Tip korisni⌂kog registra. Postoji broj unaprijed definiranih tipova korisni⌂kih registara koje EIM omogu⌂uje za pokrivanje ve⌂ine operativnih korisni⌂kih registara sistema. To uklju⌂uje:
  - AIX
  - Domino - dugo ime
  - Domino - kratko ime
  - Kerberos
  - Kerberos - osjetljiv na velika i mala slova
  - LDAP
  - Linux
  - Novell
  - Poslu⌂itelj direktorija
  - OS/400
  - Tivoli Upravitelj Pristupa
  - RACF
  - Windows - lokalni
  - Windows domena (Kerberos) (Ovaj tip je osjetljiv na velika i mala slova).
  - X.509

Bilješka: Iako unaprijed definirani tipovi definicije registra pokrivaju ve⌂inu operativnih korisni⌂kih registara, mo⌂da ⌂ete trebati kreirati definiciju registra za koju EIM ne uklju⌂uje unaprijed definirane tipove registra. U ovoj situaciji imate dvije mogu⌂nosti. Mo⌂ete ili koristiti postoje⌂u definiciju registra koja se podudara s karakteristikama va⌂eg korisni⌂kog registra ili mo⌂ete definirati privatni tip korisni⌂kog registra. Za primjer na Slici 6, administrator je izveo potrebni postupak i definirao tip registra kao WebSphere LTPA za System_A_WAS definiciju registra aplikacije.

Na slici 6., administrator je kreirao EIM definicije registra sistema koje predstavljaju Sistem A, Sistem B, Sistem C i Windows Active Directory koji sadr⌂i korisnikove Kerberos principale s kojima se korisnici prijavljuju na svoje radne stanice. Dodatno, administrator je kreirao definiciju registra aplikacije za WebSphere (R) Lightweight Third-Party Authentication (LTPA), koja se izvodi na Sistemu A. Ime definicije registra koje administrator koristi poma⌂e pri identificiranju specifi⌂nog pojavljivanja tipa korisni⌂kog registra. Na primjer, IP adresa ili ime hosta ⌂esto je dovoljno za mnoge tipove korisni⌂kih registara. U ovom primjeru, administrator koristi System_A_WAS kao ime definicije registra aplikacije za identificiranje ove specifi⌂ne instance WebSphere LTPA aplikacije. On tako⌂er navodi da je registar sistema nadre⌂en definiciji registra aplikacije System_A registar.

Slika 6: EIM definicije registra za pet korisni⌂kih registara u poduze⌂u



Bilješka: Da bi se dalje smanjila potreba upravljanja korisni⌂kim lozinkama, administrator na slici 6 postavlja na *NONE lozinke OS/400 korisni⌂kih profila za Sistem A i za Sistem C. Administrator je u ovom slu⌂aju konfigurirao okolinu jednostruke prijave i jedina aplikacija s kojom ⌂e njen korisnik raditi je EIM-omogu⌂ena aplikacija poput iSeries Navigatora. Prema tome, administrator ⌂eli ukloniti lozinke s njihovih OS/400 korisni⌂kih profila tako da korisnik i on imaju manje lozinki za upravljanje.

Definicije EIM registra i zamjensko ime

Tako⌂er mo⌂ete kreirati zamjenska imena za definicije EIM registra. Za definiciju registra mogu biti navedeni jedan ili vi⌂e zamjenskih imena. Ova podr⌂ka zamjenskog imena dozvoljava programerima da pi⌂u aplikacije bez unaprijed poznavanja proizvoljnog imena EIM registra izabranog od administratora koji razvija aplikaciju. Dokumentaciju aplikacije mo⌂e dobaviti EIM administrator sa zamjenskim imenom koje aplikacija koristi. Kori⌂tenjem ovih informacija, EIM administrator mo⌂e dodijeliti ovo zamjensko ime definiciji EIM registra koja predstavlja stvarni korisni⌂ki registar za koji administrator ⌂eli da ga aplikacija koristi.

Kada administrator dodaje zamjenska imena u EIM definiciju registra, aplikacija mo⌂e koristiti eimGetRegistryFromAlias() EIM API za izvo⌂enje pregledavanja zamjenskih imena da bi prona⌂la EIM ime registra prilikom inicijalizacije. Pregledavanje po zamjenskom imenu dozvoljava aplikaciji da odredi ime ili imena EIM registra za kori⌂tenje kao ulaza u API-je koji izvode EIM operaciju pregledavanja.

Na primjer, aplikacija koja je napisana za kori⌂tenje EIM-a mo⌂e specificirati zamjensko ime izvornog registra ili zamjensko ime ciljnog registra ili zamjenska imena za oboje. Kada ova zamjenska imena dodijelite odgovaraju⌂im definicijama registra, aplikacija mo⌂e izvesti pregledavanje zamjenskog imena da bi prona⌂la EIM definiciju registra ili definicije koje odgovaraju zamjenskim imenima u aplikaciji. To pregledavanja zamjenskog imena osigurava da

| aplikacija koristi korisni⌂ki registar ili korisni⌂ke registre koje administrator ⌂eli da ona koristi. Ovisno o zahtjevima
| aplikacije, administrator mo⌂e dodijeliti vi⌂e zamjenskih imena jednostrukoj definiciji registra.

| Kada navedete zamjensko ime za definiciju registra, za zamjensko ime morate navesti tip i ime. Mo⌂ete koristiti
| predefinirane tipove zamjenskog imena ili mo⌂ete sami definirati tipove zamjenskog imena za kori⌂tenje. Predefinirani
| tipovi zamjenskog imena uklju⌂uju:

- Sistem imena domene (DNS) ime hosta
- Kerberos podru⌂je
- Razlikovno ime izdava⌂a (DN)
- Razlikovno ime korijena (DN)
- TCP/IP adresa
- LDAP DNS ime hosta
- Drugo

| Zamjensko ime ne mora biti u specifi⌂nom formatu. Za tip mo⌂ete unijeti vrijednost po ⌂elji.

| Na primjer, aplikacija mo⌂e specificirati da administrator dodjeljuje zamjensko ime s tipom zamjenskog imena appl i
| imenom zamjenskog imena izvornog registra. Aplikacija zatim mo⌂e koristiti eimGetRegistryNameFromAlias()
| API i specificirati tip i ime zamjenskog imena za API da dohvati korisni⌂ki registar koji aplikacija treba.

Definicije registra sistema

Definicija registra sistema je unos koji kreirate u EIM-u, a koji predstavlja i opisuje zasebni korisni⌂ki registar unutar radne stanice ili poslu⌂itelja. Mo⌂ete kreirati definiciju EIM registra sistema za korisni⌂ki registar kada registar u poduze⌂u ima jedno od sljede⌂ih obilje⌂ja:

- Registar osigurava operativni sistem poput AIX, OS/400 ili proizvoda upravljanja sigurnosti poput z/OS Security Server Resource Access Control Facility RACF).
- Registar sadr⌂i korisni⌂ke identitete koji su jedinstveni specifi⌂nim aplikacijama poput Lotus Notes.
- Registar sadr⌂i distribuirane korisni⌂ke identitete kao ⌂to su Kerberos principali ili Lightweight Directory Access Protocol (LDAP) razlikovna imena.

EIM operacije pregledavanja izvode se ispravno bez obzira definira li EIM administrator registar kao sistemski ili aplikacijski. Me⌂utim, odvojene definicije registra dozvoljavaju da mapiranje podataka bude upravljano na aplikacijskoj osnovi. Odgovornost upravljanja aplikacijski specifi⌂nih mapiranja mo⌂e biti dodijeljeno administratoru za specifi⌂ni registar.

Definicije registra aplikacije

| Definicija registra aplikacije je unos u EIM koji kreirate za opis i predstavljanje podskupa identiteta koji su definirani u
| registru sistema. Ovi korisni⌂ki identiteti dijele zajedni⌂ki skup atributa ili karakteristika koje im dozvoljavaju
| kori⌂tenje pojedina⌂ne aplikacije ili skupa aplikacija. Definicije registra aplikacije predstavljaju korisni⌂ke registre
| koji postoje unutar drugih korisni⌂kih registara. Na primjer, registar z/OS Poslu⌂itelja Sigurnosti (RACF) mo⌂e
| sadr⌂avati specifi⌂ne korisni⌂ke registre koji su podskup korisnika unutar svih RACF korisni⌂kih registara. Zbog
| ovog odnosa, morate navesti ime nadre⌂enog registra sistema za bilo koju definiciju registra aplikacije koju ste kreirali.

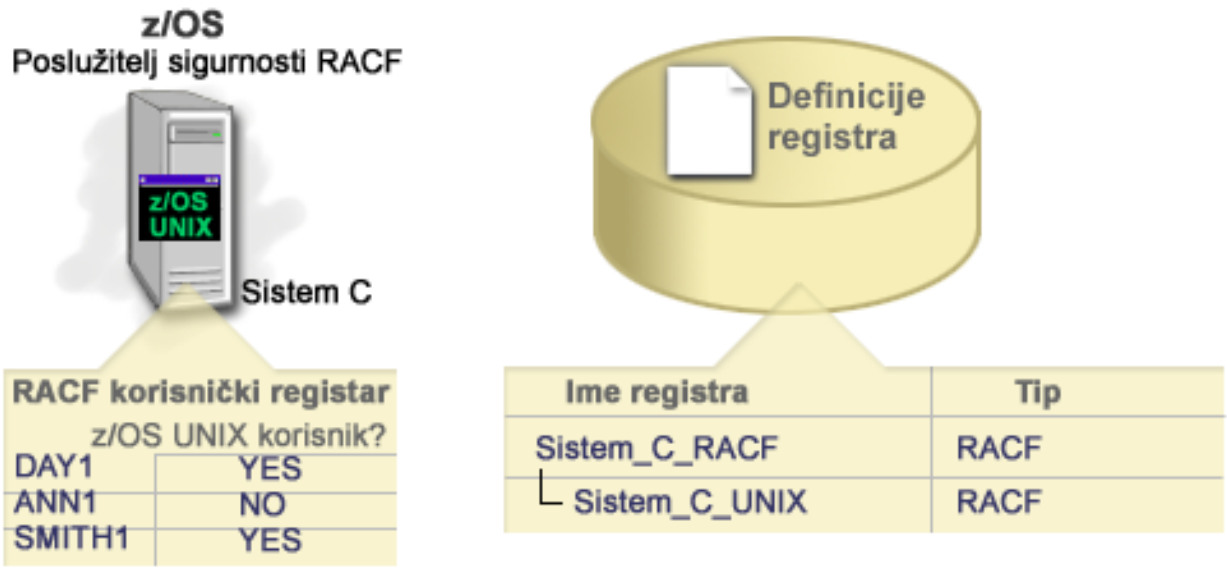
Mo⌂ete kreirati EIM definiciju registra aplikacije za korisni⌂ki registar kada korisni⌂ki identiteti u registru imaju sljede⌂a obilje⌂ja:

- Korisni⌂ki identiteti za aplikaciju nisu spremljeni u korisni⌂kom registru specifi⌂nom za aplikaciju.
- Korisni⌂ki identiteti za aplikaciju pohranjeni su u registru sistema koji sadr⌂i korisni⌂ke identitete za ostale aplikacije.

EIM operacije pregledavanja izvode se ispravno bez obzira je li EIM administrator kreirao aplikaciju ili definiciju registra sistema za korisni⌂ki registar. Me⌂utim, odvojene definicije registra dozvoljavaju da mapiranje podataka bude upravljano na aplikacijskoj osnovi. Odgovornost upravljanja aplikacijski specifi⌂nih mapiranja mo⌂e biti dodijeljeno administratoru za specifi⌂ni registar.

Na primjer, Slika 7 pokazuje kako je EIM administrator kreirao definiciju registra sistema za predstavljanje registra z/OS Poslu⌂itelja Sigurnosti RACF. Administrator je tako⌂er kreirao definiciju registra aplikacije za predstavljanje korisni⌂kog identiteta unutar RACF registra koji koristi z/OS(TM) UNIX Sistemski servis (z/OS UNIX). Sistem C sadr⌂i RACF korisni⌂ki registar koji sadr⌂i informacije za tri korisni⌂ka identiteta, DAY1, ANN1 i SMITH1. Dva od tih korisni⌂kih identiteta (DAY1 i SMITH1) pristupaju z/OS UNIX-u na Sistem C. Ovi su korisni⌂ki identiteti zapravo RACF korisnici s jedinstvenim atributima koji ih identificiraju kao z/OS UNIX korisnike. Unutar EIM definicije registra, EIM administrator je definirao System_C_RACF za predstavljanje cijelog RACF korisni⌂kog registra. Administrator je tako⌂er definirao System_C_UNIX za predstavljanje korisni⌂kih identiteta koji imaju z/OS UNIX atribute.

Slika 7: EIM definicije registra za RACF korisni⌂ki registar i za korisnike z/OS UNIX-a



EIM asocijacije

EIM asocijacija je unos koji kreirate u EIM domeni da definirate odnos izme⌂u korisni⌂kih identiteta u razli⌂itim korisni⌂kim registrima. Tip asocijacije koju kreirate odre⌂uje je li definirani odnos direktan ili indirektan. U EIM-u mo⌂ete kreirati jedan od dva tipa asocijacija: asocijacije identifikatora i asocijacije politika. Asocijacije politika mo⌂ete koristiti umjesto ili u kombinaciji s asocijacijama identifikatora. Na⌂in na koji koristite asocijacije ovisi o sveukupnom planu EIM implementacije.

Da biste nau⌂ili raditi s asocijacijama, pogledajte sljede⌂e informacije:

- Asocijacije identifikatora
  Nau⌂ite kako koristiti asocijacije identifikatora za opis odnosa izme⌂u EIM identifikatora i korisni⌂kih identiteta u korisni⌂kim registrima koji predstavljaju tu osobu. Asocijacija identifikatora kreira mapiranje s jednog na jedan izme⌂u EIM identifikatora i specifi⌂nog korisni⌂kog identiteta. Asocijacije identifikatora mo⌂ete koristiti za indirektno definiranje odnosa izme⌂u korisni⌂kih identiteta upotrebom EIM identifikatora.
- Asocijacije politika
  Nau⌂ite o tome kako koristiti asocijacije politika za opis odnosa izme⌂u vi⌂estrukih korisni⌂kih identiteta i

| jednostrukih korisni⌂kih identiteta u korisni⌂kom registru. Asocijacije politike koriste EIM podr⌂ku politike
| mapiranja za kreiranje mapiranja me⌂u korisni⌂kim identitetima s vi⌂e na jednog bez uklju⌂ivanja EIM
| identifikatora.

| Informacije pregledavanja
| Nau⌂ite kako mo⌂ete koristiti ove opcijske podatke za daljnju identifikaciju ciljnog korisni⌂kog identiteta koje
| EIM API-ji mogu koristiti za vrijeme operacije pregledavanja mapiranja za daljnju precizniju pretragu za ciljnim
| korisni⌂kim identitetom koji je objekt operacije.

Asocijacije identifikatora

| EIM identifikator predstavlja odre⌂enu osobu ili cjelinu u poduze⌂u. EIM asocijacija identifikatora opisuje odnos
| izme⌂u nekog EIM identifikatora i pojedina⌂nog jednostrukog korisni⌂kog identiteta u korisni⌂kom registru koji
| tako⌂er predstavlja tu osobu. Kada kreirate asocijacije izme⌂u EIM identifikatora i svih korisni⌂kih identiteta osobe ili
| cjeline, tada osiguravate jedno, potpuno razumijevanje o tome kako ta osoba ili cjelina koristi resurse u poduze⌂u.

Korisni⌂ki identiteti mogu se koristiti za provjeru autenti⌂nosti, autorizaciju ili oboje. *Provjera autenti⌂nosti* je obrada provjeravanja da cjelina ili osoba koja dobavlja korisni⌂ki identitet ima pravo na pretpostavku tog identiteta. Provjera se ⌂esto posti⌂e prisiljavanjem osobe koja ⌂alje korisni⌂ki identitet za dobavljanje tajnih ili privatnih informacija udru⌂enih s korisni⌂kim identitetom, kao ⌂to je lozinka. *Autorizacija* je obrada osiguravanja da ispravno ovla⌂teni korisni⌂ki identitet mo⌂e izvoditi samo funkcije ili pristupati resursima za koje su identitetu dane povlastice. U pro⌂losti, gotovo sve aplikacije su bile prisiljene koristiti identitete u jednostrukom korisni⌂kom registru i za provjeru autenti⌂nosti i za ovla⌂tenje. Kori⌂tenjem operacija EIM pregledavanja, aplikacije sada mogu koristiti identitete u jednom korisni⌂kom registru za provjeru autenti⌂nosti dok koriste pridru⌂ene korisni⌂ke identitete u razli⌂itom korisni⌂kom registru za ovla⌂tenje.

| EIM identifikator osigurava neizravnu asocijaciju izme⌂u onih korisni⌂kih identiteta koji dozvoljavaju aplikacijama da
| na⌂u drugi korisni⌂ki identitet za neki EIM identifikator baziran na poznatom korisni⌂kom identitetu. EIM osigurava
| API-je koji dozvoljavaju aplikacijama da prona⌂u nepoznati korisni⌂ki identitet u specifi⌂nom (ciljnom) korisni⌂kom
| registru dobavljanjem poznatog korisni⌂kog identiteta u nekom drugom (izvornom) korisni⌂kom registru. Taj se
| proces zove mapiranje identiteta.

| U EIM-u administrator mo⌂e definirati tri razli⌂ita tipa asocijacija za opis odnosa izme⌂u EIM identifikatora i
| korisni⌂kog identiteta. Asocijacije identiteta mogu biti sljede⌂eg tipa: izvorne, ciljne ili administrativne. Tip asocijacije
| koji kreirate je baziran na na⌂inu kori⌂tenja korisni⌂kog identiteta. Na primjer, kreirate izvorne i ciljne asocijacije za
| one korisni⌂ke identitete za koje ⌂elite da sudjeluju u operacijama pregledavanja mapiranja. Tipi⌂no, ako se korisni⌂ki
| identitet koristi za provjeru autenti⌂nosti, trebate kreirati za njega izvornu asocijaciju. Nakon toga kreirate ciljne
| asocijacije za one korisni⌂ke identitete koji se koriste za ovla⌂tenje.

Prije no ⌂to mo⌂ete kreirati asocijaciju identifikatora, prvo morate kreirati odgovaraju⌂i EIM identifikator i odgovaraju⌂u EIM definiciju registra za korisni⌂ki registar koji sadr⌂i pridru⌂eni korisni⌂ki identitet. Asocijacija definira vezu izme⌂u EIM identifikatora i korisni⌂kog identiteta kori⌂tenjem sljede⌂ih informacija:

- Ime EIM identifikatora
- Ime korisni⌂kog identiteta
- Ime definicije EIM registra
- Tip asocijacije
| • Opcijski: informacije pregledavanja prema daljem identitetu ciljnog korisni⌂kog identiteta u ciljnoj asocijaciji.

Izvorna asocijacija

Izvorna asocijacija dozvoljava kori⌂tenje korisni⌂kog identiteta kao izvora u operaciji EIM pregledavanja za pronala⌂enje korisni⌂kog identiteta koji je udru⌂en s istim EIM identifikatorom.

| Kada se koristi korisni⌂ki identitet za *provjeru autenti⌂nosti*, taj korisni⌂ki identitet bi trebao imati izvornu asocijaciju
| s EIM identifikatorom. Na primjer, mogli ste kreirati izvornu asocijaciju za Kerberos principala zato, jer se taj oblik
| korisni⌂kog identiteta koristi za provjeru autenti⌂nosti. Za osiguranje uspjeha operacija pregledavanja mapiranja za
| EIM identifikatore, izvorne i ciljne asocijacije se moraju koristiti zajedno za jednostruki EIM identifikator.

Ciljna asocijacija

Ciljna asocijacija dozvoljava vra⌂anje korisni⌂kog identiteta kao rezultata operacije EIM pregledavanja. Korisni⌂ki identiteti koji predstavljaju krajnje korisnike normalno trebaju samo ciljnu asocijaciju.

Kada se korisni⌂ki identitet koristi za *autorizaciju*, a ne za provjeru autenti⌂nosti, tada bi taj korisni⌂ki identitet trebao imati ciljnu asocijaciju s EIM identifikatorom. Na primjer, mogli ste kreirati ciljnu asocijaciju za neki OS/400 korisni⌂ki profil zato, jer taj oblik korisni⌂kog identiteta odre⌂uje koje resurse i povlastice ima korisnik nad odre⌂enim iSeries sistemom. Za osiguranje uspjeha operacija pregledavanja mapiranja za EIM identifikatore, izvorne i ciljne asocijacije se moraju koristiti zajedno za jednostruki EIM identifikator.

Odnos izvorne i ciljne asocijacije

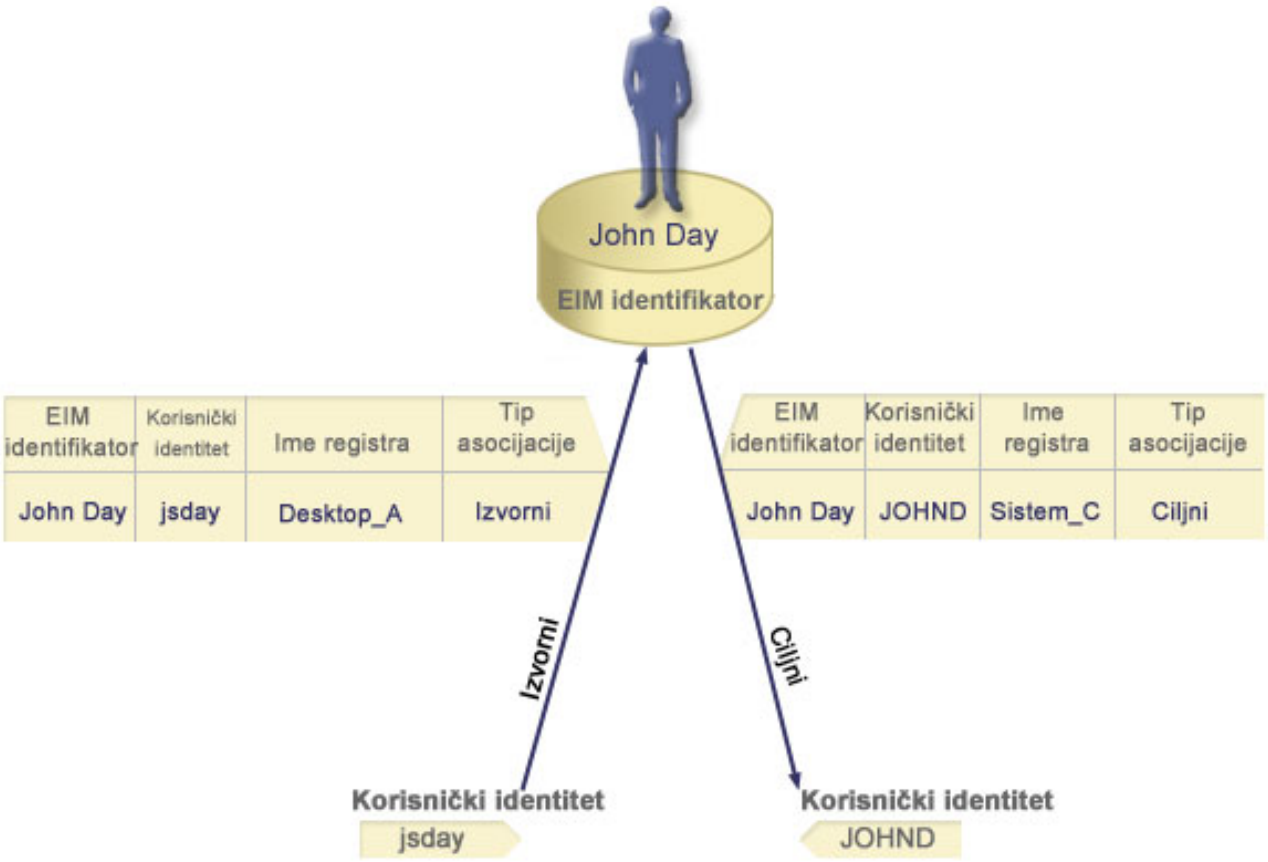
| Za osiguranje uspjeha operacija pregledavanja mapiranja, trebate kreirati barem jednu izvornu i jednu ili vi⌂e ciljnih
| asocijacija za jednostruki EIM identifikator. Obi⌂no kreirate ciljnu asocijaciju za svaki korisni⌂ki identitet u
| korisni⌂kom registru koju osoba mo⌂e koristiti za ovla⌂tenje nad sistemom ili aplikacijom s kojom se podudara
| korisni⌂ki registar.

| Na primjer, korisnici u va⌂em poduze⌂u se normalno prijavljuju i autoriziraju na Windows (R) stolnim ra⌂unalima i
| pristupaju iSeries poslu⌂itelju za izvo⌂enje brojnih zadataka. Korisnici se prijavljuju na njihovim stolnim ra⌂unalima
| koriste⌂i Kerberos principal i pristupaju iSeries poslu⌂itelju koriste⌂i OS/400 korisni⌂ki profil. Vi ⌂elite kreirati
| okru⌂enje jednostruke prijave u kojem se korisnici autoriziraju preko njihovih stolnih ra⌂unala kori⌂tenjem Kerberos
| principala i ne trebaju se vi⌂e ru⌂no autorizirati na iSeries poslu⌂itelju.

| Kako bi se taj cilj postigao, trebate kreirati izvornu asocijaciju za Kerberos principal za svakog korisnika i taj
| korisnikov EIM identifikator. Nakon toga kreirate ciljnu asocijaciju za OS/400 korisni⌂ki profil za svakog korisnika i
| taj korisnikov EIM identifikator. Ova konfiguracija osigurava da OS/400 mo⌂e izvesti operaciju pregledavanja
| mapiranja kako bi se odredio ispravan korisni⌂ki profil potreban korisniku koji pristupa iSeries poslu⌂itelju nakon ⌂to
| se autorizirao na svojem stolnom ra⌂unalu. OS/400 tada dozvoljava korisniku pristup resursima na poslu⌂itelju baziran
| na prikladnom korisni⌂kom profilu bez potrebe da se korisnik ru⌂no autorizira na poslu⌂itelju.

| Slika 6 ilustrira drugi primjer u kojem EIM administrator kreira dvije asocijacije, izvornu asocijaciju i ciljnu asocijaciju
| za EIM identifikator John Day kako bi se definirao odnos izme⌂u tog identifikatora i dva pridru⌂ena korisni⌂ka
| identiteta. Administrator kreira izvornu asocijaciju za jsday, Kerberos principal u Stolna ra⌂unala korisni⌂kom
| registru. Administrator tako⌂er kreira ciljnu asocijaciju za JOHND, OS/400 (R) korisni⌂ki profil u Sistem_C
| korisni⌂kom registru. Ove asocijacije dobavljaju zna⌂enja aplikacijama kako bi se dobio nepoznat korisni⌂ki identitet
| (ciljni, JOHND) baziran na poznatom korisni⌂kom identitetu (izvorni, jsday) kao dio operacije EIM pregledavanja.

Slika 6: EIM ciljne i izvorne asocijacije za EIM identifikator John Day



Za neke bi korisnike moglo biti potrebno kreirati i ciljnu i izvornu asocijaciju za isti korisni⌂ki identitet. Ovo je potrebno kada pojedinac koristi jedan sistem kao klijent i kao poslu⌂itelj ili za pojedince koji se pona⌂aju kao administratori.

Bilješka: Korisni⌂ki identiteti koji predstavljaju tipi⌂ne korisnike normalno trebaju samo ciljnu asocijaciju.

Na primjer, administrator koristi funkciju Sredi⌂njeg Upravljanja u iSeries Navigatoru za upravljanje sredi⌂njim sistemom i nekoliko krajnjim sistemima. Administrator izvodi raznolike funkcije i te funkcije mogu biti na sredi⌂njem sistemu ili na krajnjem sistemu. U toj bi situaciji kreirali i izvornu asocijaciju i ciljnu asocijaciju za sve administratorske korisni⌂ke identitete na svim sistemima. To osigurava da, kojigod sistem administrator koristi za izvorni pristup na jedno od ostalih sistema, kori⌂teni se korisni⌂ki identitet za izvorni pristup na drugi sistem mo⌂e mapirati u prikladan korisni⌂ki identitet za sljede⌂i sistem kojemu administrator pristupa.

Administrativna asocijacija

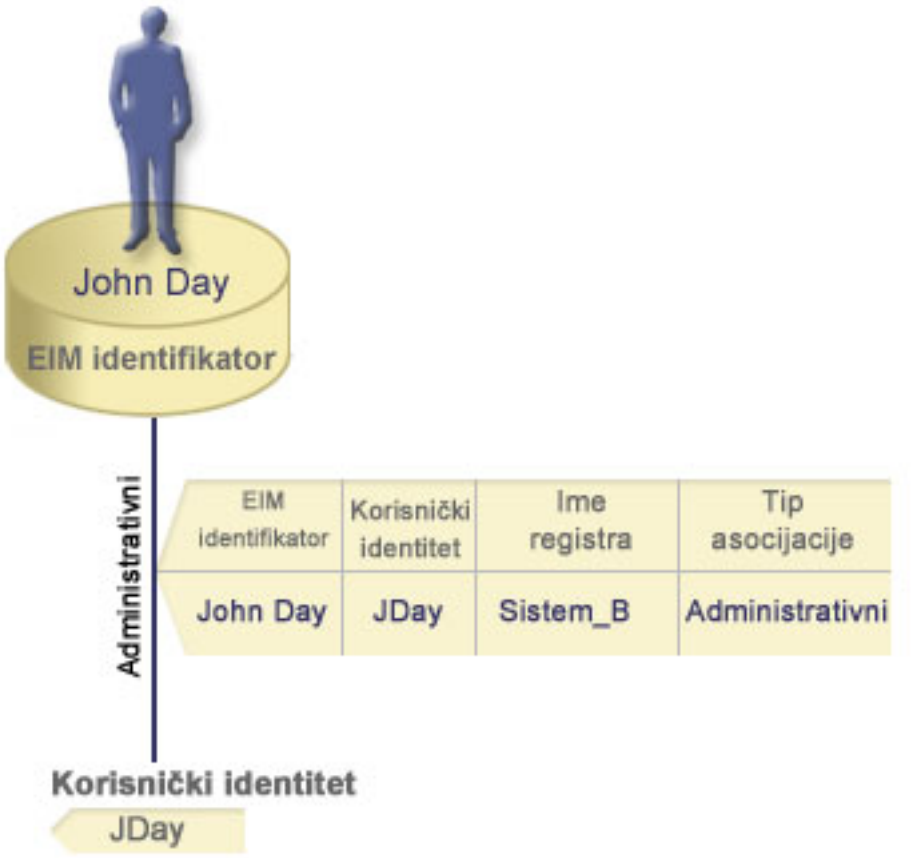
Administrativna asocijacija za EIM identifikator tipi⌂no se koristi da poka⌂e da osoba ili cjelina predstavljena EIM identifikatorom posjeduje korisni⌂ki identitet koji zahtijeva specijalna razmatranja kod specificiranog sistema. Ovaj tip asocijacije se mo⌂e koristiti, na primjer, s visoko osjetljivim korisni⌂kim registrima.

U skladu s posebnom prirodom administracijskih asocijacija, ovaj tip asocijacija ne mo⌂e sudjelovati u operacijama EIM pregledavanja mapiranja. Kao posljedica, operacija EIM pregledavanja koja dobavlja izvorni korisni⌂ki identitet s administracijskom asocijacijom ne vra⌂a rezultate. Sli⌂no, korisni⌂ki identitet s administrativnom asocijacijom nikad se ne vra⌂a kao rezultat operacije EIM pregledavanja.

Slika 7 prikazuje primjer administrativne asocijacije. U ovom primjeru, zaposlenik pod imenom John Day ima korisni⌂ki identitet John_Day na Sistemu A i korisni⌂ki identitet JDay na Sistemu B koji je sistem s visokom

sigurno⌂⌂u. Sistemski administrator ⌂eli osigurati provjeru autenti⌂nosti korisnika na Sistemu B kori⌂tenjem samo lokalnog korisni⌂kog registra ovog sistema. Administrator ne ⌂eli dozvoliti aplikaciji da ovlasti John Day na sistemu upotrebom nekog drugog mehanizma provjere autenti⌂nosti. Kori⌂tenjem administrativne asocijacije za JDay korisni⌂ki identitet na Sistemu B, EIM administrator mo⌂e vidjeti da John Day posjeduje ra⌂un na Sistemu B, ali EIM ne vra⌂a informacije o JDay identitetu kod operacije EIM pregledavanja. ⌂ak i ako aplikacije postoje na ovom sistemu koji koristi operacije EIM pregledavanja, one ne mogu prona⌂i korisni⌂ke identitete koji imaju administrativne asocijacije.

Slika 7: EIM administracijska asocijacija za EIM identifikator John Day



Asocijacije politike

S po⌂etkom u V5R3, podr⌂ka politike Mapiranja identiteta u poduze⌂u (EIM) dozvoljava da EIM administrator kreira i koristi asocijacije politike kako bi definirao odnos izme⌂u vi⌂estrukih korisni⌂kih identiteta u jednom ili vi⌂e korisni⌂kih registara i jednostrukog korisni⌂kog identiteta u drugom korisni⌂kom registru. Asocijacije politike koriste podr⌂ku politike EIM mapiranja za kreiranje vi⌂e-prema-jedan mapiranja izme⌂u korisni⌂kih identiteta bez uklju⌂ivanja EIM identifikatora. Asocijacije politike mo⌂ete koristiti umjesto ili u kombinaciji s asocijacijama identifikatora koje osiguravaju jedan-prema-jedan mapiranje izme⌂u EIM identifikatora i jednostrukog korisni⌂kog identiteta.

Asocijacija politike utje⌂e samo na one korisni⌂ke identitete za koje odre⌂ene pojedina⌂ne EIM asocijacije ne postoje. Kada odre⌂ene asocijacije identifikatora postoje izme⌂u EIM identifikatora i korisni⌂kih identiteta, tada se ciljni korisni⌂ki identitet iz asocijacije identifikatora vra⌂a aplikaciji s izvo⌂enjem operacije pregledavanja, ⌂ak ako asocijacija politike postoji i ako je kori⌂tenje asocijacije politike omogu⌂eno. Za vi⌂e informacija o tome kako operacije pregledavanja obra⌂uju asocijacije, pogledajte “Operacije pregledavanja Mapiranja identiteta u poduze⌂u” na stranici 25.

Mo⌂ete kreirati tri razli⌂ita tipa asocijacije politike:

- Asocijacije politike default domene, koje vam dozvoljavaju postavljanje odnosa mapiranja za sve korisni⌂ke identitete u domeni.
- Asocijacije politike default registra, koje vam dozvoljavaju postavljanje odnosa mapiranja za sve korisni⌂ke identitete u pojedina⌂nom registru.
- Asocijacije politike filtera certifikata, koje vam dozvoljavaju postavljanje odnosa mapiranja za skup korisni⌂kih identiteta (u obliku digitalnog certifikata) u pojedina⌂nom X.509 registru.

Asocijacije politika default domene: Asocijacija politike default domene je jedan tip asocijacije politike koji mo⌂ete koristiti za kreiranje mapiranja vi⌂e-prema-jedan izme⌂u identiteta korisnika. Mo⌂ete koristiti asocijaciju politike default domene za mapiranje izvornog skupa vi⌂estrukih korisni⌂kih identiteta (u ovom slu⌂aju, svi korisnici u domeni) u jednostruki ciljni korisni⌂ki identitet u odre⌂enom ciljnom korisni⌂kom registru. U asocijaciji politike default domene, svi su korisnici u domeni izvor asocijacije politike i mapiraju se u jednostruki ciljni registar i ciljni korisni⌂ki identitet.

Da biste koristili asocijacije politike default domene, morate omogu⌂iti pregledavanje mapiranja upotrebom asocijacija politike za domenu. Morate tako⌂er omogu⌂iti pregledavanje mapiranja za ciljni korisni⌂ki registar asocijacije politike. Kada konfigurirate ovu mogu⌂nost, registri korisnika u asocijaciji politike mogu sudjelovati u operacijama pregledavanja mapiranja.

Asocijacija politike default domene ima u⌂inak kada operacija pregledavanja mapiranja nije zadovoljena asocijacijama identifikatora, asocijacijama politike filtera certifikata ili asocijacijama politike default registra za ciljni registar. Rezultat je da su svi korisni⌂ki identiteti u domeni mapirani u pojedina⌂ni identitet ciljnog korisnika kako je specificirano asocijacijom politike default domene.

Na primjer, mo⌂ete kreirati asocijaciju politike default domene s ciljnim korisni⌂kim identitetom John_Day u ciljnom registru Registry_xyz, a da niste kreirali nikakve asocijacije identifikatora ili druge asocijacije politike koje se mapiraju u ovaj korisni⌂ki identitet. Zato, kada je Registry_xyz specificiran kao ciljni registar u operacijama pregledavanja, politika default domene osigurava da se ciljni identitet korisnika od John_Day vrati za sve korisni⌂ke identitete u domeni koji nemaju za njih definirane druge asocijacije.

Mo⌂ete definirati ove dvije stvari za asocijaciju politike default domene:

- **Ciljni registar**. Specificirani ciljni registar je ime definicije registra Mapiranja identiteta u poduze⌂u (EIM) koji sadr⌂i korisni⌂ki identitet u koji se trebaju mapirati svi korisni⌂ki identiteti u domeni.
- **Ciljni korisnik**. Ciljni korisnik je ime korisni⌂kog identiteta koje se vra⌂a kao cilj operacije EIM pregledavanja mapiranja bazirane na ovoj asocijaciji politike.

Mo⌂ete definirati default asocijaciju politike domene za svaki registar u domeni. Ako se dvije ili vi⌂e asocijacija politike domene odnose na isti ciljni registar, morate definirati jedinstvene informacije pregledavanja za svaku od tih asocijacija politike kako bi osigurali da ih operacije pregledavanja mapiranja mogu razlikovati. Ina⌂e, operacije pregledavanja mapiranja mogu vratiti vi⌂estruke ciljne korisni⌂ke identitete. Rezultat ovih dvosmislenih rezultata je da aplikacija koja ovisi o EIM-u ne⌂e mo⌂i odrediti koji to⌂no ciljni identitet treba koristiti.

Budu⌂i da mo⌂ete koristiti asocijacije politike na mno⌂tvo preklapaju⌂ih na⌂ina, morate detaljno razumjeti EIM podr⌂ku politike mapiranja i kako operacije pregledavanja rade prije no ⌂to kreirate i koristite asocijacije politika.

Asocijacije politika default registra: Asocijacija politike default registra je jedan tip asocijacije politike koji mo⌂ete koristiti za kreiranje mapiranja vi⌂e-prema-jedan izme⌂u identiteta korisnika. Mo⌂ete koristiti asocijaciju politike default registra za mapiranje izvornog skupa vi⌂estrukih korisni⌂kih identiteta (u ovom slu⌂aju onih u jednostrukom registru) u jednostruki ciljni korisni⌂ki identitet u odre⌂enom ciljnom korisni⌂kom registru. U default asocijaciji politike registra, svi su korisnici u jednostrukom registru izvor asocijacija politike i mapiraju se u jednostruki ciljni registar i ciljnog korisnika.

Da biste koristili asocijacije politike default registra, morate omogu⌂iti pregledavanje mapiranja upotrebom asocijacija politike za domenu. Morate tako⌂er omogu⌂iti pregledavanje mapiranja za izvorni registar i omogu⌂iti pregledavanje

mapiranja i kori⌂tenje asocijacija politike za ciljni registar korisnika asocijacije politike. Kada konfigurirate ovu mogu⌂nost, registri korisnika u asocijaciji politike mogu sudjelovati u operacijama pregledavanja mapiranja.

Asocijacija politike default registra ima u⌂inak kada operacija pregledavanja mapiranja nije zadovoljena asocijacijama identifikatora, asocijacijama politike filtera certifikata ili asocijacijama politike default registra za ciljni registar. Rezultat je da su svi korisni⌂ki identiteti u izvornom registru mapirani u pojedina⌂ni identitet ciljnog korisnika kako je specificirano asocijacijom politike default registra.

Na primjer, mo⌂ete kreirati asocijaciju politike default registra koja ima izvorni registar my_realm.com, ⌂to su principali u specifi⌂nom Kerberos podru⌂ju. Za ovu asocijaciju politike, tako⌂er trebate specificirati ciljni korisni⌂ki identitet general_user1 u ciljnom registru os/400_system_reg koji je odre⌂eni profil korisnika u OS/400 korisni⌂kom registru. U tom slu⌂aju, niste kreirali nikakve asocijacije identifikatora ili asocijacije politike koje se primjenjuju na bilo koje identitete korisnika u izvornom registru. Zato, kada je os/400_system_reg specificiran kao ciljni registar, a my_realm.com je specificiran kao izvorni registar u operacijama pregledavanja, asocijacija politike default registra osigurava da se ciljni identitet korisnika od general_user1 vrati za sve identitete korisnika u my_realm.com registru koji nemaju za njih nikakve definirane specifi⌂ne asocijacije identifikatora ili asocijacije politike filtera certifikata.

Mo⌂ete specificirati ove tri stvari za definiranje asocijacije politike default registra:

- **Izvorni registar**. Ovo je definicija registra koju ⌂elite da koristi asocijacija politke kao izvor mapiranja. Svi korisni⌂ki identiteti u izvornom korisni⌂kom registru se trebaju mapirati u specifi⌂nog ciljnog korisnika asocijacije politike.
- **Ciljni registar**. Specificirani ciljni registar je ime definicije registra Mapiranja identiteta u poduze⌂u (EIM). Ciljni registar mora sadr⌂avati ciljni korisni⌂ki identitet u kojeg se svi korisni⌂ki identiteti u izvornom registru mapiraju.
- **Ciljni korisnik**. Ciljni korisnik je ime korisni⌂kog identiteta koje se vra⌂a kao cilj operacije EIM pregledavanja mapiranja bazirane na ovoj asocijaciji politike.

Mo⌂ete definirati vi⌂e od jedne asocijacije politike default registra. Ako se dvije ili vi⌂e asocijacija politike s istim izvornim registrom odnose na isti ciljni registar, morate definirati jedinstvene informacije pregledavanja za svaku od tih asocijacija politike kako bi osigurali da ih operacije pregledavanja mapiranja mogu razlikovati. Ina⌂e, operacije pregledavanja mapiranja mogu vratiti vi⌂estruke ciljne korisni⌂ke identitete. Rezultat ovih dvosmislenih rezultata je da aplikacija koja ovisi o EIM-u ne⌂e mo⌂i odrediti koji to⌂no ciljni identitet treba koristiti.

Budu⌂i da mo⌂ete koristiti asocijacije politike na mno⌂tvo preklapaju⌂ih na⌂ina, morate detaljno razumjeti EIM podr⌂ku politike mapiranja i kako operacije pregledavanja rade prije no ⌂to kreirate i koristite asocijacije politika.

Asocijacije politika filtera certifikata: Asocijacija politike filtera certifikata je jedan tip asocijacije politike koji mo⌂ete koristiti za kreiranje mapiranja vi⌂e-prema-jedan izme⌂u identiteta korisnika. Mo⌂ete koristiti asocijaciju politike filtera certifikata za mapiranje izvornog skupa certifikata u jednostruki ciljni korisni⌂ki identitet u odre⌂enom ciljnom korisni⌂kom registru.

U asocijaciji politike filtera certifikata u jednostrukom X.509 registru kao izvor asocijacije politike odre⌂ujete skup certifikata. Ovi se certifikati mapiraju u jednostruki ciljni registar i u ciljnog korisnika kojeg navedete. Za razliku od default asocijacije politike registra u kojoj su svi korisnici u jednostrukom registru izvor asocijacije politike, djelokrug asocijacije politike filtera certifikata je fleksibilniji. Kao izvor mo⌂ete u registru navesti podskup certifikata. Filter certifikata koji ste naveli za asocijaciju politike odre⌂uje svoj opseg.

Bilješka: Kreirajte i koristite default asocijaciju politike registra kada ⌂elite sve certifikate iz X.509 korisni⌂kog registra mapirati u jednostruki ciljni korisni⌂ki identitet.

Da biste koristili asocijacije politike filtera certifikata, morate omogu⌂iti pregledavanje mapiranja upotrebom asocijacija za domenu. Morate tako⌂er omogu⌂iti pregledavanje mapiranja za izvorni registar i omogu⌂iti pregledavanje mapiranja i kori⌂tenje asocijacija politike za ciljni registar korisnika asocijacije politike. Kada konfigurirate ovu mogu⌂nost, registri korisnika u asocijaciji politike mogu sudjelovati u operacijama pregledavanja mapiranja.

Kada je digitalni certifikat izvorni korisni⌂ki identitet u EIM operaciji pregledavanja mapiranja (nakon ⌂to zahtijevana aplikacija koristi eimFormatUserIdentity() EIM API za formatiranje imena korisni⌂kog identiteta), EIM prvo uspore⌂uje kako bi provjerio da li postoji asocijacija identifikatora izme⌂u EIM identifikatora i specificiranog korisni⌂kog identiteta. Ako ne postoji, EIM tada uspore⌂uje DN informacije u certifikatu s DN ili djelomi⌂nim DN informacijama specificiranim u filteru asocijacije politike. Ako DN informacije u certifikatu zadovoljavaju kriterij u filteru, EIM vra⌂a identitet ciljnog korisnika kojeg je specificirala asocijacija politike. Rezultat je da su certifikati u izvornom X.509 registru koji zadovoljavaju kriterije filtera certifikata mapirani u pojedina⌂ni identitet ciljnog korisnika kako je specificirano asocijacijom politike filtera certifikata.

Na primjer, mo⌂ete kreirati asocijaciju politike filtera certifikata koja ima izvorni registar certificates.x509. Ovaj registar sadr⌂i certifikate za sve zaposlenike poduze⌂a, uklju⌂uju⌂i i one koje svi upravitelji u odjelu za ljudske resurse koriste za pristup odre⌂enim privatnim internim Web stranicama i ostalima resursima kojima pristupaju preko iSeries poslu⌂itelja. Za ovu asocijaciju politike, tako⌂er trebate specificirati identitet ciljnog korisnika hr_managers u ciljnom registru system_abc koji je odre⌂eni profil korisnika u OS/400 korisni⌂kom registru. Za osiguranje da su samo certifikati koji pripadaju upraviteljima ljudskih resursa pokriveni ovom asocijacijom politike, trebate specificirati filter certifikata s razlikovnim imenom u naslovu (SDN) ou=hrmgr,o=myco.com,c=us.

U tom slu⌂aju, niste kreirali nikakve asocijacije identifikatora ili druge asocijacije politike filtera certifikata koje se primjenjuju na bilo koje identitete korisnika u izvornom registru. Zato, kada je system_abc specificiran kao ciljni registar, a certificates.x509 je specificiran kao izvorni registar u operacijama pregledavanja, asocijacija politike filtera certifikata osigurava da se ciljni identitet korisnika od hr_managers vrati za sve certifikate u certificates.x509 registru koji se podudaraju sa specificiranim filterom certifikata i koji nemaju za njih definirane specifi⌂ne asocijacije identifikatora.

Trebate specificirati sljede⌂e informacije za definiranje asocijacije politike filtera certifikata:

- **Izvorni registar**. Definicija izvornog registra koju ste specificirali mora biti X.509 tipa korisni⌂kog registra. Politika filtera certifikata kreira asocijaciju izme⌂u identiteta korisnika u ovom X.509 korisni⌂kom registru i pojedina⌂nog specifi⌂nog ciljnog korisni⌂kog identiteta. Asocijacija se primjenjuje samo na one korisni⌂ke identitete u registru koji zadovoljavaju kriterije filtera certifikata koji ste specificirali za ovu politiku.
- **Filter certifikata**. Filter certifikata definira skup sli⌂nih atributa certifikata korisnika. Asocijacija politike filtera certifikata mapira sve certifikate s tako definiranim atributima u X.509 korisni⌂kom registru u specifi⌂ni ciljni korisni⌂ki identitet. Trebate specificirati filter baziran na kombinaciji Razlikovnog imena naslova (SDN) i Razlikovnog imena izdava⌂a (IDN) koji se podudara s certifikatima koje ⌂elite koristiti kao izvor mapiranja. Filter certifikata koji ste specificirali za politiku mora ve⌂ postojati u EIM domeni.
- **Ciljni registar**. Definicija ciljnog registra koju ste specificirali je korisni⌂ki registar koji sadr⌂i korisni⌂ke identitete u koje ⌂elite mapirati certifikate koji se podudaraju s filterom certifikata.
- **Ciljni korisnik**r. Ciljni korisnik je ime korisni⌂kog identiteta koji je vra⌂en kao cilj iz operacije EIM pregledavanja mapiranja baziran na asocijaciji politike.

Budu⌂i da mo⌂ete koristiti asocijacije politike certifikata i ostale asocijacije na mno⌂tvo sli⌂nih na⌂ina, morate detaljno razumjeti i EIM podr⌂ku politike mapiranja i kako operacije pregledavanja rade prije no ⌂to kreirate i koristite asocijacije politika certifikata.

Filteri certifikata: Filter certifikata definira skup sli⌂nih razlikovnih imena atributa certifikata za grupu certifikata korisnika u X.509 izvornom korisni⌂kom registru. Filter certifikata mo⌂ete koristiti ka osnovu asocijacije politike filtera certifikata. Filter certifikata u asocijaciji politike odre⌂uje koji certifikat u specificiranom izvornom X.509 registru mapirati u specificiranog ciljnog korisnika. Ti certifikati koji imaju informacije DN Predmeta i DN Izdava⌂a koje zadovoljavaju kriterije filtera, mapiraju se na specificiranog ciljnog korisnika za vrijeme operacija EIM pregledavanja mapiranja.

Na primjer, mo⌂ete kreirati filter certifikata s razlikovnim imenom naslova (SDN) o=ibm,c=us. Svi certifikati s tim DN-ovima kao dijelovima njihovih SDN informacija zadovoljavaju kriterije filtera, kao certifikat sa SDN-om cn=JohnDay,ou=LegalDept,o=ibm,c=us. Ako postoji vi⌂e od jednog filtera certifikata kod kojeg certifikat zadovoljava kriterije, prednost ima specifi⌂nija vrijednost filtera certifikata s kojom se certifikat najbolje podudara. Na primjer, imate filter certifikata sa SDN-om o=ibm,c=us i imate drugi filter certifikata sa SDN-om

ou=LegalDept,o=ibm,c=us. Ako imate certifikat u izvornom X.509 registru sa SDN-om cn=JohnDay,ou=LegalDept,o=ibm,c=us, tada se koristi drugi ili specifi⌂niji filter certifikata. Ako imate certifikat u izvornom X.509 registru sa SDN-om cn=SharonJones,ou=LegalDept,o=ibm,c=us, tada se koristi manje specifi⌂niji filter certifikata zbog boljeg podudaranja certifikata s njegovim kriterijima.

Od sljede⌂eg mo⌂ete specificirati jedno ili oboje za definiranje filtera certifikata:

- Razlikovno ime naslova (SDN). Potpuni ili djelomi⌂ni DN koji ste specificirali za filter mora odgovarati dijelu DN naslova od digitalnog certifikata ⌂to opisuje vlasnika certifikata. Mo⌂ete dobaviti potpuni niz znakova DN naslova ili mo⌂ete dobaviti jedan ili vi⌂e djelomi⌂nih DN-ova koji obuhva⌂aju potpuni SDN.
- Razlikovno ime izdava⌂a (IDN). Potpuni ili djelomi⌂ni DN koji ste specificirali za filter mora odgovarati dijelu DN izdava⌂a od digitalnog certifikata ⌂to opisuje Izdava⌂a certifikata koji je izdao certifikat. Mo⌂ete dobaviti potpuni niz znakova DN izdava⌂a ili mo⌂ete dobaviti jedan ili vi⌂e djelomi⌂nih DN-ova koji bi mogli obuhvatiti potpuni IDN.

Postoji nekoliko metoda koje mo⌂ete koristiti za kreiranje filtera certifikata, koje uklju⌂uju kori⌂tenje Formatiranja EIM filtera politike (eimFormatPolicyFilter()) API za generiranje filtera certifikata kori⌂tenjem certifikata kao predlo⌂ka za kreiranje potrebnih DN-ova ispravno poredanih i formatiranih za SDN i IDN.

Informacije pregledavanja

Po⌂ev⌂i u V5R3, mo⌂ete osigurati *neobavezne* podatke koji se zovu informacije pregledavanja da bi bolje identificirali ciljni korisni⌂ki identitet. Taj ciljni korisni⌂ki identitet mo⌂e biti specifi⌂an u asocijaciji identifikatora ili u asocijaciji politike. Informacije pregledavanja su jedinstveni niz znakova koji eimGetTargetFromSource EIM API ili eimGetTargetFromIdentifier EIM API mogu koristiti za vrijeme operacije pregledavanja mapiranja za daljnje pobolj⌂avanje tra⌂enja ciljnog korisni⌂kog identiteta koji je objekt operacije. Podaci koje navedete za informacije pregledavanja odgovaraju dodatnim informacijskim parametrima korisni⌂kog registra za te EIM API-je.

Informacija pregledavanja je potrebna samo kada operacija pregledavanja mapiranja mo⌂e vratiti vi⌂e od jedan ciljni korisni⌂ki identitet. Operacija pregledavanja mapiranja mo⌂e vratiti vi⌂estruke korisni⌂ke registre kada postoji jedna ili vi⌂e od sljede⌂ih situacija:

- EIM identifikator ima vi⌂estruke individualne ciljne asocijacije na istom ciljnom registru.
- Vi⌂e od jednog EIM identifikatora ima isti korisni⌂ki identitet naveden u izvornoj asocijaciji i svaki od tih EIM identifikatora ima ciljnu asocijaciju na istom ciljnom registru, iako korisni⌂ki identitet naveden za svaku ciljnu asocijaciju mo⌂e biti razli⌂it.
- Vi⌂e od jedne asocijacije politike default domene specificiraju isti ciljni registar.
- Vi⌂e od jedne default asocijacije politike registra specificiraju isti izvorni registar i isti ciljni registar.
- Vi⌂e od jedne asocijacije politike filtera certifikata specificiraju isti izvorni X.509 registar, filter certifikata i ciljni registar.

Bilješka: Operacija pregledavanja mapiranja koja vra⌂a vi⌂e od jednog ciljnog korisni⌂kog identiteta mo⌂e stvarati probleme za EIM-omogu⌂ene aplikacije uklju⌂uju⌂i OS/400 aplikacije i proizvode koji nisu dizajnirani za rukovanje tim dvosmislenim rezultatima. Me⌂utim, osnovne OS/400 aplikacije poput iSeries Access za Windows ne mogu koristiti informacije pregledavanja za razlikovanje vi⌂estrukih ciljnih korisni⌂kih identiteta koje vra⌂a operacija pregledavanja. Prema tome, mo⌂ete razmotriti ponovno definiranje asocijacija za domenu da osigurate da operacija pregledavanja mapiranja mo⌂e vratiti jednostruki ciljni korisni⌂ki identitet za osiguranje da osnovne OS/400 aplikacije mogu uspje⌂no izvesti operacije pregledavanja i mapirati identitete.

Informacije pregledavanja mo⌂ete koristiti za izbjegavanje situacija u kojima je mogu⌂e da operacije pregledavanja mapiranja vrate vi⌂e od jednog ciljnog korisni⌂kog identiteta. Za spre⌂avanje da operacije pregledavanja mapiranja vra⌂aju vi⌂estruke korisni⌂ke ciljne identitete morate definirati jedinstvene informacije pregledavanja za svaki ciljni korisni⌂ki identitet u svakoj situaciji. Te se informacije pregledavanja moraju dati operaciji pregledavanja mapiranja da bi se osiguralo da operacija mo⌂e vratiti jedinstveni ciljni korisni⌂ki identitet. U suprotnom, aplikacije koje ovise o EIM-u mo⌂da ne⌂e mo⌂i odrediti koji to⌂no ciljni identitet upotrijebiti.

Na primjer, imate EIM identifikator imena John Day koji za Sistem A ima dva korisni⌂ka profila. Jedan od tih korisni⌂kih profila je JDUSER za Sistem A, a drugi je JDSECADM koji ima posebna ovla⌂tenja administratora sigurnosti. Postoje dvije ciljne asocijacije za identifikator Johna Daya. Jedna od tih ciljnih asocijacije je za JDUSER korisni⌂ki identitet u ciljnom registru System_A i ima informacije pregledavanja od korisni⌂kog ovla⌂tenja navedenog za JDUSER. Druga je asocijacija za korisni⌂ki identitet JDSECADM u ciljnom registru System_A i ima informacije pregledavanja od slu⌂benika sigurnosti navedenog za JDSECADM.

Ako operacija pregledavanja mapiranja ne specificira nikakve informacije pregledavanja, operacija pregledavanja vra⌂a korisni⌂ke identitete JDUSER i JDSECADM. Ako operacija pregledavanja mapiranja specificira informacije pregledavanja korisni⌂kog ovla⌂tenja, operacija pregledavanja vra⌂a samo korisni⌂ki identitet JDUSER. Ako operacija pregledavanja mapiranja specificira informacije slu⌂benika sigurnosti, operacija pregledavanja vra⌂a samo korisni⌂ki identitet JDSECADM.

Bilješka: Ako obri⌂ete zadnju ciljnu asocijaciju za korisni⌂ki identitet (bilo asocijaciju identifikatora ili asocijaciju politike), ciljni korisni⌂ki identitet i informacije pregledavanja tako⌂er se bri⌂u iz domene.

Budu⌂i da mo⌂ete koristiti asocijacije politike certifikata i ostale asocijacije na mno⌂tvo preklapaju⌂ih na⌂ina, morate detaljno razumjeti EIM podr⌂ku politike mapiranja i kako operacije pregledavanja rade da biste mogli kreirati i koristiti asocijacije politika.

Operacije pregledavanja Mapiranja identiteta u poduze⌂u

Aplikacija ili operativni sistem koriste EIM API za izvo⌂enje *operacije pregledavanja* tako da aplikacija ili operativni sistem mo⌂e mapirati s jednog korisni⌂kog identiteta u jednom registru u drugi korisni⌂ki identitet u drugom registru. EIM operacija pregledavanja je proces preko koje aplikacija ili operativni sistem pronalazi nepoznate pridru⌂ene korisni⌂ke identitete u odre⌂enom ciljnom registru tako da osigurava poznate i pouzdane 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 mo⌂e izvesti jedan od dva tipa EIM operacija pregledavanja na osnovu tipa informacija koje aplikacija dobavlja kao izvor EIM operacije pregledavanja: korisni⌂ki identitet ili EIM identifikator.

Kada aplikacije ili operativni sistemi koriste eimGetTargetFromSource() API za dobivanje ciljnog korisni⌂kog identiteta za dani ciljni registar, moraju osigurati *korisni⌂ki identitet kao cilj* operacije pregledavanja. Da bi se koristio kao izvor u EIM operaciji pregledavanja, korisni⌂ki identitet mora imati definiranu asocijaciju izvornog identifikatora ili imati asocijaciju politike. Kada aplikacija ili operativni sistem koristi ovaj API, aplikacija ili operativni sistem mora osigurati tri informacije:

- Korisni⌂ki identitet kao izvor ili po⌂etnu to⌂ku operacije.
- Ime EIM definicije registra za izvorni korisni⌂ki identitet.
- Ime EIM definicije registra koje je cilj EIM operacije pregledavanja. Ova definicija registra opisuje korisni⌂ki registar koji sadr⌂i korisni⌂ki identitet koji aplikacija tra⌂i.

Kada aplikacije ili operativni sistemi koriste eimGetTargetFromIdentifier() API za dobivanje korisni⌂kog identiteta za dani ciljni registar, moraju osigurati *EIM identifikator kao cilj* EIM operacije pregledavanja. Kada aplikacija koristi ovaj API, aplikacija mora osigurati dvije informacije:

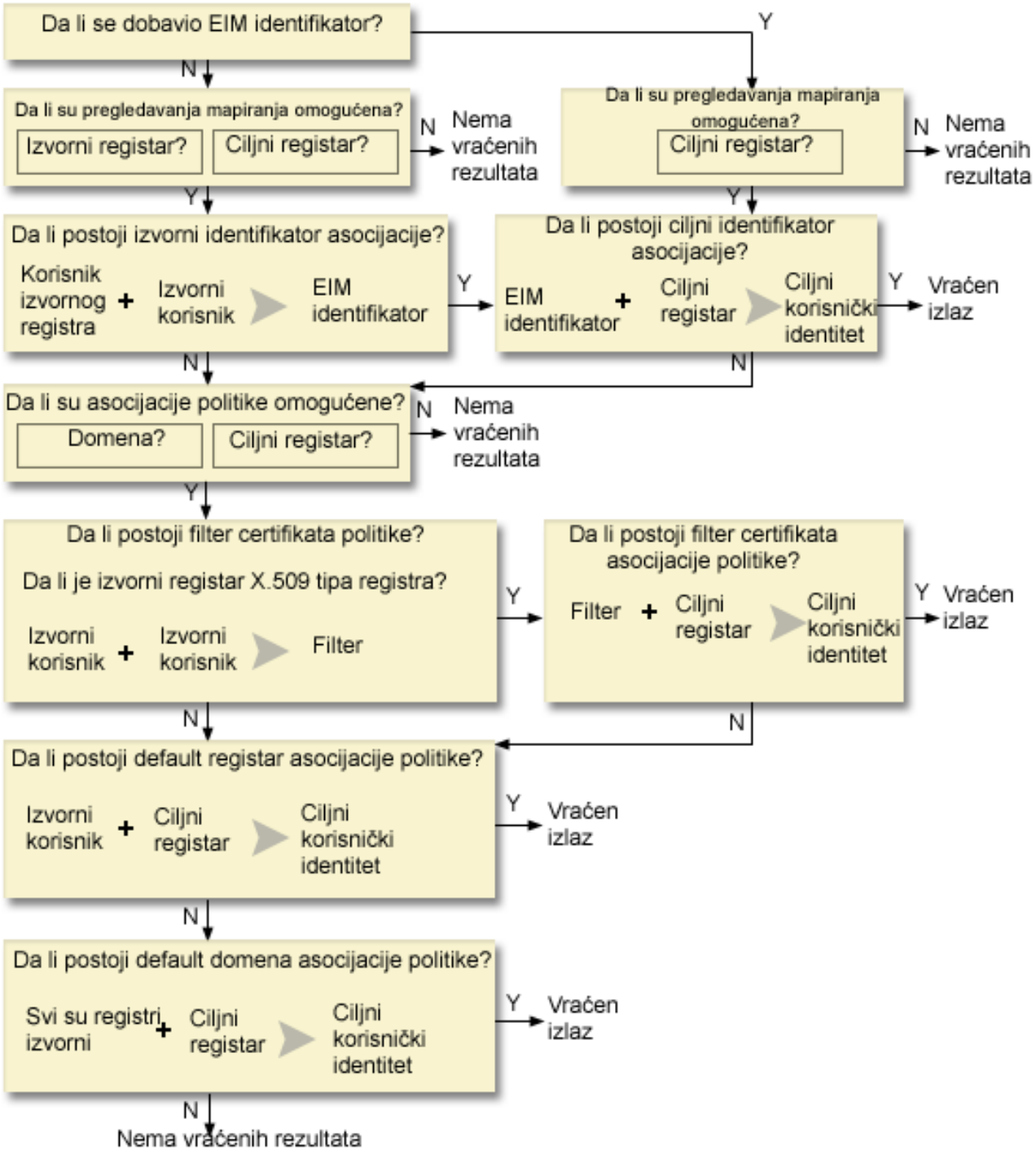
- EIM identifikator kao izvor ili po⌂etnu to⌂ku operacije.
- Ime EIM definicije registra koje je cilj EIM operacije pregledavanja. Ova definicija registra opisuje korisni⌂ki registar koji sadr⌂i korisni⌂ki identitet koji aplikacija tra⌂i.

Da bi korisni⌂ki identitet bio vra⌂en kao cilj bilo kojeg tipa EIM operacije pregledavanja, korisni⌂ki identitet mora za njega imati definiranu ciljnu asocijaciju. Ova ciljna asocijacija mo⌂e biti u obliku asocijacije identifikatora ili asocijacije politike.

Osigurana se informacija daje EIM-u i EIM operacija pretra⌂ivanja tra⌂i i vra⌂a bilo koji ciljni korisni⌂ki identitet pretra⌂uju⌂i EIM podatke sljede⌂im redoslijedom kao ⌂to prikazuje slika 10:

1. Ciljna asocijacija identifikatora za EIM identifikator. EIM identifikator se identificira na jedan od dva na⌂ina: osigurava ga eimGetTargetFromIdentifier() API. ili se EIM identifikator odre⌂uje iz informacije koju je osigurao eimGetTargetFromSource() API.
2. Asocijacije politike filtera certifikata.
3. Asocijacije politike default registra.
4. Asocijacije politike default domene.

Slika 10: Dijagram toka EIM operacije pregledavanja op⌂enite obrade



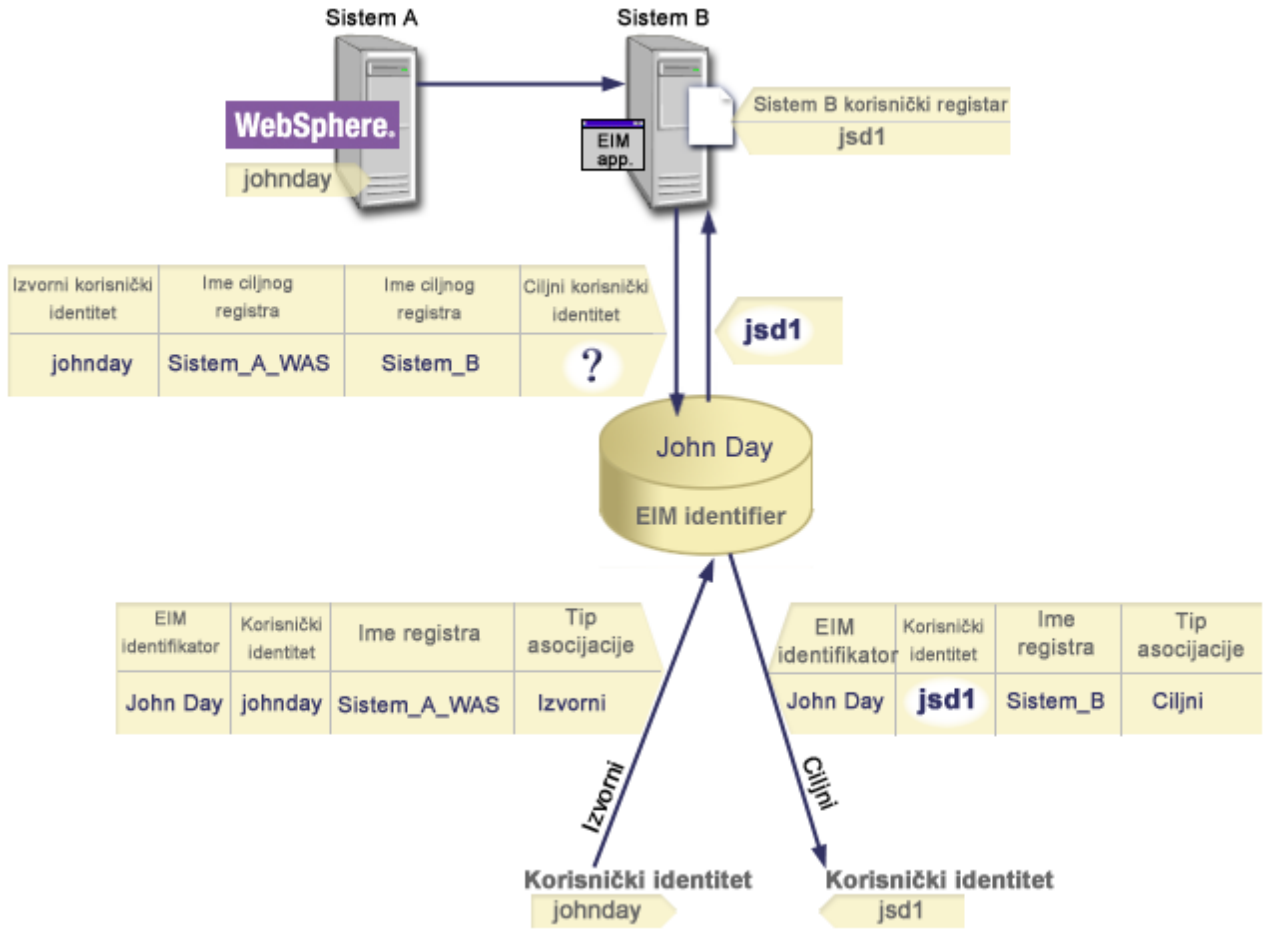
Pretraga operacije pregledavanja te∆e na sljede∆i na∆in:

1. Operacija pregledavanja provjerava jesu li pregledavanja mapiranja omogu∆ena. Operacija pregledavanja odre∆uje jesu li pregledavanja mapiranja omogu∆ena za navedeni izvorni registar, navedeni ciljni registar ili oba navedena registra. Ako pregledavanje mapiranja nije omogu∆eno za jedan ili oba registra, tada operacija pregledavanja zavr∆ava vra∆aju∆i ciljni korisni∆ki identitet.
2. Operacija pregledavanja provjerava postoje li asocijacije identifikatora koje odgovaraju kriterijima pregledavanja.Ako je omogu∆en EIM identifikator, operacija pregledavanja koristi navedeno ime EIM identifikatora. Ina∆e, operacija pregledavanja provjerava postoji li specifi∆na izvorna asocijacija identifikatora koja odgovara osiguranom izvornom korisni∆kom identitetu i izvornom registru. Ako postoji, operacija pregledavanja ju koristi za odre∆ivanje odgovaraju∆eg imena EIM identifikatora. Operacija pregledavanja tada koristi ime EIM identifikatora za pretra∆ivanje ciljnih asocijacija identifikatora za EIM identifikator koji odgovara navedenom imenu ciljne EIM definicije registra. Ako postoji ciljna asocijacija identifikatora koja odgovara, operacija pregledavanja vra∆a ciljni korisni∆ki identitet definiran u ciljnoj asocijaciji.
3. Operacija pregledavanja provjerava je li kori∆tenje asocijacija politika omogu∆eno. Operacija pregledavanja provjerava je li domena omogu∆ena kako bi mogla dopustiti pregledavanje mapiranja upotrebom asocijacija politike. Operacija pregledavanja tako∆er provjerava je li ciljni registar omogu∆en za kori∆tenje asocijacija politike. Ako domena nije omogu∆ena za asocijacije politika ili registar nije omogu∆en za asocijacije politika, tada operacija pregledavanja zavr∆ava bez vra∆anja ciljnog korisni∆kog identiteta.
4. Operacija pregledavanja tra∆i asocijacije politika filtera certifikata. Operacija pregledavanja provjerava je li izvorni registar tipa X.509. Ako je registar tipa X.509, operacije pregledavanja provjeravaju postoji li asocijacija politike filtera certifikata koja odgovara izvornom i ciljnom imenu definicije registra. Operacija pregledavanja provjerava postoje li certifikati u izvornom X.509 registru koji zadovoljavaju kriterije navedene u asocijaciji politike filtera certifikata. Ako postoji podudaraju∆a asocijacija politike i postoje certifikati koji zadovoljavaju kriterij filtera certifikata, operacija mapiranja vra∆a odgovaraju∆i ciljni korisni∆ki identitet za tu asocijaciju politike.
5. Operacija pregledavanja tra∆i default asocijacije politike registra.Operacija pregledavanja provjerava postoji li default asocijacija politike registra koja odgovara izvornim i ciljnim imenima definicije registra. Postoji li podudaraju∆a asocijacija politike, operacija pregledavanja vra∆a odgovaraju∆i ciljni korisni∆ki identitet za tu asocijaciju politika.
6. Operacija pregledavanja tra∆i asocijacije politike default domene.Operacija pregledavanja provjerava postoji li asocijacija politike default domene koja je definirana za ciljnu definiciju registra. Postoji li podudaraju∆a asocijacija politike, operacija pregledavanja vra∆a pridru∆eni ciljni korisni∆ki identitet za tu asocijaciju politika.
7. Operacija pregledavanja ne mo∆e vratiti nikakav rezultat.

Primjeri operacije pregledavanja: Primjer 1

Na slici 11, korisni∆kom se identitetu johnday provjerava autenti∆nost na WebSphere Poslu∆itelju Aplikacija upotrebom Lightweight Third-Party Authentication (LPTA) na sistemu A. WebSphere Poslu∆itelj Aplikacija na sistemu A poziva doma∆i program na sistemu B da pristupi podacima na sistemu B. Doma∆i program koristi EIM API za izvo∆enje EIM operacije pregledavanja zasnovane na korisni∆kom identitetu sa sistema A kao izvoru operacije. Aplikacija dobavlja sljede∆e informacije za izvo∆enje operacije: johnday kao izvorni korisni∆ki identitet, System_A_WAS kao izvorno ime definicije EIM registra i System_B kao ciljno ime definicije EIM registra. Ove izvorne informacije se predaju EIM-u i EIM operacija pregledavanja pronalazi izvornu asocijaciju identifikatora koja odgovara informacijama. Upotrebom imena EIM identifikatora John Day, EIM operacije pregledavanja tra∆e ciljnu asocijaciju identifikatora za ovaj identifiaktor koja se podudara s ciljnim imenom EIM definicije registra za System_B. Kada je prona∆ena podudaraju∆a ciljna asocijacija EIM operacija pregledavanja aplikaciji vra∆a jsd1 korisni∆ki identitet.

Slika 11: EIM operacija pregledavanja vra∆a ciljni korisni∆ki identitet iz odre∆ene asocijacije identifikatora zasnovane na poznatom korisni∆kom identitetu johnday



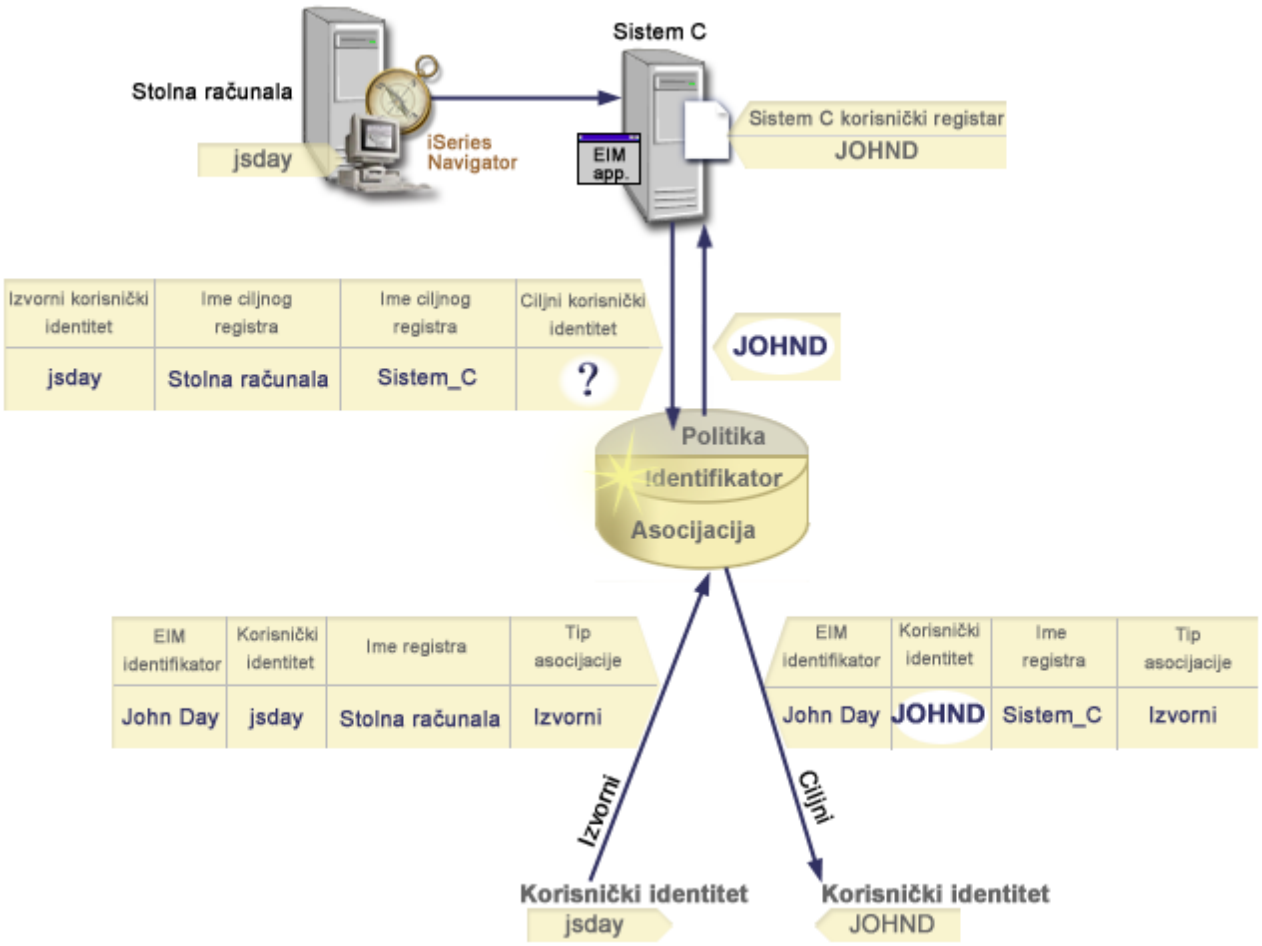
Primjeri operacije pregledavanja: Primjer 2

Na slici 12, administrator ∆eli mapirati Windows korisnika iz Windows Aktivni direktorij registra u OS/400 korisni∆ki profil. Kerberos je metoda provjere autenti∆nosti koju Windows koristi, a ime Windows Aktivni direktorij registra koje je administrator definirao u EIM-u je Desktops. Korisni∆ki identitet iz kojeg administrator ∆eli mapirati je Kerberos principal imena jsday. Ime OS/400 registra kao ∆to ga je definirao administrator u EIM-u je System_C i korisni∆ki identitet koji administrator ∆eli mapirati u korisni∆ki profil imena JOHND.

Administrator kreira EIM identifikator imena John Day. Zatim dodaje dvije asocijacije u taj EIM identifikator:

- Izvornu asocijaciju za Kerberos principal imena jsday u registru Desktops.
- Ciljnu asocijaciju za OS/400 korisni∆ki profil imena JOHND u registru System_C.

Slika 12: EIM operacija pregledavanja vra∆a ciljni korisni∆ki identitet iz odre∆enih asocijacija identifikatora zasnovanih na poznatom Kerberos principalu jsday



Ta konfiguracija omogu⌂uje da operacije pregledavanja mapiranja mapiraju iz Kerberos principala u OS/400 korisni⌂ki profil kao ⌂to slijedi:

Izvorni korisni⌂ki identitet i registar	**--->**	**EIM identifikator**	**--->**	**Ciljni korisni⌂ki identitet**
jsday u registru Desktops	--->	John Day	--->	JOHND (u registru System_C)

Pretraga operacije pregledavanja te⌂e na sljede⌂i na⌂in:

1. Korisnik jsday prijavljuje se i provjeru autenti⌂nosti radi Windows upotrebom njegovih Kerberos principala u Windows Aktivni direktorij registru Desktops.
2. Korisnik otvara iSeries Navigator za pristup podacima na System_C.
3. OS/400 koristi EIM API za izvo⌂enje EIM operacija pregledavanja s izvornim korisni⌂kim identitetom jsday, izvornim registrom Stolna ra⌂unala i ciljnim registrom System_C.
4. EIM operacija pregledavanja provjerava jesu li omogu⌂eni pregledi mapiranja za izvorni registar Desktops i ciljni registar System_C. Jesu.
5. Operacija pregledavanja tra⌂i odre⌂enu izvornu asocijaciju identifikatora koja se podudara s navedenim izvornim korisni⌂kim identitetom jsday iz izvornog registra Desktops.
6. Operacija pregledavanja koristi podudaraju⌂u izvornu asocijaciju identifikatora za odre⌂ivanje odgovaraju⌂eg imena EIM identifikatora koji je John Day.

7. Operacija pregledavanja koristi to ime EIM identifikatora za tra⌂enje ciljne asocijacije identifikatora za EIM identifikator koji se podudara s navedenim ciljnim imenom EIM definicije registra System_C.
8. Postoji takva ciljna asocijacija identifikatora i operacija pregledavanja ciljni korisni⌂ki identitet JOHND vra⌂a kao definiran u ciljnoj asocijaciji.
9. Kada je operacija pregledavanja mapiranja zavr⌂ena, iSeries Navigator pokre⌂e se pod korisni⌂kim profilom JOHND. Korisni⌂ko ovla⌂tenje za pristup resursima i izvo⌂enje akcija unutar iSeries Navigatora odre⌂eno je ovla⌂tenjem koje je definirano u JOHND korisni⌂kom profilu, a ne ovla⌂tenjem definirano za jsday korisni⌂ki identitet.

Sljede⌂i primjer opisuje tok pretrage operacija pregledavanja kada su asocijacije politika na mjestu, dok za korisni⌂ki identitet ne postoje asocijacije identifikatora.

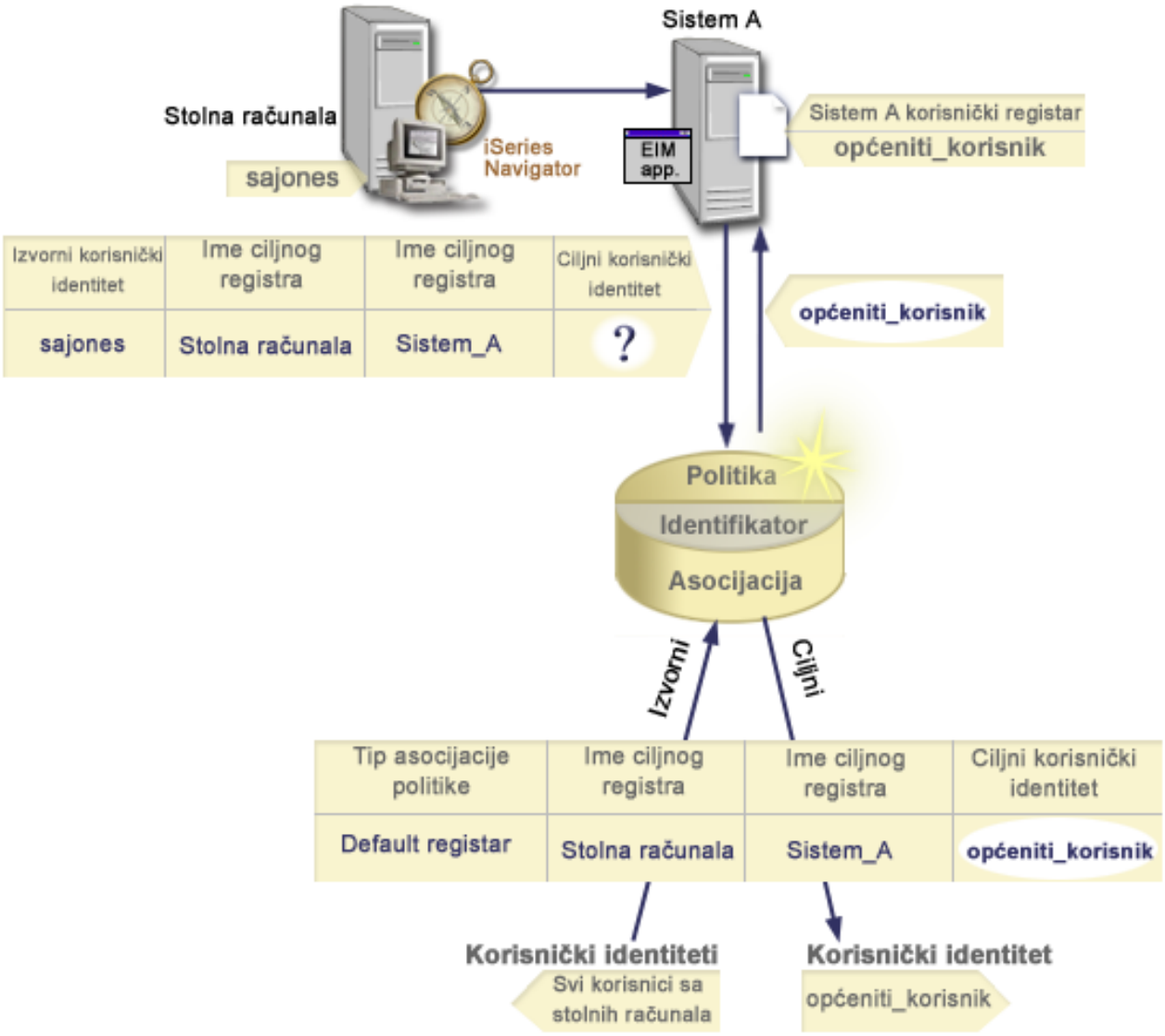
Primjeri operacije pregledavanja: Primjer 3

Na slici 13, administrator ⌂eli mapirati sve korisnike radnih stanica u registru Windows Aktivnog direktorija u jednostruki OS/400 korisni⌂ki profil s imenom general_user u OS/400 registru koji je u EIM-u nazvao System_A. Kerberos je metoda provjere autenti⌂nosti koju Windows koristi, a ime registra u Windows Aktivnom direktoriju koje je administrator definirao u EIM-u je Desktops. Jedan od korisni⌂kih identiteta iz kojeg administrator ⌂eli mapirati je Kerberos principal s imenom sajones.

Administrator kreira default asocijaciju politike registra sa sljede⌂im informacijama:

- Izvorni registar od Desktops.
- Ciljni registar od System_A.
- Ciljni korisni⌂ki identitet od general_user.

Slika 13: Operacija pregledavanja vra⌂a ciljni korisni⌂ki identitet iz default asocijacije politike registra.



Ova konfiguracija omogu⌂uje operaciju pregledavanja mapiranja da mapira sve Kerberos principale u registar Desktops, uklju⌂uju⌂i sajones principal, u OS/400 korisni⌂ki profil naziva general_user kao ⌂to slijedi:

Izvorni korisni⌂ki identitet i registar	**--->**	**Default asocijacije politike registra**	**--->**	**Ciljni korisni⌂ki identitet**
sajones u Desktops registru	--->	Default asocijacije politike registra	--->	general_user (u System_A registru)

Pretraga operacije pregledavanja te⌂e na sljede⌂i na⌂in:

1. Korisnik sajones prijavljuje se i njegovu autenti⌂nost provjerava Windows stolno ra⌂unalo upotrebom Kerberos principala iz Desktops registra.
2. Korisnik otvara iSeries Navigator za pristup podacima na System A.
3. OS/400 koristi EIM API za izvo⌂enje EIM operacija pregledavanja s korisni⌂kim identitetom sajones, izvornim registrom od Desktops i ciljnim registrom od System_A.
4. EIM operacija pregledavanja provjerava jesu li pregledavanja mapiranja omogu⌂ena za izvorni registar Desktops i ciljni registar System_A. Jesu.

5. Operacija pregledavanja tra∆i odre∆enu izvornu asocijaciju identifikatora koja se podudara s navedenim izvornim korisni∆kim identitetom sajones iz izvornog registra Desktops. Ne pronalazi podudaraju∆u asocijaciju identifikatora.
6. Operacija pregledavanja provjerava je li domena omogu∆ena za upotrebu asocijacija politika. Jest.
7. Operacija pregledavanja provjerava je li ciljni registar (System_A) omogu∆en za upotrebu asocijacija politika. Jest.
8. Operacija pregledavanja provjerava je li izvorni registar (Desktops) X.509 registar. Nije.
9. Operacija pregledavanja provjerava postoji li default asocijacija politike registra koja odgovara imenu definicije izvornog registra (Desktops) i imenu definicije ciljnog registra (System_A).
10. Operacija pregledavanja odre∆uje da postoji i kao ciljni korisni∆ki identitet vra∆a general_user.

Ponekad EIM operacija pregledavanja vra∆a dvosmislene rezultate. Ovo se mo∆e desiti, na primjer, kada se vi∆e od jednog ciljnog korisni∆kog identiteta podudara s navedenim kriterijem operacije pregledavanja. Neke EIM omogu∆ene aplikacije, uklju∆uju∆i OS/400 aplikacije i proizvode, nisu oblikovani za rukovanje tim dvosmislenim rezultatima i mogu ne uspjeti ili dati neo∆ekivane rezultate. Mo∆da ∆ete trebati poduzeti neke mjere da rije∆ite tu situaciju. Na primjer, morat ∆ete promijeniti EIM konfiguraciju ili definirati informacije pregledavanja za svaki ciljni korisni∆ki identitet da sprije∆ite vi∆estruka podudaranja ciljnih korisni∆kih identiteta. Tako∆er, mo∆ete testirati mapiranja da odredite da li promjene koje ste napravili rade prema o∆ekivanjima.

Mapiranje identiteta u poduze∆u: podr∆ka i omogu∆avanja politike mapiranja

Podr∆ka politike Mapiranja identiteta u poduze∆u (EIM) dozvoljava vam kori∆tenje asocijacija politike kao i odre∆enih asocijacija identifikatora u nekoj EIM domeni. Asocijacije politika mo∆ete koristiti umjesto ili u kombinaciji s asocijacijama identifikatora.

Podr∆ka politike EIM mapiranja osigurava zna∆enja omogu∆avanja i onemogu∆avanja kori∆tenja asocijacija politike za cijelu domenu kao i za svaki specifi∆ni ciljni korisni∆ki registar. EIM vam tako∆er dozvoljava da postavite da li odre∆eni registar mo∆e sudjelovati op∆enito u operacijama pregledavanja mapiranja. Kao posljedica, mo∆ete koristiti podr∆ku politike mapiranja za precizniju kontrolu kako operacije pregledavanja mapiranja vra∆aju rezultate.

Default postavka za EIM domenu je da su pregledavanja mapiranja koja koriste asocijacije politike onemogu∆ena za domenu. Kada je onemogu∆eno kori∆tenje asocijacija politike za domenu, sve operacije pregledavanja mapiranja za domenu vra∆aju rezultate kori∆tenjem samo odre∆enih asocijacija identifikatora izme∆u korisni∆kih identiteta i EIM identifikatora.

Default postavke za svaki pojedina∆ni registar su takve da je sudjelovanje pregledavanja mapiranja omogu∆eno, a kori∆tenje asocijacija politike onemogu∆eno. Kada omogu∆ite kori∆tenje asocijacija politike za pojedina∆ni ciljni registar, trebate tako∆er osigurati da je ta postavka omogu∆ena za domenu.

Mo∆ete konfigurirati sudjelovanje pregledavanja mapiranja i kori∆tenje asocijacija politike za svaki registar na jedan od tri na∆ina:

- Operacije pregledavanja mapiranja se ne mogu u potpunosti koristiti za odre∆eni registar. Drugim rije∆ima, neka aplikacija koja izvodi operaciju pregledavanja mapiranja uklju∆uju∆i taj registar ne∆e uspjeti vratiti rezultate.
- Operacije pregledavanja mapiranja mogu koristiti odre∆ene asocijacije identifikatora izme∆u samo korisni∆kih identiteta i EIM identifikatora. Pregledavanja mapiranja su omogu∆ena za registar, ali je zato kori∆tenje asocijacija politike onemogu∆eno za registar.
- Operacije pregledavanja mapiranja mogu koristiti odre∆ene asocijacije identifikatora kada postoje i asocijacije politike kada odre∆ene asocijacije identifikatora ne postoje (sve su postavke omogu∆ene).

Za informacije o tome kako omogu∆iti postavke podr∆ke politike mapiranja i postavke sudjelovanja pregledavanja mapiranja, pogledajte:

- Omogu∆avanje asocijacija politike za domenu
- Omogu∆avanje podr∆ke pregledavanja mapiranja i kori∆tenje asocijacija politike za ciljni registar

EIM kontrola pristupa

EIM korisnik je korisnik koji posjeduje EIM kontrolu pristupa zasnovanu na njegovom ∆lanstvu u unaprijed definiranoj Lightweight Directory Access Protocol (LDAP) korisni∆koj grupi za specifi∆nu domenu. Navo∆enje EIM *kontrole pristupa* za korisnika dodaje tog korisnika u odre∆enu LDAP korisni∆ku grupu odre∆ene domene. Svaka LDAP grupa ima ovla∆tenje za izvo∆enje odre∆enih EIM administrativnih zadataka za tu domenu. Koje i kakve tipove administrativnih zadataka, uklju∆uju∆i operacije pregledavanja, EIM korisnik mo∆e izvesti odre∆eno je grupom za kontrolu pristupa kojoj EIM korisnik pripada.

Bilješka: Za konfiguriranje EIM-a morate dokazati da ste pouzdani unutar cijele mre∆e a ne samo na odre∆enom sistemu. Ovla∆tenje za konfiguriranje EIM-a nije zasnovano na va∆em OS/400 ovla∆tenju korisni∆kog profila nego na ovla∆tenju EIM kontrole pristupa. EIM je mre∆ni resurs, a ne resurs za odre∆eni sistem, prema tome EIM ne prepoznaje ovla∆tenja koja su specifi∆na za OS/400 poput *ALLOBJ i *SECADM za konfiguraciju. Kada je EIM konfiguriran, ovla∆tenje za izvo∆enje zadataka mo∆e biti zasnovano na broju razli∆itih korisni∆kih tipova uklju∆uju∆i OS/400 korisni∆ke profile. Na primjer, IBM Poslu∆itelj direktorija za iSeries (LDAP) tretira OS/400 profile s *ALLOBJ i *IOSYSCFG posebnim ovla∆tenjem kao administratore direktorija.

Samo korisnici s administratorskom EIM kontrolom pristupa mogu dodati druge korisnike u grupu za EIM kontrolu pristupa ili mijenjati ostale korisni∆ke postavke kontrole pristupa. Da bi korisnik mogao postati ∆lanom grupe EIM kontrole pristupa on mora imati unos u poslu∆itelju direktorija koji djeluje kao kontroler EIM domene. Tako∆er, samo odre∆eni tipovi korisnika mogu biti ∆lanovi grupe EIM kontrole pristupa. Korisni∆ki identitet mo∆e biti u obliku Kerberos principala, LDAP razlikovnog imena ili OS/400 korisni∆kog profila toliko dugo koliko je korisni∆ki profil definiran na poslu∆itelju direktorija.

Opaska: Da biste imali tip korisnika Kerberos principala dostupan u EIM-u, na sistemu mora biti konfigurirana usluga mre∆ne provjere autenti∆nosti. Da biste imali tip OS/400 korisni∆kog profila dostupan u EIM-u, sufiks sistemskog objekta na poslu∆itelju direktorija mora biti konfiguriran. Ovo omogu∆uje poslu∆itelju direktorija referenciranje OS/400 sistemskih objekata, poput OS/400 korisni∆kih profila.

Slijede kratki opisi funkcija koje svaka grupa EIM ovla∆tenja mo∆e izvoditi:

- **Lightweight Directory Access Protocol (LDAP) administrator.** LDAP administrator je posebno razlikovno ime (DN) u direktoriju koji je administrator cijelog direktorija. Prema tome, LDAP administrator ima pristup svim EIM administrativnim funkcijama kao i pristup cijelom direktoriju. Korisnik s ovom kontrolom pristupa mo∆e izvesti sljede∆e funkcije:
  - Kreirati domenu.
  - Izbrisati domenu.
  - Kreirati i ukloniti EIM identifikatore.
  - Kreirati i ukloniti EIM definicije registara.
  - Kreirati i ukloniti izvorne, ciljne i administrativne asocijacije.
  - Kreirati i ukloniti asocijacije politika.
  - Kreirati i ukloniti filtere certifikata.
  - Omogu∆iti i onemogu∆iti kori∆tenje asocijacija politika za domenu.
  - Omogu∆iti i onemogu∆iti pregledavanja mapiranja za registar.
  - Omogu∆iti i onemogu∆iti kori∆tenje asocijacija politika za registar.
  - Izvoditi EIM operacije pregledavanja.
  - Dohva∆ati asocijacije identifikatora, asocijacije politika, filtere certifikata, EIM identifikatore i EIM definicije registara.
  - Dodavati, uklanjati i ispisivati informacije EIM kontrole pristupa.
- **EIM administrator.** ∆lanstvo u ovoj grupi kontrole pristupa omogu∆ava korisniku upravljanje svim EIM podacima unutar EIM domene. Korisnik s ovom kontrolom pristupa mo∆e izvesti sljede∆e funkcije:
  - Izbrisati domenu.

- Kreirati i ukloniti EIM identifikatore.
- Kreirati i ukloniti EIM definicije registara.
- Kreirati i ukloniti izvorne, ciljne i administrativne asocijacije.
- Kreirati i ukloniti asocijacije politika.
- Kreirati i ukloniti filtere certifikata.
- Omogu⌂iti i onemogu⌂iti kori⌂tenje asocijacija politika za domenu.
- Omogu⌂iti i onemogu⌂iti pregledavanja mapiranja za registar.
- Omogu⌂iti i onemogu⌂iti kori⌂tenje asocijacija politika za registar.
- Izvoditi EIM operacije pregledavanja.
- Dohva⌂ati asocijacije identifikatora, asocijacije politika, filtere certifikata, EIM identifikatore i EIM definicije registara.
- Dodavati, uklanjati i ispisivati informacije EIM kontrole pristupa.

- **Administrator identifikatora.** ⌂lanstvo u ovoj grupi kontrole pristupa omogu⌂ava korisniku dodavanje i mijenjanje EIM identifikatora i upravljanje izvornim i administrativnim asocijacijama. Korisnik s ovom kontrolom pristupa mo⌂e izvesti sljede⌂e funkcije:
  - Kreirati EIM identifikatore.
  - Kreirati i ukloniti izvorne asocijacije.
  - Kreirati i ukloniti administrativne asocijacije.
  - Izvoditi EIM operacije pregledavanja.
  - Dohva⌂ati asocijacije identifikatora, asocijacije politika, filtere certifikata, EIM identifikatore i EIM definicije registara.
- **EIM operacije mapiranja.** ⌂lanstvo u ovoj grupi kontrole pristupa omogu⌂ava korisniku izvo⌂enje EIM operacija pregledavanja mapiranja. Korisnik s ovom kontrolom pristupa mo⌂e izvesti sljede⌂e funkcije:
  - Izvoditi EIM operacije pregledavanja.
  - Dohva⌂ati asocijacije identifikatora, asocijacije politika, filtere certifikata, EIM identifikatore i EIM definicije registara.
- **Administrator registra.** ⌂lanstvo u ovoj grupi kontrole pristupa omogu⌂ava korisniku upravljanje definicijama EIM registra. Korisnik s ovom kontrolom pristupa mo⌂e izvesti sljede⌂e funkcije:
  - Dodati i ukloniti ciljne asocijacije.
  - Kreirati i ukloniti asocijacije politika.
  - Kreirati i ukloniti filtere certifikata.
  - Omogu⌂iti i onemogu⌂iti pregledavanja mapiranja za registar.
  - Omogu⌂iti i onemogu⌂iti kori⌂tenje asocijacija politika za registar.
  - Izvoditi EIM operacije pregledavanja.
  - Dohva⌂ati asocijacije identifikatora, asocijacije politika, filtere certifikata, EIM identifikatore i EIM definicije registara.
- **Administrator za izabrane registre.** ⌂lanstvo u ovoj grupi kontrole pristupa korisniku omogu⌂uje upravljanje EIM informacijama samo za odre⌂enu definiciju korisni⌂kog registra (poput Registry_X). ⌂lanstvo u ovoj grupi kontrole pristupa tako⌂er omogu⌂uje korisniku dodavanje i uklanjanje ciljnih asocijacija samo za odre⌂enu definiciju korisni⌂kog registra. Za potpunu prednost operacija pregledavanja mapiranja i asocijacija politike, korisnik s ovom kontrolom pristupa tako⌂er treba imati kontrolu pristupa **EIM operacije mapiranja**. Ova kontrola pristupa omogu⌂uje korisniku izvo⌂enje sljede⌂e funkcije za odre⌂ene ovla⌂tene definicije registra:
  - Kreiranje, uklanjanje i ispis ciljnih asocijacija samo za navedene EIM definicije registara.
  - Dodavanje i uklanjanje asocijacija politika default domene.
  - Dodavanje i uklanjanje asocijacija politike samo za navedene definicije registara.
  - Dodavanje filtera certifikata samo za navedene definicije registara.
  - Omogu⌂avanje i onemogu⌂avanje pregledavanja mapiranja samo za navedene definicije registara.

– Omogu⌂avanje i onemogu⌂avanje kori⌂tenje asocijacija politika samo za navedene definicije registara.
– Dohva⌂anje EIM identifikatora.
– Dohva⌂anje asocijacije identifikatora i filtera certifikata samo za navedene definicije registara.
– Dohva⌂anje informacija EIM definicije registara samo za navedene definicije registara.

Bilješka: Korisnik koji ima kontrolu pristupa **Administrator za izabrane registre** i kontrolu pristupa **EIM operacije pregledavanja mapiranja** dobiva mogu⌂nost izvo⌂enja sljede⌂ih funkcija:
– Dodavanje i uklanjanje asocijacija politike samo za navedene registre.
– Izvoditi EIM operacije pregledavanja.
– Dohva⌂ati sve asocijacije identifikatora, asocijacije politika, filtere certifikata, EIM identifikatore i EIM definicije registara.

Da utvrdite ima li odre⌂ena grupa EIM kontrole pristupa ovla⌂tenje za izvo⌂enje odre⌂ene akcije, pogledajte sljede⌂e stranice:
- Grupa EIM kontrole pristupa: API ovla⌂tenje
- Grupa EIM kontrola pristupa: ovla⌂tenje EIM zadataka

EIM grupa kontrole pristupa: API ovla⌂tenje

Svaka od sljede⌂ih tablica je organizirana po EIM operaciji koju izvodi API. Svaka tablica prikazuje svaki EIM API, razli⌂ite grupe EIM kontrole pristupa i da li grupa kontrole pristupa ima ovla⌂tenje za izvo⌂enje specifi⌂ne EIM funkcije.

Tablica 1. Rad s domenama

EIM API	LDAP administrator	EIM administrator	Administrator identifikatora	EIM pregledavanje mapiranja	Administrator registra	Administrator za izabrani registar
eimChangeDomain	X	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	-	-	-	-
eimGetAssociated Identifikatori	X	X	X	X	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
eimAddApplication Registar	X	X	-	-	-	-
eimAddSystemRegistry	X	X	-	-	-	-
eimChangeRegistry	X	X	-	-	X	X
eimChange RegistryUser	X	X	-	-	X	X

Tablica 3. Rad s registrima (nastavak)

EIM API	LDAP administrator	EIM administrator	Administrator EIM identifikatora	EIM pregledavanje mapiranja	Administrator EIM registara	Administrator EIM registra X
eimChangeRegistryAlias	X	X	-	-	X	X
eimGetRegistry NameFromAlias	X	X	X	X	X	X
eimListRegistries	X	X	X	X	X	X
eimListRegistry Asocijacije	X	X	X	X	X	X
eimListRegistryAliases	X	X	X	X	X	X
eimListRegistry Korisnici	X	X	X	X	X	X
eimRemoveRegistry	X	X	-	-	-	-

Tablica 4. Rad s asocijacijama identifikatora. Za eimAddAssociation() i eimRemoveAssociation() API-ije postoje ⌂etiri parametara koja odre⌂uju tip asocijacije koja se ili dodala ili uklonila. Ovla⌂tenje za ove API-je se razlikuje na osnovu tipa asocijacije specificirane u ovim parametrima. U sljede⌂oj tablici uklju⌂en je tip asocijacije 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 (administrativna)	X	X	X	-	-	-
eimAddAssociation (izvorna)	X	X	X	-	-	-
eimAddAssociation (izvorna i ciljna)	X	X	X	-	X	X
eimAddAssociation (ciljna)	X	X	-	-	X	X
eimListAssociations	X	X	X	X	X	X
eimRemoveAssociation (administrativna)	X	X	X	-	-	-
eimRemoveAssociation (izvorna)	X	X	X	-	-	-
eimRemoveAssociation (izvorna i ciljna)	X	X	X	-	X	X
eimRemoveAssociation (ciljna)	X	X	-	-	X	X

Tablica 5. Rad s asocijacijama politike

EIM API	LDAP administrator	EIM administrator	Administrator EIM identifikatora	EIM pregledavanje mapiranja	Administrator EIM registara	Administrator EIM registra X
eimAddPolicyAssociation	X	X	-	-	X	X
eimAddPolicyFilter	X	X	-	-	X	X
eimListPolicyFilters	X	X	X	X	X	X
eimRemove PolicyAssociation	X	X			X	X
eimRemovePolicyFilter	-	-	-	-	-	

Tablica 6. 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

Tablica 6. Rad s mapiranjima (nastavak)

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

Tablica 7. 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	-	-	-	-

Grupa kontrole pristupa za Mapiranje identiteta u poduze⌂u: EIM ovla⌂tenje zadatka

Sljede⌂a tablica prikazuje odnose izme⌂u razli⌂itih grupa kontrole pristupa za Mapiranje identiteta u poduze⌂u (EIM) i EIM zadataka koji grupe mogu izvesti.

Premda LDAP administrator nije ispisan u tablici, ta je razina kontrole pristupa potrebna za kreiranje nove EIM domene. Tako⌂er, LDAP administrator ima istu kontrolu pristupa kao i EIM administrator, dok EIM administrator nema automatski i LDAP administratorsku kontrolu pristupa.

Tablica 8. Tablica 1: EIM grupe kontrole pristupa

EIM zadatak	EIM administrator	Administrator identifikatora	Operacije pregledavanja EIM mapiranja	Administrator registra	Administrator za izabrani registar
Kreiranje domene	-	-	-	-	-
Brisanje domene	X	-	-	-	-
Modificiranje domene	X	-	-	-	-
Omogu⌂avanje/ Onemogu⌂avanje asocijacija politike za domenu	X	-	-	-	-
Tra⌂enje domena	X	-	-	-	-
Dodavanje sistemskog registra	X	-	-	-	-
Dodavanje aplikacijskog registra	X	-	-	-	-
Uklanjanje registra	X	-	-	-	-
Modificiranje registra	X	-	-	X	X

Tablica 8. Tablica 1: EIM grupe kontrole pristupa (nastavak)

EIM zadatak	EIM administrator	Administrator identifikatora	Operacije pregledavanja EIM mapiranja	Administrator registra	Administrator za izabrani registar
Omogu⌂avanje/ Onemogu⌂avanje pregledavanje mapiranja za registar	X	-	-	X	X
Omogu⌂avanje/ Onemogu⌂avanje asocijacija politike za registar	X	-	-	X	X
Tra⌂enje registara	X	X	X	X	X
Dodavanje identifikatora	X	X	-	-	-
Uklanjanje identifikatora	X	-	-	-	-
Modificiranje identifikatora	X	X	-	-	-
Tra⌂enje identifikatora	X	X	X	X	X
Dohvat pridru⌂enih identifikatora	X	X	X	X	X
Dodavanje/ Uklanjanje administrativne asocijacije	X	X	-	-	-
Dodavanje/ Uklanjanje izvorne asocijacije	X	X	-	-	-
Dodavanje/ Uklanjanje ciljne asocijacije	X	-	-	X	X
Dodavanje/ Uklanjanje asocijacije politike	X	-	-	X	X
Dodavanje/ Uklanjanje filtera certifikata	X	-	-	X	X
Tra⌂enje filtera certifikata	X	X	X	X	X
Tra⌂enje asocijacija	X	X	X	X	X
Tra⌂enje asocijacija politike	X	X	X	X	X
Dohvat ciljne asocijacije iz izvorne asocijacije	X	X	X	X	-

Tablica 8. Tablica 1: EIM grupe kontrole pristupa (nastavak)

EIM zadatak	EIM administrator	Administrator identifikatora	Operacije pregledavanja EIM mapiranja	Administrator registra	Administrator za izabrani registar
Dohvat ciljne asocijacije iz identifikatora	X	X	X	X	X
Modificiranje korisnika registra	X	-	-	X	X
Tra⌂enje korisnika registra	X	X	X	X	X
Modificiranje pseudonima registra	X	-	-	X	X
Tra⌂enje pseudonima registra	X	X	X	X	X
Dohvat registra iz pseudonima	X	X	X	X	X
Dodavanje/ Uklanjanje EIM kontrole pristupa	X	-	-	-	-
Prikaz ⌂lanova grupe kontrole pristupa	X	-	-	-	-
Prikaz EIM kontrole pristupa za specificiranog korisnika	X	-	-	-	-
Upit u EIM kontrolu pristupa	X	-	-	-	-

LDAP koncepti za EIM

Mapiranje identiteta u poduze⌂u (EIM) koristi Lightweight Directory Access Protocol (LDAP) poslu⌂itelj kao kontroler domene za pohranjivanje EIM podataka. Prema tome, morate razumjeti neke LDAP koncepte koji se odnose na konfiguriranje i upotrebu EIM-a u va⌂em poduze⌂u. Na primjer, mo⌂ete koristiti LDAP razlikovno ime kao korisni⌂ki identitet za konfiguriranje EIM-a i provjere autenti⌂nosti EIM kontrolera domene.

Da bolje razumijete konfiguriranje i upotrebu EIM-a, morate razumjeti sljede⌂e LDAP koncepte:

- Razlikovno ime
- Nadre⌂eno razlikovno ime
- LDAP shema i ostala razmatranja EIM-a

Razlikovno ime

Razlikovno ime (DN) je unos Lightweight Directory Access Protocola (LDAP) koji jedinstveno identificira i opisuje unos u poslu⌂itelj direktorija (LDAP). Koristite ⌂arobnjaka EIM konfiguracije za konfiguriranje poslu⌂itelja direktorija za pohranjivanje informacija EIM domene. Budu⌂i da EIM koristi poslu⌂itelja direktorija za pohranu EIM podataka, mo⌂ete koristiti razlikovna imena kao imena za provjeru autenti⌂nosti na EIM kontroleru domene.

Razlikovna imena sastoje se od samog imena unosa kao i od imena, gledano od dolje prema gore, objekata iznad njega u LDAP direktoriju. Primjer potpunog razlikovnog imena bilo bi cn=Tim Jones, o=IBM, c=US. Svaki unos ima

barem jedan atribut koji se koristi za imenovanje unosa. Ovaj atribut imenovanja se zove relativno razlikovno ime (RDN) unosa. Unos iznad danog RDN-a se zove po njegovom nadre⌂enom razlikovnom imenu. U ovom primjeru, cn=Tim Jones imenuje unos, tako da je to RDN. o=IBM, c=US je nadre⌂eno DN za cn=Tim Jones. Pogledajte "Nadre⌂eno razlikovno ime" da nau⌂ite vi⌂e o tome kako EIM ovo koristi.

Budu⌂i da EIM koristi poslu⌂itelja direktorija za pohranjivanje EIM podataka, mo⌂ete razlikovno ime koristiti za korisni⌂ki identitet koji zadovoljava provjeru autenti⌂nosti za kontroler domene. Razlikovno ime mo⌂ete koristiti za korisni⌂ki identitet koji EIM konfigurira za va⌂ iSeries poslu⌂itelj. Na primjer, mo⌂ete koristiti razlikovno ime kada radite sljede⌂e:

- Konfigurirate poslu⌂itelj direktorija da djeluje kao EIM kontroler domene. Ovo u⌂inite tako da kreirate i koristite razlikovno ime koje identificira LDAP administratora za poslu⌂itelja direktorija. Ako poslu⌂itelj direktorija nije prethodno konfiguriran, poslu⌂itelj direktorija mo⌂ete konfigurirati kada koristite ⌂arobnjaka EIM konfiguracije za kreiranje i spajanje nove domene.
- Koristite EIM ⌂arobnjaka konfiguracije za izbor tipa korisni⌂kog identiteta koji bi ⌂arobnjak trebao koristiti u povezivanju na kontroler EIM domene. Razlikovno ime je jedno od korisni⌂kih tipova koje izaberete. Razlikovno ime mora predstavljati korisnika koji ima ovla⌂tenja za kreiranje objekata u lokalnom prostoru imena poslu⌂itelja direktorija.
- Koristite EIM ⌂arobnjaka konfiguracije za izbor tipa korisnika za izvo⌂enje EIM operacija u ime funkcija operativnog sistema. Te operacije sadr⌂e operacije pregledavanja mapiranja i brisanje asocijacija prilikom brisanja lokalnog OS/400 korisni⌂kog profila. Razlikovno ime je jedno od korisni⌂kih tipova koje izaberete.
- Povezivanja na kontroler domene za administraciju EIM-a, na primjer, za upravljanje registrima i identifikatorima te za izvo⌂enje operacija pregledavanja mapiranja.
- Kreirajte filtere certifikata da biste odredili opseg asocijacije politike filtera certifikata. Kada kreirate filter certifikata, morate osigurati informacije razlikovnog imena za DN subjekt ili DN izdava⌂a ili certifikat za specificiranje kriterija koje filter koristi za odre⌂ivanje na koje certifikate utje⌂e asocijacija politike.

Da nau⌂ite vi⌂e o razlikovnim imenima i kako ih LDAP koristi, pogledajte Koncepti poslu⌂itelja direktorija.

Nadre⌂eno razlikovno ime

Nadre⌂eno razlikovno ime (DN) je unos u Lightweight Directory Access Protocola (LDAP) imenskom prostoru poslu⌂itelja direktorija. Unosi LDAP poslu⌂itelja svrstani su u hijerarhijskoj strukturi koja mo⌂e odra⌂avati politi⌂ke, geografske, organizacijske ili domenske granice. Razlikovno ime se smatra nadre⌂enim DN-om, kad je DN unos direktorija izravno superioran danom DN-u.

Primjer potpunog razlikovnog imena bilo bi cn=Tim Jones, o=IBM, c=US. Svaki unos ima barem jedan atribut koji se koristi za imenovanje unosa. Ovaj atribut imenovanja se zove relativno razlikovno ime (RDN) unosa. Unos iznad danog RDN-a se zove po njegovom nadre⌂enom razlikovnom imenu. U ovom primjeru, cn=Tim Jones imenuje unos, tako da je to RDN. o=IBM, c=US je nadre⌂eno DN za cn=Tim Jones.

EIM koristi poslu⌂itelj direktorija kao kontroler domene za pohranjivanje EIM podataka domene. Nadre⌂eni DN u kombinaciji s imenom EIM domene odre⌂uje smje⌂taj EIM podataka domene u imenskom prostoru poslu⌂itelja direktorija. Kada za kreiranje i spajanje na novu domenu koristite ⌂arobnjaka za EIM konfiguraciju, mo⌂ete izabrati da specificirate nadre⌂eni DN za domenu koju kreirate. Upotrebom nadre⌂enog DN-a mo⌂ete odrediti gdje u LDAP imenskom prostoru EIM podaci trebaju prebivati za domenu. Kada ne navedete nadre⌂eni DN, EIM podaci prebivaju na svom vlastitom sufiksu u imenskom prostoru i default lokacija EIM podataka domene je **ibm-eimDomainName=EIM**.

Da nau⌂ite vi⌂e o razlikovnim imenima i kako se ona koriste, pogledajte Koncepti poslu⌂itelja direktorija.

LDAP shema i ostala razmatranja za Mapiranje identiteta u poduze⌂u

Za V5R3, Mapiranje identiteta u poduze⌂u (EIM) zahtijeva da je kontroler domene smje⌂ten na poslu⌂itelju direktorija koji podr⌂ava verziju 3 Lightweight Directory Access Protocol (LDAP). Dodatno, proizvod poslu⌂itelja direktorija mora biti konfiguriran tako da prihva⌂a EIM shemu i razumije sljede⌂e atribute i klase objekta.

- Atribut ibm-entryUUID.

- ibmattributetypes:
  - acIEntry
  - acIPropagate
  - acISource
  - entryOwner
  - ownerPropagate
  - ownerSource
- EIM atributi, uklju⌂uju⌂i tri nova atributa za podr⌂ku asocijaciji politike:
  - ibm-eimAdditionalInformation
  - ibm-eimAdminUserAssoc
  - ibm-eimDomainName, ibm-eimDomainVersion,
  - ibm-eimRegistryAliases
  - ibm-eimRegistryEntryName
  - ibm-eimRegistryName
  - ibm-eimRegistryType
  - ibm-eimSourceUserAssoc
  - ibm-eimTargetIdAssoc
  - ibm-eimTargetUserName
  - ibm-eimUserAssoc
  - ibm-eimFilterType
  - ibm-eimFilterValue
  - ibm-eimPolicyStatus
- EIM klase objekta, uklju⌂uju⌂i tri nove klase za podr⌂ku asocijaciji politike:
  - ibm-eimApplicationRegistry
  - ibm-eimDomain
  - ibm-eimIdentifier
  - ibm-eimRegistry
  - ibm-eimRegistryUser
  - ibm-eimSourceRelationship
  - ibm-eimSystemRegsitry
  - ibm-eimTargetRelationship
  - ibm-eimFilterPolicy
  - ibm-eimDefaultPolicy
  - ibm-eimPolicyListAux

V5R3 verzija IBM Poslu⌂itelja direktorija za iSeries osigurava ovu podr⌂ku. Za vi⌂e informacija koji IBM poslu⌂itelj direktorija osigurava potrebnu podr⌂ku za EIM i kako nau⌂iti o ostalim razmatranjima za EIM kontrolere domene, pogledajte Planiranje EIM kontrolera domene.

Ako trenutno koristite poslu⌂itelja direktorija na V5R2 iSeries sistemu kao va⌂ EIM kontroler domene, morate a⌂urirati LDAP shemu i EIM podr⌂ku za ovaj poslu⌂itelj direktorija tako da ga mo⌂ete nastaviti koristiti za upravljanje V5R3 EIM podacima domene. Kako nau⌂iti vi⌂e o tome, pogledajte iSeries LDAP stranicu na IBM Web stranici.

iSeries koncepti za Mapiranje identiteta u poduze⌂u

Mo⌂ete implementirati Mapiranje identiteta u poduze⌂u (EIM) na bilo kojoj IBM @server platformi. Me⌂utim, kad implementirate EIM na iSeries poslu⌂itelju, trebate imati na umu da su odre⌂ene informacije specifi⌂ne za

implementaciju iSeries poslu⌂itelja. Pregledajte sljede⌂e informacije da nau⌂ite o OS/400 aplikacijama koje su omogu⌂ene za EIM, o razmatranjima za profile korisnika i drugim poglavljima koja vam mogu pomo⌂i da u⌂inkovito koristite EIM na iSeries sistemu:

- RazmatranjaOS/400 korisni⌂kog profila za EIM
- OS/400 revizija za EIM
- EIM omogu⌂ene aplikacije za OS/400

Razmatranja OS/400 korisni⌂kog profila za Mapiranje identiteta u poduze⌂u

Sposobnost izvo⌂enja zadataka u Mapiranju identiteta u poduze⌂u (EIM) se ne bazira na ovla⌂tenju va⌂eg OS/400 korisni⌂kog profila nego na va⌂em "EIM kontrola pristupa" na stranici 33 ovla⌂tenju. Svakako, postoje neki dodatni zadaci koji se trebaju izvesti za postavu OS/400 da koristi EIM. Ti dodatni zadaci zahtijevaju da imate OS/400 korisni⌂ki profil s odgovaraju⌂im posebnim ovla⌂tenjima.

Za postavu OS/400 da se koristi EIM-om upotrebom iSeries Navigatora, va⌂ korisni⌂ki profila treba imati sljede⌂a posebna ovla⌂tenja:

- Administrator sigurnosti (*SECADM).
- Svi objekti (*ALLOBJ).
- Sistemska konfiguracija (*IOSYSCFG).

Pobolj⌂anje naredbi OS/400 korisni⌂kog profila za EIM identifikatore

S jednom konfiguriranim EIM-om na va⌂em sistemu, mo⌂ete iskoristiti prednost novog parametra i za naredbu Kreiranje korisni⌂kog profila (CRTUSRPRF) i za naredbu Promjena korisni⌂kog profila (CHGUSRPRF), pod nazivom EIMASSOC. Ovaj parametar mo⌂ete koristiti za definiranje asocijacija EIM identifikatora za odre⌂eni korisni⌂ki profil lokalnog registra.

Kada koristite taj parametar, mo⌂ete specificirati sljede⌂e informacije:

- Ime EIM identifikatora, ⌂to mo⌂e biti novo ime ili ve⌂ postoje⌂e ime identifikatora.
- Opcijska akcija za asocijaciju ⌂to mo⌂e biti akcija dodavanja (*ADD), zamjene (*REPLACE) ili uklanjanja (*REMOVE) specificirane asocijacije.

  Bilješka: Koristite *ADD za postavu nove asocijacije. Koristite *REPLACE opciju, na primjer, ako ste prethodno definirali asocijacije krivim identifikatorom. Opcija *REPLACE uklanja sve postoje⌂e asocijacije specificiranog tipa za lokalni registar bilo kojih ostalih identifikatora i onda dodaje jednu asocijaciju koja je specificirana za parametar. Koristite *REMOVE opciju za uklanjanje svih specificiranih asocijacija iz specificiranog identifikatora.
- Tip asocijacije identifikatora, koji mo⌂e biti ciljni, izvorni ili i ciljni i izvorni ili je to administrativna asocijacija.
- Da li kreirati specificirani EIM identifikator ako ve⌂ ne postoji.

Obi⌂no kreirate ciljnu asocijaciju za OS/400 profil, posebno u okru⌂enju jednostruke prijave. Nakon ⌂to koristite naredbu kreiranja potrebne ciljne asocijacije za korisni⌂ki profil (i EIM identifikator ako je potrebno), mo⌂da trebate kreirati i odgovaraju⌂u izvornu asocijaciju. Mo⌂ete koristiti iSeries Navigatora za kreiranje izvorne asocijacije za drugi korisni⌂ki identitet kao Kerberos principal s kojim se korisnik prijavljuje na mre⌂u.

Kada ste konfigurirali EIM na sistemu, specificirali ste korisni⌂ki identitet i lozinku koju ⌂e sistem koristiti kada izvodi EIM operacije za operacijski sistem. Taj korisni⌂ki identitet ima ovla⌂tenje EIM kontrole pristupa dovoljno za kreiranje identifikatora i dodavanje asocijacija.

Lozinke OS/400 korisni⌂kog profila i EIM

Kao administratoru, primarni vam je cilj prilikom konfiguriranja EIM-a kao dio okru⌂enja jednostruke prijave smanjiti koli⌂inu upravljanja korisni⌂kim lozinkama ⌂to morate izvesti za tipi⌂ne krajnje korisnike u va⌂em poduze⌂u. Kori⌂tenjem mapiranja identiteta koje osigurava EIM u kombinaciji s Kerberos provjerom autenti⌂nosti, znate da ⌂e vam korisnici izvoditi manje prijava i pamtiti i upravljati manjim brojem lozinki. Od toga imate koristi, jer imate manji

broj poziva za rje⌂avanje problema od mapiranih korisni⌂kih identiteta kao ⌂to su pozivi za reset tih lozinki kada ih korisnici zaborave. Svakako, uloge lozinka sigurnosne politike su stalno djelotvorne i vi morate stalno upravljati tim korisni⌂kim profilima za korisnike kada god istekne lozinka.

Da bi dalje koristili prednost va⌂eg okru⌂enja jednostruke prijave, mogli biste razmotriti promjenu postavke lozinke za one korisni⌂ke profile koji su ciljevi mapiranja identiteta. Kao cilj mapiranja identiteta, korisnik vi⌂e ne treba osiguravati lozinku za korisni⌂ki profil kada pristupa iSeries sistemu ili EIM-omogu⌂enom OS/400 resursu. Za naj⌂e⌂⌂e korisnike, mo⌂ete promijeniti postavke lozinke na *NONE tako da se ne mora koristiti lozinka s korisni⌂kim profilom. Vlasnik korisni⌂kog profila vi⌂e ne treba lozinku zbog mapiranja identiteta i jednostruke prijave. Postavom lozinke na *NONE, koristite dalje prednost, jer vi ne morate i va⌂i korisnici ne moraju vi⌂e upravljati istekom lozinke; dodatno, nitko ne mo⌂e koristiti profil za izravnu prijavu na iSeries ili pristup EIM-omogu⌂enim OS/400 resursima. Me⌂utim, mo⌂da ⌂elite da administratori i dalje imaju vrijednost lozinke njihovih korisni⌂kih profila u slu⌂aju da se ikad zatrebaju izravno prijaviti na iSeries sistem. Na primjer, ako je va⌂ EIM kontroler domene uga⌂en i ne mo⌂e do⌂i do mapiranje identiteta, administrator bi ⌂elio biti sposoban izravno se prijaviti na iSeries sistem sve dok se problem s kontrolerom domene ne rije⌂i.

OS/400 revizija za Mapiranje identiteta u poduze⌂u

Va⌂no je uzeti u obzir koju reviziju obavljate za va⌂ ukupni sigurnosni plan. Kada konfigurirate i koristite Mapiranje identiteta u poduze⌂u (EIM), mo⌂da ⌂ete htjeti konfigurirati podr⌂ku za reviziju za direktorij poslu⌂itelja kako biste osigurali da vam se dobavi prikladna razina pouzdanosti koju va⌂a sigurnosna politika treba. Na primjer, podr⌂ka za reviziju mo⌂e biti korisna kod odre⌂ivanja koji je od korisnika, mapiran od strane asocijacije politike izveo akciju na va⌂em sistemu ili izmijenio objekt.

Da biste nau⌂ili vi⌂e o podr⌂ci za reviziju za IBM Poslu⌂itelja direktorija iSeries (LDAP), pogledajte pod Revizija u IBM Poslu⌂itelju direktorija u poglavlju iSeries (LDAP) Informacijskog Centra. Ove informacije tako⌂er osiguravaju prikladne reference na razmatranje OS/400 revizije i postavke koje trebate omogu⌂iti kako biste osigurali ispravnu konfiguraciju revizije poslu⌂itelja direktorija.

Aplikacije omogu⌂ene za Mapiranje identiteta u poduze⌂u za OS/400

Sljede⌂e se OS/400 aplikacije mogu konfigurirati da koriste Mapiranje identiteta u poduze⌂u (EIM):

- OS/400 host poslu⌂itelji (trenutno ih koristi iSeries Pristup za Windows i iSeries Navigator)
- Telnet Poslu⌂itelj (trenutno ga koriste PC5250 i IBM Websphere host po potrebi)
- QFileSrv.400 ODBC (dozvoljava kori⌂tenje jednostruke prijave preko SQL-a)
- JDBC (dozvoljava kori⌂tenje EIM-a preko SQL-a)
- Arhitektura Distribuirane Relacijske Baze Podataka (DRDA) (dozvoljava kori⌂tenje EIM-a preko SQL-a)
- IBM WebSphere Host On-Demand Verzija 8, (Web Express Logon funkcija)
- NetServer
- QFileSvr.400

Planiranje Mapiranja identiteta u poduze⌂u

Plan implementacije je bitan za uspje⌂no konfiguriranje i upotrebu Mapiranja identiteta u poduze⌂u (EIM) u va⌂em poduze⌂u. Da razvijete plan, morate skupiti podatke o sistemima, aplikacijama i korisnicima koji ⌂e koristiti EIM. Skupljene informacije ⌂ete koristiti za odluke o tome kako najbolje konfigurirati EIM za va⌂e poduze⌂e.

Budu⌂i da je EIM infrastruktura tehnologije IBM @server dostupna svim IBM platformama, kako planirate svoju implementaciju ovisi o tome koje se platforme nalaze u va⌂em poduze⌂u. Iako postoji mno⌂tvo aktivnosti planiranja koje su specifi⌂ne za svaku platformu, mnoge aktivnosti planiranja EIM-a odnose se na sve IBM platforme. Trebate raditi pomo⌂u uobi⌂ajenih aktivnosti planiranja EIM-a za kreiranje cijelog plana implementacije. Da nau⌂ite vi⌂e o tome kako planirati implementaciju EIM-a, pogledajte sljede⌂e stranice:

- Planiranje EIM-a za @server Pro⌂itajte ovaj materijal da biste razvili svoj cjelokupni plan implementacije EIM-a.

| • Planiranje EIM-a za OS/400 Pro⌂itajte ovaj materijal da biste razvili svoj cjelokupni plan za va⌂u OS/400 EIM
| implementaciju.

| Planiranje Mapiranja identiteta u poduze⌂u za eServer

| Plan implementacije je bitan za uspje⌂no konfiguriranje i upotrebu Mapiranja identiteta u poduze⌂u (EIM) u poduze⌂u
| s pomije⌂anim platformama. Za razvoj va⌂eg plana implementacije trebate skupiti podatke o sistemima, aplikacijama i
| korisnicima koji ⌂e koristiti EIM. Skupljene informacije ⌂ete koristiti za odluke o tome kako najbolje konfigurirati
| EIM u okru⌂enju s mije⌂anim platformama.

| Sljede⌂a lista dobavlja putokaz zadataka planiranja koje bi trebali dovr⌂iti prije konfiguriranja i kori⌂tenja EIM-a u
| okru⌂enju s mije⌂anim platformama. Prou⌂ite informacije na tim stranicama da nau⌂ite kako uspje⌂no planirati
| potrebe za va⌂u EIM konfiguraciju ⌂to uklju⌂uje osobine koje treba va⌂ tim za implementaciju, informacije koje
| trebate skupiti i odluke konfiguriranja koje trebate donijeti. Bit ⌂e vam od pomo⌂i ako ispi⌂ete radne tablice EIM
| planiranja (broj 8 na donjem popisu) tako da ih mo⌂ete dovr⌂iti kako prolazite kroz proces planiranja.

| 1. Zahtjevi EIM postava
| 2. Identifikacija potrebnih vje⌂tina, uloga i ovla⌂tenja
| 3. Planiranje EIM domene
| 4. Planiranje EIM kontrolera domene
| 5. Razvoj plana imenovanja za definiciju EIM registra
| 6. Razvoj plana EIM mapiranja identiteta
| 7. Razmatranja razvoja aplikacije
| 8. Radne tablice planiranja EIM implementacije

| Zahtjevi postava Mapiranja identiteta u poduze⌂u za eServer

| Za uspje⌂nu implementaciju EIM-a u va⌂e poduze⌂e, postoje tri skupa zahtjeva koje morate provjeriti da su
| zadovoljeni:

| 1. Zahtjevi na razini poduze⌂a ili mre⌂e
| 2. Sistemski zahtjevi
| 3. Zahtjevi aplikacije

| Zahtjevi na razini poduze⌂a ili mre⌂e

| Morate konfigurirati jedan sistem u va⌂em poduze⌂u ili mre⌂i tako da se pona⌂a kao EIM kontroler domene ⌂to je
| posebno konfigurirani Lightweight Directory Access Protocol (LDAP) poslu⌂itelj koji pohranjuje i dobavlja EIM
| podatke domene. Postoje brojna razmatranja kod izbora proizvoda za usluge direktorija za kori⌂tenje kao kontrolera
| domene, uklju⌂uju⌂i ⌂injenicu da ne osiguravaju svi proizvodi LDAP poslu⌂itelja podr⌂ku za EIM kontrolera
| domene.

| Drugo ⌂to se mora uzeti u obzir je dostupnost administracijskih alata. Jedna je opcija kori⌂tenje EIM API-ija u va⌂im
| vlastitim aplikacijama za obavljanje administrativnih funkcija. Ako za Poslu⌂itelja direktorija planirate koristiti iSeries
| (LDAP) proizvod kao EIM kontrolera domene, mo⌂ete koristiti iSeries Navigator za upravljanje EIM-om. Ako
| planirate koristiti proizvod IBM Direktorij, mo⌂ete koristiti eimadmin pomo⌂ni program koji je dio V1R4 LDAP SPE.

| Sljede⌂e informacije osiguravaju osnovne informacije o IBM platformama koje osiguravaju proizvod poslu⌂itelja
| direktorija koji podr⌂ava EIM. Detaljnije informacije o izboru poslu⌂itelja direktorija za osiguravanje podr⌂ke EIM
| kontroleru domene mo⌂ete prona⌂i pod Planiranje EIM kontrolera domene.

| Sistemski i aplikacijski zahtjevi

| Svaki sistem koji sudjeluje u EIM domeni mora zadovoljavati sljede⌂e uvjete:

| • Da ima instaliran LDAP klijentski softver.
| • Da ima implementirane EIM API-ije.

Svaka aplikacija koja ⌂e sudjelovati u EIM domeni mora mo⌂i koristiti EIM API-ije za izvo⌂enje operacija pregledavanja mapiranja i ostalih operacija.

Bilješka: U slu⌂aju distribuirane aplikacije, nije potrebno da i poslu⌂iteljska strana i klijentska strana trebaju biti sposobni koristiti EIM API-ije. Tipi⌂no, samo poslu⌂iteljska strana aplikacije treba mo⌂i koristiti EIM API-ije.

Sljede⌂a tablica sadr⌂i informacije o EIM podr⌂ci koju osiguravaju @server platforme. Informacije su organizirane po platformi sa stupcima koji imaju sljede⌂e zna⌂enje:

- EIM klijent koji je potreban platformi za podr⌂ku EIM API-ija.
- Tipovi EIM konfiguracijskih i administracijskih alata dostupnih za platformu.
- Proizvod poslu⌂itelja direktorija koji se mo⌂e instalirati za platformu kako bi slu⌂io kao EIM kontroler domene.

Platforma ne treba biti sposobna slu⌂iti kao EIM kontroler domene da bi sudjelovala u EIM domeni.

Tablica 9. eServer EIM podr⌂ka

Platforma	EIM klijent (API podr⌂ka)	Kontroler domene	EIM administracijski alati
AIX na pSeriesu	AIX R5.2	IBM Direktorij V5.1	Nedostupan
LINUX • SLES8 na PPC64 • Red Hat 7.3 na i386 • SLES7 na zSeries	Spustite jedno od sljede⌂eg: • IBM Direktorij V4.1 klijent • IBM Direktorij V5.1 klijent • Otvorite LDAP v2.0.23 klijenta	IBM Direktorij V5.1	Nedostupan
OS/400 na iSeriesu	OS/400 V5R2 i OS/400 V5R3	OS/400 V5R2 i V5R3 Poslu⌂itelj direktorija	iSeries Navigator V5R2 i V5R3
Windows 2000 na xSeries	Spustite jedno od sljede⌂eg: • IBM Direktorij V4.1 klijent • IBM Direktorij V5.1 klijent	IBM Direktorij V5.1 klijent	Nedostupan
z/OS na zSeriesu	z/OS V1R4 LDAP SPE OW57137	z/OS V1R4 LDAP	V1R4 LDAP SPE OW57137

Bilješka: Za vi⌂e informacija o proizvodu IBM Direktorij poslu⌂itelj pogledajte Web stranicuIBM Web proizvodi na http://www-3.ibm.com/software/network/help-directory/

Sve dok platforma osigurava EIM klijent (API) podr⌂ku da sistem mo⌂e sudjelovati u EIM domeni. Nije potrebno da platforma osigurava podr⌂ku EIM kontrolera domene sve dok ne ⌂elite koristiti ovu posebnu platformu kao EIM kontroler domene za va⌂e poduze⌂e.

Nakon ⌂to ste provjerili da su svi EIM zahtjevi ispunjeni, mo⌂ete po⌂eti identificirati potrebne karakteristike, uloge i ovla⌂tenja za konfiguraciju EIM-a.

Identificiranje potrebnih vje⌂tina i uloga

EIM je dizajniran tako da pojedina⌂na osoba mo⌂e lako biti odgovorna za konfiguraciju i administraciju u malenoj organizaciji. Ili u ve⌂im organizacijama, mo⌂da ⌂elite imati ve⌂i broj razli⌂itih pojedinaca koji rukuju tim odgovornostima. Broj ljudi koji trebate u va⌂em timu ovisi o broju zahtijevanih sposobnosti koje posjeduje svaki ⌂lan tima, o tipovima platformi koje su uklju⌂ene u va⌂u EIM implementaciju i o tome kako va⌂a organizacija ⌂eli podijeliti svoje sigurnosne uloge i odgovornosti.

Uspje⌂na EIM implementacija treba konfiguraciju i interakciju nekoliko softverskih proizvoda. Zato ⌂to svaki od tih proizvoda treba posebne sposobnosti i uloge, mo⌂ete se odlu⌂iti kreirati tim za EIM implementaciju koji se sastoji od ljudi iz nekoliko razli⌂itih podru⌂ja, naro⌂ito ako radite u velikoj organizaciji.

Sljede⌂e informacije opisuju sposobnosti i "EIM kontrola pristupa" na stranici 33 ovla⌂tenje potrebna za uspje⌂nu EIM implementaciju. Te sposobnosti su predstavljene u obliku naziva zanimanja za ljude koji su specijalizirani za te sposobnosti. Na primjer, zadatak koji tra⌂i Lightweight Directory Access Protocol (LDAP) osobine se odnosi na zadatak za administratora Poslu⌂itelja direktorija.

⌂lanovi tima i njihove uloge

Sljede⌂e informacije opisuju odgovornosti i potrebno ovla⌂tenje uloga koje su potrebne za upravljanje EIM-om. Mo⌂ete se koristiti ovom listom uloga kako bi odredili ⌂lanove tima koji su potrebni za instaliranje i konfiguriranje preduvjetnih proizvoda i za konfiguriranje EIM-a i jedne ili vi⌂e EIM domena.

Jedan od prvih skupova uloga koje trebate definirati je broj i tip administratora za va⌂u EIM domenu. Svo osoblje kojemu su dane EIM administrativne obaveze i ovla⌂tenje trebaju se uklju⌂iti u proces planiranja EIM-a kao ⌂lanovi tima za EIM implementaciju.

Bilješka: EIM administratori imaju va⌂nu ulogu u va⌂oj organizaciji i imaju takve ovlasti kao osobe da im je dozvoljeno kreiranje korisni⌂kih identiteta na va⌂im sistemima. Kada kreirate EIM asocijacije za korisni⌂ke identitete, oni odre⌂uju tko mo⌂e pristupiti va⌂im ra⌂unalnim sistemima i s kakvim povlasticama. IBM preporu⌂a da date ovo ovla⌂tenje onim osobama u koje imate visoku razinu povjerenja baziranu na sigurnosnoj politici va⌂eg poduze⌂a.

Sljede⌂a tablica ispisuje uloge potencijalnog ⌂lana tima i zadatke i potrebne sposobnosti za konfiguriranje i upravljanje EIM-om. Za vi⌂e detaljnih informacija o EIM administrativnim zadacima koje svaka uloga mo⌂e izvesti, pogledajte "EIM kontrola pristupa" na stranici 33.

Bilješka: Ako ⌂e neka osoba u va⌂oj organizaciji biti odgovorna za sve zadatke EIM konfiguriranja i administracije, toj bi se osobi trebala dati uloga i ovla⌂tenje EIM administratora.

Tablica 10. Uloge, zadaci i osobine za konfiguriranje EIM-a

Uloga	Ovla⌂teni zadaci	Potrebne osobine
EIM administrator	• Koordinacija operacija na domeni • Dodavanje, uklanjanje i mijenjanje definicija registra, EIM identifikatora i asocijacija za korisni⌂ke identitete • Kontroler ovla⌂tenja za podatke unutar EIM domene	Znanje o alatima za EIM administraciju
Administrator EIM identifikatora	• Kreiranje i mijenjanje EIM identifikatora • Dodavanje i uklanjanje administrativnih i izvornih asocijacija (ne mogu se dodati ili ukloniti ciljne asocijacije)	Znanje o alatima za EIM administraciju
Administrator EIM registara	Upravljanje svim definicijama EIM registra: • Dodavanje i uklanjanje ciljnih asocijacija (ne mogu se dodati ili ukloniti administrativne asocijacije) • A⌂uriranje definicija EIM registra	Znanje o: • Svim korisni⌂kim registrima definiranih u EIM domeni (kao ⌂to su informacije o korisni⌂kim identitetima) • Alatima EIM administracije

Tablica 10. Uloge, zadaci i osobine za konfiguriranje EIM-a (nastavak)

Uloga	Ovla⌂teni zadaci	Potrebne osobine
Administrator EIM registra X	Upravljanje odre⌂enom definicijom EIM registra: • Dodavanje i uklanjanje ciljnih asocijacija za odre⌂eni registar korisnika (na primjer, registar X) • A⌂uriranje odre⌂ene definicije EIM registra	Znanje o: • Posebnom korisni⌂kom registru definiranom u EIM domeni (kao ⌂to su informacije o korisni⌂kim identitetima) • Alatima EIM administracije
Administrator poslu⌂itelja direktorija (LDAP)	• Instaliranje i konfiguriranje poslu⌂itelja direktorija (ako je potrebno) • Prilagodba konfiguracije poslu⌂itelja direktorija za EIM • Kreiranje EIM domene (pogledati opasku) • Definiranje korisnika koji imaju ovla⌂tenje pristupa EIM kontroleru domene • Opcijski: Definiranje prvog EIM administratora **Bilješka:** Administrator poslu⌂itelja direktorija mo⌂e ⌂initi sve ⌂to mo⌂e i EIM administrator.	Znanje o: • Instaliranje, konfiguriranje i prilagodba poslu⌂itelja direktorija • EIM administracijski alati
Administrator registra korisnika	• Postavljanje korisni⌂kog profila ili korisni⌂kog identiteta za odre⌂eni registar korisnika • Opcijski: Slu⌂enje kao EIM administrator registra za odre⌂eni registar korisnika	Znanje o: • Alati za administraciju registra korisnika • EIM administracijski alati
Sistemski programer ili sistemski administrator	Instaliranje potrebnih softverskih proizvoda (uklju⌂uje i instaliranje EIM-a)	Znanje o: • Sistemsko programiranje i administracijske osobine • Instalacijske procedure za platformu
Programer aplikacije	Pisanje aplikacija koje koriste EIM API-ije	Znanje o: • Platforma • Programerske osobine • Kompiliranje programa

Nakon ⌂to ste odredili koje uloge ⌂elite koristiti za konfiguriranje i upravljanje EIM-om u va⌂em poduze⌂u, mo⌂ete planirati EIM domenu.

Planiranje domene Mapiranja identiteta u poduze⌂u

Dio po⌂etnog procesa planiranja implementacije Mapiranja identiteta u poduze⌂u (EIM) zahtijeva da definirate EIM domenu. Za postizanje maksimalne koristi od posjedovanja centraliziranog repozitorija informacija o mapiranju, trebate planirati domenu koja ⌂e biti dijeljena izme⌂u nekih aplikacija i sistema.

Kako prolazite kroz poglavlje o EIM planiranju, skupljat ⌂ete informacije koje trebate za definiranje domene i njihovo zapisivanje u radne tablice planiranja. U ovom poglavlju primjeri odlomaka iz radnih tablica vam mogu pomo⌂i kao vodi⌂i o skupljanju i zapisivanju informacija na svakom stupnju planiranja.

Sljede⌂a tablica ispisuje informacije koje trebate skupiti prilikom planiranja va⌂e domene i predla⌂e ulogu tima za EIM implementaciju ili uloge koje bi mogle biti odgovorne za svaku potrebnu stavku informacija.

Bilješka: Premda tablica ispisuje posebnu ulogu kao prijedlog za dodjelu odgovornosti za skupljanje opisanih informacija, trebali biste dodijeliti uloge bazirane na potrebama i sigurnosnoj politici va⌂e organizacije. Na primjer, u manjoj organizaciji preferirate imenovati pojedinu osobu za EIM administratora koja ⌂e biti odgovorna za sve aspekte planiranja, konfiguriranja i upravljanja EIM-om.

Tablica 11. Informacije potrebne za planiranje EIM domene

Potrebne informacije	Uloga
1. Da li ve⌂ postoji domena za upotrebu koja zadovoljava va⌂e potrebe ili je pak trebate kreirati.	EIM administrator
2. Koji ⌂e se posslu⌂itelj direktorija pona⌂ati kao EIM kontroler domene. (Pogledajte Planiranje EIM kontrolera domene za detaljne informacije o izboru kontrolera domene.)	Administrator poslu⌂itelja direktorija (LDAP) ili EIM administrator
3. Ime za domenu. (Tako⌂er mo⌂ete dobaviti opcijski opis.)	EIM administrator
4. Gdje u direktoriju pohraniti EIM podatke o domeni. **Bilješka:** Ovisno o va⌂em izboru sistema koji ⌂e biti host poslu⌂itelju direktorija i va⌂em izboru direktorija za pohranu podataka o EIM domeni, trebate izvesti neke zadatke konfiguriranja usluga direktorija prije no ⌂to kreirate domenu.	I administrator poslu⌂itelja direktorija (LDAP) i EIM administrator
5. Aplikacije i operacijski sistemi koji ⌂e sudjelovati u domeni. Ako konfigurirate va⌂u prvu domenu, ovaj po⌂etni skup se mo⌂e sastojati od samo jednog sistema. (Pogledajte Razvoj plana imenovanja za definiciju EIM registra za vi⌂e informacija.)	EIM tim
6. Ljudi i cjeline koji ⌂e sudjelovati u domeni. **Bilješka:** Kako bi olak⌂ali po⌂etno testiranje, mogli biste ograni⌂iti broj sudionika na jedan ili dva.	EIM tim

Sada kada razumijete ⌂to trebate za definiranje va⌂e EIM domene, mo⌂ete po⌂eti planirati EIM kontroler domene za pohranu podataka o EIM domeni.

Planiranje kontrolera domene Mapiranja identiteta u poduze⌂u

Kada skupite informacije za definiranje domene Mapiranja identiteta u poduze⌂u (EIM), trebate odrediti koji ⌂e se proizvod poslu⌂itelja direktorija pona⌂ati kao EIM kontroler domene. EIM zahtijeva da je kontroler domene smje⌂ten na poslu⌂itelju direktorija koji podr⌂ava verziju 3 Lightweight Directory Access Protocola (LDAP). Dodatno, proizvod poslu⌂itelja direktorija mora biti konfiguriran tako da prihva⌂a LDAP shemu i ostala razmatranja za EIM i razumije odre⌂ene atribute i objektne klase.

Ako va⌂e poduze⌂e posjeduje vi⌂e od jednog poslu⌂itelja direktorija koji mo⌂e biti host EIM kontroleru domene, trebali biste tako⌂er razmotriti da li koristiti sekundarno replicirane kontrolere domene. Na primjer, ako o⌂ekujete da ⌂ete imati veliki broj operacija EIM pregledavanja mapiranja, replike mogu poboljˆati performansu operacija pregledavanja.

Tako⌂er trebate razmotriti da li postaviti *lokalni* ili *udaljeni* kontroler domene u odnosu na sistem za koji se o⌂ekuje da ⌂e izvoditi najve⌂i broj operacija pregledavanja mapiranja. S lokalno postavljenim kontrolerom domene u odnosu na visoko optere⌂eni sistem, mo⌂ete poboljˆati performansu operacija pregledavanja na lokalnom sistemu. Koristite radne tablice za zapis tih odluka planiranja kao i one tablice koje ste napravili za informacije o va⌂oj domeni i ostale informacije o direktoriju.

Nakon ⌂to ste odredili koji ⌂e poslu⌂itelj direktorija u va⌂em poduze⌂u biti host va⌂em EIM kontroleru domene, trebate donijeti neke odluke o pristupu kontroleru domene.

Planiranje pristupa kontroleru domene

Trebate planirati kako ∆ete vi i EIM omogu∆ene aplikacije i operacijski sistemi pristupati posslu∆itelju direktorija koji je host EIM kontroleru domene. Za pristup EIM domeni trebate:

1. Biti sposobni vezati se na EIM kontrolera domene
2. Osigurati da je subjekt vezivanja ∆lan kontrolne grupe za EIM pristup ili LDAP administrator. Pogledajte Upravljanje kontrolom EIM pristupa za vi∆e informacija.

EIM API-iji podr∆avaju nekoliko razli∆itih mehanizama za uspostavu povezivanja, tako∆er poznati pod nazivom vezivanje, s EIM kontrolerom domene. Svaki tip mehanizma vezivanja omogu∆ava razli∆ite razine provjere autenti∆nosti i ∆ifriranje za povezivanje. Mogu∆i izbori su:

- **Jednostavna vezivanja** Jednostavno vezivanje je LDAP povezanost gdje LDAP klijent dobavlja razlikovno ime vezivanja i lozinku vezivanja LDAP poslu∆itelju za provjeru autenti∆nosti. Razlikovno ime vezivanja i lozinka su definirani od strane LDAP administratora u LDAP direktoriju. To je najslabiji oblik provjere autenti∆nosti i najmanje siguran, jer su razlikovno ime vezivanja i lozinka poslani poslu∆itelju bez ∆ifriranja i ranjivi su na tajno pra∆enje protoka informacija. Koristi se CRAM-MD5 (izazov-odgovor mehanizam provjere autenti∆nosti) za dodavanje pove∆avaju∆e razine za∆tite lozinke vezivanja. S CRAM-MD5 protokolom, klijent ∆alje raspr∆enu vrijednost umjesto ∆istog teksta lozinke poslu∆itelju za provjeru autenti∆nosti.
- **Provjera autenti∆nosti poslu∆itelja sa Slojem Sigurnih Uti∆nica (SSL) - provjera autenti∆nosti na strani poslu∆itelja** LDAP poslu∆itelj mo∆e biti konfiguriran za SSL ili Sigurnost Transportnog Sloja (TLS) povezivanja. LDAP poslu∆itelj koristi digitalni certifikat za provjeru autenti∆nosti poslu∆itelja na LDAP klijentu i uspostavlja sesiju ∆ifrirane komunikacije izme∆u njih. Po zna∆enju certifikata provjerava se autenti∆nost samo LDAP poslu∆itelja. Autenti∆nost krajnjeg korisnika se provjerava preko zna∆enja razlikovnog imena vezivanja i lozinke. Snaga provjere autenti∆nosti je ista kao i kod jednostavnog vezivanja samo ∆to se svi podaci (uklju∆uju∆i razlikovno ime vezivanja i lozinka) ∆ifriraju zbog privatnosti.
- **Provjera autenti∆nosti klijenta sa SSL-om** LDAP poslu∆itelj se mo∆e konfigurirati tako da zahtjeva provjeru autenti∆nosti krajnjeg korisnika preko zna∆enja digitalnog certifikata umjesto razlikovnog imena vezivanja i lozinke za SSL ili TLS sigurno povezivanje na LDAP poslu∆itelja. Provjerava se autenti∆nost i klijenta i poslu∆itelja, a sesija je ∆ifrirana. Ova opcija osigurava ja∆u razinu provjere autenti∆nosti korisnika i za∆titu privatnosti svi poslanih podataka.
- **Kerberos provjera autenti∆nosti** Mo∆e se provjeriti autenti∆nost LDAP klijenta na poslu∆itelju kori∆tenjem Kerberos ulaznice kao opcijska zamjena za razlikovno ime vezivanja i lozinke. (Kerberos), kao provjereni sistem mre∆ne provjere autenti∆nosti preko tre∆e strane, dozvoljava principalu (korisniku ili usluzi) da doka∆e svoj identitet drugoj usluzi unutar nesigurne mre∆e. Provjera autenti∆nosti principala se izvodi preko centraliziranog poslu∆itelja pod nazivom centar distribucije klju∆a (KDC). KDC provjerava korisnika s Kerberos ulaznicom. Te ulaznice dokazuju principalov identitet drugim uslugama na mre∆i. Nakon ∆to se provjerila autenti∆nost principala preko tih ulaznica, principal i usluga mogu izmjenjivati ∆ifrirane podatke s ciljnom uslugom. Ova opcija osigurava ja∆u razinu provjere autenti∆nosti korisnika i ∆titi privatnost informacija provjere autenti∆nosti.

Izbor mehanizama vezivanja ovisi o razini sigurnosti koju trebaju EIM-omogu∆ena aplikacija i mehanizmi provjere autenti∆nosti koje podr∆ava LDAP poslu∆itelj kao host EIM domeni.

Tako∆er, mo∆da trebate izvesti dodatne zadatke konfiguracije LDAP poslu∆itelja kako bi omogu∆ili mehanizam koji ste odlu∆ili koristiti. Provjerite dokumentaciju LDAP poslu∆itelja koji je host va∆em kontroleru domene kako bi odredili koje ostale konfiguracijske zadatke mo∆da trebate izvesti.

Primjer radne tablice planiranja: informacije o kontroleru domene

Nakon odluka koje ste donijeli o va∆em EIM kontroleru domene, upotrijebite radne tablice za zapis informacija o EIM kontroleru domene koje trebaju va∆i EIM-omogu∆eni operacijski sistemi i aplikacije. Informacije koje ste skupili kao dio ovog procesa mo∆e koristiti LDAP administrator za definiciju identiteta vezivanja aplikacije ili operacijskog sistema na LDAP poslu∆itelju direktorija koji je host EIM kontroleru domene.

Sljede∆i dio uzorka radnih tablica planiranja pokazuje tip informacija koje trebate skupiti. Tako∆er su uklju∆eni primjeri vrijednosti koje bi mogli koristiti prilikom konfiguracije EIM kontrolera domene.

Tablica 12. Domena i informacije o kontroleru domene za radnu tablicu EIM planiranja

Informacije potrebne za konfiguraciju EIM domene i kontrolera domene	**Primjeri odgovora**
Smisleno ime za domenu. To bi moglo biti ime poduze⌂a, odjela ili aplikacije koja koristi domenu.	MojaDomena
Opcijski: Ako konfigurirate EIM domenu u ve⌂ postoje⌂em LDAP direktoriju, specificirajte nadre⌂eno razlikovno ime za domenu. To je razlikovno ime koje predstavlja unos odmah iznad unosa imena va⌂e domene u stablastoj hijerarhiji informacija o direktoriju, na primjer, o=ibm,c=us.	o=ibm,c=us
Rezultiraju⌂e potpuno kvalificirano razlikovno ime EIM domene. To je potpuno definirano ime EIM domenu koje opisuje smje⌂taj direktorija za EIM podatke o domeni. Potpuno kvalificirano razlikovno ime domene se sastoji od barem DN-a za domenu (ibm-eimDomainName=), plus imena domene koje ste specificirali. Ako ste izabrali specifikaciju nadre⌂enog DN-a za domenu tada se potpuno kvalificirani DN domene sastoji od relativnog DN-a domene (ibm-eimDomainName=), imena domene (MyDomain) i nadre⌂enog DN-a (o=ibm,c=us). **Bilješka:**	Bilo ⌂to od sljede⌂eg, ovisno da li ste izabrali nadre⌂eni DN: • ibm-eimDomainName=MojaDomena • ibm-eimDomainName=MojaDomena,o=ibm,c=us
Adresa povezivanja za kontroler domene. Sastoji se od tipa povezivanja (osnovni ldap ili sigurni ldap, na primjer, ldap:// ili ldaps://) plus sljede⌂e informacije:	ldap://
• Opcijski: Host ime ili IP adresa • Opcijski: Broj porta	• some.ldap.host • 389
Rezultiraju⌂a potpuna adresa povezivanja za kontroler domene.	ldap://some.ldap.host:389
Mehanizam vezivanja potreban za aplikacije ili sisteme. Izbori uklju⌂uju: • Jednostavno vezivanje • CRAM MD5 • Provjera autenti⌂nosti poslu⌂itelja • Provjera autenti⌂nosti klijenta • Kerberos	Kerberos

Ako se va⌂ tim za EIM konfiguraciju i administraciju sastoji od vi⌂e ⌂lanova tima, trebat ⌂ete odrediti identitet vezivanja i mehanizam koji ⌂e koristiti svaki ⌂lan tima za pristup EIM domeni baziran na njegovoj ulozi. Tako⌂er, trebate odrediti identitet vezivanja i mehanizam za krajnje korisnike EIM aplikacije. Sljede⌂a bi vam radna tablica mogla pomo⌂i kao primjer skupljanja ovih informacija.

Tablica 13. Primjer radne tablice planiranja identiteta vezivanja

EIM ovla⌂tenje ili uloga	**Identitet vezivanja**	**Mehanizam vezivanja**	**Potreban razlog**
EIM administrator	eimadmin@krbrealm1.com	kerberos	EIM konfiguracija i upravljanje
LDAP administrator	cn=administrator	jednostavno vezivanje	konfiguracija EIM kontrolera domene
Administrator EIM registra X	cn=admin2	CRAM MD5	upravljanje odre⌂enom definicijom registra
EIM pregledavanje mapiranja	cn=MyApp,c=US	jednostavno vezivanje	izvo⌂enje operacija pregledavanja mapiranja aplikacije

Nakon ∆to ste skupili informacije potrebne za konfiguriranje va∆eg kontrolera domene, mo∆ete razviti plan mapiranja identiteta.

Razvoj plana imenovanja definicije registra za Mapiranje identiteta u poduze∆u

Da bi se kori∆tenjem Mapiranja identiteta u poduze∆u (EIM) mapirao korisni∆ki identitet iz jednog registra korisnika u ekvivalentan korisni∆ki identitet u drugom registru korisnika, oba registra korisnika moraju biti definirana u EIM-u. Trebate kreirati EIM definiciju registra za svaki korisni∆ki registar aplikacije ili operacijskog sistema koji ∆e sudjelovati u EIM domeni. Korisni∆ki registri mogu predstavljati registre operacijskog sistema kao ∆to je to Svojstvo kontrole pristupa resursu (RACF) ili OS/400, distribuirani registar kao ∆to je to Kerberos ili podskup sistemskog registra koji koristi isklju∆ivo neka aplikacija.

EIM domena mo∆e sadr∆avati definicije registra za korisni∆ke registre koji postoje na platformi. Na primjer, domena kojom upravlja kontroler domene na OS/400 mo∆e sadr∆avati definicije registra za ne-OS/400 platforme (kao ∆to je to AIX registar). Premda mo∆ete definirati bilo koji korisni∆ki registar na EIM domeni, definiraju se korisni∆ki registri za one aplikacije i operacijske sisteme koji su EIM-omogu∆eni.

Mo∆ete imenovati definiciju EIM registra kako god ∆elite sve dok je ime jedinstveno u EIM domeni. Na primjer, mo∆ete imenovati definiciju EIM registra na osnovu imena sistema koji je host korisni∆kom registru. Ako to nije dovoljno za razlikovanje definicija registra od sli∆nih definicija, mo∆ete koristiti to∆ku (.) ili podcrtavanje (_) za dodavanje tipa korisni∆kog registra koji definirate. Bez obzira na kriterije izabrane za kori∆tenje, trebali bi razmotriti razvoj konvencije imenovanja za va∆e definicije EIM registra. ∆ine∆i to osiguravate konzistentnost imena definicije po cijeloj domeni kao i prikladan opis tipa i instance definiranog korisni∆kog registra i njegovog kori∆tenja. Na primjer, mo∆ete izabrati ime svake definicije registra upotrebom kombinacije imena aplikacije ili operacijskog sistema koji koristi registar i fizi∆ke lokacije korisni∆kog registra u poduze∆u.

Aplikacija koja je napisana za kori∆tenje EIM-a mo∆e specificirati zamjensko ime izvornog registra ili zamjensko ime ciljnog registra ili zamjenska imena za oboje. Kada kreirate definicije EIM registra, trebate provjeriti dokumentaciju va∆ih aplikacija kako biste odredili da li trebate specificirati jedno ili vi∆e zamjenskih imena za definicije registra. Kada ova zamjenska imena dodijelite odgovaraju∆im definicijama registra, aplikacija mo∆e izvesti pregledavanje zamjenskog imena da bi prona∆la EIM definiciju registra ili definicije koje odgovaraju zamjenskim imenima u aplikaciji.

Sljede∆i vam dio primjera radne tablice planiranja mo∆e pomo∆i kao vodi∆ za kori∆tenje zapisivanja informacija o sudjelovanju korisni∆kih registara. Mo∆ete koristiti stvarnu radnu tablicu za specificiranje imena definicije registra za svaki korisni∆ki registar, za specificiranje da li koristi zamjensko ime i za opis i kori∆tenje lokacije korisni∆kog registra. Dokumentacija za instalaciju i konfiguraciju aplikacije ∆e osigurati neke informacije koje trebate za radnu tablicu.

Tablica 14. Primjer radne tablice planiranja informacija o definiciji EIM registra

Ime definicije registra	Tip korisni∆kog registra	Pseudonim definicije registra	Opis registra
Sistem_C	OS/400 sistemski korisni∆ki registar	Pogledajte dokumentaciju aplikacije	Glavni sistemski korisni∆ki registar za OS/400 Sistemu C
Sistem_A_WAS	WebSphere LTPA	app_23_alias_source	WebSphere LTPA korisni∆ki registar na Sistemu A
Sistem_B	Linux	Pogledajte dokumentaciju aplikacije	Linux korisni∆ki registar na Sistemu B
Sistem_A	OS/400 sistemski korisni∆ki registar	app_23_alias_target app_xx_alias_target	Glavni sistemski korisni∆ki registar za OS/400 Sistemu A
Sistem_D	Kerberos korisni∆ki registar	app_xx_alias_source	legal.mydomain.com Kerberos podru∆je
Sistem_4	Windows 2000 korisni∆ki registar	Pogledajte dokumentaciju aplikacije	Korisni∆ki registar aplikacije ljudskih resursa na Sistemu 4

Bilješka: Tipovi asocijacije za svaki registar ∆e se odrediti kasnije u procesu planiranja.

Nakon ∆to dovr∆ite ovu sekciju radne tablice planiranja, trebali biste razviti va∆ plan mapiranja identiteta kako bi odredili da li koristiti asocijacije identifikatora, asocijacije politike ili oba tipa asocijacija za kreiranje mapiranja koja trebate za korisni∆ke identitete u svakom definiranom korisni∆kom registru.

Razvijanje plana mapiranja identiteta

Za kriti∆ni dio po∆etnog procesa planiranja implementacije Mapiranja identiteta u poduze∆u (EIM) je potrebno odrediti kako ∆elite koristiti mapiranje identiteta u va∆em poduze∆u. Postoje dvije metode koje mo∆ete koristiti za mapiranje identiteta u EIM-u:

- **Asocijacije identifikatora** opisuju odnose izme∆u nekog EIM identifikatora i korisni∆kih identiteta u korisni∆kim registrima koji predstavljaju tu osobu. Asocijacija identifikatora kreira izravno jedan-prema-jedan mapiranje izme∆u nekog EIM identifikatora i odre∆enog korisni∆kog identiteta. Asocijacije identifikatora mo∆ete koristiti za indirektno definiranje odnosa izme∆u korisni∆kih identiteta upotrebom EIM identifikatora.

  Ako va∆a sigurnosna politika treba visok stupanj detaljne pouzdanosti, trebat ∆ete koristiti gotovo isklju∆ivo asocijacije identifikatora za va∆u implementaciju mapiranja identiteta. Zato ∆to koristite asocijacije identiteta za kreiranje jedan-prema-jedan mapiranja za korisni∆ke identitete koje korisnici posjeduju, mo∆i ∆ete uvijek odrediti to∆no tko je obavio akciju na nekom objektu ili na sistemu.
- **Asocijacije politike** opisuju odnos izme∆u vi∆estrukih korisni∆kih identiteta i pojedina∆nog korisni∆kog identiteta u korisni∆kom registru. Asocijacije politike koriste podr∆ku politike EIM mapiranja za kreiranje vi∆e-prema-jedan mapiranja izme∆u korisni∆kih identiteta bez uklju∆ivanja EIM identifikatora.

  Asocijacije politike mogu biti korisne kada imate jednu ili vi∆e velikih grupa korisnika koji trebaju pristup sistemima ili aplikacijama u va∆em poduze∆u, a pritom ne ∆elite da imaju odre∆ene korisni∆ke identitete za dobivanje tog pristupa. Na primjer, odr∆avate Web aplikaciju koja pristupa odre∆enoj internoj aplikaciji. Ne ∆elite pritom postaviti stotine ili tisu∆e korisni∆kih identiteta kako biste ovlastili korisnike za te interne aplikacije. U tom slu∆aju ∆elite konfigurirati mapiranje identiteta tako da su svi korisnici ove Web aplikacije mapirani u jedan korisni∆ki identitet s najmanjom razinom ovla∆tenja potrebnom za izvo∆enje aplikacije. Taj tip mapiranja identiteta mo∆ete napraviti kori∆tenjem asocijacija politike.

Mo∆da odlu∆ite koristiti asocijacije identifikatora kako biste osigurali najbolju kontrolu korisni∆kih identiteta u va∆em poduze∆u dobivaju∆i pritom visok stupanj upravljanja pojednostavljenom lozinkom. Ili odlu∆ite koristiti spoj asocijacija politike i asocijacija identifikatora za, tamo gdje je to prikladno, pojednostavljenu jednostruku prijavu, zadr∆avaju∆i odre∆enu kontrolu nad korisni∆kim identitetima za administratore. Bez obzira na tip mapiranja identiteta za koji ste odlu∆ili da najbolje odgovara va∆im poslovnim potrebama i da je prikladan za va∆u sigurnosnu politiku, trebate kreirati plan mapiranja kako biste osigurali prikladno implementiranje mapiranja identiteta.

Za kreiranje plana mapiranja identiteta, trebate u∆initi sljede∆e:

- “Razvoj plana imenovanja EIM identifikatora” na stranici 54
- “Planiranje asocijacija Mapiranja identiteta u poduze∆u”

Planiranje asocijacija Mapiranja identiteta u poduze∆u: Asocijacije su unosi koje kreirate u nekoj EIM domeni za definiranje odnosa izme∆u korisni∆kih identiteta u razli∆itim korisni∆kim registrima. U EIM-u mo∆ete kreirati jedan od dva tipa asocijacija: asocijacije identifikatora za definiranje jedan-prema-jedan mapiranja i asocijacije politika za definiranje vi∆e-prema-jedan mapiranja. Asocijacije politika mo∆ete koristiti umjesto ili u kombinaciji s asocijacijama identifikatora.

Odre∆eni tipovi asocijacija koje ste odlu∆ili kreirati ovise o tome kako korisnik koristi odre∆eni korisni∆ki identitet kao i o sveukupnom planu mapiranja identiteta.

Mo∆ete kreirati bilo koji od sljede∆ih tipova asocijacija identifikatora:

- **Ciljne asocijacije**

  Ciljne asocijacije se definiraju za korisnike koji u pravilu samo pristupaju ovom sistemu kao poslu∆itelju s nekog drugog klijentskog sistema. Ovaj se tip asocijacije koristi kada neka aplikacija izvodi operacije pregledavanja mapiranja.
- **Izvorne asocijacije**

Izvorne asocijacije se definiraju kada je korisni⌂ki identitet prvo ⌂to korisnik osigura za prijavu na sistemu ili mre⌂i. Ovaj se tip asocijacije koristi kada neka aplikacija izvodi operacije pregledavanja mapiranja.

- **Administrativne asocijacije**

  Administrativne se asocijacije definiraju kada se ⌂elite osposobiti za tra⌂enje ⌂injenice da korisni⌂ki identitet pripada odre⌂enom korisniku, a ne ⌂elite da korisni⌂ki identitet bude dostupan operacijama pregledavanja mapiranja. Mo⌂ete koristiti ovaj tip asocijacije za tra⌂enje svih korisni⌂kih identiteta koje osoba koristi u poduze⌂u.

Asocijacija politike uvijek definira ciljnu asocijaciju.

Mogu⌂e je da definicija jednostrukog registra ima vi⌂e od jednog tipa asocijacije ovisno o tome kako se koristi korisni⌂ki registar na koji se definicija odnosi. Premda ne postoje ograni⌂enja na broj ili kombinacije asocijacija koje mo⌂ete definirati, dr⌂ite broj na minimumu kako bi pojednostavili administraciju va⌂e EIM domene.

Obi⌂no ⌂e aplikacija osigurati upute o tome koje definicije registra o⌂ekuje za izvorne i ciljne registre, ali ne i za tipove asocijacija. Svaki krajnji korisnik aplikacije treba biti mapiran u aplikaciju s barem jednom asocijacijom. Ta asocijacija mo⌂e biti jedan-prema-jedan mapiranje izme⌂u njezinog jedinstvenog EIM identifikatora i korisni⌂kog identiteta u potrebnom ciljnom registru ili vi⌂e-prema-jedan mapiranje izme⌂u izvornog registra ⌂iji je korisni⌂ki identitet ⌂lan i potrebnog ciljnog registra. Koju asocijaciju koristite ovisi o zahtjevima mapiranja identiteta i kriterijima koja postavlja aplikacija.

Prethodno ste kao dio procesa planiranja popunili dvije radne tablice planiranja za korisni⌂ke identitete u va⌂oj organizaciji s informacijama o EIM identifikatorima i potrebnim EIM definicijama registra. Sada trebate spojiti te informacije specificiranjem tipova asocijacija koje ⌂elite koristiti za mapiranje korisni⌂kih identiteta u va⌂em poduze⌂u. Trebate odrediti da li definirati asocijaciju politike za odre⌂enu aplikaciju i njezin registar korisnika ili definirati odre⌂ene asocijacije identifikatora (izvorne, ciljne ili administrativne) za svaki korisni⌂ki identitet u sistemu ili registru aplikacije. To mo⌂ete u⌂initi zapisivanjem informacija o potrebnim tipovima asocijacije i u radnoj tablici planiranja definicije registra i u odgovaraju⌂im recima svake radne tablice asocijacija.

Za dovr⌂etak va⌂eg plana mapiranja identiteta, mo⌂ete koristiti sljede⌂i primjer radnih tablica kao vodi⌂ za pomo⌂ oko zapisivanja informacija o asocijacijama koje trebate za opis potpune slike o tome kako planirate implementirati mapiranje identiteta.

Tablica 15. Primjer radne tablice planiranja informacija o definiciji EIM registra

Ime definicije registra	Tip korisni⌂kog registra	Pseudonim definicije registra	Opis registra	Tipovi asocijacija
Sistem_C	OS/400 system korisni⌂ki registar	Pogledajte dokumentaciju aplikacije	Glavni sistemski korisni⌂ki registar za OS/400 Sistemu C	Ciljni
Sistem_A_WAS	WebSphere LTPA	app_23_alias_source	WebSphere LTPA korisni⌂ki registar na Sistemu A	Primarni izvor
Sistem_B	Linux	Pogledajte dokumentaciju aplikacije	Linux korisni⌂ki registar na Sistemu B	Izvorni i ciljni
Sistem_A	OS/400 system korisni⌂ki registar	app_23_alias_target app_xx_alias_target	Glavni sistemski korisni⌂ki registar za OS/400 Sistemu A	Ciljni
Sistem_D	Kerberos korisni⌂ki registar	app_xx_alias_source	legal.mydomain.com Kerberos podru⌂je	Izvorni
Sistem_4	Windows 2000 korisni⌂ki registar	Pogledajte dokumentaciju aplikacije	Korisni⌂ki registar aplikacije ljudskih resursa na Sistemu 4	Administrativni

Tablica 15. Primjer radne tablice planiranja informacija o definiciji EIM registra (nastavak)

Ime definicije registra	Tip korisni⌂kog registra	Pseudonim definicije registra	Opis registra	Tipovi asocijacija
order.mydomain.com	Windows 2000 korisni⌂ki registar		Glavni registar prijave za zaposlenike odjela nabave	Default politika registra (izvorni registar)
System_A_order_app	Aplikacija Odjela Nabave		Specifi⌂ni registar aplikacije za a⌂uriranja u nabavi	Default politika registra (ciljni registar)
System_C_order_app	Aplikacija Odjela Nabave		Specifi⌂ni registar aplikacije za a⌂uriranja u nabavi	Default politika registra (ciljni registar)

Tablica 16. Primjer radne tablice planiranja EIM identifikatora

Jedinstveno ime identifikatora	Opis identifikatora ili identiteta korisnika	Pseudonim identifikatora
John S Day	Upravitelj ljudskim resursima	app_23_admin
John J Day	Pravni Odjel	app_xx_admin
Sharon A. Jones	Administrator Odjela Nabave	

Tablica 17. Primjer radne tablice planiranja asocijacije identifikatora

Jedinstveno ime identifikatora: _____Ivan S Dan_____		
Korisni⌂ki registar	**Korisni⌂ki identitet**	**Tipovi asocijacija**
Sistem A WAS na Sistemu A	johnday	Izvorni
Linux na Sistemu B	jsd1	Izvorni i ciljni
OS/400 na Sistemu C	JOHND	Ciljni
Registar 4 na sistemu Windows 2000 za ljudske resurse	JDAY	Administrativni

Tablica 18. Primjer radne tablice planiranja za asocijacije politike

Tip asocijacije politike	Izvorni korisni⌂ki registar	Ciljni korisni⌂ki registar	Korisni⌂ki identitet	Opis
Default registar	order.mydomain.com	System_A_order_app	SYSUSERA	Mapira autenti⌂nog Windows korisnika odjela nabave u prikladan korisni⌂ki identitet aplikacije
Default registar	order.mydomain.com	System_C_order_app	SYSUSERB	Mapira autenti⌂nog Windows korisnika odjela nabave u prikladan korisni⌂ki identitet aplikacije

Razvoj plana imenovanja EIM identifikatora: Prilikom planiranja va⌂ih potreba EIM mapiranja identiteta, mo⌂ete kreirati jedinstvene EIM identifikatore za korisnike EIM omogu⌂enih aplikacija i operacijskih sistema u va⌂em poduze⌂u onda kada ⌂elite kreirati jedan-prema-jedan mapiranje izme⌂u korisni⌂kih identiteta za korisnika. Upotrebom asocijacija identifikatora za kreiranje jedan-prema-jedan mapiranja mo⌂ete maksimizirati koristi od upravljanja lozinkom koje omogu⌂ava EIM.

Plan imenovanja koji ste razvili ovisi o va⌂im poslovnim potrebama i preferencama; jedini zahtjev na imena EIM identifikatora je da budu jedinstveni. Neka poduze⌂a mogu preferirati kori⌂tenje potpunog i zakonitog imena za svaku osobu; druga poduze⌂a mogu preferirati kori⌂tenje drugog tipa podataka, kao npr. zaposleni⌂kog broja za svaku osobu. Ako ⌂elite kreirati imena EIM identifikatora bazirana na potpunom imenu svake osobe, mo⌂ete anticipirati mogu⌂e dupliciranje imena. Kako ⌂ete rukovati s potencijalnim duplim imenima identifikatora stvar je osobne preference. Mo⌂da biste ⌂eljeli rukovati svakim slu⌂ajem ru⌂no s dodavanjem predodre⌂enog niza znakova u svako ime identifikatora za osiguranje jedinstvenosti; na primjer mogli biste odlu⌂iti dodati broj odjela svake osobe.

Kao dio razvoja plana imenovanja EIM identifikatora, trebate se odlu⌂iti na ukupnom planu mapiranja identiteta. To vam mo⌂e pomo⌂i da odlu⌂ite kada trebate koristiti identifikatore i asocijacije identifikatora, a kada asocijacije politike za mapiranje identiteta unutar va⌂eg poduze⌂a. Za razvoj plana imenovanja EIM identifikatora, mo⌂ete koristiti dolje navedenu radnu tablicu za pomo⌂ prilikom skupljanja informacija o korisni⌂kim identitetima u va⌂oj organizaciji i planiranju EIM identifikatora za korisni⌂ke identitete. Radna tablica prikazuje vrstu informacija koju treba EIM administrator da bi saznao kada kreirati EIM identifikatore ili asocijacije politike za korisnike neke aplikacije.

Tablica 19. Primjer radne tablice planiranja EIM identifikatora

Jedinstveno ime identifikatora	**Opis identifikatora ili identiteta korisnika**	**Pseudonim identifikatora**
John S Day	Upravitelj ljudskim resursima	app_23_admin
John J Day	Pravni Odjel	app_xx_admin
Sharon A. Jones	Administrator Odjela Nabave	

Aplikacija koja koristi EIM mo⌂e navesti zamjensko ime koje koristi za pronalazak odgovaraju⌂eg EIM identifikatora za aplikaciju kojeg ista mo⌂e koristiti u zamjenu za odre⌂ivanje odre⌂enog korisni⌂kog identiteta koji ⌂e koristiti. Trebate provjeriti dokumentaciju va⌂ih aplikacija da odredite da li trebate specificirati jedno ili vi⌂e zamjenskih imena za identifikator. Opisna polja EIM identifikatora ili korisni⌂kog identiteta nemaju formu i mogu se koristiti za dobavu opisnih informacija o korisniku.

Ne trebate odjednom kreirati EIM identifikatore za sve ⌂lanove va⌂eg poduze⌂a. Nakon kreiranja po⌂etnog EIM identifikatora i njegovog kori⌂tenja za provjeru va⌂e EIM konfiguracije, mo⌂ete kreirati dodatne EIM identifikatore bazirane na ciljevima kori⌂tenja EIM-a u va⌂oj organizaciji. Na primjer, mo⌂ete dodati EIM identifikatore za podru⌂je odjela ili ⌂ire podru⌂je. Ili, mo⌂ete dodati EIM identifikatore kako podi⌂ete dodatne EIM aplikacije.

Nakon ⌂to skupite potrebne informacije za razvoj plana imenovanja EIM identifikatora, mo⌂ete planirati asocijacije za va⌂e korisni⌂ke identitete.

Radne tablice za planiranje implementacije Mapiranja identiteta u poduze⌂u

Dok ste radili s procesom planiranja Mapiranja identiteta u poduze⌂u (EIM), mogli ste primijetiti da je korisno kori⌂tenje tih radnih tablica za skupljanje informacija koje ⌂ete trebati za konfiguraciju i kori⌂tenje EIM-a u va⌂em poduze⌂u. Dani su prikladni primjeri dovr⌂enih odlomaka radnih tablica na stranicama za planiranje.

Te su radne tablice dane kao primjer tipova radnih tablica koje trebate za kreiranje va⌂eg plana EIM implementacije. Broj osiguranih unosa je manji od broja koji ⌂ete vjerojatno trebati za va⌂e EIM informacije. Mo⌂ete ure⌂ivati te radne tablice kako biste ih prilagodili va⌂oj situaciji.

Tablica 20. Radna tablica informacija o domeni i kontroleru domene

Informacije potrebne za konfiguraciju EIM domene i kontrolera domene	**Odgovori**
Smisleno ime za domenu. To bi moglo biti ime poduze⌂a, odjela ili aplikacije koja koristi domenu.	

Tablica 20. Radna tablica informacija o domeni i kontroleru domene (nastavak)

Informacije potrebne za konfiguraciju EIM domene i kontrolera domene	**Odgovori**
Opcijski: Razlikovno ime po nadre⌂enom za domenu. To je razlikovno ime koje predstavlja unos odmah iznad unosa imena va⌂e domene u stablastoj hijerarhiji informacija o direktoriju, na primjer, o=ibm,c=us.	
Rezultiraju⌂e potpuno kvalificirano razlikovno ime EIM domene. To je potpuno definirano ime EIM domenu koje opisuje smje⌂taj direktorija za EIM podatke o domeni. Potpuno kvalificirano razlikovno ime domene se sastoji od barem DN-a za domenu (ibm-eimDomainName=), plus imena domene koje ste specificirali. Ako ste izabrali specifikaciju nadre⌂enog DN-a za domenu tada se potpuno kvalificirani DN domene sastoji od relativnog DN-a domene (ibm-eimDomainName=), imena domene (MyDomain) i nadre⌂enog DN-a (o=ibm,c=us).	
Adresa povezivanja za kontroler domene. Sastoji se od tipa povezivanja (osnovni ldap ili sigurni ldap, na primjer, ldap:// ili ldaps://) plus sljede⌂e informacije:	
• Opcijski: Host ime ili IP adresa • Opcijski: Broj porta	
Rezultiraju⌂a potpuna adresa povezivanja za kontroler domene.	
Mehanizam vezivanja potreban za aplikacije ili sisteme. Izbori uklju⌂uju: • Jednostavno vezivanje • CRAM MD5 • Provjera autenti⌂nosti poslu⌂itelja • Provjera autenti⌂nosti klijenta • Kerberos	

Pogledajte Planiranje EIM kontrolera domene za primjer kako koristiti ovu radnu tablicu.

Tablica 21. Radna tablica za planiranje identiteta vezivanja

EIM ovla⌂tenje ili uloga	**Identitet vezivanja**	**Mehanizam vezivanja**	**Potreban razlog**

Pogledajte Planiranje EIM kontrolera domene za primjer kako koristiti ovu radnu tablicu.

Tablica 22. Radna tablica za planiranje informacija za definiranje EIM registra

Ime definicije registra	Tip korisni⌂kog registra	Pseudonim definicije registra	Opis registra	Tipovi asocijacija

Pogledajte Razvoj plana imenovanja za definiciju EIM kontrolera za primjer kako koristiti ovu radnu tablicu.

Tablica 23. Radna tablica za planiranje EIM identifikatora

Jedinstveno ime identifikatora	Opis identifikatora ili identiteta korisnika	Pseudonim identifikatora

Pogledajte Razvoj plana imenovanja za EIM identifikator za primjer kako koristiti ovu radnu tablicu.

Tablica 24. Radna tablica za planiranje asocijacije identifikatora

Jedinstveno ime identifikatora: _____Ivan S Dan_____		
Korisni⌂ki registar	**Korisni⌂ki identitet**	**Tipovi asocijacija**

Tablica 24. Radna tablica za planiranje asocijacije identifikatora (nastavak)

Jedinstveno ime identifikatora: _____Ivan S Dan_____		
Korisni⌂ki registar	**Korisni⌂ki identitet**	**Tipovi asocijacija**

Pogledajte Planiranje EIM asocijacija za primjer kako koristiti ovu radnu tablicu.

Tablica 25. Radna tablica za planiranje asocijacije politike

Tip asocijacije politike	**Izvorni korisni⌂ki registar**	**Ciljni korisni⌂ki registar**	**Korisni⌂ki identitet**	**Opis**

Pogledajte Planiranje EIM asocijacija za primjer kako koristiti ovu radnu tablicu.

Plan za razvoj aplikacije Mapiranja identiteta u poduze⌂u

Da bi aplikacija mogla koristiti Mapiranje identiteta u poduze⌂u (EIM) i sudjelovati u domeni, ista mora biti sposobna koristiti EIM API-ije. Trebali biste pregledati EIM API dokumentaciju i dokumentaciju o specifi⌂nosti platforme za EIM kako biste odredili da li postoji ikakva posebna razmatranja u planiranju koja trebate razumjeti kada pi⌂ete ili prilago⌂avate aplikacije koje koriste EIM API-ije. Na primjer, mogu postojati razmatranja prevo⌂enja i ostala razmatranja za C ili C++ aplikacije koje pozivaju EIM API-ije. Ovisno o platformi aplikacije, mogu postojati razmatranja vezivanja i ure⌂ivanja kao i ostala razmatranja.

Planiranje Mapiranje identiteta u poduze⌂u za OS/400

Postoje vi⌂estruke tehnologije i usluge koje objedinjuje Mapiranje identiteta u poduze⌂u (EIM) na iSeries poslu⌂itelju. Prije konfiguriranja EIM-a na va⌂em poslu⌂itelju, trebali biste odlu⌂iti koju funkcionalnost ⌂elite implementirati s upotrebom EIM-a i sposobnosti jednostruke prijave.

Prije implementiranje EIM-a trebali biste odlu⌂iti o osnovnim sigurnosnim zahtjevima za va⌂u mre⌂u i implementirati te sigurnosne mjere. EIM osigurava administratorima i korisnicima lak⌂e upravljanje identitetom kroz poduze⌂e. Kada se koristi s uslugom mre⌂ne provjere autenti⌂nosti, EIM osigurava sposobnosti jednostruke prijave za va⌂e poduze⌂e.

Da nau⌂ite vi⌂e o tome kako planirati va⌂u iSeries EIM konfiguraciju, pregledajte slijede⌂e informacije:

- "Preduvjeti EIM instalacije za iSeries"
- "Opcije potrebne za instalaciju iSeries Navigatora" na stranici 59
- "Razmatranja o kopiranju i obnavljanju Mapiranja identiteta u poduze⌂u" na stranici 59

Ako planirate koristiti Kerberos za provjeru autenti⌂nosti korisnika kao dio implementacije jednostruke prijave, trebali biste tako⌂er konfigurirati uslugu mre⌂ne provjere autenti⌂nosti. Pogledajte Planiranje usluge mre⌂ne provjere autenti⌂nosti za informacije o planiranju usluge mre⌂ne provjere autenti⌂nosti i Planiranje jednostruke prijave za informacije o planiranju okru⌂enja jednostruke prijave.

Preduvjeti EIM instalacije za iSeries

Slijede⌂a radna tablica za planiranje identificira usluge koje trebate instalirati prije konfiguriranja EIM-a.

Tablica 26. Radna tablica planiranja EIM instalacije

Radna tablica planiranja EIM preduvjeta	**Odgovori**
Je li va⌂ OS/400 V5R2 (5722-SS1) ili noviji?	

Tablica 26. Radna tablica planiranja EIM instalacije (nastavak)

Radna tablica planiranja EIM preduvjeta	Odgovori
Da li su sljede⌂e opcije i licencni proizvodi instalirani na iSeriesu™? • OS/400 Host Poslu⌂itelj (5722-SS1 Opcija 12) • iSeries Access za Windows® (5722-XE1) • Cryptographic Access Provider (5722-AC3) • Qshell Interpreter (5722-SS1 Option 30) Potreban ako namjeravate konfigurirati mre⌂nu uslugu provjere autenti⌂nosti kao i EIM.	
Je li iSeries Navigator instaliran na administratorovom PC-u, uklju⌂uju⌂i sljede⌂e podkomponente? • Sigurnost Neophodna ⌂elite li konfigurirati uslugu mre⌂ne provjere autenti⌂nosti kao i EIM. • Mre⌂a	
Jeste li instalirali zadnji uslu⌂ni paket iSeries Access za Windows? Pogledajte iSeries Access za zadnji uslu⌂ni paket.	
Ako je trenutno konfiguriran poslu⌂itelj direktorija, na primjer IBM Poslu⌂itelj direktorija za iSeries (LDAP) i ⌂elite ga koristiti kao EIM kontroler domene, znate li LDAP administratorsko ime (DN) i lozinku?	
Ako je trenutno konfiguriran poslu⌂itelj direktorija mo⌂e li se privremeno zaustaviti? (Ovo ⌂e biti potrebno za dovr⌂avanje EIM konfiguracijske obrade.)	
Imate li *SECADM, *ALLOBJ i *IOSYSCFG specijalna ovla⌂tenja?	
Jeste li primijenili zadnje privremene popravke programa (PTF-ove)?	

Opcije potrebne za instalaciju iSeries Navigatora

Za omogu⌂avanje okoline jednostruke prijave s EIM-om i uslugom mre⌂ne provjere autenti⌂nosti morate instalirati opciju **Mre⌂a** i opciju **Sigurnost** iSeries Navigatora. EIM je smje⌂ten unutar opcije **Mre⌂a**, a usluga mre⌂ne provjere autenti⌂nosti nalazi se u opciji **Sigurnost**. Ako ne planirate kori⌂tenje usluge mre⌂ne provjere autenti⌂nosti na va⌂oj mre⌂i, ne trebate instalirati opciju **Sigurnost** iSeries Navigatora.

Za instaliranje opcije Mre⌂a iSeries Navigatora ili za provjeru da je ta opcija trenutno instalirana, osigurajte da je iSeries Access za Windows instaliran na PC-u koji koristite za administriranje iSeries poslu⌂itelja.

Za instaliranje opcije **Mre⌂a**:

1. Kliknite **Start > Programi > IBM iSeries Access za Windows > Selektivan Postav**.
2. Pratite upute u dijalogu. U dijalogu **Izbor komponenti** pro⌂irite **iSeries Navigator** i zatim izaberite opciju **Mre⌂a**. Ako planirate koristiti usluge mre⌂ne provjere autenti⌂nosti, tako⌂er bi trebali izabrati opciju **Sigurnost**.
3. Nastavite s ostatkom **Selektivnog Postava**.

Razmatranja o kopiranju i obnavljanju Mapiranja identiteta u poduze⌂u

Trebate razviti plan kopiranja i obnavljanja va⌂ih podataka Mapiranja identiteta u poduze⌂u (EIM) kako biste osigurali za⌂titu va⌂ih EIM podataka i njihovu obnovu ako se ikada pojavi problem s poslu⌂iteljem direktorija koji je host EIM kontroleru domene. Postoje tako⌂er va⌂ne EIM informacije o konfiguraciji koje trebate za razumijevanje postupka obnove.

Kopiranje i obnova podataka EIM domene

Kako ⌂ete spremati va⌂e EIM podatke ovisi o tome kako ⌂ete odlu⌂iti upravljati ovim aspektom poslu⌂itelja koji se pona⌂a kao kontroler domene za va⌂e EIM podatke.

Jedan na⌂in za kopiranje podataka, posebno u svrhu obnavljanja iz katastrofa, je da spremite knji⌂nicu baze podataka. Po defaultu, to je QUSRDIRDB. Ako je changelog omogu⌂en, tada trebate tako⌂er spremiti knji⌂nicu QUSRDIRCL. Poslu⌂itelj direktorija na sistemu na kojem ⌂elite vratiti knji⌂nicu mora imati istu LDAP shemu i

konfiguraciju kao i originalni poslu∆itelj direktorija. Datoteke koje sadr∆e te informacije su u /QIBM/UserData/OS400/DirSrv. Dodatni podaci o konfiguraciji su pohranjeni u QUSRSYS/QGLDCFG (*USRSPC objekt) i QUSRSYS/QGLDVLDL (*VLDL objekt). Da bi imali potpunu sigurnosnu kopiju svega za va∆ poslu∆itelj direktorija, trebate spremiti obje knji∆nice, datoteke integriranog sistema datoteka i QUSRSYS objekte.

Mo∆ete pogledati pod Informacije o spremanju i vra∆anju Poslu∆itelja direktorija u IBM Poslu∆itelju direktorija u poglavlju iSeries (LDAP) Informacijskog Centra kako biste nau∆ili vi∆e o spremanju i vra∆anju va∆nih podataka poslu∆itelja direktorija.

Na primjer, mo∆ete koristiti LDIF datoteku za spremanje cijelog ili dijelova sadr∆aja poslu∆itelja direktorija. Za kopiranje informacija o domeni za IBM Poslu∆itelj direktorija za iSeries kontroler domene dovr∆ite ove korake:

- U iSeries Navigatoru, pro∆irite **Mre∆a > Poslu∆itelji > TCP/IP**.
- Desno kliknite na **IBM Poslu∆itelj direktorija**, izaberite **Alati**, tada izaberite **Eksport datoteke** za prikaz stranice koja vam dozvoljava specifikaciju dijelova sadr∆aja poslu∆itelja direktorija koje ∆elite eksportirati u datoteku.
- Prenesite eksportiranu datoteku na iSeries poslu∆itelj koji ∆elite koristiti kao va∆ rezervni poslu∆itelj direktorija.
- U iSeries Navigatoru na rezervnom poslu∆itelju, pro∆irite **Mre∆a > Poslu∆itelji > TCP/IP**.
- Desno kliknite na **IBM Poslu∆itelj direktorija**, izaberite **Alati**, tada izaberite **Import** za u∆itavanje sadr∆aja prenesene datoteke u novi poslu∆itelj direktorija.

Drugi na∆in koji mo∆ete uzeti u obzir prilikom spremanja va∆ih EIM podataka o domeni, je da konfigurirate i koristite kopiju poslu∆itelja direktorija. Sve promjene EIM podataka o domeni se automatski proslje∆uju kopiji poslu∆itelja direktorija, tako da ako poslu∆itelj direktorija koji je host kontrolera domene ne uspije ili izgubi EIM podatke, mo∆ete jo∆ uvijek dohvatiti podatke s kopije poslu∆itelja.

Kako ∆ete konfigurirati i koristiti kopiju poslu∆itelja direktorija mijenja se ovisno o tipu replikacijskog modela koji ste izabrali za kori∆tenje. Za vi∆e informacija o replikaciji i konfiguriranju poslu∆itelja direktorija za replikaciju, pogledajte Replikacija i Upravljanje replikacijom u IBM Poslu∆itelju direktorija u poglavlju iSeries (LDAP) Informacijski Centar.

Kopiranje i obnavljanje informacija EIM konfiguracije

Ako se va∆ sistem sru∆i, trebat ∆ete vratiti informacije o EIM konfiguraciji za taj sistem. Te se informacije ne mogu spremiti i vratiti lako izme∆u sistema.

Ove opcije su vam dostupne za spremanje i povrat EIM konfiguracije:

- Koristite naredbu Spremanje sigurnosnih podataka (SAVSECDTA) na svakom sistemu za spremanje EIM i ostalih va∆nih informacija o konfiguraciji. Tada vratite QSYS objekt profila korisnika na svaki sistem.

  Bilješka: Morate koristiti SAVSECDTA naredbu i vratiti QSYS objekt profila korisnika pojedina∆no na svaki sistem s EIM konfiguracijom. Mo∆ete nai∆i na probleme ako poku∆ate na nekom sistemu obnoviti QSYS objekt profila korisnika koji je bio spremljen na drugom sistemu.
- Ili ponovno izvedite EIM ∆arobnjaka konfiguracije ili ru∆no a∆urirajte svojstva foldera EIM Konfiguracije. Za olak∆anje ovog procesa, trebali biste spremiti va∆e radne tablice planiranja EIM implementacije ili zapisati informacije o EIM konfiguraciji za svaki sistem.

Dodatno, trebate razmotriti i planirati kako napraviti sigurnosno kopiranje i obnavljanje va∆ih podataka usluga mre∆ne provjere autenti∆nosti ako ste konfigurirali usluge mre∆ne provjere autenti∆nosti kao dio implementiranja okru∆enja pojedina∆ne prijave.

Konfiguriranje Mapiranja identiteta u poduze⌂u

| ⌂arobnjak EIM konfiguracije dozvoljava vam brzo i lako izvo⌂enje osnovne konfiguracije Mapiranja identiteta u
| poduze⌂u (EIM) za va⌂ iSeries. ⌂arobnjak vam osigurava tri opcije EIM sistemske konfiguracije. Kako ⌂ete koristiti
| ⌂arobnjaka za EIM konfiguraciju na odre⌂enom sistemu ovisi o ukupnom planu kori⌂tenja EIM-a u va⌂em poduze⌂u i
| va⌂im potrebama EIM konfiguracije. Na primjer, neki administratori ⌂ele koristiti EIM u spoju s uslugom mre⌂ne
| provjere autenti⌂nosti za kreiranje okru⌂enja jednostruke prijave preko vi⌂estrukih sistema i platformi bez potrebe za
| promjenom pripadaju⌂ih sigurnosnih politika. Konzekventno, ⌂arobnjak EIM konfiguracije vam dozvoljava
| konfiguraciju usluge mre⌂ne provjere autenti⌂nosti kao dio va⌂e EIM konfiguracije. Me⌂utim, konfiguriranje i
| kori⌂tenje usluge provjere autenti⌂nosti mre⌂e nije preduvjet ili zahtjev za konfiguriranje i kori⌂ten je EIM-a.

| Prije no ⌂to zapo⌂nete proces konfiguriranja EIM-a za jedan ili vi⌂e sistema, planirajte va⌂u EIM implementaciju za
| skupljanje potrebnih informacija. Na primjer, trebate odlu⌂iti o sljede⌂em:

- Koji iSeries poslu⌂itelj ⌂elite konfigurirati kao EIM kontrolera domene za EIM domenu? Prvo koristite ⌂arobnjaka EIM konfiguracije za kreiranje nove domene na ovom sistemu, nakon toga koristite ⌂arobnjaka za konfiguriranje svih dodatnih iSeries poslu⌂itelja koji ⌂e se priklju⌂iti toj domeni.
- Da li ⌂elite konfigurirati usluge mre⌂ne provjere autenti⌂nosti na svakom sistemu koji konfigurirate za EIM? Ako ⌂elite, mo⌂ete koristiti ⌂arobnjaka EIM konfiguracije za kreiranje osnovne konfiguracije usluga mre⌂ne provjere autenti⌂nosti na svakom iSeries poslu⌂itelju. Me⌂utim, morate izvesti ostale zadatke za dovr⌂enje va⌂e konfiguracije usluga mre⌂ne provjere autenti⌂nosti.

Nakon ⌂to ste koristili ⌂arobnjaka EIM konfiguracije za kreiranje osnovne konfiguracije za svaki iSeries poslu⌂itelj, postoji jo⌂ uvijek velik broj zadataka EIM konfiguracije koje morate izvesti prije no ⌂to dovr⌂ite EIM konfiguraciju. Pogledajte Scenarij: Omogu⌂avanje jednostruke prijave za primjer koji pokazuje kako je fiktivno poduze⌂e konfiguriralo okru⌂enje jednostruke prijave kori⌂tenjem usluge mre⌂ne provjere autenti⌂nosti i EIM-a.

Za konfiguraciju EIM-a, morate imate sva od sljede⌂ih posebnih ovla⌂tenja:

- Administrator sigurnosti (*SECADM).
- Svi objekti (*ALLOBJ).
- Sistemska konfiguracija (*IOSYSCFG).

| Prije no ⌂to koristite ⌂arobnjaka EIM konfiguracije, trebali biste izvesti sve “Planiranje Mapiranja identiteta u
| poduze⌂u” na stranici 43 korake za to⌂no odre⌂ivanje na⌂ina kori⌂tenja EIM-a. Ako konfigurirate EIM kao dio
| kreiranja okru⌂enja jednostruke prijave, tada bi trebali dovr⌂iti i sve korake planiranja jednostruke prijave.

| Kada dovr⌂ite va⌂ plan, mo⌂ete koristiti ⌂arobnjaka EIM konfiguracije za kreiranje jedne od tri osnovne EIM
| konfiguracije. Mo⌂ete koristiti ⌂arobnjaka za spajanje na postoje⌂u domenu ili za kreiranje i spajanje na novu domenu.
| Kada za kreiranje i spajanje na novu domenu koristite ⌂arobnjaka za EIM konfiguraciju, mo⌂ete izabrati da li
| konfigurirati EIM kontroler domene na lokalnom ili na udaljenom sistemu. Sljede⌂e informacije dobavljaju upute za
| konfiguriranje EIM-a bazirane na potrebnom tipu osnovne EIM konfiguracije:

> **“Kreiranje i spajanje nove lokalne domene” na stranici 62** Izaberite ovaj zadatak za kreiranje nove EIM domene za va⌂e poduze⌂e i za konfiguriranje lokalnog poslu⌂itelja direktorija koji bi bio EIM kontroler domene za novu domenu. Tako⌂er, ako Kerberos nije trenutno konfiguriran na iSeries poslu⌂itelju, pojavi se ⌂arobnjakov prompt za lansiranje ⌂arobnjaka za Konfiguraciju Usluga mre⌂ne provjere autenti⌂nosti. Nakon ⌂to dovr⌂ite taj zadatak, mo⌂ete konfigurirati ostale iSeries poslu⌂itelje koji ⌂e se spojiti na domenu. Za konfiguriranje ostalih poslu⌂itelja koji ⌂e sudjelovati u domeni, pove⌂ite se na svakog od njih i koristite ⌂arobnjaka EIM konfiguracije za konfiguraciju spajanja poslu⌂itelja na postoje⌂u EIM domenu.
>
> **“Kreiranje i spajanje nove udaljene domene” na stranici 66** Izaberite ovaj zadatak za kreiranje nove EIM domene za va⌂e poduze⌂e i za konfiguriranje udaljenog poslu⌂itelja direktorija koji bi bio EIM kontroler domene za novu domenu. Tako⌂er, ako Kerberos nije trenutno konfiguriran na iSeries poslu⌂itelju, pojavi se ⌂arobnjakov prompt za lansiranje ⌂arobnjaka za Konfiguraciju Usluga mre⌂ne provjere autenti⌂nosti. Nakon ⌂to dovr⌂ite taj zadatak, mo⌂ete konfigurirati ostale iSeries poslu⌂itelje koji ⌂e se spojiti na domenu. Za

konfiguriranje ostalih poslu⌂itelja koji ⌂e sudjelovati u domeni, pove⌂ite se na svakog od njih i koristite ⌂arobnjaka EIM konfiguracije za konfiguraciju spajanja poslu⌂itelja na postoje⌂u EIM domenu.

“Pristup postoje⌂oj domeni” na stranici 72 Kada jednom koristite ⌂arobnjaka EIM konfiguracije na jednom iSeries sistemu za konfiguraciju kontrolera domene i kreirate EIM domenu, izaberite ovaj zadatak ⌂arobnjaka za konfiguriranje iSeries poslu⌂itelja koji ⌂e sudjelovati u domeni. Trebate pokrenuti ⌂arobnjaka i dovr⌂iti ovaj zadatak na svakom iSeries poslu⌂itelju u mre⌂i koja ⌂e koristiti EIM. Morate dobaviti informacije o domeni na koju se spajate, uklju⌂uju⌂i informacije povezivanja (kao ⌂to su to broj porta i da li koristiti Sigurnost Transportnog Sloja (TLS) ili Sloj sigurnih uti⌂nica (SSL) za EIM kontroler domene). Ako Kerberos nije trenutno konfiguriran na iSeries poslu⌂itelju, pojavi se ⌂arobnjakov prompt za lansiranje ⌂arobnjaka za Konfiguraciju Usluga mre⌂ne provjere autenti⌂nosti.

Kako pristupiti ⌂arobnjaku EIM konfiguracije

Za pristup EIM Konfiguracijskom ⌂arobnjaku, pratite ove korake:

1. Pokrenite iSeries Navigator.
2. Prijavite se na iSeries poslu⌂itelj na kojem ⌂elite konfigurirati EIM. Ako konfigurirate EIM za vi⌂e od jednog iSeries poslu⌂itelja, zapo⌂nite s onim na kojem ⌂elite konfigurirati kontroler domene za EIM.
3. Pro⌂irite **Mre⌂a → Mapiranje identiteta u poduze⌂u**.
4. Desno kliknite **Konfiguracija** i izaberite **Konfiguriraj...** za lansiranje EIM Konfiguracijskog ⌂arobnjaka.
5. Izaberite opciju EIM konfiguracije i slijedite upute koje osigurava ⌂arobnjak za dovr⌂etak ⌂arobnjaka.
6. Ako je potrebno kliknite **Pomo⌂** da odredite koje informacije specificirati kako prolazite kroz ⌂arobnjaka.

Kreiranje i spajanje nove lokalne domene

| Kada za kreiranje i spajanje na novu domenu koristite ⌂arobnjaka za EIM konfiguraciju, mo⌂ete izabrati da li
| konfigurirati EIM kontroler domene na lokalnom sistemu kao dio kreiranja va⌂e EIM konfiguracije. Ako je potrebno
| ⌂arobnjak EIM konfiguracije osigurava da vi dobavite osnovne konfiguracijske informacije za poslu⌂itelja direktorija.
| Tako⌂er, ako Kerberos nije trenutno konfiguriran na iSeries poslu⌂itelju, pojavi se ⌂arobnjakov prompt za lansiranje
| ⌂arobnjaka za Konfiguraciju Usluga mre⌂ne provjere autenti⌂nosti.

| Kada zavr⌂ite s ⌂arobnjakom EIM konfiguracije, mo⌂ete obaviti sljede⌂e zadatke:

| • Kreirati novu EIM domenu.
| • Konfigurirati lokalnog poslu⌂itelja direktorija da djeluje kao EIM kontroler domene.
| • Konfigurirati uslugu mre⌂ne provjere autenti⌂nosti za sistem.
| • Kreirati definicije EIM registra za lokalni registar OS/400 i Kerberos registar.
| • Konfigurirati sistem da sudjeluje u novoj EIM domeni.

Da konfigurirate va⌂ sistem za kreiranje i spajanje na novu EIM domenu, morate imati sva od sljede⌂ih posebnih ovla⌂tenja:

- Administrator sigurnosti (*SECADM).
- Svi objekti (*ALLOBJ).
- Sistemska konfiguracija (*IOSYSCFG).

Da koristite ⌂arobnjaka EIM konfiguracije za kreiranje i spajanje na novu lokalnu domenu, izvedite sljede⌂e korake:

1. U iSeries Navigatoru izaberite sistem za koji ⌂elite konfigurirati EIM i pro⌂irite **Mre⌂a > Mapiranje identiteta u poduze⌂u**.
2. Desno kliknite **Konfiguracija** i izaberite **Konfiguriraj...** da pokrenete ⌂arobnjaka EIM konfiguracije.

   Bilješka: Ova opcija je ozna⌂ena kao **Rekonfiguriraj...** ako je EIM prethodno konfiguriran na sistemu.
3. Na stranici ⌂arobnjaka **Dobro do⌂li!**, izaberite **Kreiranje i spajanje nove domene** i kliknite **Sljede⌂e**.

4. Na stranici **Specificiranje lokacije EIM domene**, izaberite **Na lokalnom poslu⌂itelju direktorija** i kliknite **Sljede⌂e**.

   Bilješka: Ova opcija konfigurira lokalnog poslu⌂itelja direktorija da djeluje kao EIM kontroler domene. Zato ⌂to ovaj poslu⌂itelj direktorija pohranjuje sve EIM podatke za domenu, on mora biti aktivan i ostati aktivan za podr⌂ku EIM pregledavanju mapiranja i ostale operacije.

   Bilješka: Ako usluga mre⌂ne provjere autenti⌂nosti nije trenutno konfigurirana na iSeries poslu⌂itelju ili su potrebne dodatne informacije za mre⌂nu provjeru autenti⌂nosti za konfiguriranje okru⌂enja jednostruke prijave, prikazuje se stranica **Konfiguracija Usluga Mre⌂ne Provjere Autenti⌂nosti**. Ova vam stranica omogu⌂uje pokretanje ⌂arobnjaka Konfiguracije Usluga mre⌂ne provjere autenti⌂nosti tako da mo⌂ete konfigurirati uslugu mre⌂ne provjere autenti⌂nosti. Ili Usluge mre⌂ne provjere autenti⌂nosti mo⌂ete konfigurirati kasnije upotrebom ⌂arobnjaka konfiguracije tih usluga pomo⌂u iSeries Navigatora. Kada dovr⌂ite konfiguraciju usluga mre⌂ne provjere autenti⌂nosti, nastavlja se EIM Konfiguracijski ⌂arobnjak.

5. Da konfigurirate usluge mre⌂ne provjere autenti⌂nosti, izvedite sljede⌂e korake:
   a. Na stranici **Konfiguracija Usluga mre⌂ne provjere autenti⌂nosti** izaberite **Da** da pokrenete ⌂arobnjaka Konfiguracije Usluga mre⌂ne provjere autenti⌂nosti. S ovim ⌂arobnjakom, mo⌂ete konfigurirati nekoliko OS/400 su⌂elja i usluga da sudjelujete u Kerberos podru⌂ju kao i konfigurirati okru⌂enje jednostruke prijave koje koristi EIM i usluge mre⌂ne provjere autenti⌂nosti.
   b. Na stranici **Specificiranje informacija podru⌂ja** navedite ime default podru⌂ja u polju **Default podru⌂je**. Ako koristite Microsoft Aktivni direktorij za Kerberos provjeru autenti⌂nosti izaberite **Microsoft Aktivni direktorij se koristi za Kerberos provjeru autenti⌂nosti** i kliknite **Sljede⌂e**.
   c. Na stranici **Specificiranje KDC informacija** navedite puno ispravno ime Kerberos poslu⌂itelja za ovo podru⌂je u **KDC** polju, navedite 88 u polju **Port**, a zatim kliknite **Sljede⌂e**.
   d. Na stranici **Specificiranje informacija lozinke poslu⌂itelja** izaberite ili **Da** ili **Ne** za postavljanje lozinke poslu⌂itelja. Poslu⌂itelj lozinki dozvoljava principalima mijenjanje lozinke na Kerberos poslu⌂itelju. Ako izaberete **Da**, unesite ime poslu⌂itelja lozinke u polje **Poslu⌂itelj lozinke**. U polju **Port** prihvatite default vrijednost 464, a zatim kliknite Sljede⌂e.
   e. Na stranici **Izbor unosa tablice klju⌂eva** izaberite **OS/400 Kerberos provjera autenti⌂nosti**, a zatim kliknite **Sljede⌂e**.

      Bilješka: Tako⌂er mo⌂ete kreirati unose tablice klju⌂eva za IBM poslu⌂itelj direktorija za iSeries (LDAP), iSeries NetServer i iSeries HTTP poslu⌂itelj ako ⌂elite da ove usluge koriste Kerberos provjeru autenti⌂nosti. Mo⌂da ⌂ete trebati dodatno konfigurirati ove usluge da bi mogle koristiti Kerberos provjeru autenti⌂nosti.

   f. Na stranici **Kreiranje OS/400 unosa tablice klju⌂eva** unesite i potvrdite lozinku, a zatim kliknite **Sljede⌂e**. Ovo je ista lozinka koju ⌂ete koristiti kada u Kerberos poslu⌂itelj dodate OS/400 principale.
   g. Na stranici **Kreiranje Paketne Datoteke** izaberite **Da**, navedite sljede⌂e informacije i kliknite **Sljede⌂e**:
      - U polju **Paketna datoteka** a⌂urirajte stazu direktorija. Kliknite **Pregled** da biste prona⌂li odgovaraju⌂u stazu direktorija ili u polju **Paketna datoteka** uredili stazu.
      - U polju **Uklju⌂i lozinku** izaberite **Da**. Ovo osigurava da su sve lozinke koje su pridru⌂ene principalima OS/400 usluge sadr⌂ane u paketnoj datoteci. Va⌂no je primijetiti da su lozinke prikazane u ⌂istom tekstu i da ih mo⌂e pro⌂itati bilo tko tko ima dozvolu za ⌂itanje paketne datoteke. Prema tome, bitno je da paketnu datoteku izbri⌂ete s Kerberos poslu⌂itelja i s PC-ja odmah nakon njene upotrebe. Ako lozinku ne uklju⌂ite, ona ⌂e se od vas zatra⌂iti prilikom pokretanja paketne datoteke.

        Bilješka: Tako⌂er mo⌂ete ru⌂no dodati principale usluge koje generira ⌂arobnjak u Microsoft Aktivnom direktoriju. Da biste nau⌂ili kako to u⌂initi, pogledajte Dodavanje OS/400 principala u Kerberos poslu⌂itelj

      - Na stranici **Sa⌂etak** pregledajte pojedinosti konfiguracije usluge mre⌂ne provjere autenti⌂nosti, a zatim kliknite **Zavr⌂i** da biste se vratili u ⌂arobnjak EIM konfiguracije.

6. Ako lokalni poslu⌂itelj direktorija nije trenutno konfiguriran, prikazuje se stranica **Konfiguriraj Poslu⌂itelja direktorija** kada ⌂arobnjak EIM konfiguracije ponovo zapo⌂ne. Osigurajte sljede⌂e informacije za konfiguraciju lokalnog poslu⌂itelja direktorija:

   Bilješka: Ako konfigurirate lokalnog poslu⌂itelja direktorija prije kori⌂tenja ⌂arobnjaka EIM konfiguracije, prikazuje se stranica **Specificiranje korisnika za Povezivanje** umjesto ⌂arobnjaka. Koristite ovu stranicu za specifikaciju razlikovnog imena i lozinke za LDAP administratora kako bi osigurali da ⌂arobnjak ima dovoljno ovla⌂tenje za administraciju EIM domene i objekata u njoj i nastavite sa sljede⌂im korakom u ovoj proceduri. Ako je potrebno kliknite **Pomo⌂** da odredite koje informacije osigurati za ovu stranicu.

   - U polju **Port** prihvatite default broj porta 389 ili specificirajte drugi broj porta koji se koristi za nesigurne EIM komunikacije s poslu⌂iteljem direktorija.
   - U polju **Razlikovno ime** navedite LDAP razlikovno ime (DN) koje identificira LDAP administratora za poslu⌂itelja direktorija. ⌂arobnjak EIM konfiguracije kreira taj DN LDAP administratora i koristi ga za konfiguraciju poslu⌂itelja direktorija kao kontrolera domene za novu domenu koju kreirate.
   - U polju **Lozinka**, specificirajte lozinku za LDAP administratora.
   - U polju **Potvrda lozinke** drugi put navedite lozinku za svrhu provjere valjanosti.
   - Kliknite **Sljede⌂e**.

7. Na stranici **Specificiranje domene** , osigurajte sljede⌂e informacije:
   - U polju **Domena** specificirajte ime EIM domene koju ⌂elite kreirati. Prihvatite defaultno ime EIM ili upotrijebite bilo koji niz znakova koji vam imaju smisla. Svakako ne mo⌂ete koristiti posebne znakove kao ⌂to su to **= + < > , # ;** \ i *****.
   - U polju **Opis** unesite tekst za opis domene.
   - Kliknite **Sljede⌂e**.

8. Na stranici **Specificiranje nadre⌂enog DN-a za domenu** izaberite **Da** za specifikaciju nadre⌂enog DN-a za domenu koju kreirate ili specificirajte **Ne** da imate EIM podatke pohranjene na lokaciji direktorija sa sufiksom ⌂ije je ime izvedeno iz imena EIM domene.

   Bilješka: Kada kreirate domenu na lokalnom poslu⌂itelju direktorija, nadre⌂eni DN je opcija. Specificiranjem nadre⌂enog DN-a, mo⌂ete specificirati gdje se trebaju nalaziti EIM podaci u lokalnom LDAP imenskom prostoru. Kada ne trebate specificirati nadre⌂eni DN, EIM podaci se nalaze u svom vlastitom sufiksu u imenskom prostoru. Ako izaberete **Da**, koristite ku⌂icu s popisom u izboru lokalnog LDAP sufiksa za upotrebu kao nadre⌂enog DN-a ili unesite tekst za kreiranje i imenovanje novog nadre⌂enog DN-a. Nije potrebno specificirati nadre⌂eni DN nove domene. Kliknite **Pomo⌂** za dodatne informacije o kori⌂tenju nadre⌂enog DN-a.

9. Na stranici **Informacije registra** navedite treba li dodati lokalne korisni⌂ke registre u EIM domenu kao definicije registra. Izaberite jedan ili oboje od ovih korisni⌂kih tipova registra:

   Bilješka: U ovom trenutku ne morate kreirati definicije registra. Ako kasnije izaberete kreirati definicije registra, morate dodati sistemske definicije registra i a⌂urirati EIM konfiguracijska svojstva.

   - Izaberite **Lokalni OS/400** da dodate definiciju registra za lokalni registar. U navedenom polju, prihvatite default vrijednost imena definicije registra ili navedite drugu vrijednost imena definicije registra. Ime EIM registra je proizvoljan niz znakova koji predstavlja tip registra i specifi⌂nu instancu tog registra.
   - Izaberite **Kerberos** da dodate definiciju registra za Kerberos registar. U navedenom polju, prihvatite default vrijednost imena definicije registra ili navedite drugu vrijednost imena definicije registra. Default ime definicije registra isto je kao i ime podru⌂ja. Prihva⌂anjem default imena i upotrebom istog imena Kerberos registra kao imena podru⌂ja, mo⌂ete pove⌂ati performansu pri dohva⌂anju informacija iz registra. Ako je potrebno, izaberite **Kerberos korisni⌂ki identiteti osjetljivi su na velika i mala slova**.
   - Kliknite **Sljede⌂e**.

10. Na stranici **Specificiranje EIM sistemskog korisnika** izaberite **Tip korisnika** kojeg ⌂elite da sistem koristi kada izvodi EIM operacije za funkcije operativnog sistema. Te operacije uklju⌂uju operacije pregledavanja mapiranja i brisanje asocijacija prilikom brisanja lokalnog OS/400 korisni⌂kog profila. Mo⌂ete izabrati jedan od sljede⌂ih

korisni⌂kih tipova: **Razlikovno ime i lozinka**, **Kerberos datoteka tablice klju⌂eva i principal** ili **Kerberos principal i lozinka**. Tip korisnika koji mo⌂ete izabrati varira ovisno o trenutnoj konfiguraciji sistema. Na primjer, ako Usluga Mre⌂ne Provjere Autenti⌂nosti nije konfigurirana za sistem, tada Kerberos korisni⌂ki tipovi mo⌂da ne⌂e biti dostupni za izbor. Tip korisnika koji izaberete odre⌂uje ostale informacije koje morate osigurati da bi se stranica ispunila kako slijedi:

Bilješka: Morate navesti korisnika koji je trenutno definiran u poslu⌂itelju direktorija koji je host EIM kontrolera domene. Korisnik kojeg specificirate mora imati minimalne povlastice za izvo⌂enje pregledavanja mapiranja i administraciju registra za lokalni korisni⌂ki registar. Ako korisnik kojeg ste naveli nema ove povlastice, tada odre⌂ene funkcije operativnog sistema koje se odnose na kori⌂tenje jednostruke prijave i brisanje korisni⌂kih profila mogu ne uspjeti.

Ako niste konfigurirali poslu⌂itelj direktorija prije izvo⌂enja ovog ⌂arobnjaka, jedini tip korisnika kojeg mo⌂ete izabrati je **Razlikovno ime i lozinka**, a jedino razlikovno ime koje mo⌂ete specificirati je DN LDAP administratora.

- Ako izaberete **Razlikovno ime i lozinka**, osigurajte sljede⌂e informacije:
  - U polju **Razlikovno ime** navedite LDAP razlikovno ime koje identificira korisnika, a koje ⌂e sistem koristiti prilikom izvo⌂enja EIM operacija.
  - U polju **Lozinka** navedite lozinku razlikovnog imena.
  - U polju **Potvrda lozinke** drugi put navedite lozinku za svrhu provjere valjanosti.
- Ako izaberete **Kerberos principal i lozinka**, osigurajte sljede⌂e informacije:
  - U polju **Principal** navedite ime Kerberos principala kojeg ⌂e sistem koristiti prilikom izvo⌂enja EIM operacija.
  - U polju **Podru⌂je** navedite puno ispravno ime Kerberos podru⌂ja ⌂iji je principal ⌂lan. Ime principala i podru⌂ja jedinstveno identificira Kerberos korisnike u datoteci tablice klju⌂eva. Na primjer, principal jsmith u podru⌂ju ordept.myco.com u datoteci tablice klju⌂eva predstavljen je kao jsmith@ordept.myco.com.
  - U polju **Lozinka** unesite lozinku za korisnika.
  - U polju **Potvrda lozinke** drugi put navedite lozinku za svrhu provjere valjanosti.
- Ako ste izabrali **Kerberos tablica klju⌂eva i principal**, osigurajte sljede⌂e informacije:
  - U polju **Datoteka tablice klju⌂eva** navedite punu ispravnu stazu i ime datoteke tablice klju⌂eva koja sadr⌂i Kerberos principala kojeg ⌂e sistem koristiti prilikom izvo⌂enja EIM operacija. Ili kliknite **Pregled...** za pregled direktorija u iSeries integriranom sistemu datoteka i izbor datoteke tablice klju⌂eva.
  - U polju **Principal** navedite ime Kerberos principala kojeg ⌂e sistem koristiti prilikom izvo⌂enja EIM operacija.
  - U polju **Podru⌂je** navedite puno ispravno ime Kerberos podru⌂ja ⌂iji je principal ⌂lan. Ime principala i podru⌂ja jedinstveno identificira Kerberos korisnike u datoteci tablice klju⌂eva. Na primjer, principal jsmith u podru⌂ju ordept.myco.com u datoteci tablice klju⌂eva predstavljen je kao jsmith@ordept.myco.com.
- Kliknite **Provjeri Vezu** da osigurate da ⌂arobnjak mo⌂e koristiti navedene korisni⌂ke informacije za uspje⌂nu uspostavu veze s EIM kontrolerom domene.
- Kliknite **Sljede⌂e**.

11. Na panelu **Sa⌂etak** pregledajte konfiguracijske informacije koje ste dobavili. Ako su sve informacije to⌂ne, kliknite **Zavr⌂etak**.

Kada ⌂arobnjak zavr⌂i on dodaje novu domenu u folder **Upravljanje domenom** i na taj ste na⌂in kreirali osnovnu EIM konfiguraciju za ovaj sistem. Me⌂utim, ove zadatke trebate dovr⌂iti da biste zavr⌂ili va⌂u EIM konfiguraciju za domenu:

1. Koristite ⌂arobnjaka EIM konfiguracije na svakom dodatnom poslu⌂itelju kojeg ⌂elite spojiti na domenu.

2. Ako je potrebno, dodajte EIM definicije registra u EIM domenu za ostale ne-iSeries poslu⌂itelje i aplikacije za koje ⌂elite da sudjeluju u EIM domeni. Ove definicije registra odnose se na stvarne korisni⌂ke registre koji moraju sudjelovati u domeni. Mo⌂etedodati sistemske definicije registra ili dodati definicije registra aplikacije ovisno o potrebama va⌂e EIM implementacije.
3. Ovisno o potrebama va⌂e EIM implementacije odredite da li:
   - Kreirati EIM identifikatore za svakog jedinstvenog korisnika ili cjelinu u domeni i za njih kreirati identifikator asocijacija.
   - Kreirati asocijacije politike za mapiranje grupe korisnika u jednostruki ciljni korisni⌂ki identitet.
   - Kreirati kombinaciju istih.
4. Koristite EIM funkciju testiranja mapiranja da testirate mapiranja identiteta va⌂e EIM konfiguracije.
5. Ako je jedini EIM korisnik kojeg ste definirali DN za LDAP administratora, tada va⌂ EIM korisnik ima visoku razinu ovla⌂tenja nad svim podacima na poslu⌂itelju direktorija. Prema tome mo⌂ete razmotriti kreiranje jednog ili vi⌂e DN-ova kao dodatnih korisnika koji imaju prikladniju i ograni⌂enu kontrolu pristupa EIM podacima. Da nau⌂ite vi⌂e o kreiranju DN-ova za ovaj poslu⌂itelj direktorija pogledajte Razlikovna imena u poglavlju IBM poslu⌂itelj direktorija za iSeries (LDAP). Broj dodatnih EIM korisnika koje definirate ovisi o va⌂oj sigurnosnoj politici s naglaskom na razdvajanju sigurnosnih zadataka i odgovornosti. Tipi⌂no, mo⌂ete kreirati barem dva sljede⌂a tipa DN-ova:
   - **Korisnik koji ima kontrolu pristupa EIM administratora**

     Ovaj EIM administratorski DN omogu⌂uje prikladnu razinu ovla⌂tenja za administratora koji je odgovoran za upravljanje EIM domenom. Ovaj EIM administratorski DN mo⌂e se koristiti za povezivanje s kontrolerom domene prilikom upravljanja svim aspektima EIM domene upotrebom iSeries Navigatora.
   - **Barem jedan korisnik koji ima sve od sljede⌂ih kontrola pristupa**:
     - Administrator identifikatora
     - Administrator registra
     - EIM operacije mapiranja

     Ovaj korisnik osigurava odgovaraju⌂u razinu kontrole pristupa koja je potrebna korisniku sistema koji izvodi EIM operacije za operativni sistem.

   Bilješka: Da umjesto LDAP administratorskog DN-a koristite ovaj novi DN za sistemskog korisnika, morate promijeniti svojstva EIM konfiguracije iSeries poslu⌂itelja. Pogledajte Upravljanje svojstvima EIM konfiguracije da nau⌂ite kako mijenjati DN sistemskog korisnika.

Dodatno, mo⌂da ⌂ete ⌂eljeti koristiti Sloj Sigurnih Uti⌂nica (SSL) ili Sigurnost Transportnog Sloja (TLS) za konfiguraciju sigurnog povezivanja na EIM kontroler domene za za⌂titu prijenosa EIM podataka. Ako omogu⌂ite SSL za poslu⌂itelja direktorija, morate a⌂urirati svojstva EIM konfiguracije da specificirate da iSeries poslu⌂itelj koristi sigurno SSL povezivanje. Tako⌂er morate a⌂urirati svojstva za domenu kako bi specificirali da EIM koristi SSL povezivanja za upravljanje domenom preko iSeries Navigatora.

Bilješka: Mo⌂da ⌂ete morati izvesti dodatne zadatke ako ste kreirali osnovnu konfiguraciju mre⌂ne usluge za provjeru autenti⌂nosti, posebno ako ste implementirali okru⌂enje jednostruke prijave. Informacije o ovim dodatnim koracima mo⌂ete prona⌂i tako da ponovno u cijelosti pogledate korake konfiguracije koji su prikazani scenarijem Omogu⌂i jednostruku prijavu za OS/400.

Kreiranje i spajanje nove udaljene domene

Kada za kreiranje i spajanje na novu domenu koristite ⌂arobnjaka za EIM konfiguraciju, mo⌂ete izabrati da li konfigurirati poslu⌂itelja direktorija na udaljenom sistemu koji djeluje kao EIM kontroler domene, kao dio kreiranja va⌂e EIM konfiguracije. Morate specificirati odgovaraju⌂e informacije za povezivanje na udaljeni poslu⌂itelj direktorija kako bi konfigurirali EIM. Ako Kerberos nije trenutno konfiguriran na iSeries poslu⌂itelju, pojavi se ⌂arobnjakov prompt za lansiranje ⌂arobnjaka za Konfiguraciju Usluga mre⌂ne provjere autenti⌂nosti.

Bilješka: Poslu⌂itelj direktorija na udaljenom sistemu mora osiguravati EIM podr⌂ku. EIM zahtjeva da je kontroler domene smje⌂ten na poslu⌂itelju direktorija koji podr⌂ava verziju 3 Lightweight Directory Access Protocola (LDAP). Dodatno, proizvod poslu⌂itelja direktorija mora imati konfiguriranu EIM shemu. Na primjer, IBM Poslu⌂itelj direktorija V5.1 osigurava tu podr⌂ku. Za detaljnije informacije o zahtjevima EIM kontrolera domene mo⌂ete prona⌂i pod Planiranje EIM kontrolera domene.

Kada zavr⌂ite s ⌂arobnjakom EIM konfiguracije, mo⌂ete obaviti sljede⌂e zadatke:

- Kreirati novu EIM domenu.
- Konfigurirati udaljenog poslu⌂itelja direktorija da djeluje kao EIM kontroler domene.
- Konfigurirati uslugu mre⌂ne provjere autenti⌂nosti za sistem.
- Kreirati definicije EIM registra za lokalni OS/400 registar i Kerberos registar.
- Konfigurirati sistem da sudjeluje u novoj EIM domeni.

Da konfigurirate va⌂ sistem za kreiranje i spajanje na novu EIM domenu, morate imati sva od sljede⌂ih posebnih ovla⌂tenja:

- Administrator sigurnosti (*SECADM).
- Svi objekti (*ALLOBJ).
- Sistemska konfiguracija (*IOSYSCFG).

Da koristite ⌂arobnjaka EIM konfiguracije za kreiranje i spajanje na novu udaljenu domenu, izvedite sljede⌂e korake:

1. Provjerite da je poslu⌂itelj direktorija na udaljenom sistemu aktivan. Pogledajte dokumentaciju proizvoda poslu⌂itelja direktorija da odredite kako to u⌂initi.
2. U iSeries Navigatoru izaberite sistem za koji ⌂elite konfigurirati EIM i pro⌂irite **Mre⌂a > Mapiranje identiteta u poduze⌂u**.
3. Desno kliknite **Konfiguracija** i izaberite **Konfiguriraj...** da pokrenete ⌂arobnjaka EIM konfiguracije.

   Bilješka: Ova opcija je ozna⌂ena kao **Rekonfiguriraj...** ako je EIM prethodno konfiguriran na sistemu.
4. Na stranici ⌂arobnjaka **Dobro do⌂li!**, izaberite **Kreiranje i spajanje nove domene** i kliknite **Sljede⌂e**.
5. Na stranici **Specificiranje lokacije EIM domene**, izaberite **Na udaljenom poslu⌂itelju direktorija** i kliknite **Sljede⌂e**.

   Bilješka: Ova opcija konfigurira udaljenog poslu⌂itelja direktorija da djeluje kao EIM kontroler domene. Da bi slu⌂io kao EIM kontroler domene, udaljeni poslu⌂itelj direktorija mora osigurati EIM podr⌂ku i mora biti aktivan da uspje⌂no dovr⌂i ovu EIM konfiguraciju. Tako⌂er mora ostati aktivan za podr⌂ku EIM pregledavanju mapiranja i za ostale operacije.

   Bilješka: Ako usluga mre⌂ne provjere autenti⌂nosti nije trenutno konfigurirana na iSeries poslu⌂itelju ili su potrebne dodatne informacije za mre⌂nu provjeru autenti⌂nosti za konfiguriranje okru⌂enja jednostruke prijave, prikazuje se stranica **Konfiguracija Usluga Mre⌂ne Provjere Autenti⌂nosti**. Ova vam stranica omogu⌂uje pokretanje ⌂arobnjaka Konfiguracije Usluga mre⌂ne provjere autenti⌂nosti tako da mo⌂ete konfigurirati uslugu mre⌂ne provjere autenti⌂nosti. Ili Usluge mre⌂ne provjere autenti⌂nosti mo⌂ete konfigurirati kasnije upotrebom ⌂arobnjaka konfiguracije tih usluga pomo⌂u iSeries Navigatora. Kada dovr⌂ite konfiguraciju usluga mre⌂ne provjere autenti⌂nosti, nastavlja se EIM Konfiguracijski ⌂arobnjak.
6. Da konfigurirate usluge mre⌂ne provjere autenti⌂nosti, izvedite sljede⌂e korake:
   a. Na stranici **Konfiguracija Usluga mre⌂ne provjere autenti⌂nosti** izaberite **Da** da pokrenete ⌂arobnjaka Konfiguracije Usluga mre⌂ne provjere autenti⌂nosti. S ovim ⌂arobnjakom, mo⌂ete konfigurirati nekoliko OS/400 su⌂elja i usluga da sudjelujete u Kerberos podru⌂ju kao i konfigurirati okru⌂enje jednostruke prijave koje koristi EIM i usluge mre⌂ne provjere autenti⌂nosti.
   b. Na stranici **Specificiranje informacija podru⌂ja** navedite ime default podru⌂ja u polju **Default podru⌂je**. Ako koristite Microsoft Aktivni direktorij za Kerberos provjeru autenti⌂nosti izaberite **Microsoft Aktivni direktorij se koristi za Kerberos provjeru autenti⌂nosti** i kliknite **Sljede⌂e**.

c. Na stranici **Specificiranje KDC informacija** navedite puno ispravno ime Kerberos poslu⌂itelja za ovo podru⌂je u **KDC** polju, navedite 88 u polju **Port**, a zatim kliknite **Sljede⌂e**.

d. Na stranici **Specificiranje informacija Lozinke poslu⌂itelja** izaberite ili **Da** ili **Ne** za postavljanje lozinke poslu⌂itelja. Poslu⌂itelj lozinki dozvoljava principalima mijenjanje lozinke na Kerberos poslu⌂itelju. Ako izaberete **Da**, unesite ime poslu⌂itelja lozinke u polje **Poslu⌂itelj lozinke**. U polju **Port** prihvatite default vrijednost 464, a zatim kliknite Sljede⌂e.

e. Na stranici **Izbor unosa tablice klju⌂eva** izaberite **OS/400 Kerberos provjera autenti⌂nosti**, a zatim kliknite **Sljede⌂e**.

Bilješka: Tako⌂er mo⌂ete kreirati unose tablice klju⌂eva za IBM poslu⌂itelja direktorija za iSeries (LDAP), iSeries NetServer i iSeries HTTP poslu⌂itelja ako ⌂elite da ove usluge koriste Kerberos provjeru autenti⌂nosti. Mo⌂da ⌂ete trebati dodatno konfigurirati ove usluge da bi mogle koristiti Kerberos provjeru autenti⌂nosti.

f. Na stranici **Kreiranje OS/400 unosa tablice klju⌂eva** unesite i potvrdite lozinku, a zatim kliknite **Sljede⌂e**. Ovo je ista lozinka koju ⌂ete koristiti kada u Kerberos poslu⌂itelj dodate OS/400 principale.

g. Na stranici **Kreiranje Paketne Datoteke** izaberite **Da**, navedite sljede⌂e informacije i kliknite **Sljede⌂e**:

- U polju **Paketna datoteka** a⌂urirajte stazu direktorija. Kliknite **Pregled** da biste prona⌂li odgovaraju⌂u stazu direktorija ili u polju **Paketna datoteka** uredili stazu.
- U polju **Uklju⌂i lozinku** izaberite **Da**. Ovo osigurava da su sve lozinke koje su pridru⌂ene principalima OS/400 usluge sadr⌂ane u paketnoj datoteci. Va⌂no je primijetiti da su lozinke prikazane u ⌂istom tekstu i da ih mo⌂e pro⌂itati bilo tko tko ima dozvolu za ⌂itanje paketne datoteke. Prema tome, bitno je da paketnu datoteku izbri⌂ete s Kerberos poslu⌂itelja i s PC-ja odmah nakon njene upotrebe. Ako lozinku ne uklju⌂ite, ona ⌂e se od vas zatra⌂iti prilikom pokretanja paketne datoteke.

Bilješka: Tako⌂er mo⌂ete ru⌂no dodati principale usluge koje generira ⌂arobnjak u Microsoft Aktivnom direktoriju. Da biste nau⌂ili kako to u⌂initi, pogledajte Dodavanje OS/400 principala u Kerberos poslu⌂itelj

- Na stranici **Sa⌂etak** pregledajte pojedinosti konfiguracije usluge mre⌂ne provjere autenti⌂nosti, a zatim kliknite **Zavr⌂i** da biste se vratili u ⌂arobnjak EIM konfiguracije.

7. Koristite stranicu **Specificiranje EIM kontrolera domene** za specifikaciju informacija povezivanja kako slijedi za udaljenog EIM kontrolera domene kojeg ⌂elite konfigurirati:
   - U polju **Ime kontrolera domene** navedite ime udaljenog poslu⌂itelja direktorija kojeg ⌂elite konfigurirati kao EIM kontroler domene za domenu koju kreirate. Ime EIM kontrolera domene mo⌂e biti ime TCP/IP hosta poslu⌂itelja direktorija i ime domene ili adresa poslu⌂itelja direktorija.
   - Specificirajte informacije povezivanja za povezivanje na kontroler domene kako slijedi:
     – Izaberite **Koristi sigurnu vezu (SSL ili TLS)** ako ⌂elite koristiti sigurnu vezu s EIM kontrolerom domene. Kada je ovo izabrano, veza koristi ili Sloj Sigurnih Uti⌂nica (SSL) ili Sigurnost Transportnog Sloja (TLS) za uspostavu sigurne veze za za⌂titu EIM prijenosa podataka preko nepouzdane mre⌂e kakav je Internet.

     Bilješka: Morate provjeriti je li EIM kontroler domene konfiguriran za kori⌂tenje sigurne veze. U suprotnom, veza s kontrolerom domene mo⌂e ne uspjeti.

     – U polju **Port** navedite TCP/IP port na kojem slu⌂a poslu⌂itelj direktorija. Ako je izabrano **Koristi sigurnu vezu**, default port je 636; u suprotnom je port 389.
   - Kliknite **Provjera veze** da provjerite mo⌂e li ⌂arobnjak koristiti navedene informacije za uspje⌂nu uspostavu veze s EIM kontrolerom domene.
   - Kliknite **Sljede⌂e**.
8. Na stranici **Specificiranje korisnika za vezu** izaberite **Tip korisnika** za povezivanje. Mo⌂ete izabrati jednog od sljede⌂ih tipova korisnika: **Razlikovno ime i lozinka**, **Kerberos datoteka tablice klju⌂eva i principal**, **Kerberos principal i lozinka** ili **Korisni⌂ki profil i lozinka**. Dva Kerberos tipa korisnika dostupna su samo ako je usluga mre⌂ne provjere autenti⌂nosti konfigurirana za lokalni iSeries sistem. Tip korisnika koji izaberete odre⌂uje druge informacije koje morate dobaviti za dovr⌂avanje dijaloga kako slijedi:

Bilješka: Da osigurate da ⌂arobnjak ima dovoljno ovla⌂tenje za kreiranje potrebnih EIM objekata, izaberite **Razlikovno ime i lozinka** kao tip korisnika i navedite LDAP administratorski DN i lozinku kao korisnika.

Mo⌂ete navesti razli⌂itog korisnika za vezu, me⌂utim, korisnik kojeg navedete mora imati ekvivalent LDAP administratorskom ovla⌂tenju za udaljenog poslu⌂itelja direktorija.

- Ako izaberete **Razlikovno ime i lozinka**, osigurajte sljede⌂e informacije:
  - U polje **Razlikovno ime** upi⌂ite LDAP administratorsko razlikovno ime (DN) i lozinku da osigurate da ⌂arobnjak ima dovoljno ovla⌂tenja za administriranje EIM domene i objekata u njoj.
  - U polju **Lozinka** navedite lozinku razlikovnog imena.
  - U polju **Potvrda lozinke** drugi put navedite lozinku za svrhu provjere valjanosti.
- Ako ste izabrali **Kerberos datoteka tablice klju⌂eva i principal**, osigurajte sljede⌂e informacije:
  - U polju **Datoteka tablice klju⌂eva** navedite punu ispravnu stazu i ime datoteke tablice klju⌂eva koja sadr⌂i Kerberos principala kojeg ⌂e ⌂arobnjak koristiti prilikom povezivanja na EIM domenu. Ili kliknite **Pregled...** za pregled direktorija u iSeries integriranom sistemu datoteka i izbor datoteke tablice klju⌂eva.
  - U polju **Principal** navedite ime Kerberos principala koji ⌂e se koristiti za identificiranje korisnika.
  - U polju **Podru⌂je** navedite puno ispravno ime Kerberos podru⌂ja ⌂iji je principal ⌂lan. Ime principala i podru⌂ja jedinstveno identificira Kerberos korisnike u datoteci tablice klju⌂eva. Na primjer, principal jsmith u podru⌂ju ordept.myco.com, predstavljeno je u datoteci tablice klju⌂eva kao jsmith@ordept.myco.com.
- Ako izaberete **Kerberos principal i lozinka**, osigurajte sljede⌂e informacije:
  - U polju **Principal** navedite ime Kerberos principala koje ⌂e ⌂arobnjak koristiti prilikom spajanja na EIM domenu.
  - U polju **Podru⌂je** navedite puno ispravno ime Kerberos podru⌂ja ⌂iji je principal ⌂lan. Ime principala i podru⌂ja jedinstveno identificira Kerberos korisnike u datoteci tablice klju⌂eva. Na primjer, principal jsmith u podru⌂ju ordept.myco.com u datoteci tablice klju⌂eva predstavljen je kao jsmith@ordept.myco.com.
  - U polju **Lozinka** navedite lozinku Kerberos principala.
  - U polju **Potvrda lozinke** drugi put navedite lozinku za svrhu provjere valjanosti.
- Ako izaberete **Korisni⌂ki profil i lozinka**, navedite sljede⌂e informacije:
  - U polju **Korisni⌂ki profil** navedite ime korisni⌂kog profila koje ⌂e ⌂arobnjak koristiti prilikom spajanja na EIM domenu.
  - U polju **Lozinka** navedite lozinku korisni⌂kog profila.
  - U polju **Potvrda lozinke** drugi put navedite lozinku za svrhu provjere valjanosti.
- Kliknite **Provjera veze** da provjerite mo⌂e li ⌂arobnjak koristiti navedene korisni⌂ke informacije za uspje⌂nu uspostavu veze s EIM kontrolerom domene.
- Kliknite **Sljede⌂e**.

9. Na stranici **Specificiranje domene** , osigurajte sljede⌂e informacije:
   - U polju **Domena** specificirajte ime EIM domene koju ⌂elite kreirati. Prihvatite defaultno ime EIM ili upotrijebite bilo koji niz znakova koji vam imaju smisla. Svakako ne mo⌂ete koristiti posebne znakove kao ⌂to su to **= + < > , # ;** \ i *****.
   - U polju **Opis** unesite tekst za opis domene.
   - Kliknite **Sljede⌂e**.
10. U dijalogu **Specificiranje nadre⌂enog DN-a za domenu**, izaberite **Da** za specifikaciju nadre⌂enog DN-a koje ⌂e ⌂arobnjak koristiti za lokaciju EIM domene koju kreirate. To je DN koji predstavlja unos odmah iznad unosa imena va⌂e domene u stablastoj hijerarhiji informacija o direktoriju. Ili specificirajte **Ne** da imate EIM podatke pohranjene na lokaciji direktorija sa sufiksom ⌂ije je ime izvedeno iz imena EIM domene.

    Bilješka: Kada koristite ⌂arobnjaka za konfiguraciju domene na udaljenom kontroleru domene, trebate specificirati odgovaraju⌂i nadre⌂eni DN za domenu. Zato ⌂to svi potrebni konfiguracijski objekti za

nadre⌂eni DN moraju ve⌂ postojati, jer u suprotnom EIM konfiguracija ne⌂e uspjeti, trebate pregledati kako bi na⌂li prikladan nadrfe⌂eni DN umjesto da ru⌂no unesete DN informacije. Kliknite **Pomo⌂** za dodatne informacije o kori⌂tenju nadre⌂enog DN-a.

11. Na stranici **Informacije registra** navedite treba li dodati lokalne korisni⌂ke registre u EIM domenu kao definicije registra. Izaberite jedan od sljede⌂ih ili oba korisni⌂ka tipa registra:

    Bilješka: U ovom trenutku ne morate kreirati definicije registra. Ako kasnije izaberete kreirati definicije registra, morate dodati sistemske definicije registra i a⌂urirati EIM konfiguracijska svojstva.

    - Izaberite **Lokalni OS/400** da dodate definiciju registra za lokalni registar. U navedenom polju, prihvatite default vrijednost imena definicije registra ili navedite drugu vrijednost imena definicije registra. Ime EIM registra je proizvoljan niz znakova koji predstavlja tip registra i specifi⌂nu instancu tog registra.
    - Izaberite **Kerberos** da dodate definiciju registra za Kerberos registar. U navedenom polju, prihvatite default vrijednost imena definicije registra ili navedite drugu vrijednost imena definicije registra. Default ime definicije registra isto je kao i ime podru⌂ja. Prihva⌂anjem default imena i upotrebom istog imena Kerberos registra kao imena podru⌂ja, mo⌂ete pove⌂ati performansu pri dohva⌂anju informacija iz registra. Ako je potrebno, izaberite **Kerberos korisni⌂ki identiteti osjetljivi su na velika i mala slova**.
    - Kliknite **Sljede⌂e**.

12. Na stranici **Specificiranje EIM sistemskog korisnika** izaberite **Tip korisnika** kojeg ⌂elite da sistem koristi kada izvodi EIM operacije za funkcije operativnog sistema. Te operacije uklju⌂uju operacije pregledavanja mapiranja i brisanje asocijacija prilikom brisanja lokalnog OS/400 korisni⌂kog profila. Mo⌂ete izabrati jedan od sljede⌂ih korisni⌂kih tipova: **Razlikovno ime i lozinka**, **Kerberos datoteka tablice klju⌂eva i principal** ili **Kerberos principal i lozinka**. Tip korisnika koji mo⌂ete izabrati varira ovisno o trenutnoj konfiguraciji sistema. Na primjer, ako Usluga Mre⌂ne Provjere Autenti⌂nosti nije konfigurirana za sistem, tada Kerberos korisni⌂ki tipovi mo⌂da ne⌂e biti dostupni za izbor. Tip korisnika koji izaberete odre⌂uje ostale informacije koje morate osigurati da bi se stranica ispunila kako slijedi:

    Bilješka: Morate navesti korisnika koji je trenutno definiran u poslu⌂itelju direktorija koji je host EIM kontrolera domene. Korisnik kojeg specificirate mora imati minimalne povlastice za izvo⌂enje pregledavanja mapiranja i administraciju registra za lokalni korisni⌂ki registar. Ako korisnik kojeg ste naveli nema ove povlastice tada odre⌂ene funkcije operativnog sistema koje se odnose na kori⌂tenje jednostruke prijave i brisanje korisni⌂kih profila mogu neuspijeti.

    Ako niste konfigurirali poslu⌂itelj direktorija prije izvo⌂enja ovog ⌂arobnjaka, jedini tip korisnika koji mo⌂ete izabrati je **Razlikovno ime i lozinka**, a jedino razlikovno ime koje mo⌂ete specificirati je DN LDAP administratora.

    - Ako izaberete **Razlikovno ime i lozinka**, osigurajte sljede⌂e informacije:
      - U polju **Razlikovno ime** navedite LDAP razlikovno ime koje identificira korisnika, a koje ⌂e sistem koristiti prilikom izvo⌂enja EIM operacija.
      - U polju **Lozinka** navedite lozinku razlikovnog imena.
      - U polju **Potvrda lozinke** drugi put navedite lozinku za svrhu provjere valjanosti.
    - Ako izaberete **Kerberos principal i lozinka**, osigurajte sljede⌂e informacije:
      - U polju **Principal** navedite ime Kerberos principala kojeg ⌂e sistem koristiti prilikom izvo⌂enja EIM operacija.
      - U polju **Podru⌂je** navedite puno ispravno ime Kerberos podru⌂ja ⌂iji je principal ⌂lan. Ime principala i podru⌂ja jedinstveno identificira Kerberos korisnike u datoteci tablice klju⌂eva. Na primjer, principal jsmith u podru⌂ju ordept.myco.com u datoteci tablice klju⌂eva predstavljen je kao jsmith@ordept.myco.com.
      - U polju **Lozinka** unesite lozinku za korisnika.
      - U polju **Potvrda lozinke** drugi put navedite lozinku za svrhu provjere valjanosti.
    - Ako ste izabrali **Kerberos datoteka tablice klju⌂eva i principal**, osigurajte sljede⌂e informacije:

– U polju **Datoteka tablice klju⌂eva** navedite punu ispravnu stazu i ime datoteke tablice klju⌂eva koja sadr⌂i Kerberos principala kojeg ⌂e sistem koristiti prilikom izvo⌂enja EIM operacija. Ili kliknite **Pregled...** za pregled direktorija u iSeries integriranom sistemu datoteka i izbor datoteke tablice klju⌂eva.

– U polju **Principal** navedite ime Kerberos principala kojeg ⌂e sistem koristiti prilikom izvo⌂enja EIM operacija.

– U polju **Podru⌂je** navedite puno ispravno ime Kerberos podru⌂ja ⌂iji je principal ⌂lan. Ime principala i podru⌂ja jedinstveno identificiraju Kerberos korisnike u datoteci tablice klju⌂eva. Na primjer, principal jsmith u podru⌂ju ordept.myco.com u datoteci tablice klju⌂eva predstavljen je kao jsmith@ordept.myco.com.

- Kliknite **Provjera veze** da osigurate da ⌂arobnjak mo⌂e koristiti navedene korisni⌂ke informacije za uspje⌂nu uspostavu veze s EIM kontrolerom domene.
- Kliknite **Sljede⌂e**.

13. Na panelu **Sa⌂etak** pregledajte konfiguracijske informacije koje ste dobavili. Ako su sve informacije to⌂ne, kliknite **Zavr⌂etak**.

Kada ⌂arobnjak zavr⌂i on dodaje novu domenu u folder **Upravljanje domenom** i na taj ste na⌂in kreirali osnovnu EIM konfiguraciju za ovaj sistem. Me⌂utim, ove zadatke trebate dovr⌂iti da biste zavr⌂ili va⌂u EIM konfiguraciju za domenu:

1. Koristite ⌂arobnjaka EIM konfiguracije na svakom dodatnom poslu⌂itelju kojeg ⌂elite spojiti na novu domenu.
2. Ako je potrebno, dodajte EIM definicije registra u EIM domenu za ostale ne-iSeries poslu⌂itelje i aplikacije za koje ⌂elite da sudjeluju u EIM domeni. Ove definicije registra odnose se na stvarne korisni⌂ke registre koji moraju sudjelovati u domeni. Mo⌂ete Dodati sistemske definicije registra ili Dodati definicije registra aplikacije ovisno o potrebama va⌂e EIM implementacije.
3. Ovisno o potrebama va⌂e EIM implementacije odredite da li:
   - Kreirati EIM identifikatore za svakog jedinstvenog korisnika ili cjelinu u domeni i za njih kreirati identifikator asocijacija.
   - Kreirati asocijacije politike za mapiranje grupe korisnika u jednostruki ciljni korisni⌂ki identitet.
   - Kreirati kombinaciju istih.
4. Koristite EIM funkciju testiranja mapiranja da testirate mapiranja identiteta va⌂e EIM konfiguracije.
5. Ako je jedini EIM korisnik kojeg ste definirali DN za LDAP administratora, tada va⌂ EIM korisnik ima visoku razinu ovla⌂tenja nad svim podacima na poslu⌂itelju direktorija. Prema tome mo⌂ete razmotriti kreiranje jednog ili vi⌂e DN-ova kao dodatnih korisnika koji imaju prikladniju i ograni⌂enu kontrolu pristupa EIM podacima. Da nau⌂ite vi⌂e o kreiranju DN-ova za ovaj poslu⌂itelj direktorija pogledajte Razlikovna imena u poglavlju IBM poslu⌂itelj direktorija za iSeries (LDAP). Broj dodatnih EIM korisnika koje definirate ovisi o va⌂oj sigurnosnoj politici s naglaskom na razdvajanju sigurnosnih zadataka i odgovornosti. Tipi⌂no, mo⌂ete kreirati barem dva sljede⌂a tipa DN-ova:
   - **Korisnik koji ima kontrolu pristupa EIM administratora**

     Ovaj EIM administratorski DN omogu⌂uje prikladnu razinu ovla⌂tenja za administratora koji je odgovoran za upravljanje EIM domenom. Ovaj EIM administratorski DN mo⌂e se koristiti za povezivanje s kontrolerom domene prilikom upravljanja svim aspektima EIM domene upotrebom iSeries Navigatora.
   - **Barem jedan korisnik koji ima sve od sljede⌂ih kontrola pristupa**:
     – Administrator identifikatora
     – Administrator registra
     – EIM operacije mapiranja

     Ovaj korisnik osigurava odgovaraju⌂u razinu kontrole pristupa koja je potrebna sistemskom korisniku koji izvodi EIM operacije za operativni sistem.

Bilješka: Da umjesto LDAP administratorskog DN-a koristite ovaj novi DN za sistemskog korisnika, morate promijeniti svojstva EIM konfiguracije iSeries poslu⌂itelja. Pogledajte Upravljanje svojstvima EIM konfiguracije da nau⌂ite kako mijenjati DN sistemskog korisnika.

Bilješka: Mo⌂da ⌂ete morati izvesti dodatne zadatke ako ste kreirali osnovnu konfiguraciju mre⌂ne usluge za provjeru autenti⌂nosti, posebno ako ste implementirali okru⌂enje jednostruke prijave. Informacije o ovim dodatnim koracima mo⌂ete prona⌂i tako da ponovno u cijelosti pogledate korake konfiguracije koji su prikazani scenarijem Omogu⌂i jednostruku prijavu za OS/400.

Pristup postoje⌂oj domeni

Nakon ⌂to ste kreirali EIM domenu i posslu⌂itelj direktorija konfigurirali kao kontrolora domene na jednom sistemu, sve dodatne posslu⌂itelje iSeries (V5R2 ili novije) mo⌂ete konfigurirati tako da se spoje na postoje⌂u EIM domenu. Kako radite kroz ⌂arobnjaka, morate dobaviti informacije o domeni, uklju⌂uju⌂i informacije povezivanja na EIM kontroler domene. Kada koristite EIM ⌂arobnjak konfiguracije za spajanje na postoje⌂u domenu, ⌂arobnjak vam i dalje omogu⌂uje mogu⌂nost pokretanja ⌂arobnjaka Konfiguracije usluge mre⌂ne provjere autenti⌂nosti za konfiguraciju Kerberosa kao dijela konfiguriranja EIM-a na sistemu.

Kada zavr⌂ite s ⌂arobnjakom EIM konfiguracije tako da se spoji na postoje⌂u domenu, mo⌂ete izvesti sljede⌂e zadatke:

- Konfigurirati uslugu mre⌂ne provjere autenti⌂nosti za sistem.
- Kreirati definicije EIM registra za lokalni registar OS/400 i Kerberos registar.
- Konfigurirati sistem da sudjeluje u postoje⌂oj EIM domeni.

Da konfigurirate sistem da se spoji na postoje⌂u EIM domenu, morate imati sva od sljede⌂ih posebnih ovla⌂tenja:

- Administrator sigurnosti (*SECADM).
- Svi objekti (*ALLOBJ).

Da zapo⌂nete i koristite ⌂arobnjaka EIM konfiguracije za spajanje na postoje⌂u EIM domenu, izvedite sljede⌂e korake:

1. Provjerite da je posslu⌂itelj direktorija na udaljenom sistemu aktivan. Pogledajte dokumentaciju proizvoda posslu⌂itelja direktorija da odredite kako to u⌂initi.
2. U iSeries Navigatoru izaberite sistem za koji ⌂elite konfigurirati EIM i pro⌂irite **Mre⌂a > Mapiranje identiteta u poduze⌂u**.
3. Desno kliknite **Konfiguracija** i izaberite **Konfiguriraj...** da zapo⌂nete ⌂arobnjaka EIM konfiguracije.

   Bilješka: Ova je opcija je ozna⌂ena kao **Rekonfiguriraj...** ako je EIM prethodno konfiguriran na sistemu.
4. Na stranici ⌂arobnjaka **Dobro do⌂li** izaberite **Spajanje na postoje⌂u domenu**, a zatim kliknite **Sljede⌂e**.

   Bilješka: Ako usluga provjere valjanosti mre⌂e nije trenutno konfigurirana na iSeries posslu⌂itelju ili su potrebne dodatne informacije za mre⌂nu provjeru autenti⌂nosti za konfiguriranje okoline za jednostruku prijavu, prikazuje se stranica **Konfiguracija Usluga mre⌂ne provjere autenti⌂nosti**. Ova vam stranica omogu⌂uje pokretanje ⌂arobnjaka Konfiguracije Usluga mre⌂ne provjere autenti⌂nosti tako da mo⌂ete konfigurirati uslugu mre⌂ne provjere autenti⌂nosti. Ili Usluge mre⌂ne provjere autenti⌂nosti mo⌂ete konfigurirati kasnije upotrebom ⌂arobnjaka konfiguracije tih usluga pomo⌂u iSeries Navigatora. Kada dovr⌂ite konfiguraciju usluga mre⌂ne provjere autenti⌂nosti, nastavlja se EIM Konfiguracijski ⌂arobnjak.
5. Da konfigurirate usluge mre⌂ne provjere autenti⌂nosti, izvedite sljede⌂e korake:
   a. Na stranici **Konfiguracija Usluga mre⌂ne provjere autenti⌂nosti** izaberite **Da** da pokrenete ⌂arobnjaka Konfiguracije Usluga mre⌂ne provjere autenti⌂nosti. S ovim ⌂arobnjakom, mo⌂ete konfigurirati nekoliko OS/400 su⌂elja i usluga da sudjelujete u Kerberos podru⌂ju kao i konfigurirati okolinu jednostruke prijave koja koristi EIM uslugu i uslugu mre⌂ne provjere autenti⌂nosti.
   b. Na stranici **Specificiranje informacija podru⌂ja** navedite ime default podru⌂ja u polju **Default podru⌂je**. Ako koristite Microsoft Aktivni direktorij za Kerberos provjeru autenti⌂nosti izaberite **Microsoft Aktivni direktorij se koristi za Kerberos provjeru autenti⌂nosti** i kliknite **Sljede⌂e**.
   c. Na stranici **Specificiranje KDC informacija** navedite puno ispravno ime Kerberos posslu⌂itelja za ovo podru⌂je u **KDC** polju, navedite 88 u polju **Port**, a zatim kliknite **Sljede⌂e**.

d. Na stranici **Specificiranje informacija Lozinke poslu⌂itelja** izaberite ili **Da** ili **Ne** za postavljanje lozinke poslu⌂itelja. Poslu⌂itelj lozinki dozvoljava principalima mijenjanje lozinke na Kerberos poslu⌂itelju. Ako izaberete **Da**, unesite ime poslu⌂itelja lozinke u polje **Poslu⌂itelj lozinke**. U polju **Port** prihvatite default vrijednost 464, a zatim kliknite Sljede⌂e.

e. Na stranici **Izbor unosa tablice klju⌂eva** izaberite **OS/400 Kerberos provjera autenti⌂nosti**, a zatim kliknite **Sljede⌂e**.

Bilješka: Tako⌂er mo⌂ete kreirati unose tablice klju⌂eva za IBM poslu⌂itelj direktorija za iSeries (LDAP), iSeries NetServer i iSeries HTTP poslu⌂itelj ako ⌂elite da ove usluge koriste Kerberos provjeru autenti⌂nosti. Mo⌂da ⌂ete trebati dodatno konfigurirati ove usluge da bi mogle koristiti Kerberos provjeru autenti⌂nosti.

f. Na stranici **Kreiranje OS/400 unosa tablice klju⌂eva** unesite i potvrdite lozinku, a zatim kliknite **Sljede⌂e**. Ovo je ista lozinka koju ⌂ete koristiti kada u Kerberos poslu⌂itelj dodate OS/400 principale.

g. Na stranici **Kreiranje paketne datoteke** izaberite **Da**, navedite sljede⌂e informacije i kliknite **Sljede⌂e**:

- U polju **Paketna datoteka** a⌂urirajte stazu direktorija. Kliknite **Pregled** da biste prona⌂li odgovaraju⌂u stazu direktorija ili u polju **Paketna datoteka** uredili stazu.
- U polju **Uklju⌂i lozinku** izaberite **Da**. Ovo osigurava da su sve lozinke koje su pridru⌂ene principalima OS/400 usluge sadr⌂ane u paketnoj datoteci. Va⌂no je primijetiti da su lozinke prikazane u jasnom tekstu i da ih mo⌂e pro⌂itati bilo tko tko ima dozvolu za ⌂itanje paketne datoteke. Prema tome, bitno je da paketnu datoteku izbri⌂ete s Kerberos poslu⌂itelja i s PC-ja odmah nakon njene upotrebe. Ako lozinku ne uklju⌂ite, ona ⌂e se od vas zatra⌂iti prilikom pokretanja paketne datoteke.

Bilješka: Tako⌂er mo⌂ete ru⌂no dodati principale usluge koje generira ⌂arobnjak u Microsoft Aktivnom direktoriju. Da biste nau⌂ili kako to u⌂initi, pogledajte Dodavanje OS/400 principala u Kerberos poslu⌂itelj

- Na stranici **Sa⌂etak** pregledajte pojedinosti konfiguracije usluge mre⌂ne provjere autenti⌂nosti, a zatim kliknite **Zavr⌂i** da biste se vratili u ⌂arobnjak EIM konfiguracije.

6. Na stranici **Specificiranje kontrolera domene** osigurajte sljede⌂e informacije:

Bilješka: Poslu⌂itelj direktorija koji djeluje kao kontroler domene mora biti aktivan da bi uspje⌂no dovr⌂io EIM konfiguraciju.

- U polju **Ime kontrolora domene** navedite ime sistema koji slu⌂i kao kontrolor domene za EIM domenu na koju ⌂elite da se iSeries poslu⌂itelj spoji.
- Kliknite **Koristi sigurnu vezu (SSL ili TLS)** ako ⌂elite koristiti sigurnu vezu s EIM kontrolorom domene. Kada je ovo izabrano, veza koristi ili Sloj Sigurnih Uti⌂nica (SSL) ili Sigurnost Transportnog Sloja (TLS) za uspostavu sigurne veze za za⌂titu EIM prijenosa podataka preko nepouzdane mre⌂e kakav je Internet.

Bilješka: Morate provjeriti je li EIM kontroler domene konfiguriran za kori⌂tenje sigurne veze. U suprotnom, veza s kontrolerom domene mo⌂e ne uspjeti.

- U polju **Port** navedite TCP/IP port na kojem slu⌂a poslu⌂itelj direktorija. Ako je izabrano **Koristi sigurnu vezu**, default port je 636; u suprotnom je port 389.
- Kliknite **Provjeri vezu** da provjerite mo⌂e li ⌂arobnjak koristiti navedene informacije za uspje⌂nu uspostavu veze s EIM kontrolerom domene.
- Kliknite **Sljede⌂e**.

7. Na stranici **Specificiranje korisnika za vezu** za vezu izaberite **Tip korisnika**. Mo⌂ete izabrati jednog od sljede⌂eg tipa korisnika: **Razlikovno ime i lozinka**, **Kerberos datoteka tablice klju⌂eva i principal**, **Kerberos principal i lozinka** ili **Korisni⌂ki profil i lozinka**. Dva Kerberos tipa korisnika dostupni su samo ako je usluga mre⌂ne provjere autenti⌂nosti konfigurirana za lokalni iSeries sistem. Tip korisnika koji izaberete odre⌂uje druge informacije koje morate dobaviti za dovr⌂avanje dijaloga kako slijedi:

Bilješka: Da osigurate da ⌂arobnjak ima dovoljna ovla⌂tenja za kreiranje potrebnih EIM objekata, izaberite **Razlikovno ime i lozinka** kao tip korisnika i navedite LDAP administratorski DN i lozinku kao korisnika.

Mo⌂ete navesti razli⌂itog korisnika za vezu, me⌂utim, korisnik kojeg navedete mora imati ekvivalent LDAP administratorskom ovla⌂tenju za udaljenog poslu⌂itelja direktorija.

- Ako izaberete **Razlikovno ime i lozinka**, omogu⌂ite sljede⌂e informacije:
  - U polju **Razlikovno ime** navedite LDAP razlikovno ime (DN) koje identificira korisnika koji ima ovla⌂tenja za kreiranje objekata u lokalnom prostoru LDAP poslu⌂itelja. Ako ste ovog ⌂arobnjaka koristili za konfiguriranje LDAP poslu⌂itelja u ranijem koraku, trebate unijeti razlikovno ime LDAP administratora kojeg ste u tom koraku kreirali.
  - U polju **Lozinka** navedite lozinku razlikovnog imena.
  - U polju **Potvrda lozinke** drugi put navedite lozinku za svrhu provjere valjanosti.
- Ako ste izabrali **Kerberos tablica klju⌂eva i principal**, omogu⌂ite sljede⌂e informacije:
  - U polju **Datoteka tablice klju⌂eva** navedite punu ispravnu stazu i ime datoteke tablice klju⌂eva koja sadr⌂i Kerberos principala kojeg ⌂e ⌂arobnjak koristiti prilikom povezivanja na EIM domenu. Ili kliknite **Pregled...** za pregled direktorija u iSeries integriranom sistemu datoteka i izbor datoteke tablice klju⌂eva.
  - U polju **Principal** navedite ime Kerberos principala koji ⌂e se koristiti za identificiranje korisnika.
  - U polju **Podru⌂je** navedite puno ispravno ime Kerberos podru⌂ja ⌂iji je principal ⌂lan. Ime principala i podru⌂ja jedinstveno identificira Kerberos korisnike u datoteci tablice klju⌂eva. Na primjer, principal jsmith u podru⌂ju ordept.myco.com, predstavljeno je u datoteci tablice klju⌂eva kao jsmith@ordept.myco.com.
- Ako izaberete **Kerberos principal i lozinka**, osigurajte sljede⌂e informacije:
  - U polju **Principal** navedite ime Kerberos principala koje ⌂e ⌂arobnjak koristiti prilikom spajanja na EIM domenu.
  - U polju **Podru⌂je** navedite puno ispravno ime Kerberos podru⌂ja ⌂iji je principal ⌂lan. Ime principala i podru⌂ja jedinstveno identificiraju Kerberos korisnike u datoteci tablice klju⌂eva. Na primjer, principal jsmith u podru⌂ju ordept.myco.com u datoteci tablice klju⌂eva predstavljen je kao jsmith@ordept.myco.com.
  - U polju **Lozinka** navedite lozinku Kerberos principala.
  - U polju **Potvrda lozinke** drugi put navedite lozinku za svrhu provjere valjanosti.
- Ako izaberete **Korisni⌂ki profil i lozinka**, navedite sljede⌂e informacije:
  - U polju **Korisni⌂ki profil** navedite ime korisni⌂kog profila koje ⌂e ⌂arobnjak koristiti prilikom spajanja na EIM domenu.
  - U polju **Lozinka** navedite lozinku korisni⌂kog profila.
  - U polju **Potvrda lozinke** drugi put navedite lozinku za svrhu provjere valjanosti.
- Kliknite **Provjera veze** da provjerite mo⌂e li ⌂arobnjak koristiti navedene korisni⌂ke informacije za uspje⌂nu uspostavu veze s EIM kontrolerom domene.
- Kliknite **Sljede⌂e**.

8. Na stranici **Specificiranje domene** izaberite ime domene kojoj ⌂elite pristupiti i kliknite **Sljede⌂e**.
9. Na stranici **Informacije registra** navedite treba li dodati korisni⌂ke registre u EIM domenu kao definicije registra. Izaberite jedan ili oba korisni⌂ka tipa registra:
   - Izaberite **Lokalni OS/400** da dodate definiciju registra za lokalni registar. U navedenom polju, prihvatite default vrijednost imena definicije registra ili navedite drugu vrijednost imena definicije registra. Ime EIM registra je proizvoljan niz znakova koji predstavlja tip registra i specifi⌂nu instancu tog registra.

     Bilješka: U ovom trenutku ne morate kreirati lokalnu OS/400 definiciju registra. Ako kasnije izaberete kreirati OS/400 definiciju registra, morate dodati sistemsku definiciju registra i a⌂urirati EIM konfiguracijska svojstva.
   - Izaberite **Kerberos** da dodate definiciju registra za Kerberos registar. U navedenom polju, prihvatite default vrijednost imena definicije registra ili navedite drugu vrijednost imena definicije registra. Default ime definicije registra isto je kao i ime podru⌂ja. Prihva⌂anjem default imena upotrebom istog imena Kerberos registra mo⌂ete pove⌂ati performanse pri dohva⌂anju informacija iz registra. Ako je potrebno, izaberite **Kerberos korisni⌂ki identiteti osjetljivi su na velika i mala slova**.

Bilješka: Ako ste koristili ⌂arobnjaka EIM konfiguracije na drugom sistemu za dodavanje definicije registra za Kerberos registar za koji ovaj iSeries sistem ima principala usluge, tada kao dio ove konfiguracije ne trebate dodati Kerberos definiciju registra. Me⌂utim, ime Kerberos registra trebat ⌂ete navesti u konfiguracijskim svojstvima za ovaj sistem nakon ⌂to zavr⌂ite s ⌂arobnjakom.

- Kliknite **Sljede⌂e**.

10. Na stranici **Specificiranje EIM sistemskog korisnika** izaberite **Tip korisnika** kojeg ⌂elite da korisnik koristi kada izvodi EIM operacije za funkcije operativnog sistema. Te operacije sadr⌂e operacije pregledavanja mapiranja i brisanje asocijacija prilikom brisanja lokalnog OS/400 korisni⌂kog profila. Mo⌂ete izabrati jedan od sljede⌂ih korisni⌂kih tipova: **Razlikovno ime i lozinka**, **Kerberos datoteka tablice klju⌂eva i principal** ili **Kerberos principal i lozinka**. Tip korisnika koji mo⌂ete izabrati varira ovisno o trenutnoj konfiguraciji sistema. Na primjer, ako Usluga Mre⌂ne Provjere Autenti⌂nosti nije konfigurirana za sistem, tada Kerberos tip korisnika mo⌂da ne⌂e biti dostupan za izbor. Tip korisnika koji izaberete odre⌂uje ostale informacije koje morate omogu⌂iti da bi se stranica ispunila na sljede⌂i na⌂in:

   Bilješka: Morate navesti korisnika koji je trenutno definiran u poslu⌂itelju direktorija na kojem je smje⌂ten EIM kontroler domene. Korisnik kojeg specificirate mora imati minimalne povlastice za izvo⌂enje pregledavanja mapiranja i administracije registra za lokalni korisni⌂ki registar. Ako korisnik kojeg ste naveli nema ove povlastice tada odre⌂ene funkcije operativnog sistema koje se odnose na kori⌂tenje jednostruke prijave i brisanje korisni⌂kih profila mogu ne uspijeti.

   - Ako izaberete **Razlikovno ime i lozinka**, omogu⌂ite sljede⌂e informacije:
     - U polju **Razlikovno ime** navedite LDAP razlikovno ime koje identificira korisnika, a koje ⌂e sistem koristiti prilikom izvo⌂enja EIM operacija.
     - U polju **Lozinka** navedite lozinku razlikovnog imena.
     - U polju **Potvrda lozinke** drugi put navedite lozinku za svrhu provjere valjanosti.
   - Ako izaberete **Kerberos principal i lozinka**, osigurajte sljede⌂e informacije:
     - U polju **Principal** navedite ime Kerberos principala kojeg ⌂e sistem koristiti prilikom izvo⌂enja EIM operacija.
     - U polju **Podru⌂je** navedite puno ispravno ime Kerberos podru⌂ja ⌂iji je principal ⌂lan. Ime principala i podru⌂ja jedinstveno identificira Kerberos korisnike u datoteci tablice klju⌂eva. Na primjer, principal jsmith u podru⌂ju ordept.myco.com u datoteci tablice klju⌂eva predstavljen je kao jsmith@ordept.myco.com.
     - U polju **Lozinka** unesite lozinku za korisnika.
     - U polju **Potvrda lozinke** drugi put navedite lozinku za svrhu provjere valjanosti.
   - Ako ste izabrali **Kerberos tablica klju⌂eva i principal**, osigurajte sljede⌂e informacije:
     - U polju **Datoteka tablice klju⌂eva** navedite punu ispravnu stazu i ime datoteke tablice klju⌂eva koja sadr⌂i Kerberos principala kojeg ⌂e sistem koristiti prilikom izvo⌂enja EIM operacija. Ili kliknite **Pregled...** za pregled direktorija u iSeries integriranom sistemu datoteka i izbor datoteke tablice klju⌂eva.
     - U polju **Principal** navedite ime Kerberos principala kojeg ⌂e sistem koristiti prilikom izvo⌂enja EIM operacija.
     - U polju **Podru⌂je** navedite puno ispravno ime Kerberos podru⌂ja ⌂iji je principal ⌂lan. Ime principala i podru⌂ja jedinstveno identificira Kerberos korisnike u datoteci tablice klju⌂eva. Na primjer, principal jsmith u podru⌂ju ordept.myco.com u datoteci tablice klju⌂eva predstavljen je kao jsmith@ordept.myco.com.
   - Kliknite **Provjera veze** da osigurate da ⌂arobnjak mo⌂e koristiti navedene korisni⌂ke informacije za uspje⌂nu uspostavu veze s EIM kontrolerom domene.
   - Kliknite **Sljede⌂e**.

11. Na stranici **Sa⌂etak** pregledajte informacije konfiguracije koje ste osigurali. Ako su sve informacije to⌂ne, kliknite **Zavr⌂etak**.

Kada se ⌂arobnjak zavr⌂i on dodaje domenu u folder **Upravljanje domenom** i na taj ste na⌂in kreirali osnovnu EIM konfiguraciju za ovaj sistem. Me⌂utim, mo⌂da ⌂ete ove zadatke trebati dovr⌂iti da biste va⌂u EIM konfiguraciju za domenu zavr⌂ili:

1. Ako je potrebno, dodajte EIM definicije registra u EIM domenu za ostale ne-iSeries poslu⌂itelje i aplikacije za koje ⌂elite da sudjeluju u EIM domeni. Ove definicije registra odnose se na stvarne korisni⌂ke registre koji moraju sudjelovati u domeni. Mo⌂ete Dodati sistemske definicije registra ili Dodati definicije registra aplikacije ovisno o potrebama va⌂e EIM implementacije.
2. Ovisno o potrebama va⌂e EIM implementacije odredite da li:
   - Kreirati EIM identifikatore za svakog jedinstvenog korisnika ili cjelinu u domeni i za njih kreirati identifikator asocijacija.
   - Kreirati asocijacije politike za mapiranje grupe korisnika u jednostruki ciljni korisni⌂ki identitet.
   - Kreirati kombinaciju istih.
3. Koristite EIM funkciju testiranje mapiranja da testirate mapiranje identiteta va⌂e EIM konfiguracije.
4. Ako je jedini EIM korisnik kojeg ste definirali, DN za LDAP administratora, tada va⌂ EIM korisnik ima visoku razinu ovla⌂tenja nad svim podacima na poslu⌂itelju direktorija. Prema tome mo⌂ete razmotriti kreiranje jednog ili vi⌂e DN-ova kao dodatnih korisnika koji imaju prikladniju i ograni⌂enu kontrolu pristupa EIM podacima. Da nau⌂ite vi⌂e o kreiranju DN-ova za ovaj poslu⌂itelj direktorija pogledajte Razlikovna imena u poglavlju IBM poslu⌂itelj direktorija za iSeries (LDAP). Broj dodatnih EIM korisnika koje definirate ovisi o va⌂oj sigurnosnoj politici s naglaskom na razdvajanju sigurnosnih zadataka i odgovornosti. Tipi⌂no, mo⌂ete kreirati barem dva sljede⌂a tipa DN-ova:
   - **Korisnik koji ima kontrolu pristupa EIM administratora**

     Ovaj EIM administratorski DN omogu⌂uje prikladnu razinu ovla⌂tenja za administratore koji su odgovorni za upravljanje EIM domenom. Ovaj EIM administratorski DN mo⌂e se koristiti za povezivanje s kontrolerom domene prilikom upravljanja svim aspektima EIM domene upotrebom iSeries Navigatora.
   - **Barem jedan korisnik koji ima sljede⌂e kontrole pristupa**:
     - Administrator identifikatora
     - Administrator registra
     - EIM operacije mapiranja

     Ovaj korisnik osigurava odgovaraju⌂u razinu kontrole pristupa koja je potrebna korisniku sistema koji izvodi EIM operacije za operativni sistem.

   Bilješka: Da umjesto LDAP administratorskog DN-a koristite ovaj DN za korisnika sistema, morate promijeniti EIM svojstva konfiguracije iSeries poslu⌂itelja. Pogledajte Upravljanje EIM svojstvima konfiguracije da nau⌂ite kako mijenjati DN korisnika sistema.

Bilješka: Mo⌂da ⌂ete morati izvesti dodatne zadatke ako ste kreirali osnovnu konfiguraciju usluge za mre⌂nu provjeru autenti⌂nosti, posebno ako ste implementirali okolinu jednostruke prijave. Informacije o ovim dodatnim koracima mo⌂ete prona⌂i tako da ponovno u cijelosti pogledate korake konfiguracije koji su prikazani scenarijem Omogu⌂i jednostruku prijavu za OS/400.

Konfiguriranje sigurne veze s EIM kontrolerom domene

Mo⌂da ⌂ete htjeti koristiti Sloj Sigurnih Uti⌂nica (SSL) ili Sigurnost Transportnog Sloja (TLS) za uspostavu sigurne veze s EIM kontrolerom domene za za⌂titu prijenosa EIM podataka.

Da konfigurirate SSL ili TLS za EIM, morate dovr⌂iti sljede⌂e zadatke:

1. Ako je potrebno, koristite Upravitelja Digitalnih certifikata (DCM) za kreiranje certifikata tako da poslu⌂itelj direktorija koristi SSL.
2. Omogu⌂ite SSL za lokalne poslu⌂itelje direktorija na kojem je smje⌂ten EIM kontroler domene.
3. A⌂urirajte EIM svojstva konfiguracije za specificiranje da iSeries poslu⌂itelj koristi sigurnu SSL vezu.

   Za a⌂uriranje EIM svojstava konfiguracije, izvedite sljede⌂e korake:

a. U iSeries Navigatoru, izaberite sistem na kojem ⌂elite konfigurirati EIM i pro⌂irite **Mre⌂a → Mapiranje identiteta u poduze⌂u**.
b. Desno kliknite **Konfiguracija** i izaberite **Svojstva**.
c. Na stranici **Domena** izaberite **Koristi sigurnu vezu (SSL ili TLS)**, navedite sigurni port na kojem poslu⌂itelj direktorija slu⌂a ili prihva⌂a default vrijednost 636 u polju **Port**, a zatim kliknite **OK**.

4. A⌂urirajte svojstva EIM domene za svaku EIM domenu navode⌂i da EIM koristi SSL vezu kada domenama upravlja pomo⌂u iSeries Navigatora.

   Za a⌂uriranje svojstava EIM domene, izvedite sljede⌂e korake:

   a. U iSeries Navigatoru, izaberite sistem na kojem ste konfigurirali EIM i pro⌂irite **Mre⌂a → Mapiranje identiteta u poduze⌂u → Upravljanje domenom**.
   b. Izaberite EIM domenu u kojoj ⌂elite raditi.
      - Ako EIM domena s kojom ⌂elite raditi nije ispisana u **Upravljanje domenom**, pogledajte Dodavanje EIM domene u Upravitelja domenom.
      - Ako trenutno niste povezani s EIM domenom u kojoj ⌂elite raditi, pogledajte Povezivanje s EIM kontrolerom domene.
   c. Desno kliknite EIM domenu na koju ste sada spojeni i izaberite **Svojstva**.
   d. Na stranici **Domena** izaberite **Koristi sigurnu vezu (SSL ili TLS)**, navedite sigurni port na kojem poslu⌂itelj direktorija slu⌂a ili prihva⌂a default vrijednost 636 u polju **Port**, a zatim kliknite **OK**.

Upravljanje Mapiranjem identiteta u poduze⌂u

Nakon ⌂to konfigurirate Mapiranje identiteta u poduze⌂u (EIM) na va⌂em iSeries poslu⌂itelju, trebat ⌂ete povremeno izvesti nekoliko administrativnih zadataka za upravljanje va⌂om EIM domenom i podacima za domenu. Za nau⌂iti vi⌂e o EIM upravljanju u va⌂em poduze⌂u, pregledajte ove stranice.

“Upravljanje domenama Mapiranja identiteta u poduze⌂u” Nau⌂ite kako upravljati va⌂om EIM domenom i svojstvima EIM domene.

“Upravljanje definicijama registra Mapiranja identiteta u poduze⌂u” na stranici 82 Nau⌂ite kako kreirati i upravljati definicijama EIM registra za one korisni⌂ke registre u va⌂em poduze⌂u koji sudjeluju u EIM-u.

“Upravljanje identifikatorima Mapiranja identiteta u poduze⌂u” na stranici 87 Nau⌂ite kako kreirati i upravljati EIM identifikatorima za domenu.

“Upravljanje asocijacijama” na stranici 90 Nau⌂ite kako kreirati i brisati asocijacije identifikatora i asocijacije politike kao i kako upravljati ostalim svojstvima za informacije o asocijaciji u EIM domeni.

“Upravljanje svojstvima EIM konfiguracije” na stranici 104 Nau⌂ite kako upravljati EIM konfiguracijom za va⌂ sistem, uklju⌂uju⌂i sistemskog korisnika i ostala svojstva.

“Upravljanje EIM kontrolom korisni⌂kog pristupa” na stranici 104 Nau⌂ite kako upravljati grupama za kontrolu pristupa korisnika za korisnike koji kontroliraju korisni⌂ki pristup EIM podacima i EIM administrativnim zadacima i ostalim operacijama.

Upravljanje domenama Mapiranja identiteta u poduze⌂u

| Mo⌂ete koristiti iSeries Navigator za upravljanje svim va⌂im domenama Mapiranja identiteta u poduze⌂u (EIM). Za
| upravljanje EIM domenom, domena mora biti izlistana ili se mora dodati u folder **Upravljanje domenom** pod
| folderom **Mre⌂a** u iSeries Navigatoru. Kada koristite ⌂arobnjaka EIM konfiguracije za kreiranje i konfiguriranje nove
| EIM domene, domena se automatski dodaje u folder **Upravljanje domenom** tako da mo⌂ete upravljati domenom i
| informacijama u domeni.

| Mo⌂ete koristiti bilo koje iSeries povezivanje za upravljanje EIM domenom koja se nalazi bilo gdje u istoj mre⌂i, ⌂ak
| i kada iSeries koji koristite ne sudjeluje u domeni.

Mo⌂ete izvesti sljede⌂e zadatke upravljanja za domenu:

- "Dodavanje domene Mapiranja identiteta u poduze⌂u u folder Upravljanja domenom"
- "Povezivanje na domenu Mapiranja identiteta u poduze⌂u"
- "Omogu⌂avanje asocijacija politika za domenu" na stranici 79
- "Testiranje EIM mapiranja" na stranici 79
- "Uklanjanje domene Mapiranja identiteta u poduze⌂u iz foldera Upravljanje domenom" na stranici 81
- "Brisanje domene Mapiranja identiteta u poduze⌂u i svih konfiguracijskih objekata" na stranici 82

Tako⌂er mo⌂ete upravljati korisni⌂kim pristupom domeni i informacijama u domeni kako slijedi:

- "Upravljanje EIM kontrolom korisni⌂kog pristupa" na stranici 104
- "Upravljanje definicijama registra Mapiranja identiteta u poduze⌂u" na stranici 82
- "Upravljanje asocijacijama" na stranici 90
- "Upravljanje identifikatorima Mapiranja identiteta u poduze⌂u" na stranici 87

Dodavanje domene Mapiranja identiteta u poduze⌂u u folder Upravljanja domenom

Da izvedete ovaj zadatak trebate imati *SECADM posebno ovla⌂tenje, a domena koju ⌂elite dodati mora postojati prije no ⌂to se doda u folder **Upravljanje domenom**.

Za dodavanje postoje⌂e domene Mapiranja identiteta u poduze⌂u (EIM) u folder **Upravljanje domenom**, izvedite ove korake:

1. Pro⌂irite **Mre⌂a > Mapiranje identiteta u poduze⌂u**.
2. Desno kliknite na **Upravljanje domenom** i izaberite **Dodaj domenu...**.
3. U dijalogu **Dodavanje domene**, specificirajte potrebnu domenu i informacije povezivanja. Ili kliknite **Pregled...** za pogled na listu domena kojima upravlja specificirani kontroler domene.

   Bilješka: Ako kliknete **Pregled...**, pokazuje se dijalog **Povezivanje na EIM kontrolera domene**. Da pogledate listu domena, morate se povezati na kontrolera domene ili s LDAP administratorskom kontrolom pristupa ili EIM administratorskom kontrolom pristupa. Sadr⌂aji liste domena variraju ovisno o tipu EIM kontrole pristupa koju imate. Ako imate LDAP administratorsku kontrolu pristupa, mo⌂ete gledati listu domena kojima upravlja kontroler domene. U suprotnom, lista prikazuje samo one domene za koje imate EIM administratorsku kontrolu pristupa.
4. Ako je potrebno kliknite **Pomo⌂** da odredite koje informacije navesti u odre⌂enom polju.
5. Kliknite **OK** za dodavanje domene.

Povezivanje na domenu Mapiranja identiteta u poduze⌂u

Prije no ⌂to po⌂nete raditi s domenom Mapiranja identiteta u poduze⌂u (EIM), morate se prvo povezati na EIM kontroler domene za domenu. Mo⌂ete se povezati na EIM domenu ⌂ak ako va⌂ iSeries posluⓈitelj nije trenutno konfiguriran za sudjelovanje u toj domeni.

Za povezivanje na EIM kontroler domene, korisnik s kojim se se povezujete mora biti ⌂lan "EIM kontrola pristupa" na stranici 33 grupe. Va⌂e ⌂lanstvo grupe za EIM kontrolu pristupa odre⌂uje koje zadatke mo⌂ete izvoditi u domeni i koje EIM podatke mo⌂ete pregledavati ili mijenjati.

Da se pove⌂ete na EIM domenu, dovr⌂ite sljede⌂e korake:

1. Pro⌂irite **Mre⌂a > Mapiranje identiteta u poduze⌂u > Upravljanje domenom**.
2. Desno kliknite na domenu na koju se ⌂elite povezati.

   Bilješka: Ako domena s kojom ⌂elite raditi nije ispisana pod **Upravljanje domenom**, morate "Dodavanje domene Mapiranja identiteta u poduze⌂u u folder Upravljanja domenom".
3. Desno kliknite na EIM domenu na koju se ⌂elite povezati i izaberite **Povezivanje...**.

4. U dijalogu **Povezivanje na EIM kontroler domene**, specificirajte **Tip korisnika**, osigurajte potrebne identifikacijske informacije za korisnika i izaberite opciju lozinke za povezivanje na kontroler domene.
5. Ako je potrebno kliknite **Pomo⌂** da odredite koje informacije navesti u svakom polju u dijalogu.
6. Kliknite **OK** za povezivanje na kontroler domene.

Omogu⌂avanje asocijacija politika za domenu

Asocijacija politika je sredstvo pomo⌂u kojeg se kreiraju mapiranja s vi⌂e na jedno u situaciji u kojoj asocijacije izme⌂u korisni⌂kih identiteta i EIM identifikatora ne postoje. Asocijaciju politike mo⌂ete koristiti za mapiranje izvornog skupa vi⌂estrukih korisni⌂kih identiteta (umjesto jednostrukog korisni⌂kog identiteta) na jednostruki ciljni korisni⌂ki identitet u odre⌂enom ciljnom korisni⌂kom registru. Da biste mogli koristiti asocijacije politike morate biti sigurni da ste domenu omogu⌂ili za kori⌂tenje asocijacija politika za operacije pregledavanja mapiranja.

Za omogu⌂avanje podr⌂ke politike mapiranja da koristi asocijacije politike za domenu, morate biti spojeni na EIM domenu u kojoj ⌂elite raditi i morate imati kontrolu pristupa EIM administratora.

Za omogu⌂avanje podr⌂ke pregledavanja mapiranja da koristi asocijacije politike za domenu, izvedite sljede⌂e korake:

1. Pro⌂irite **Mre⌂a > Mapiranje identiteta u poduze⌂u > Upravljanje domenom**.
2. Desno kliknite EIM domenu u kojoj ⌂elite raditi i izaberite **Politika mapiranja...**
   - Ako EIM domena s kojom ⌂elite raditi nije ispisana u **Upravljanje domenom**, pogledajte "Dodavanje domene Mapiranja identiteta u poduze⌂u u folder Upravljanja domenom" na stranici 78.
   - Ako trenutno niste povezani s EIM domenom u kojoj ⌂elite raditi, pogledajte Povezivanje s EIM kontrolerom domene. (Opcija **Politika mapiranja...** nije dostupna sve dok se ne spojite na domenu.)
3. Na stranici **Op⌂enito** izaberite **Omogu⌂i pregledavanje mapiranja kori⌂tenjem asocijacija politika za domenu**.
4. Kliknite**OK**.

Bilješka: Morate omogu⌂iti pregledavanja mapiranja i koristiti asocijacije politike za svaku definiciju ciljnog registra za koju postoje definirane asocijacije politika. Ako ne omogu⌂ite pregledavanja mapiranja za definiciju ciljnog registra, taj registar ne mo⌂e sudjelovati u EIM operacijama pregledavanja mapiranja. Ako ne navedete da ciljni registar mo⌂e koristiti asocijacije politike, tada EIM operacije pregledavanja mapiranja ignoriraju bilo koju definiranu asocijaciju politike za taj registar.

Testiranje EIM mapiranja

Podr⌂ka testiranja EIM mapiranja omogu⌂uje vam izdavanje operacija pregledavanja EIM mapiranja za va⌂u EIM konfiguraciju. Testiranje mo⌂ete koristiti za provjeravanje da se specifi⌂ni izvorni korisni⌂ki identitet ispravno mapira na odgovaraju⌂i ciljni korisni⌂ki identitet. Takvo testiranje osigurava da operacije pregledavanja EIM mapiranja mogu vratiti ispravni ciljni korisni⌂ki identitet zasnovan na specifi⌂nim informacijama.

Za kori⌂tenje funkcije testiranja mapiranja za testiranje va⌂e EIM konfiguracije, morate biti spojeni na EIM domenu u kojoj ⌂elite raditi i morate imati EIM kontrolu pristupa na jednoj od sljede⌂ih razina:

- EIM administrator
- Administrator identifikatora
- Administrator registra
- Operacije EIM pregledavanja mapiranja

Za kori⌂tenje podr⌂ke testiranja mapiranja za testiranje va⌂e EIM konfiguracije, izvedite sljede⌂e korake:

1. Pro⌂irite **Mre⌂a > Mapiranje identiteta u poduze⌂u > Upravljanje domenom**.
2. Izaberite EIM domenu u kojoj ⌂elite raditi.
   - Ako EIM domena s kojom ⌂elite raditi nije ispisana u **Upravljanje domenom**, pogledajte Dodavanje EIM domene u Upravitelja domenom.

- Ako trenutno niste povezani s EIM domenom u kojoj ∆elite raditi, pogledajte Povezivanje s EIM kontrolerom domene.

3. Desno kliknite EIM domenu na kojoj ste spojeni i izaberite **Testiraj mapiranje...**
4. U dijalogu **Testiranje mapiranja** navedite sljede∆e informacije:
   - U polju **Izvorni registar** osigurajte ime definicije registra koje se odnosi na korisni∆ki registar koji ∆elite koristiti kao izvor testiranja operacije pregledavanja mapiranja.
   - U polju **Izvorni korisnik** osigurajte ime korisni∆kog identiteta koji ∆elite koristiti kao izvor testiranja operacije pregledavanja mapiranja.
   - U polju **Ciljni registar** osigurajte ime definicije registra koje se odnosi na korisni∆ki registar koji ∆elite koristiti kao cilj testiranja operacije pregledavanja mapiranja.
   - Opcijski. U polje **Informacije pregledavanja** unesite bilo koje informacije pregledavanja koje su definirane za ciljnog korisnika.
5. Ako je potrebno, za vi∆e pojedinosti o tome koje informacije su potrebne za svako polje dijaloga kliknite **Pomo∆**.
6. Kliknite **Testiraj** i pogledajte rezultate operacije pregledavanja mapiranja kada se oni pojave.
7. Nastavite testirati va∆u konfiguraciju ili za izlaz kliknite **Zatvori**.

Rad s rezultatima testiranja i rje∆avanje problema

Kada se test izvodi, vra∆a se ciljni korisni∆ki identitet ako obrada testa prona∆e asocijaciju izme∆u izvornog korisni∆kog identiteta i ciljnog korisni∆kog identiteta koji je osigurao administrator. Test tako∆er pokazuje tip asocijacije koji je prona∆en izme∆u dva korisni∆ka identiteta. Kada postupak testa ne prona∆e asocijaciju koja je zasnovana na osiguranim informacijama, test vra∆a za ciljni korisni∆ki identitet ni∆ta.

Test, poput svake EIM operacije pregledavanja mapiranja, tra∆i i vra∆a prvi odgovaraju∆i ciljni identitet registra pretra∆uju∆i sljede∆im redoslijedom:

1. Specifi∆na asocijacija identifikatora
2. Asocijacija politike filtera certifikata
3. Asocijacije politike default registra
4. Asocijacija politike default domene

U nekim slu∆ajevima, test ne vra∆a rezultat ciljnog korisni∆kog identiteta iako su asocijacije za domenu konfigurirane. Provjerite da ste za test osigurali ispravne informacije. Ako su informacije ispravne i test ne vra∆a rezultate, tada problem mo∆e biti uzrokovan jednim od sljede∆eg:

- Podr∆ka asocijacije politike nije omogu∆ena na razini domene. Trebat ∆ete omogu∆iti asocijacije politike za domenu.
- Podr∆ka pregledavanja mapiranja ili podr∆ka asocijacije politike nije omogu∆ena na individualnoj razini registra. Mo∆da ∆ete morati omogu∆iti podr∆ku pregledavanja mapiranja i kori∆tenje asocijacija politike za ciljni registar.
- Ciljna ili izvorna asocijacija nije ispravno konfigurirana za EIM identifikator. Na primjer, ne postoji izvorna asocijacija za Kerberos principal (ili windows korisnika) ili je neispravna. Ili, ciljna asocijacija navodi neto∆ni korisni∆ki identitet. Prika∆ite sve asocijacije identifikatora za EIM identifikator da provjerite asocijacije za specifi∆ni identifikator.
- Asocijacija politike nije ispravno konfigurirana. Prika∆ite sve asocijacije politika za domenu da provjerite izvorne i ciljne informacije za sve asocijacije politike definirane u domeni.
- Definicija registra i korisni∆ki identitet ne podudaraju se zbog osjetljivosti na velika i mala slova. Registar mo∆ete obrisati i ponovno kreirati ili izbrisati i ponovno kreirati asocijaciju s ispravnom veli∆inom slova.

U drugim slu∆ajevima, test mo∆e imati dvosmislene rezultate. U takvim slu∆ajevima, prikazuje se poruka pogre∆ke koja na to ukazuje. Test vra∆a dvosmislene rezultate kada vi∆e od jednog ciljnog korisni∆kog rezultata odgovara navedenim kriterijima testa. Operacija pregledavanja mapiranja mo∆e vratiti vi∆estruke korisni∆ke registre kada postoji jedna ili vi∆e od sljede∆ih situacija:

- EIM identifikator ima vi∆estruke individualne ciljne asocijacije na istom ciljnom registru.

- Vi⌂e od jednog EIM identifikatora ima isti korisni⌂ki identitet naveden u izvornoj asocijaciji i svaki ih tih EIM identifikatora ima ciljnu asocijaciju na istom ciljnom registru, iako korisni⌂ki identitet naveden za svaku ciljnu asocijaciju mo⌂e biti razli⌂it.
- Vi⌂e od jedne asocijacije politike default domene specificira isti ciljni registar.
- Vi⌂e od jedne default asocijacije politike registra specificira isti izvorni registar i isti ciljni registar.
- Vi⌂e od jedne asocijacije politike filtera certifikata specificira isti izvorni X.509 registar, filter certifikata i ciljni registar.

Operacija pregledavanja mapiranja koja vra⌂a vi⌂e od jedan ciljni korisni⌂ki identitet mo⌂e stvarati probleme za EIM-omogu⌂ene aplikacije uklju⌂uju⌂i OS/400 aplikacije i proizvode. Prema tome potrebno je odrediti uzrok dvosmislenih rezultata i koje akcije treba poduzeti da bi se rije⌂ila situacija. Ovisno o uzroku mo⌂ete u⌂initi jedno ili vi⌂e od sljede⌂eg:

- Test vra⌂a ne⌂eljene vi⌂estruke ciljne identitete. To ukazuje da konfiguracije asocijacije za domenu nije ispravna zbog jednog od sljede⌂eg:
  - Ciljna ili izvorna asocijacija nije ispravno konfigurirana za EIM identifikator. Na primjer, ne postoji izvorna asocijacija za Kerberos principal (ili windows korisnika) ili je neispravna. Ili, ciljna asocijacija navodi neto⌂ni korisni⌂ki identitet. Prika⌂ite sve asocijacije identifikatora za EIM identifikator da provjerite asocijacije za specifi⌂ni identifikator.
  - Asocijacija politike nije ispravno konfigurirana. Prika⌂ite sve asocijacije politika za domenu da provjerite izvorne i ciljne informacije za sve asocijacije politike definirane u domeni.
- Ako test vra⌂a vi⌂estruke ciljne korisni⌂ke identitete i ti su rezultati odgovaraju⌂i za na⌂in na koji ste konfigurirali asocijacije, tada morate navesti informacije pregledavanja za svaki ciljni korisni⌂ki identitet. Morate definirati jedinstvene informacije pregledavanja za sve ciljne korisni⌂ke identitete koji imaju isti cilj (bilo EIM identifikator za asocijacije identifikatora ili ciljni korisni⌂ki registar za asocijacije politika). Definiranjem informacija pregledavanja za svaki ciljni korisni⌂ki identitet osiguravate da operacija pregledavanja vra⌂a jednostruki ciljni korisni⌂ki identitet umjesto svih mogu⌂ih ciljnih korisni⌂kih identiteta. Pogledajte Dodavanje informacija pregledavanja u ciljni korisni⌂ki identitet. Te informacije pregledavanja morate navesti u operaciji pregledavanja mapiranja.

Bilješka: Ovaj pristup radi samo ako je aplikacija omogu⌂ena za kori⌂tenje informacija pregledavanja. Me⌂utim, osnovne OS/400 aplikacije poput iSeries Access za Windows ne mogu koristiti informacije pregledavanja za razlikovanje vi⌂estrukih ciljnih korisni⌂kih identiteta koje vra⌂a operacija pregledavanja. Prema tome, mo⌂ete razmotriti ponovno definiranje asocijacija za domenu da osigurate da operacija pregledavanja mapiranja mo⌂e vratiti jednostruki ciljni korisni⌂ki identitet za osiguranje da osnovne OS/400 aplikacije mogu uspje⌂no izvesti operacije pregledavanja i mapirati identitete.

Za dodatne informacije o mogu⌂im problemima mapiranja i dodatnim rje⌂enjima osim onih ovdje opisanih, pogledajte “Rje⌂avanje problema Mapiranja identiteta u poduze⌂u: problemi mapiranja” na stranici 109.

Uklanjanje domene Mapiranja identiteta u poduze⌂u iz foldera Upravljanje domenom

Mo⌂ete ukloniti EIM domenu kojom ne ⌂elite vi⌂e upravljati iz foldera **Upravljanje domenom**. Me⌂utim, uklanjanje domene iz foldera **Upravljanje domenom nije** isto ⌂to i brisanje domene, jer se pritom ne bri⌂u podaci domene iz kontrolera domene. Pogledajte brisanje domene ako ⌂elite stvarno obrisati domenu i sve podatke domene.

Ne trebate nikakvo “EIM kontrola pristupa” na stranici 33 za ukloniti domenu.

Da uklonite EIM domenu kojom vi⌂e ne ⌂elite upravljati iz foldera **Upravljanje domenom**, izvedite ove korake:

1. Pro⌂irite **Mre⌂a > Mapiranje identiteta u poduze⌂u**.
2. Desno kliknite **Upravljanje domenom** i izaberite **Ukloni domenu...**.
3. Izaberite EIM domenu koju ⌂elite ukloniti iz **Upravljanja domenom**.
4. Kliknite **OK** za uklanjanje domene.

Brisanje domene Mapiranja identiteta u poduze⌂u i svih konfiguracijskih objekata

| Prije no ⌂to mo⌂ete obrisati EIM domenu, morate obrisati sve definicije registara i sve identifikatore Mapiranja
| identiteta u poduze⌂u (EIM) u domeni. Ako ne ⌂elite obrisati domenu i sve podatke domene, a pritom ne ⌂elite vi⌂e
| upravljati domenom, mo⌂ete umjesto toga ukloniti domenu.

| Za obrisati EIM domenu, morate imati "EIM kontrola pristupa" na stranici 33 na jednoj od ovih razina:
| • LDAP administrator.
| • EIM administrator.

Za brisanje EIM domene dovr⌂ite sljede⌂e korake.

1. Pro⌂irite **Mre⌂a > Mapiranje identiteta u poduze⌂u > Upravljanje domenom**.
2. Ako je potrebno obri⌂ite sve definicije registra iz EIM domene.
3. Ako je potrebno obri⌂ite sve EIM identifikatore iz EIM domene.
4. Desno kliknite na domenu koju ⌂elite izbrisati i izaberite **Brisanje...**.
5. Kliknite **Da** u dijalogu **Potvrda brisanja**.

Upravljanje definicijama registra Mapiranja identiteta u poduze⌂u

| Ako ⌂elite da korisni⌂ki registri i u njima sadr⌂ani korisni⌂ki identiteti sudjeluju u domeni Mapiranja identiteta u
| poduze⌂u (EIM) morate za njih kreirati definicije registra. Tada mo⌂ete upravljati kako korisni⌂ki registri i njihovi
| korisni⌂ki identiteti sudjeluju u EIM-u s upravljanjem tim EIM definicijama registra.

Mo⌂ete izvesti sljede⌂e zadatke upravljanja za definicije registra:

| • "Dodavanja definicije registara sistema"
| • "Dodavanje definicije registara aplikacije" na stranici 83
• "Dodavanja zamjenskog imena definiciji registra" na stranici 83
• "Definiranje privatnog tipa korisni⌂kog registra u Mapiranju identiteta u poduze⌂u" na stranici 84
| • "Omogu⌂avanje podr⌂ke pregledavanja mapiranja i kori⌂tenje asocijacija politika za ciljni registar" na stranici 85
| • "Prikaz svih asocijacija politike za definiciju registra" na stranici 102
• "Uklanjanje zamjenskog imena iz definicije registra" na stranici 87
• "Brisanje definicije registra" na stranici 86

| Dodatno vam ovi povezani zadaci mogu biti od koristi za pomo⌂ oko upravljanja ili rada s EIM podacima koji utje⌂u
| na definicije registra:

| • "Kreiranje asocijacije politike" na stranici 92
| • "Brisanje asocijacije politike" na stranici 103

Dodavanja definicije registara sistema

| Za kreiranje definicije sistemskog registra morate biti spojeni na EIM domenu u kojoj ⌂elite raditi i morate imati EIM
| administrator kontrolu pristupa.

Za dodavanje definicije sistemskog registra u EIM domenu, izvedite sljede⌂e korake.

1. Pro⌂irite **Mre⌂a > Mapiranje identiteta u poduze⌂u > Upravljanje domenom**.
2. Izaberite EIM domenu u kojoj ⌂elite raditi.
   - Ako EIM domena u kojoj ⌂elite raditi nije ispisana pod Upravljanje domenom, pogledajte "Dodavanje domene Mapiranja identiteta u poduze⌂u u folder Upravljanja domenom" na stranici 78.
   - Ako trenutno niste povezani s EIM domenom u kojoj ⌂elite raditi, pogledajte "Povezivanje na domenu Mapiranja identiteta u poduze⌂u" na stranici 78.
3. Pro⌂irite EIM domenu na koju ste sada povezani.
| 4. Desno kliknite **Korisni⌂ki registri**, izaberite **Dodavanje registra** i onda izaberite **Sistem...**.

5. U dijalogu **Dodavanje sistemskog registra** osigurajte informacije o definiciji sistemskog registra kako slijedi:
   - Ime za definiciju sistemskog registra.
   - Tip definicije registra.
   - Opis definicije sistemskog registra.
   - (Opcijski.) Korisni⌂ki registar URL.
   - Ako je potrebno, jedno ili vi⌂e zamjenskih imena za definiciju sistemskog registra.
6. Ako je potrebno kliknite **Pomo⌂** da odredite koje informacije osigurati za svako polje.
7. Kliknite **OK** za spremanje informacija i dodavanje definicije registra u EIM domenu.

Dodavanje definicije registara aplikacije

Za kreiranje definicije registra aplikacije morate biti spojeni na EIM domenu u kojoj ⌂elite raditi i morate imati EIM administrator kontrolu pristupa.

Za dodavanje definicije registra aplikacije u EIM domenu, izvedite sljede⌂e korake:

1. Pro⌂irite **Mre⌂a > Mapiranje identiteta u poduze⌂u > Upravljanje domenom**.
2. Izaberite EIM domenu u kojoj ⌂elite raditi.
   - Ako EIM domena u kojoj ⌂elite raditi nije ispisana pod Upravljanje domenom, pogledajte "Dodavanje domene Mapiranja identiteta u poduze⌂u u folder Upravljanja domenom" na stranici 78.
   - Ako trenutno niste povezani s EIM domenom u kojoj ⌂elite raditi, pogledajte "Povezivanje na domenu Mapiranja identiteta u poduze⌂u" na stranici 78.
3. Pro⌂irite EIM domenu na koju ste sada povezani.
4. Desno kliknite **Korisni⌂ki registri**, izaberite **Dodavanje registra** i onda izaberite **Aplikacija...**.
5. U dijalogu **Dodavanje registra aplikacija** osigurajte informacije o definiciji registra aplikacije kako slijedi:
   - Ime za definiciju registra aplikacije.
   - Ime definicije registra aplikacije ⌂iji je podskup korisni⌂ki registar aplikacije koji definirate. Definicija sistemskog registra koji specificirate mora ve⌂ postojati u EIM-u ina⌂e kreiranje definicije registra aplikacije ne⌂e uspjeti.
   - Tip definicije registra.
   - Opis definicije registra aplikacije.
   - Ako je potrebno, jedno ili vi⌂e zamjenskih imena za definiciju registra aplikacije.
6. Ako je potrebno kliknite **Pomo⌂** da odredite koje informacije osigurati za svako polje.
7. Kliknite **OK** za spremanje informacija i dodavanje definicije registra u EIM domenu.

Dodavanja zamjenskog imena definiciji registra

Vi ili razvija⌂ aplikacije ⌂elite specificirati dodatne razlikovne informacije za definiciju registra. To mo⌂ete napraviti s kreiranjem zamjenskog imena za definiciju registra. Vi mo⌂ete ili netko drugi mo⌂e onda koristiti zamjensko ime za definiciju registra za lak⌂e razlikovanje jednog korisni⌂kog registra od ostalih.

Ova podr⌂ka zamjenskog imena dozvoljava programerima da pi⌂u aplikacije bez poznavanja unaprijed proizvoljnog imena definicije EIM registra izabranog od administratora koji razvija aplikaciju. Dokumentaciju aplikacije mo⌂e dobaviti EIM administrator sa zamjenskim imenom koje aplikacija koristi. Kori⌂tenjem ovih informacija, EIM administrator mo⌂e dodijeliti ovo zamjensko ime definiciji EIM registra koja predstavlja stvarni korisni⌂ki registar za koji administrator ⌂eli da ga aplikacija koristi.

Za dodavanje zamjenskog imena u definiciju registra, morate biti spojeni na EIM domenu u kojoj ⌂elite raditi i morate imati "EIM kontrola pristupa" na stranici 33 jednu od sljede⌂ih razina:

- Administrator registra.
- Administrator za izabrane registre (za registar koji modificirate)
- EIM administrator.

Za dodavanje zamjenskog imena definiciji EIM registra, izvedite sljede⌂e korake:

1. Pro⌂irite **Mre⌂a > Mapiranje identiteta u poduze⌂u > Upravljanje domenom**.
2. Izaberite EIM domenu u kojoj ⌂elite raditi.
   - Ako EIM domena u kojoj ⌂elite raditi nije ispisana pod Upravljanje domenom, pogledajte "Dodavanje domene Mapiranja identiteta u poduze⌂u u folder Upravljanja domenom" na stranici 78.
   - Ako trenutno niste povezani s EIM domenom u kojoj ⌂elite raditi, pogledajte "Povezivanje na domenu Mapiranja identiteta u poduze⌂u" na stranici 78.
3. Pro⌂irite EIM domenu na koju ste sada povezani.
4. Za prikaz popisa definicija registra za domenu kliknite **Korisni⌂ki registri**.

   Bilješka: Ako za kontrolu pristupa izabranih registara imate Administrator, popis sadr⌂i samo one definicije registara nad kojima imate specifi⌂na ovla⌂tenja.
5. Desno kliknite na definiciju registra za koju ⌂elite dodati zamjensko ime i izaberite **Svojstva...**
6. Izaberite stranicu **Zamjenska imena** i specificirajte ime i tip zamjenskog imena koje ⌂elite dodati.

   Bilješka: Mo⌂ete specificirati tip zamjenskog imena koji nije uklju⌂en u popis tipova.
7. Ako je potrebno kliknite **Pomo⌂** da odredite koje informacije navesti u odre⌂enom polju.
8. Kliknite **Dodaj**.
9. Kliknite **OK** za spremanje promjena u definiciju registra.

Definiranje privatnog tipa korisni⌂kog registra u Mapiranju identiteta u poduze⌂u

Kada kreirate definiciju registra za Mapiranje identiteta u poduze⌂u (EIM) mo⌂ete specificirati jedan od brojnih predefiniranih tipova korisni⌂kog registra za predstavljanje stvarnog korisni⌂kog registra koji postoji na sistemu unutar poduze⌂a. Iako unaprijed definirani tipovi definicije registra pokrivaju ve⌂inu operativnih korisni⌂kih registara, mo⌂da ⌂ete trebati kreirati definiciju registra za koju EIM ne uklju⌂uje unaprijed definirane tipove registra. U ovoj situaciji imate dvije mogu⌂nosti. Mo⌂ete ili koristiti postoje⌂u definiciju registra koja se podudara s karakteristikama va⌂eg korisni⌂kog registra ili mo⌂ete definirati privatni tip korisni⌂kog registra.

Za definiranje tipa korisni⌂kog registra za koji EIM nije predefiniran da prepoznaje, morate koristiti objektni identitet (OID) za specificiranje tipa registra u obliku **ObjectIdentifier-normalizacija**, gdje je **ObjectIdentifier** objektni identifikator s decimalnom to⌂kom kao 1.2.3.4.5.6.7, a **normalizacija** ili vrijednost **caseExact** ili vrijednost **caseIgnore**. Na primjer, objektni identifikator (OID) za OS/400 je 1.3.18.0.2.33.2-caseIgnore.

Trebali biste pribaviti sve OID-e koje trebate od legitimnih OID ovla⌂tenja registracije za osiguranje da kreirate i koristite jedinstvene OID-e. Jedinstveni OID-i poma⌂u vam u izbjegavanju mogu⌂ih sukoba s OID-ima kreiranim od drugih organizacija ili aplikacija.

Postoje dva na⌂ina dobavljanja OID-a:

- **Registriranje objekata s ovla⌂tenjem**. Ova metoda je dobar izbor kada trebate manji broj ⌂vrstih OID-a za predstavljanje informacija. Na primjer, ovi OID-ovi mogu predstavljati police certifikata za korisnike u va⌂em poduze⌂u.
- **Postizanje dodjele luka iz ovla⌂tenja registracije i dodjeljivanje va⌂ih vlastitih OID-a prema potrebi**. Ova metoda, dodjela raspona identifikatora objekta s decimalnom to⌂kom, dobar je izbor ako trebate velik broj OID-a ili ako su va⌂e dodjele OID-a podlo⌂ne promjeni. Dodjela luka sastoji se od po⌂etnih brojeva s decimalnom to⌂kom iz kojih morate zasnovati va⌂ **ObjectIdentifier**. Na primjer, dodjela luka mogla bi biti 1.2.3.4.5.. Tada mo⌂ete 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).

Mo⌂ete nau⌂iti vi⌂e o registriranju va⌂ih OID-a s ovla⌂tenjem registracije, pregledavanjem ovih Internet resursa:

- American National Standards Institute (ANSI) je ovla⌂tenje registracije Sjedinjenih dr⌂ava za imena organizacija pod globalnom registracijskom obradom uspostavljenom od International Standards Organization (ISO) i International Telecommunication Union (ITU). Stranicu ⌂injenica u Microsoft Word formatu o primjeni za Identifikator registriranog dobavlja⌂a aplikacija (RID), lociran je na Web stranici ANSI Javna knji⌂nica dokumenata

http://public.ansi.org/ansionline/Documents/ . Stranicu ⌂injenica mo⌂ete na⌂i izborom **Ostale usluge > Programi registracije**. ANSI OID luk za organizacije je 2.16.840.1. ANSI napla⌂uje pristojbu za dodjele OID luka. Potrebno je otprilike dva tjedna za primanje dodijeljenog OID luka iz ANSI-a. ANSI ⌂e dodijeliti broj (NEWNUM) za kreiranje novog OID luka; na primjer: 2.16.840.1.NEWNUM.

- U ve⌂ini zemalja ili regija, udru⌂enje nacionalnih standarda odr⌂ava OID registar. Kao kod ANSI luka, ovi su op⌂eniti lukovi dodijeljeni pod OID-om 2.16. Mo⌂e biti potrebno malo istra⌂ivanje da se prona⌂e OID ovla⌂tenje za odre⌂enu zemlju ili regiju. Adresa za ISO nacionalne ⌂lanove tijela mo⌂e se prona⌂i na http://www.iso.ch/addresse/membodies.html . Informacije uklju⌂uju po⌂tansku adresu i elektroni⌂ku po⌂tu. U mnogim slu⌂ajevima specificirana je i Web stranica.
- Ovla⌂tenje Dodijele Brojeva Internetom (IANA) dodjeljuje privatne brojeve za poduze⌂a, ⌂to su OID-ovi u luku 1.3.6.1.4.1. IANA je dodijelila lukove vi⌂e od 7500 tvrtki do danas. Aplikacijska stranica smje⌂tena je na http://www.iana.org/cgi-bin/enterprise.pl , pod Brojevima privatnih poduze⌂a. IANA obi⌂no traje oko jedan tjedan. OID od IANA-e je besplatan. IANA ⌂e dodijeliti broj (NEWNUM) za kreiranje novog OID luka; na primjer: 1.3.6.1.4.1.NEWNUM.
- Savezna vlada Sjedinjenih Dr⌂ava odr⌂ava Computer Security Objects Registry (CSOR). CSOR je ovla⌂tenje imenovanja za luk 2.16.840.1.101.3 i za trenutne objekte registriranja za sigurnosne labele, kriptografi⌂ke algoritme i politike certifikata. OID-ovi politike certifikata su definirani u luku 2.16.840.1.101.3.2.1. CSOR osigurava politiku OID-a za agencije Vlade Sjedinjenih dr⌂ava. Za vi⌂e informacija o CSOR-u, pogledajte http://csrc.nist.gov/csor/ .

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

Omogu⌂avanje podr⌂ke pregledavanja mapiranja i kori⌂tenje asocijacija politika za ciljni registar

EIM podr⌂ka politike mapiranja omogu⌂uje vam kori⌂tenje asocijacija politike kao sredstvo kreiranja mapiranja s vi⌂e na jedno u situacijama gdje asocijacije izme⌂u korisni⌂kih identiteta i EIM identifikatora ne postoje. Asocijaciju politike mo⌂ete koristiti za mapiranje izvornog skupa vi⌂estrukih korisni⌂kih identiteta (umjesto jednostrukog korisni⌂kog identiteta) na jednostruki ciljni korisni⌂ki identitet u odre⌂enom ciljnom korisni⌂kom registru.

Da biste mogli koristiti asocijacije politika morate prvo biti sigurni da ste omogu⌂ili pregledavanje mapiranja upotrebom asocijacija za domenu. Tako⌂er morate omogu⌂iti jednu ili dvije postavke za svaki registar:

- **Omogu⌂avanje pregledavanja mapiranja za registar** Izaberite ovu opciju da osigurate da registar mo⌂e sudjelovati u EIM operacijama pregledavanja mapiranja bez obzira je li za registar definirana bilo kakva asocijacija politika.
- **Upotreba asocijacija politika** Izaberite ovu opciju da omogu⌂ite da ovaj registar bude ciljni registar asocijacije politike i da osigurate da mo⌂e sudjelovati u EIM operacijama pregledavanja mapiranja.

Ako ne omogu⌂ite pregledavanja mapiranja za registar, taj registar ne mo⌂e sudjelovati u EIM operacijama pregledavanja mapiranja. Ako ne navedete da registar koristi asocijacije politika tada EIM operacije pregledavanja mapiranja zanemaruju sve asocijacije politika za registar kada je registar cilj operacije.

Za omogu⌂avanje da pregledavanje mapiranja koristi asocijacije politika za ciljni registar morate biti spojeni na EIM domenu u kojoj ⌂elite raditi i morate imati “EIM kontrola pristupa” na stranici 33 na jednoj od sljede⌂ih razina:

- EIM administrator
- Administrator registra
- Administrator za izabrane registre (za registar koji ⌂elite omogu⌂iti)

Za op⌂enito omogu⌂avanje podr⌂ke pregledavanja mapiranja i dozvole specifi⌂nog kori⌂tenja asocijacija politike, izvedite sljede⌂e korake:

1. Pro⌂irite **Mre⌂a > Mapiranje identiteta u poduze⌂u > Upravljanje domenom**.

2. Izaberite EIM domenu u kojoj ⌂elite raditi.
   - Ako EIM domena s kojom ⌂elite raditi nije ispisana u **Upravljanje domenom**, pogledajte “Dodavanje domene Mapiranja identiteta u poduze⌂u u folder Upravljanja domenom” na stranici 78.
   - Ako trenutno niste povezani s EIM domenom u kojoj ⌂elite raditi, pogledajte Povezivanje s EIM kontrolerom domene.
3. Za prikaz popisa definicija registra za domenu izaberite **Korisni⌂ki registri**.

   Bilješka: Ako za kontrolu pristupa izabranih registara imate Administrator, popis sadr⌂i samo one definicije registara nad kojima imate specifi⌂no ovla⌂tenje.
4. Desno kliknite definiciju registra za koju ⌂elite omogu⌂iti podr⌂ku politike mapiranja za asocijacije politika i izaberite **Politika mapiranja...**
5. Na stranici **Op⌂enito** izaberite **Omogu⌂i pregledavanja mapiranja za registar**. Izbor ove opcije omogu⌂uje da registar sudjeluje u EIM operacijama pregledavanja mapiranja. Ako ova opcija nije izabrana, operacija pregledavanja ne mo⌂e vratiti podatke za registar, bez obzira je li registar u operaciji pregledavanja izvorni registar ili ciljni registar.
6. Izaberite **Koristi asocijacije politike**. Izborom ove opcije omogu⌂uje se da operacije pregledavanja koriste asocijacije politika kao osnovu za vra⌂anje podataka kada je registar cilj operacije pregledavanja.
7. Kliknite **OK** da spremite promjene.

Bilješka: Da bi registar mogao koristiti asocijacije politika, morate tako⌂er osigurati da ste omogu⌂ili asocijacije politika za domenu.

Brisanje definicije registra

Kada bri⌂ete definiciju registra iz EIM domene, ne utje⌂ete na korisni⌂ki registar na koji se odnosi definicija registra, ali taj korisni⌂ki registar ne mo⌂e vi⌂e sudjelovati u EIM domeni. Zato morate razmotriti sljede⌂e stvari kada bri⌂ete definiciju registra:

- Kada bri⌂ete definiciju registra, gubite sve asocijacije za taj korisni⌂ki registar. Ako ponovo definirate registar u domeni, morate kreirati ponovo sve potrebne asocijacije.
- Kada bri⌂ete definiciju X.509 registra, tako⌂er gubite sve filtere certifikata definirane za taj registar. Ako ponovo definirate registar u domeni, morate kreirati ponovo sve potrebne filtere certifikata.
- Ne mo⌂ete brisati definiciju sistemskog registra ako postoje definicije registra aplikacije koje specificiraju definiciju sistemskog registra kao nadre⌂enog registra.

Za brisanje definicije registra, morate biti povezani na EIM domenu u kojoj ⌂elite raditi i morate imati EIM administratorsku kontrolu pristupa.

Za brisanje EIM definicije registra, izvedite sljede⌂e korake:

1. Pro⌂irite **Mre⌂a > Mapiranje identiteta u poduze⌂u > Upravljanje domenom**.
2. Izaberite EIM domenu u kojoj ⌂elite raditi.
   - Ako EIM domena s kojom ⌂elite raditi nije ispisana u **Upravljanje domenom**, pogledajte “Dodavanje domene Mapiranja identiteta u poduze⌂u u folder Upravljanja domenom” na stranici 78.
   - Ako trenutno niste povezani s EIM domenom u kojoj ⌂elite raditi, pogledajte Povezivanje s EIM kontrolerom domene.
3. Pro⌂irite EIM domenu na koju ste povezani.
4. Za prikaz popisa definicija registra za domenu kliknite na **Korisni⌂ki registri**.

   Bilješka: Ako za kontrolu pristupa izabranih registara imate Administrator, popis sadr⌂i samo one definicije registara nad kojima imate specifi⌂na ovla⌂tenja.
5. Desno kliknite na korisni⌂ki registar koji ⌂elite izbrisati i izaberite **Brisanje...**.
6. Kliknite **Da** na dijalogu **Potvrda** za brisanje definicije registra.

Uklanjanje zamjenskog imena iz definicije registra

Za uklanjanje zamjenskog imena iz EIM definicije registra, morate biti povezani na EIM domenu u kojoj ∆elite raditi i morate imati "EIM kontrola pristupa" na stranici 33 na jednoj od ovih razina:

- Administrator registra.
- Administrator za izabrane registre (za definiciju registra s kojom ∆elite raditi)
- EIM administrator.

Za uklanjanje zamjenskog imena iz definicije EIM registra, izvedite sljede∆e korake:

1. Pro∆irite **Mre∆a > Mapiranje identiteta u poduze∆u > Upravljanje domenom**.
2. Izaberite EIM domenu u kojoj ∆elite raditi.
   - Ako EIM domena u kojoj ∆elite raditi nije ispisana pod Upravljanje domenom, pogledajte "Dodavanje domene Mapiranja identiteta u poduze∆u u folder Upravljanja domenom" na stranici 78.
   - Ako trenutno niste povezani s EIM domenom u kojoj ∆elite raditi, pogledajte "Povezivanje na domenu Mapiranja identiteta u poduze∆u" na stranici 78.
3. Pro∆irite EIM domenu na koju ste sada povezani.
4. Za prikaz popisa definicija registra za domenu kliknite **Korisni∆ki registri**.

   Bilješka: Ako za kontrolu pristupa izabranih registara imate Administrator, popis sadr∆i samo one definicije registara nad kojima imate specifi∆na ovla∆tenja.
5. Desno kliknite na definiciju registra i izaberite **Svojstva...**.
6. Izaberite stranicu **Zamjensko ime**.
7. Izaberite zamjensko ime koje ∆elite ukloniti i kliknite **Ukloni**.
8. Kliknite **OK** za spremanje promjena.

Upravljanje identifikatorima Mapiranja identiteta u poduze∆u

Kreiranje i upotreba EIM identifikatora koji predstavljaju korisnike u va∆oj mre∆i mogu biti veoma korisni za pomo∆ kada pratite koja je osoba vlasnik odre∆enog korisni∆kog identiteta. Korisnici unutar poduze∆a se skoro stalno mijenjaju, neki dolaze, neki odlaze, a neki se premje∆taju me∆u podru∆jima. Ove se promjene dodaju stalnom administrativnom problemu zadr∆avanja traga korisni∆kih identiteta i lozinki za sisteme i aplikacije u mre∆i. Dodatno, upravljanje lozinkom oduzima veliku koli∆inu vremena u nekom poduze∆u. Kreiranjem identifikatora Mapiranja identiteta u poduze∆u (EIM) i njihovim pridru∆ivanjem korisni∆kim identitetima za svakog korisnika, mo∆ete napraviti proces pra∆enja tko je vlasnik odre∆enog korisni∆kog identiteta. Time mo∆ete tako∆er pojednostaviti upravljanje lozinkom.

Implementacijom okru∆enja jednostruke prijave pojednostavljuje se proces upravljanja korisni∆kim identitetima za korisnike, posebno kada se oni premje∆taju na druge odjele ili podru∆ja unutar poduze∆a. Okru∆enje jednostruke prijave mo∆e eliminirati potrebu da ti korisnici pamte nova korisni∆ka imena i lozinke za nove sisteme.

Bilješka: Kako ∆ete kreirati i koristiti EIM identifikatore ovisi o potrebama va∆e organizacije. Za nau∆iti vi∆e, pogledajte "Razvoj plana imenovanja EIM identifikatora" na stranici 54.

Mo∆ete upravljati EIM identifikatorima za neku EIM domenu koja je dostupna pod folderom **Upravljanje domenom**. Mo∆ete izvesti bilo koji od sljede∆ih zadataka za upravljanje EIM identifikatorima u EIM domeni:

- "Kreiranje identifikatora Mapiranja identiteta u poduze∆u" na stranici 88
- "Dodavanje zamjenskog imena identifikatoru Mapiranja identiteta u poduze∆u" na stranici 88
- "Uklanjanje zamjenskog imena iz identifikatora Mapiranja identiteta u poduze∆u" na stranici 89
- "Prilagodba pogleda identifikatora Mapiranja identiteta u poduze∆u" na stranici 90
- "Brisanje identifikatora Mapiranja identiteta u poduze∆u" na stranici 89

Tako∆er vam mo∆e biti od koristi "Upravljanje asocijacijama" na stranici 90 kada upravljate EIM identifikatorima.

Kreiranje identifikatora Mapiranja identiteta u poduze⌂u

Za kreiranje EIM identifikatora morate biti povezani s domenom Mapiranja identiteta u poduze⌂u (EIM) u kojoj ⌂elite raditi i morate imati "EIM kontrola pristupa" na stranici 33 na jednoj od ovih razina:

- Administrator identifikatora.
- EIM administrator.

Za kreiranje EIM identifikatora za osobu ili cjelinu u va⌂em poduze⌂u, izvedite ove korake:

1. Pro⌂irite **Mre⌂a > Mapiranje identiteta u poduze⌂u > Upravljanje domenom**.
2. Izaberite EIM domenu u kojoj ⌂elite raditi.
   - Ako EIM domena s kojom ⌂elite raditi nije ispisana u **Upravljanje domenom**, pogledajte "Dodavanje domene Mapiranja identiteta u poduze⌂u u folder Upravljanja domenom" na stranici 78.
   - Ako trenutno niste povezani s EIM domenom u kojoj ⌂elite raditi, pogledajte Povezivanje s EIM kontrolerom domene.
3. Pro⌂irite EIM domenu na koju ste sada povezani.
4. Desno kliknite na **Identifikatori** i izaberite **Nov identifikator...**.
5. U dijalogu **Novi EIM identifikator**, osigurajte informacije o EIM identifikatoru kako slijedi:
   - Ime za identifikator.
   - Ako je potrebno da li ⌂elite da sistem generira jedinstveno ime.
   - Opis identifikatora.
   - Ako je potrebno, jedno ili vi⌂e zamjenskih imena za identifikator.
6. Ako je potrebno kliknite **Pomo⌂** da odredite koje informacije navesti u odre⌂enom polju.
7. Nakon ⌂to osigurate potrebne informacije, za kreiranje EIM identifikatora kliknite **OK**.

Bilješka: Ako kreirate veliki broj EIM identifikatora, ponekad pro⌂e puno vremena prije no ⌂to se poka⌂e popis identifikatora kada pro⌂irite folder **Identifikatori**. Da pobolj⌂ate performansu kada imate veliki broj EIM identifikatora u domeni, mo⌂ete "Prilagodba pogleda identifikatora Mapiranja identiteta u poduze⌂u" na stranici 90.

Dodavanje zamjenskog imena identifikatoru Mapiranja identiteta u poduze⌂u

Mo⌂ete kreirati zamjensko ime za osiguranje dodatnih razlikovnih informacija za "EIM identifikator" na stranici 9. Zamjenska imena mogu pomo⌂i u lociranju odre⌂enog identifikatora Mapiranja identiteta u poduze⌂u (EIM) prilikom izvo⌂enja operacije EIM pregledavanja. Na primjer, zamjenska imena mogu biti korisna u situacijama gdje je ne⌂ije zakonito ime druga⌂ije od imena pod kojim je ta osoba poznata.

Imena EIM identifikatora moraju biti jedinstvena u EIM domeni. Zamjenska imena mogu pomo⌂i u adresiranju situacija gdje kori⌂tenje jedinstvenih imena identifikatora mo⌂e biti te⌂ko. Na primjer, razli⌂iti pojedinci unutar poduze⌂a mogu dijeliti isto ime, ⌂to mo⌂e biti zbunjuju⌂e ako koristite prava imena kao EIM identifikatore. Na primjer, ako imate dva korisnika s imenom Ivan I. Ivani⌂, mogli biste kreirati zamjensko ime Ivan Ivo Ivani⌂ za jednog i Ivan Ivica Ivani⌂ za drugog kako bi lak⌂e razlikovali identitet svakog korisnika. Dodatna zamjenska imena mogu sadr⌂avati zaposleni⌂ki broj svakog korisnika, broj odjela, naziva radnog mjesta ili ostale razlikovne atribute.

Za dodavanje zamjenskog imena EIM identifikatoru, morate biti povezani na EIM domenu u kojoj ⌂elite raditi i morate imati "EIM kontrola pristupa" na stranici 33 na jednoj od sljede⌂ih razina:

- EIM administrator.
- Administrator identifikatora.

Da dodate zamjensko ime EIM identifikatoru, dovr⌂ite ove korake.

1. Pro⌂irite **Mre⌂a > Mapiranje identiteta u poduze⌂u > Upravljanje domenom**.
2. Izaberite EIM domenu u kojoj ⌂elite raditi.
   - Ako EIM domena u kojoj ⌂elite raditi nije ispisana pod Upravljanje domenom, pogledajte "Dodavanje domene Mapiranja identiteta u poduze⌂u u folder Upravljanja domenom" na stranici 78.

- Ako trenutno niste povezani s EIM domenom u kojoj ⌂elite raditi, pogledajte "Povezivanje na domenu Mapiranja identiteta u poduze⌂u" na stranici 78.

3. Pro⌂irite EIM domenu na koju ste povezani.
4. Kliknite **Identifikatori**, u oknu na desnoj strani, za prikaz popisa EIM identifikatora dostupnih u domeni.

   Bilješka: Ponekad kada poku⌂ate pro⌂iriti folder **Identifikatori** mo⌂e pro⌂i puno vremena prije nego se popis identifikatora prika⌂e. Da pobolj⌂ate performanse kada imate veliki broj EIM identifikatora u domeni, mo⌂ete "Prilagodba pogleda identifikatora Mapiranja identiteta u poduze⌂u" na stranici 90.

5. Desno kliknite na EIM identifikator za koji ⌂elite dodati zamjensko ime i izaberite **Svojstva...**
6. U polju **Zamjensko ime**, specificirajte zamjensko ime koje ⌂elite dodati u ovaj EIM identifikator i kliknite **Dodaj**.
7. Kliknite **OK** za spremanje promjena EIM identifikatora.

Uklanjanje zamjenskog imena iz identifikatora Mapiranja identiteta u poduze⌂u

Za uklanjanje zamjenskog imena iz EIM identifikatora, morate biti povezani na EIM domenu u kojoj ⌂elite raditi i morate imati "EIM kontrola pristupa" na stranici 33 na jednoj od sljede⌂ih razina:

- Administrator identifikatora
- EIM administrator

Za uklanjanje zamjenskog imena iz EIM identifikatora, izvedite sljede⌂e korake:

1. Pro⌂irite **Mre⌂a > Mapiranje identiteta u poduze⌂u > Upravljanje domenom**.
2. Izaberite EIM domenu u kojoj ⌂elite raditi.
   - Ako EIM domena u kojoj ⌂elite raditi nije ispisana pod Upravljanje domenom, pogledajte "Dodavanje domene Mapiranja identiteta u poduze⌂u u folder Upravljanja domenom" na stranici 78.
   - Ako trenutno niste povezani s EIM domenom u kojoj ⌂elite raditi, pogledajte "Povezivanje na domenu Mapiranja identiteta u poduze⌂u" na stranici 78.
3. Pro⌂irite EIM domenu na koju ste povezani.
4. Kliknite **Identifikatori**, u oknu na desnoj strani, za prikaz popisa EIM identifikatora dostupnih u domeni.

   Bilješka: Ponekad kada poku⌂ate pro⌂iriti folder **Identifikatori** mo⌂e pro⌂i puno vremena prije nego se popis identifikatora prika⌂e. Da pobolj⌂ate performanse kada imate veliki broj EIM identifikatora u domeni, mo⌂ete "Prilagodba pogleda identifikatora Mapiranja identiteta u poduze⌂u" na stranici 90.

5. Desno kliknite na EIM identifikator za koji ⌂elite dodati zamjensko ime i izaberite **Svojstva...**
6. Izaberite zamjensko ime koje ⌂elite ukloniti i kliknite **Ukloni**.
7. Za spremanje promjena kliknite **OK**.

Brisanje identifikatora Mapiranja identiteta u poduze⌂u

Za brisanje EIM identifikatora morate biti spojeni na domenu Mapiranja identiteta u poduze⌂u u kojoj ⌂elite raditi i morate imati EIM administrator kontrolu pristupa.

Za brisanje EIM identifikatora, izvedite sljede⌂e korake:

1. Pro⌂irite **Mre⌂a > Mapiranje identiteta u poduze⌂u > Upravljanje domenom**.
2. Izaberite EIM domenu u kojoj ⌂elite raditi.
   - Ako EIM domena s kojom ⌂elite raditi nije ispisana u **Upravljanje domenom**, pogledajte "Dodavanje domene Mapiranja identiteta u poduze⌂u u folder Upravljanja domenom" na stranici 78.
   - Ako trenutno niste povezani s EIM domenom u kojoj ⌂elite raditi, pogledajte Povezivanje s EIM kontrolerom domene.
3. Pro⌂irite EIM domenu na koju ste sada povezani.
4. Kliknite **Identifikatori**.

Bilješka: Ponekad kada poku⌂ate pro⌂iriti folder **Identifikatori** mo⌂e pro⌂i puno vremena prije nego se popis identifikatora prika⌂e. Da poboljˆate performanse kada imate veliki broj EIM identifikatora u domeni, mo⌂ete "Prilagodba pogleda identifikatora Mapiranja identiteta u poduze⌂u".

5. Izaberite EIM identifikator koji ⌂elite obrisati. Za brisanje vi⌂estrukih identifikatora, pritisnite **Ctrl** tipku dok birate EIM identifikatore.
6. Desno kliknite na izabrane EIM identifikatore i izaberite **Brisanje**.
7. Na dijalogu **Potvrda brisanja**, kliknite **Da** za brisanje izabranih EIM identifikatora.

Prilagodba pogleda identifikatora Mapiranja identiteta u poduze⌂u

Ponekad kada poku⌂ate pro⌂iriti folder **Identifikatori** mo⌂e pro⌂i puno vremena prije nego se popis identifikatora prika⌂e. Za poboljˆanje performanse kada imate veliki broj identifikatora Mapiranja identiteta u poduze⌂u (EIM) u domeni, mo⌂ete prilagoditi pogled za folder **Identifikatori**.

Za prilagodbu pogleda foldera **Identifikatori**, sljedite ove korake:

1. Pro⌂irite **Mre⌂a —> Mapiranje identiteta u poduze⌂u -> Upravljanje domenom**.
2. Izaberite EIM domenu u kojoj ⌂elite raditi.
   - Ako EIM domena s kojom ⌂elite raditi nije ispisana u **Upravljanje domenom**, pogledajte "Dodavanje domene Mapiranja identiteta u poduze⌂u u folder Upravljanja domenom" na stranici 78.
   - Ako trenutno niste povezani s EIM domenom u kojoj ⌂elite raditi, pogledajte Povezivanje s EIM kontrolerom domene.
3. Desno kliknite folder **Identifikatori** pa izaberite **Prilagodi Ovaj Pogled**.
4. Specificirajte kriterije koje ⌂elite koristiti za prikaz EIM identifikatora u domeni. Za smanjenje broja prikazanih EIM identifikatora, specificirajte znakove koje ⌂elite koristiti za sortiranje identifikatora. Mo⌂ete specificirati jedan ili vi⌂e generi⌂kih znakova (*) u imenu identifikatora. Na primjer, mo⌂ete upisati *JOHNSON* za va⌂ kriterij sortiranja u polje **Identifikatori**. Rezultati ⌂e vratiti sve EIM identifikatore u kojima je niz znakova JOHNSON definiran kao dio imena EIM identifikatora, a tako⌂er ⌂e vratiti i EIM identifikatore u kojima je niz znakova JOHNSON definiran kao dio zamjenskog imena za EIM identifikator.
5. Kliknite **OK** da spremite promjene.

Upravljanje asocijacijama

EIM vam dozvoljava kreiranje i upravljanje s dva tipa asocijacija, koje definiraju izravne i neizravne odnose izme⌂u korisni⌂kih identiteta: asocijacije identifikatora i asocijacije politike. EIM vam dozvoljava kreiranje i upravljanje asocijacijama identifikatora izme⌂u EIM identifikatora i njihovih korisni⌂kih identiteta ⌂to vam omogu⌂uje definiranje neizravnih ali specifi⌂nih pojedina⌂nih odnosa izme⌂u korisni⌂kih identiteta. EIM vam tako⌂er dozvoljava kreiranje asocijacija politike za opis odnosa izme⌂u vi⌂estrukih korisni⌂kih identiteta iz jednog ili vi⌂e registara i pojedina⌂nog ciljnog korisni⌂kog identiteta u drugom registru. Asocijacije politike koriste podr⌂ku politike EIM mapiranja za kreiranje vi⌂e-prema-jedan mapiranja izme⌂u korisni⌂kih identiteta bez uklju⌂ivanja EIM identifikatora. Zbog toga ⌂to oba tipa asocijacija definiraju odnose izme⌂u korisni⌂kih identiteta u nekom poduze⌂u, upravljanje asocijacijama je va⌂an element upravljanja EIM-om.

Odr⌂avanje asocijacija unutar domene je klju⌂ pojednostavljivanja administrativnih zadataka potrebnih za pra⌂enje korisnika koji imaju ra⌂une na razli⌂itim sistemima na mre⌂i. Trebate odr⌂avati teku⌂e identifikatore asocijacija i asocijacije politike kada implementirate mre⌂u sigurne jednostruke prijave.

Mo⌂ete izvesti sljede⌂e zadatke upravljanja za asocijacije:

- "Kreiranje asocijacija" na stranici 91
- Dodavanje informacija pregledavanja ciljnom korisni⌂kom identitetu.
- Uklanjanje informacija pregledavanja iz ciljnog korisni⌂kog identiteta.
- Prikaz asocijacija za EIM identifikator.
- Prikaz svih asocijacija politike za domenu.
- Prikaz svih asocijacija politike za registar.

| • “Brisanje asocijacije identifikatora” na stranici 102
| • “Brisanje asocijacije politike” na stranici 103

Kreiranje asocijacija

Mo⌂ete kreirati asocijacije na jedan od dva na⌂ina:

- Mo⌂ete kreirati neku asocijaciju identifikatora kako bi neizravno definirali odnos izme⌂u dva korisni⌂ka identiteta koja koristi jednostruki korisnik. Asocijacija identifikatora opisuje odnos izme⌂u nekog EIM identifikatora i korisni⌂kog identiteta u korisni⌂kom registru. Asocijacije identifikatora dozvoljavaju vam kreiranje jedan-prema-jedan mapiranja izme⌂u EIM identifikatora i svakog od raznolikih korisni⌂kih identiteta koji se odnose na korisnika kojeg predstavlja EIM identifikator.
- Mo⌂ete kreirati asocijaciju politike da izravno definirate odnos izme⌂u vi⌂estrukih korisni⌂kih identiteta iz jednog ili iz vi⌂e registara i pojedinog ciljnog korisni⌂kog identiteta iz drugog registra. Asocijacije politike koriste podr⌂ku politike EIM mapiranja za kreiranje vi⌂e-prema-jedan mapiranja izme⌂u korisni⌂kih identiteta bez uklju⌂ivanja EIM identifikatora. Asocijacije politike omogu⌂uju brzo kreiranje velikog broja mapiranja izme⌂u povezanih korisni⌂kih identiteta u razli⌂itim korisni⌂kim registrima.

Da li ⌂ete izabrati kreirati asocijacije identifikatora, kreirati asocijacije politike ili koristiti mje⌂avinu obje metode ovisi o va⌂im potrebama EIM implementacije. Za nau⌂iti vi⌂e, pogledajte Razvijanje ukupnog plana mapiranja identiteta.

Kreiranje asocijacije identifikatora: Asocijacije identifikatora definiraju odnos izme⌂u EIM identifikatora i korisni⌂kog identiteta u va⌂em poduze⌂u za osobu ili cjelinu na koju se EIM identifikator odnosi. Mo⌂ete kreirati tri tipa asocijacije identifikatora: ciljni, izvorni i administrativni. Da bi sprije⌂ili mogu⌂e probleme s asocijacijama i na⌂inom na koji one mapiraju identitete, prije nego po⌂nete definirati asocijacije, za svoje poduze⌂e morate razviti ukupni plan mapiranja identiteta.

Za kreiranje asocijacije identifikatora morate biti spojeni na EIM domenu u kojoj ⌂elite raditi i morate imati “EIM kontrola pristupa” na stranici 33 potrebno za tip asocijacije koju ⌂elite kreirati.

Za kreiranje izvorne ili administrativne asocijacije morate imati EIM kontrolu pristupa na jednoj od sljede⌂ih razina:

- Administrator identifikatora.
- EIM administrator.

Za kreiranje ciljne asocijacije morate imati EIM kontrolu pristupa na jednoj od sljede⌂ih razina:

- Administrator registra.
- Administrator za izabrane registre (za definiciju registra koja se odnosi na korisni⌂ki registar koji sadr⌂i ciljni korisni⌂ki identitet)
- EIM administrator.

Za kreiranje asocijacije identifikatora, izvedite sljede⌂e korake:

1. Pro⌂irite **Mre⌂a > Mapiranje identiteta u poduze⌂u > Upravljanje domenom**.
2. Izaberite EIM domenu u kojoj ⌂elite raditi.
   - Ako EIM domena s kojom ⌂elite raditi nije ispisana u **Upravljanje domenom**, pogledajte “Dodavanje domene Mapiranja identiteta u poduze⌂u u folder Upravljanja domenom” na stranici 78.
   - Ako trenutno niste povezani s EIM domenom u kojoj ⌂elite raditi, pogledajte Povezivanje s EIM kontrolerom domene.
3. Pro⌂irite EIM domenu na koju ste sada povezani.
4. Kliknite **Identifikatori** za prikaz liste EIM identifikatora za domenu.

   Bilješka: Ponekad kada poku⌂ate pro⌂iriti folder **Identifikatori** mo⌂e pro⌂i puno vremena prije nego se popis identifikatora prika⌂e. Da poboljˆate performansu kada imate veliki broj EIM identifikatora u domeni, mo⌂ete “Prilagodba pogleda identifikatora Mapiranja identiteta u poduze⌂u” na stranici 90.

5. Desno kliknite EIM identifikator za koji ∆elite kreirati asocijaciju i izaberite **Svojstva...**
6. Izaberite stranicu **Asocijacije** pa kliknite **Dodaj...**.
7. Za definiranje asocijacije u dijalogu **Dodavanje asocijacije** osigurajte informacije kao ∆to slijedi:
   - Ime registra koji sadr∆i korisni∆ki identitet koji ∆elite pridru∆iti s EIM identifikatorom. Navedite to∆no ime postoje∆e definicije registra ili ga potra∆ite i izaberite.
   - Ime korisni∆kog identiteta koje ∆elite pridru∆iti EIM identifikatoru.
   - Tip asocijacije. Mo∆ete kreirati jedan od tri razli∆ita tipa asocijacija:
     – Administrativni
     – Izvorni
     – Ciljni
8. Ako je potrebno kliknite **Pomo∆** da odredite koje informacije navesti u odre∆enom polju.
9. Opcijski. Za ciljnu asocijaciju kliknite **Napredno...** za prikaz dijaloga **Dodavanje asocijacije - Napredno**. Za ciljni korisni∆ki identitet navedite informacije pregledavanja i kliknite **OK** za povratak u dijalog **Dodavanje asocijacije**.
10. Nakon ∆to osigurate potrebne informacije za kreiranje asocijacije kliknite **OK**.

Kreiranje asocijacije politike: Asocijacija politike je sredstvo za direktno definiranje odnosa izme∆u vi∆estrukih korisni∆kih identiteta u jednom ili vi∆e registara i individualnog ciljnog korisni∆kog identiteta u drugom registru. Asocijacije politike koriste EIM podr∆ku politike mapiranja za kreiranje mapiranja me∆u korisni∆kim identitetima s vi∆e na jednog bez uklju∆ivanja EIM identifikatora. Budu∆i da mo∆ete koristiti asocijacije politika na mno∆tvo preklapaju∆ih na∆ina, morate dobro razumjeti EIM podr∆ku politike mapiranja da biste mogli kreirati i koristiti asocijacije politika. Tako∆er, da biste sprije∆ili mogu∆e probleme s asocijacijama i s na∆inom mapiranja identiteta, za va∆ posao morate razviti cjelokupni plan mapiranja identiteta prije nego po∆nete definirati asocijacije.

Da li ∆ete izabrati kreirati asocijacije identifikatora, kreirati asocijacije politike ili koristiti kombinaciju obaju metoda ovisi o va∆im potrebama EIM implementacije.

Kako ∆ete kreirati asocijacije politike varira ovisno o tipu asocijacije politike. Da nau∆ite vi∆e o tome kako kreirati asocijaciju politike pogledajte:

- Kreiranje default asocijacije politike domene.
- Kreiranje default asocijacije politike registra.
- Kreiranje asocijacije politike filtera certifikata.

Kreiranje default asocijacije politike domene: Za kreiranje default asocijacije politike domene morate biti povezani s EIM domenom u kojoj ∆elite raditi i morate imati “EIM kontrola pristupa” na stranici 33 na jednoj od tih razina:

- EIM administrator
- Administrator registra

Bilješka: Asocijacija politike opisuje odnos izme∆u vi∆estrukih korisni∆kih identiteta i jednostrukog korisni∆kog identiteta u ciljnom korisni∆kog registru. Asocijaciju politike mo∆ete koristiti za opis odnosa izme∆u izvornog skupa vi∆estrukih korisni∆kih identiteta i jednostrukog ciljnog korisni∆kog identiteta u odre∆enom ciljnom korisni∆kom registru. Asocijacije politike koriste EIM podr∆ku politike mapiranja za kreiranje mapiranja me∆u korisni∆kim identitetima s vi∆e na jednog bez uklju∆ivanja EIM identifikatora.

Budu∆i da mo∆ete koristiti asocijacije politika na mno∆tvo preklapaju∆ih na∆ina, morate dobro razumjeti EIM podr∆ku politike mapiranja da biste mogli kreirati i koristiti asocijacije politika. Tako∆er, da biste sprije∆ili mogu∆e probleme s asocijacijama i s na∆inom mapiranja identiteta, za va∆ posao morate razviti cjelokupni plan mapiranja identiteta prije nego po∆nete definirati asocijacije.

U default asocijaciji politike domene, svi su korisnici u domeni izvor asocijacija politike i mapiraju se u jednostruki ciljni registar i ciljnog korisnika. Mo∆ete definirati default asocijaciju politike domene za svaki registar u domeni. Ako se dvije ili vi∆e asocijacija politike domene odnose na isti ciljni registar, mo∆ete definirati jedinstvene informacije

pregledavanja za svaku od tih asocijacija politike da osigurate da ih operacije pregledavanja mapiranja mogu razlikovati. Ina⌂e, operacije pregledavanja mapiranja mogu vratiti vi⌂estruke ciljne korisni⌂ke identitete. Rezultat ovih dvosmislenih rezultata je da aplikacija koja ovisi o EIM-u ne⌂e mo⌂i odrediti koji to⌂no ciljni identitet treba koristiti.

Za kreiranje default asocijacije politike domene izvedite sljede⌂e korake:

1. Pro⌂irite **Mre⌂a > Mapiranje identiteta u poduze⌂u > Upravljanje domenom**.
2. Desno kliknite EIM domenu u kojoj ⌂elite raditi i izaberite **Politika mapiranja...**
   - Ako EIM domena s kojom ⌂elite raditi nije ispisana u **Upravljanje domenom**, pogledajte "Dodavanje domene Mapiranja identiteta u poduze⌂u u folder Upravljanja domenom" na stranici 78.
   - Ako trenutno niste povezani s EIM domenom u kojoj ⌂elite raditi, pogledajte Povezivanje s EIM kontrolerom domene.
3. Na stranici Op⌂enito izaberite **Omogu⌂i preglede mapiranja kori⌂tenjem asocijacija politika za domenu** .
4. Izaberite stranicu **Domena** i kliknite **Dodaj...**.
5. U dijalogu **Dodavanje default asocijacije politike domene** navedite sljede⌂e potrebne informacije:
   - Ime definicije registra **Ciljnog registra** za asocijaciju politike.
   - Ime korisni⌂kog identiteta **Ciljnog korisnika** za asocijaciju politike.
6. Ako je potrebno, za vi⌂e pojedinosti o tome kako ovo napraviti i o daljnjim dijalozima, kliknite **Pomo⌂**.
7. Opcijski. Za prikaz dijaloga **Dodavanje asocijacije - Napredno** kliknite **Napredno...**. Specificirajte **Informacije pregledavanja** za asocijaciju politike i kliknite **OK** za povratak u dijalog **Dodavanje default asocijacije politike domene**.

   Bilješka: Ako se dvije ili vi⌂e default asocijacija politike domene odnose na isti ciljni registar, za svakog od ciljnih korisni⌂kih identiteta u ovim asocijacijama politike morate definirati jedinstvene informacije pregledavanja. U ovoj situaciji definiranjem informacija pregledavanja za svaki ciljni korisni⌂ki identitet osiguravate da ih operacije pregledavanja mapiranja mogu razlikovati. Ina⌂e, operacije pregledavanja mapiranja mogu vratiti vi⌂estruke ciljne korisni⌂ke identitete. Rezultat ovih dvosmislenih rezultata je da aplikacija koja ovisi o EIM-u ne⌂e mo⌂i odrediti koji to⌂no ciljni identitet treba koristiti.
8. Za kreiranje nove asocijacije kliknite **OK** i vratite se na stranicu **Domena**. Nova asocijacija politike sada je prikazana u tablici **Default asocijacije politika**.
9. Provjerite da je nova asocijacija politike omogu⌂ena za ciljni registar.
10. Da spremite svoje promjene i iza⌂ete iz dijaloga **Politika mapiranja** kliknite **OK**.

Bilješka: Provjerite da je politika mapiranja podr⌂ana i da je kori⌂tenje asocijacija politika za ciljni korisni⌂ki registar ispravno omogu⌂eno. Ako nije omogu⌂eno, asocijacija politike ne⌂e imati nikakav u⌂inak.

Kreiranje default asocijacije politike registra: Za kreiranje default asocijacije politike registra morate biti spojeni na EIM domenu u kojoj ⌂elite raditi i morate imati "EIM kontrola pristupa" na stranici 33 na jednoj od ovih razina:

- EIM administrator
- Administrator registra

Bilješka: Asocijacija politike opisuje odnos izme⌂u vi⌂estrukih korisni⌂kih identiteta i jednostrukog korisni⌂kog identiteta u ciljnom korisni⌂kog registru. Asocijaciju politike mo⌂ete koristiti za opis odnosa izme⌂u izvornog skupa vi⌂estrukih korisni⌂kih identiteta i jednostrukog ciljnog korisni⌂kog identiteta u odre⌂enom ciljnom korisni⌂kom registru. Asocijacije politike koriste EIM podr⌂ku politike mapiranja za kreiranje mapiranja me⌂u korisni⌂kim identitetima s vi⌂e na jednog bez uklju⌂ivanja EIM identifikatora.

Budu⌂i da mo⌂ete koristiti asocijacije politika na mno⌂tvo preklapaju⌂ih na⌂ina, morate dobro razumjeti EIM podr⌂ku politike mapiranja da biste mogli kreirati i koristiti asocijacije politika. Tako⌂er, da biste sprije⌂ili mogu⌂e probleme s asocijacijama i s na⌂inom mapiranja identiteta, za va⌂ posao morate razviti cjelokupni plan mapiranja identiteta prije nego po⌂nete definirati asocijacije.

U default asocijaciji politike registra, svi su korisnici u jednostrukom registru izvor asocijacije politike i mapiraju se u jednostruki ciljni registar i ciljnog korisnika. Kada omogu⌂ite default asocijaciju politike registra za ciljni registar, asocijacija politike osigurava da se ti izvorni korisni⌂ki identiteti mogu mapirati u jednostruki odre⌂eni ciljni registar i ciljnog korisnika.

Za kreiranje default asocijacije politike registra, izvedite sljede⌂e korake:

1. Pro⌂irite **Mre⌂a > Mapiranje identiteta u poduze⌂u > Upravljanje domenom**.
2. Desno kliknite EIM domenu u kojoj ⌂elite raditi i izaberite **Politika mapiranja...**
   - Ako EIM domena s kojom ⌂elite raditi nije ispisana u **Upravljanje domenom**, pogledajte "Dodavanje domene Mapiranja identiteta u poduze⌂u u folder Upravljanja domenom" na stranici 78.
   - Ako trenutno niste povezani s EIM domenom u kojoj ⌂elite raditi, pogledajte Povezivanje s EIM kontrolerom domene.
3. Na stranici Op⌂enito izaberite **Omogu⌂i preglede mapiranja kori⌂tenjem asocijacija politika za domenu** .
4. Izaberite stranicu **Registar**, a zatim kliknite **Dodaj...**.
5. U dijalogu **Dodavanje default asocijacije politike registra** navedite sljede⌂e potrebne informacije:
   - Ime definicije registra **Izvornog registra** za asocijaciju politike.
   - Ime definicije registra **Ciljnog registra** za asocijaciju politike.
   - Ime korisni⌂kog identiteta **Ciljnog korisnika** za asocijaciju politike.
6. Ako je potrebno, za vi⌂e pojedinosti o tome kako ovo napraviti i o daljnjim dijalozima, kliknite **Pomo⌂**.
7. Opcijski. Za prikaz dijaloga **Dodavanje asocijacije - Napredno** kliknite **Napredno...**. Specificirajte **informacije pregledavanja** za asocijaciju politike i kliknite **OK** za povratak u dijalog **Dodavanje default asocijacije politike registra**.

   Bilješka: Ako se dvije ili vi⌂e asocijacija politike s istim izvornim registrom odnose na isti ciljni registar, za svaki od ciljnih korisni⌂kih identiteta u ovim asocijacijama politika morate definirati jedinstvene informacije pregledavanja. U ovoj situaciji definiranjem informacija pregledavanja za svaki ciljni korisni⌂ki identitet osiguravate da ih operacije pregledavanja mapiranja mogu razlikovati. Ina⌂e, operacije pregledavanja mapiranja mogu vratiti vi⌂estruke ciljne korisni⌂ke identitete. Rezultat ovih dvosmislenih rezultata je da aplikacija koja ovisi o EIM-u ne⌂e mo⌂i odrediti koji to⌂no ciljni identitet treba koristiti.
8. Za kreiranje nove asocijacije politike kliknite **OK** i vratite se na stranicu **Registar**. Nova asocijacija politike registra sada je prikazana u tablici **Default asocijacije politika**.
9. Provjerite da je nova asocijacija politike omogu⌂ena za ciljni registar.
10. Da spremite svoje promjene i iza⌂ete iz dijaloga **Politika mapiranja** kliknite **OK**.

Bilješka: Provjerite da je politika mapiranja podr⌂ana i da je kori⌂tenje asocijacija politika za ciljni korisni⌂ki registar ispravno omogu⌂eno. Ako nije omogu⌂eno, asocijacija politike ne⌂e imati nikakav u⌂inak.

Kreiranje asocijacije politike filtera certifikata: Za kreiranje asocijacije politike filtera certifikata morate biti spojeni na EIM domenu u kojoj ⌂elite raditi i morate imati "EIM kontrola pristupa" na stranici 33 na jednoj od sljede⌂ih razina:

- EIM administrator
- Administrator registra

Bilješka: Asocijacija politike opisuje odnos izme⌂u izvornog skupa vi⌂estrukih korisni⌂kih identiteta i jednostrukog ciljnog korisni⌂kog identiteta u odre⌂enom ciljnom korisni⌂kom registru. Asocijacije politike koriste EIM podr⌂ku politike mapiranja za kreiranje mapiranja me⌂u korisni⌂kim identitetima s vi⌂e na jednog bez uklju⌂ivanja EIM identifikatora.

Budu⌂i da mo⌂ete koristiti asocijacije politika na mno⌂tvo preklapaju⌂ih na⌂ina, morate dobro razumjeti EIM podr⌂ku politike mapiranja da biste mogli kreirati i koristiti asocijacije politika. Tako⌂er, da biste

sprije⌂ili mogu⌂e probleme s asocijacijama i s na⌂inom mapiranja identiteta, za va⌂ posao morate razviti cjelokupni plan mapiranja identiteta prije nego po⌂nete definirati asocijacije.

U asocijaciji politike filtera certifikata u jednostrukom X.509 registru kao izvor asocijacija politike odre⌂ujete skup certifikata. Ovi se certifikati mapiraju u jednostruki ciljni registar i u ciljnog korisnika kojeg navedete. Za razliku od default asocijacije politike registra u kojoj su svi korisnici u jednostrukom registru izvor asocijacije politike, djelokrug asocijacije politike filtera certifikata je fleksibilniji. Kao izvor mo⌂ete u registru navesti podskup certifikata. Filter certifikata koji ste naveli za asocijaciju politike odre⌂uje svoj opseg.

Bilješka: Kreirajte i koristite default asocijaciju politike registra kada ⌂elite sve certifikate iz X.509 korisni⌂kog registra mapirati u jednostruki ciljni korisni⌂ki identitet.

Filter certifikata kontrolira kako asocijacija politike filtera certifikata mapira jedan izvorni skup korisni⌂kih identiteta, u ovom slu⌂aju digitalne certifikate, u odre⌂eni ciljni korisni⌂ki identitet. Prema tome, da bi mogli kreirati asocijaciju politike filtera certifikata mora postojati filter certifikata koji ⌂elite koristiti.

Da biste mogli kreirati asocijaciju politike filtera certifikata prvo morate kreirati filter koji ⌂e se koristiti kao osnova asocijacije politike.

Za kreiranje asocijacije politike filtera certifikata, izvedite sljede⌂e korake:

1. Pro⌂irite **Mre⌂a > Mapiranje identiteta u poduze⌂u > Upravljanje domenom**.
2. Desno kliknite EIM domenu u kojoj ⌂elite raditi i izaberite **Politika mapiranja...**
   - Ako EIM domena s kojom ⌂elite raditi nije ispisana u **Upravljanje domenom**, pogledajte “Dodavanje domene Mapiranja identiteta u poduze⌂u u folder Upravljanja domenom” na stranici 78.
   - Ako trenutno niste povezani s EIM domenom u kojoj ⌂elite raditi, pogledajte Povezivanje s EIM kontrolerom domene.
3. Na stranici Op⌂enito izaberite **Omogu⌂i preglede mapiranja kori⌂tenjem asocijacija politika za domenu** .
4. Izaberite stranicu **Filter certifikata** i za prikaz dijaloga **Dodavanje asocijacije politike filtera certifikata** kliknite **Dodaj...**.
5. Ako je potrebno, za vi⌂e pojedinosti o tome kako ovo napraviti i o daljnjim dijalozima, kliknite **Pomo⌂**.
6. Navedite sljede⌂e potrebne informacije za definiranje asocijacije politike:
   - Unesite ime definicije registra X.509 korisni⌂kog registra koji ⌂e se koristiti kao **Izvorni X.509 registar** za asocijaciju politike. Ili, kliknite **Pregled...** da s popisa definicije registra domene izaberete jedno.
   - Za prikaz dijaloga **Izbor filtera certifikata** kliknite **Izbor** i izaberite postoje⌂i filter certifikata koji ⌂e se koristiti kao osnova za novu asocijaciju politike filtera certifikata.

     Bilješka: **Morate** koristiti postoje⌂i filter certifikata. Ako filter certifikata koji ⌂elite koristiti nije ispisan, kliknite **Dodaj...** da kreirate novi filter certifikata.
   - Navedite ime definicije registra **Ciljnog registra** ili kliknite **Pregled...** da izaberete jedno s popisa postoje⌂ih definicija registara domene.
   - Navedite ime **Ciljnog korisnika** na kojeg ⌂elite mapirati sve certifikate iz **Izvornog X.509 registra** koji odgovaraju filteru certifikata. Ili, kliknite **Pregled...** da s popisa korisnika poznatih domeni izaberete jednog.
   - Opcijski. Za prikaz dijaloga **Dodavanje asocijacije - Napredno** kliknite **Napredno...**. Za ciljni korisni⌂ki identitet navedite **Informacije pregledavanja**, a za povratak u dijalog **Dodavanje asocijacije politike filtera certifikata** kliknite **OK**.

     Bilješka: Ako se dvije ili vi⌂e asocijacija politike s istim izvornim X.509 registrom i istim kriterijem filtera certifikata odnose na isti ciljni registar, za ciljni korisni⌂ki identitet u svakoj od tih asocijacija politike morate definirati jedinstvene informacije pregledavanja. U ovoj situaciji definiranjem informacija pregledavanja za svaki ciljni korisni⌂ki identitet osiguravate da ih operacija pregledavanja mapiranja mo⌂e razlikovati. Ina⌂e, operacije pregledavanja mapiranja mogu vratiti vi⌂estruke ciljne korisni⌂ke identitete. Rezultat ovih dvosmislenih rezultata je da aplikacija koja ovisi o EIM-u ne⌂e mo⌂i odrediti koji to⌂no ciljni identitet treba koristiti.

7. Kliknite **OK** za kreiranje asocijacije politike filtera certifikata i za vra⌂anje na stranicu **Filteri certifikata**. Nova asocijacija politike prikazana je na popisu.
8. Provjerite da je nova asocijacija politike omogu⌂ena za ciljni registar.
9. Da spremite svoje promjene i iza⌂ete iz dijaloga **Politika mapiranja** kliknite **OK**.

Bilješka: Provjerite da je politika mapiranja podr⌂ana i da je kori⌂tenje asocijacija politika za ciljni korisni⌂ki registar ispravno omogu⌂eno. Ako nije omogu⌂eno, asocijacija politike ne⌂e imati nikakav u⌂inak.

Kreiranje filtera certifikata: Filter certifikata definira skup sli⌂nih razlikovnih imena atributa certifikata grupe korisnika certifikata u X.509 izvornom korisni⌂kom registru. Filter certifikata mo⌂ete koristiti kao osnovu asocijacija politika filtera certifikata. Filter certifikata u asocijaciji politike odre⌂uje koji ⌂e se certifikati u navedenom X.509 izvornom registru mapirati u odre⌂ene ciljne korisnike. Ti certifikati koji imaju informacije DN Predmeta i DN Izdava⌂a koje zadovoljavaju kriterije filtera mapiraju se na odre⌂enog ciljnog korisnika za vrijeme EIM operacija pregledavanja mapiranja.

Da kreirate filter certifikata morate biti spojeni na EIM domenu u kojoj ⌂elite raditi i morate imati "EIM kontrola pristupa" na stranici 33 barem jednu od sljede⌂ih razina:

- EIM administrator
- Administrator registra
- Administrator za izabrane registre (za definiciju registra koja se odnosi na X.509 korisni⌂ki registar za koji ⌂elite kreirati filter certifikata)

Filter certifikata kreirate ovisno o odre⌂enim informacijama razlikovnog imena (DN) iz digitalnog certifikata. DN informacija koju navedete mo⌂e biti razlikovno ime subjekta, koje ozna⌂ava vlasnika certifikata ili razlikovno ime izdava⌂a, koje ozna⌂ava izdava⌂a certifikata. Mo⌂ete ozna⌂iti potpune ili djelomi⌂ne DN informacije za filter certifikata.

Kada filter certifikata dodate u asocijaciju politike filtera certifikata, certifikat filtera odre⌂uje koji su certifikati u X.509 registru mapirani u ciljni korisni⌂ki identitet koji je navela asocijacija politike. Kada je digitalni certifikat izvorni korisni⌂ki identitet u EIM operaciji pregledavanja mapiranja (nakon ⌂to zahtijevana aplikacija koristi eimFormatUserIdentity() EIM API za formatiranje imena korisni⌂kog identiteta) i kada se primjenjuje asocijacija politike filtera certifikata, EIM uspore⌂uje DN informacije iz certifikata s DN-om ili djelomi⌂nim DN informacijama koje su navedene u filteru. Ako se DN informacije iz certifikata podudaraju s filterom, EIM vra⌂a ciljni korisni⌂ki identitet koji je navela asocijacija politike filtera certifikata.

Prilikom kreiranja filtera certifikata potrebne informacije razlikovnog imena mo⌂ete osigurati na jedan od tri na⌂ina:

- Mo⌂ete unijeti odre⌂ene pune ili djelomi⌂ne DN-ove certifikata za **DN Subjekta**, **DN Izdava⌂a** ili oboje.
- Informacije iz odre⌂enog certifikata mo⌂ete kopirati u memoriju za isje⌂ke i koristiti ih za generiranje popisa kandidata filtera certifikata zasnovanih na informacijama razlikovnog imena u certifikatu. Zatim mo⌂ete izabrati koje DN-ove koristiti za filter certifikata.

  Bilješka: ⌂elite li potrebne informacije razlikovnog imena generirati za kreiranje filtera certifikata, informacije certifikata morate kopirati u memoriju za isje⌂ke prije izvo⌂enja ovog zadatka. Tako⌂er, certifikat mora biti kodiran formatom za kodiranje base64. Za vi⌂e informacija o metodama za pribavljanje certifikata u odre⌂enom formatu, pogledajte Filter certifikata.
- Popis kandidata filtera certifikata zasnovanih na informaciji razlikovnog imena mo⌂ete generirati iz digitalnog certifikata za koji postoji izvorna asocijacija s EIM identifikatorom. Zatim mo⌂ete izabrati koje DN-ove koristiti za filter certifikata.

Za kreiranje filtera certifikata koji ⌂e se koristiti kao osnova za asocijacije politike filtera certifikata, slijedite ove korake:

1. Pro⌂irite **Mre⌂a > Mapiranje identiteta u poduze⌂u > Upravljanje domenom**.
2. Desno kliknite EIM domenu u kojoj ⌂elite raditi i izaberite **Politika mapiranja...**

- Ako EIM domena s kojom ∆elite raditi nije ispisana u **Upravljanje domenom**, pogledajte "Dodavanje domene Mapiranja identiteta u poduze∆u u folder Upravljanja domenom" na stranici 78.
- Ako trenutno niste povezani s EIM domenom u kojoj ∆elite raditi, pogledajte Povezivanje s EIM kontrolerom domene.

3. Izaberite stranicu **Filter certifikata**, a zatim kliknite **Filteri certifikata...** da prika∆ete dijalog **Filteri certifikata**.

   Bilješka: Ako kliknete **Filteri certifikata...** bez izbora asocijacije politike, tada se prikazuje dijalog **Pregledavanje EIM registara**. Ovaj vam dijalog omogu∆uje izbor X.509 registra s popisa X.509 definicija registra u domeni za koju ∆elite pogledati filtere certifikata. Sadr∆aj popisa varira ovisno o tipu EIM kontrole pristupa koju imate.

4. Kliknite **Dodavanje...** da prika∆ete dijalog **Dodavanje filtera certifikata**.
5. U dijalogu **Dodavanje filtera certifikata** morate izabrati da li dodati jednostruki filter certifikata ili generirati certifikat zasnovan na specifi∆nom digitalnom certifikatu. Ako je potrebno, za vi∆e pojedinosti o tome kako ovo napraviti i o daljnjim dijalozima, kliknite **Pomo∆**.
   a. Ako izaberete **Dodavanje jednostrukog filtera certifikata**, mo∆ete unijeti odre∆ene potpune ili djelomi∆ne informacije **DN-a subjekta**, potpune ili djelomi∆ne informacije **DN-a izdava∆a** ili oboje. Kliknite **OK** za kreiranje filtera certifikata i za vra∆anje u dijalog **Filteri certifikata**. Filter se sada pojavljuje na popisu.
   b. Ako izaberete **Generiranje filtera certifikata iz digitalnog certifikata**, kliknite **OK** za prikaz dijaloga **Generiranje filtera certifikata**.
      1) U polje **Informacije certifikata** zalijepite base64 kodiranu verziju informacija certifikata koje ste ranije kopirali u memoriju za isje∆ke.
      2) Kliknite **OK** za generiranje popisa potencijalnih filtera certifikata zasnovanih na certifikatovom **DN-u Subjekta** i **DN-u Izdava∆a**.
      3) Iz dijaloga **Pregled filtera certifikata** izaberite jedan ili vi∆e od ovih filtera certifikata. Kliknite **OK** za vra∆anje dijaloga **Izbor filtera certifikata** u kojem se sada prikazuju filteri certifikata.
   c. Ako izaberete **Generiranje filtera certifikata iz izvorne asocijacije za X.509 korisnika**, kliknite **OK** za prikaz dijaloga **Generiranje filtera certifikata**. Ovaj dijalog prikazuje popis X.509 korisni∆kih identiteta koji su u domeni izvorno asocirani s EIM identifikatorom.
      1) Izaberite X.509 korisni∆ki identitet ∆iji digitalni certifikat ∆elite koristiti za generiranje jednog ili vi∆e kandidata filtera certifikata pa kliknite **OK**.
      2) Kliknite **OK** za generiranje popisa potencijalnih filtera certifikata zasnovanih na certifikatovom **DN-u subjekta** i **DN-u izdava∆a**.
      3) Iz dijaloga **Pregled filtera certifikata** izaberite jedan ili vi∆e od ovih potencijalnih filtera certifikata. Kliknite **OK** za vra∆anje dijaloga **Izbor filtera certifikata** u kojem se sada prikazuju filteri certifikata.

Novi filter certifikata sada mo∆ete koristiti kao osnovu za kreiranje asocijacije politike filtera certifikata.

Dodavanje informacija pregledavanja ciljnom korisni∆kom identitetu

Informacije pregledavanja su neobavezni jedinstveni identifikacijski podaci za ciljni korisni∆ki identitet definiran u asocijaciji. Ta asocijacija mo∆e biti ili ciljna asocijacija identifikatora ili asocijacija politike. Informacije pregledavanja su potrebne samo kada operacija pregledavanja mapiranja mo∆e vratiti vi∆e od jedan ciljni korisni∆ki identitet. Ova situacija mo∆e kreirati probleme za EIM-omogu∆ene aplikacije, uklju∆uju∆i OS/400 aplikacije i proizvode koji nisu oblikovani za rukovanje s ovim dvosmislenim rezultatima.

Po potrebi, mo∆ete dodati jedinstvene informacije pregledavanja za svaki ciljni korisni∆ki identitet kako bi se osigurale detaljnije identifikacijske informacije za dodatni opis svakog korisni∆kog identiteta. Ako definirate informacije pregledavanja za ciljni korisni∆ki identitet, te se informacije pregledavanja moraju dobaviti operaciji pregledavanja mapiranja kako bi se osiguralo da operacija mo∆e vratiti jedinstveni ciljni korisni∆ki identitet. U suprotnom, aplikacije koje ovise o EIM-u mo∆da ne∆e mo∆i odrediti koji to∆no ciljni identitet upotrijebiti.

Bilješka: Ako ne ⌂elite da operacije EIM pregledavanja vra⌂aju vi⌂e od jedan ciljni korisni⌂ki identitet, tada trebate ispraviti va⌂u konfiguraciju EIM asocijacija umjesto kori⌂tenja informacija pregledavanja za rje⌂enje problema. Pogledajte “Rje⌂avanje problema Mapiranja identiteta u poduze⌂u: problemi mapiranja” na stranici 109 za detaljnije informacije.

Kako ⌂ete dodati informacije pregledavanja za daljnju definiciju ciljnog korisni⌂kog identiteta ovisi o tome da li je definiran korisni⌂ki identitet u asocijaciji identifikatora ili ciljnoj asocijaciji. Bez obzira na metodu kori⌂tenu za dodavanje informacija pregledavanja, specificirane informacije su povezane s ciljnim korisni⌂kim identitetom, a ne s asocijacijama identifikatora ili asocijacijama politike u kojima je prona⌂en taj korisni⌂ki identitet.

Dodavanje informacija pregledavanja ciljnom korisni⌂kom identitetu u asocijaciji identifikatora

Za dodavanje informacija pregledavanja ciljnom korisni⌂kom identitetu u asocijaciji identifikatora, morate biti povezani na EIM domenu u kojoj ⌂elite raditi i trebate imati “EIM kontrola pristupa” na stranici 33 na jednoj od ovih razina:

- Administrator registra.
- Administrator za izabrane registre (za definicije registara koje se odnose na korisni⌂ki registar koji sadr⌂i ciljni korisni⌂ki identitet).
- EIM administrator.

Za dodavanje informacija pregledavanja ciljnom korisni⌂kom identitetu u asocijaciji identifikatora izvedite sljede⌂e korake:

1. Pro⌂irite **Mre⌂a > Mapiranje identiteta u poduze⌂u > Upravljanje domenom**.
2. Izaberite EIM domenu u kojoj ⌂elite raditi.
   - Ako EIM domena s kojom ⌂elite raditi nije ispisana u **Upravljanje domenom**, pogledajte “Dodavanje domene Mapiranja identiteta u poduze⌂u u folder Upravljanja domenom” na stranici 78.
   - Ako trenutno niste povezani s EIM domenom u kojoj ⌂elite raditi, pogledajte Povezivanje s EIM kontrolerom domene.
3. Pro⌂irite EIM domenu na koju ste povezani.
4. Kliknite **Identifikatori** za prikaz liste EIM identifikatora za domenu.

   Bilješka: Ponekad kada poku⌂ate pro⌂iriti folder **Identifikatori** mo⌂e pro⌂i puno vremena prije nego se popis identifikatora prika⌂e. Za poboljšanje performansi kada imate veliki broj EIM identifikatora u domeni, mo⌂ete prilagoditi pogled foldera **Identifikatori** ograni⌂avanjem kriterija pretra⌂ivanja koji se koriste za prikaz identifikatora. Desno kliknite na **Identifikatori**, izaberite **Prilagodi ovaj pogled... > Uklju⌂i** i navedite kriterije prikazivanja koji ⌂e se koristiti za generiranje popisa EIM identifikatora koji ⌂e se uklju⌂iti u pogled.
5. Desno kliknite EIM identifikator i izaberite **Svojstva...**.
6. Izaberite stranicu **Asocijacije**, izaberite ciljnu asocijaciju kojoj ⌂elite dodati informacije pregledavanja pa kliknite **Detalji...**. Ako je potrebno kliknite **Pomo⌂** da odredite koje informacije navesti u odre⌂enom polju.
7. U dijalogu **Asocijacije - Detalji** specificirajte **Informacije pregledavanja** koje ⌂elite koristiti za daljnju identifikaciju ciljnog korisni⌂kog identiteta u ovoj asocijaciji i kliknite **Dodaj**.
8. Ponovite ovaj korak za svaki unos informacija pregledavanja koje ⌂elite dodati asocijaciji.
9. Kliknite **OK** za spremanje promjena i vra⌂anje u dijalog **Asocijacija - Detalji**.
10. Za izlaz kliknite **OK**.

Dodavanje informacija pregledavanja ciljnom korisni⌂kom identitetu u asocijaciji politike

Za dodavanje informacija pregledavanja ciljnom korisni⌂kom identitetu u asocijaciji politike, morate biti povezani na EIM domenu u kojoj ⌂elite raditi i trebate imati “EIM kontrola pristupa” na stranici 33 na jednoj od ovih razina:

- Administrator registra.
- Administrator za izabrane registre (za definiciju registara koja se odnosi na korisni⌂ki registar koji sadr⌂i ciljni korisni⌂ki identitet (ID)).
- EIM administrator.

Za dodavanje informacija pregledavanja ciljnom korisni⌂kom identitetu u asocijaciji politike izvedite sljede⌂e korake:

1. Pro⌂irite **Mre⌂a > Mapiranje identiteta u poduze⌂u > Upravljanje domenom**.
2. Desno kliknite EIM domenu u kojoj ⌂elite raditi i izaberite **Politika mapiranja...**
   - Ako EIM domena s kojom ⌂elite raditi nije ispisana u **Upravljanje domenom**, pogledajte "Dodavanje domene Mapiranja identiteta u poduze⌂u u folder Upravljanja domenom" na stranici 78.
   - Ako trenutno niste povezani s EIM domenom u kojoj ⌂elite raditi, pogledajte Povezivanje s EIM kontrolerom domene.
3. U dijalogu **Politika mapiranja** koristite stranice za gledanje asocijacija politike za domenu.
4. Prona⌂ite i izaberite asocijaciju politike za ciljni registar koji koristi ciljni korisni⌂ki identitet kojemu ⌂elite dodati informacije pregledavanja.
5. Kliknite **Detalji...** za prikaz odgovaraju⌂eg dijaloga **Asocijacija politike - Detalji** za tip asocijacije politike koji ste izabrali. Ako je potrebno kliknite **Pomo⌂** da odredite koje informacije navesti u odre⌂enom polju.
6. Specificirajte **Informacije pregledavanja** koje ⌂elite koristiti za daljnju identifikaciju ciljnog korisni⌂kog identiteta u ovoj asocijaciji politike i kliknite **Dodaj**. Ponovite ovaj korak za svaki unos informacija pregledavanja koje ⌂elite dodati asocijaciji.
7. Kliknite **OK** za spremanje promjena i vra⌂anje u originalni dijalog **Asocijacija - Detalji**.
8. Za izlaz kliknite **OK**.

Uklanjanje informacija pregledavanja ciljnom korisni⌂kom identitetu

Informacije pregledavanja su opcijski jedinstveni identifikacijski podaci za ciljni korisni⌂ki identitet definiran u asocijaciji. Ta asocijacija mo⌂e biti ili ciljna asocijacija identifikatora ili asocijacija politike. Informacije pregledavanja su potrebne samo kada operacija pregledavanja mapiranja mo⌂e vratiti jedan ili vi⌂e ciljni korisni⌂ki identitet. Ova situacija mo⌂e kreirati probleme za EIM-omogu⌂ene aplikacije, uklju⌂uju⌂i OS/400 aplikacije i proizvode koji nisu oblikovani za rukovanje s ovim dvosmislenim rezultatima.

Te se informacije pregledavanja moraju dati operaciji pregledavanja mapiranja da bi se osiguralo da operacija mo⌂e vratiti jedinstveni ciljni korisni⌂ki identitet. Me⌂utim, ako prethodno definirane informacije pregledavanja nisu vi⌂e potrebne, mo⌂da ⌂ete ih htjeti ukloniti tako da vi⌂e ne moraju biti osigurane za operacije pregledavanja.

Kako ⌂ete ukloniti informacije pregledavanja s ciljnog korisni⌂kog identiteta ovisi o tome je li ciljni korisni⌂ki identitet definiran u asocijaciji identifikatora ili ciljnoj asocijaciji. Informacije pregledavanja su vezane na ciljni korisni⌂ki identitet, a ne za asocijacije identifikatora ili asocijacije politika u kojima se taj identitet nalazi. Prema tome, kada bri⌂ete zadnju asocijaciju identifikatora ili asocijaciju politike koja se odnosi na taj ciljni korisni⌂ki identitet, iz EIM domene se bri⌂u korisni⌂ki identitet i informacije pregledavanja.

Uklanjanje informacija pregledavanja ciljnog korisni⌂kog identiteta u asocijaciji identifikatora

Za uklanjanje informacija pregledavanja ciljnog korisni⌂kog identiteta u asocijaciji identifikatora, morate biti povezani na EIM domenu u kojoj ⌂elite raditi i morate imati "EIM kontrola pristupa" na stranici 33 na jednoj od ovih razina:

- Administrator registra.
- Administrator za izabrane registre (za definicije registara koje se odnose na korisni⌂ki registar koji sadr⌂i ciljni korisni⌂ki identitet).
- EIM administrator.

Za uklanjanje informacija pregledavanja ciljnog korisni⌂kog identiteta u asocijaciji identifikatora izvedite sljede⌂e korake:

1. Pro⌂irite **Mre⌂a > Mapiranje identiteta u poduze⌂u > Upravljanje domenom**.
2. Izaberite EIM domenu u kojoj ⌂elite raditi.
   - Ako EIM domena s kojom ⌂elite raditi nije ispisana u **Upravljanje domenom**, pogledajte "Dodavanje domene Mapiranja identiteta u poduze⌂u u folder Upravljanja domenom" na stranici 78.
   - Ako trenutno niste povezani s EIM domenom u kojoj ⌂elite raditi, pogledajte Povezivanje s EIM kontrolerom domene.
3. Pro⌂irite EIM domenu na koju ste povezani.
4. Kliknite **Identifikatori** za prikaz liste EIM identifikatora za domenu.

   Bilješka: Ponekad kada poku⌂ate pro⌂iriti folder **Identifikatori** mo⌂e pro⌂i puno vremena prije nego se popis identifikatora prika⌂e. Za poboljšanje performanse kada imate veliki broj EIM identifikatora u domeni, mo⌂ete prilagoditi pogled foldera **Identifikatora** ograni⌂avanjem kriterija pretra⌂ivanja koji se koristi za prikaz identifikatora. Desno kliknite na **Identifikatori**, izaberite **Prilagodi ovaj pogled... > Uklju⌂i** i navedite kriterij prikazivanja koji ⌂e se koristiti za generiranje popisa EIM identifikatora koji ⌂e se uklju⌂iti u pogled.
5. Desno kliknite EIM identifikator i izaberite **Svojstva...**.
6. Izaberite stranicu **Asocijacije**, izaberite ciljnu asocijaciju za korisni⌂ki identitet za koji ⌂elite ukloniti informacije pregledavanja pa kliknite **Detalji...**.
7. U dijalogu **Asocijacije - Detalji** izaberite informacije pregledavanja koje ⌂elite ukloniti s ciljnog korisni⌂kog identiteta i kliknite **Ukloni**.

   Bilješka: Nakon ⌂to kliknete **Ukloni** od vas se ne tra⌂i da akciju potvrdite.
8. Kliknite **OK** za spremanje promjena i vra⌂anje u dijalog **Asocijacija - Detalji**.
9. Za izlaz kliknite **OK**.

Uklanjanje informacija pregledavanja ciljnog korisni⌂kog identiteta u asocijaciji politike

Za uklanjanje informacija pregledavanja ciljnog korisni⌂kog identiteta u asocijaciji politike, morate biti povezani na EIM domenu u kojoj ⌂elite raditi i morate imati "EIM kontrola pristupa" na stranici 33 na jednoj od ovih razina:

- Administrator registra.
- Administrator za izabrane registre (za definiciju registara koja se odnosi na korisni⌂ki registar koji sadr⌂i ciljni korisni⌂ki identitet (ID)).
- EIM administrator.

Za uklanjanje informacija pregledavanja ciljnog korisni⌂kog identiteta u asocijaciji politike izvedite sljede⌂e korake:

1. Pro⌂irite **Mre⌂a > Mapiranje identiteta u poduze⌂u > Upravljanje domenom**.
2. Desno kliknite EIM domenu u kojoj ⌂elite raditi i izaberite **Politika mapiranja...**
   - Ako EIM domena s kojom ⌂elite raditi nije ispisana u **Upravljanje domenom**, pogledajte "Dodavanje domene Mapiranja identiteta u poduze⌂u u folder Upravljanja domenom" na stranici 78.
   - Ako trenutno niste povezani s EIM domenom u kojoj ⌂elite raditi, pogledajte Povezivanje s EIM kontrolerom domene.
3. U dijalogu **Politika mapiranja** koristite stranice za gledanje asocijacija politike za domenu.
4. Prona⌂ite i izaberite asocijaciju politike za ciljni registar koji koristi ciljni korisni⌂ki identitet kojemu ⌂elite ukloniti informacije pregledavanja.
5. Kliknite **Detalji...** za prikaz odgovaraju⌂eg dijaloga **Asocijacija politike - Detalji** za tip asocijacije politike koji ste izabrali.
6. Izaberite informacije pregledavanja koje ⌂elite ukloniti s ciljnog korisni⌂kog registra, a zatim kliknite **Ukloni**.

Bilješka: Nakon ∆to kliknete **Ukloni** od vas se ne tra∆i da akciju potvrdite.

7. Kliknite **OK** za spremanje promjena i vra∆anje u originalni dijalog **Asocijacija - Detalji**.
8. Za izlaz kliknite **OK**.

Prikaz svih asocijacija identifikatora za EIM identifikator

Za prikaz svih asocijacija za EIM identifikator morate biti povezani s EIM domenom u kojoj ∆elite raditi i morate imati neku razinu "EIM kontrola pristupa" na stranici 33 da biste mogli izvesti ovaj zadatak. Mo∆ete pogledati sve asocijacije s bilo kojom razinom kontrole pristupa osim kontrole pristupa Administrator za izabrane registre. Ova razina kontrole pristupa omogu∆uje vam ispis i pogled svih onih asocijacija na registre za koje imate eksplicitno ovla∆tenje, osim ako nemate kontrolu pristupa EIM operacija pregledavanja mapiranja.

Za prikaz svih asocijacija izme∆u EIM identifikatora i korisni∆kih identiteta (ID-ova) za koje su asocijacije definirane za EIM identifikator, izvedite sljede∆e korake:

Za prikaz asocijacija za identifikator, izvedite sljede∆e korake:

1. Pro∆irite **Mre∆a > Mapiranje identiteta u poduze∆u > Upravljanje domenom**.
2. Izaberite EIM domenu u kojoj ∆elite raditi.
   - Ako EIM domena s kojom ∆elite raditi nije ispisana u **Upravljanje domenom**, pogledajte "Dodavanje domene Mapiranja identiteta u poduze∆u u folder Upravljanja domenom" na stranici 78.
   - Ako trenutno niste povezani s EIM domenom u kojoj ∆elite raditi, pogledajte Povezivanje s EIM kontrolerom domene.
3. Pro∆irite EIM domenu na koju ste povezani.
4. Kliknite **Identifikatori**.

   Bilješka: Ponekad kada poku∆ate pro∆iriti folder **Identifikatori** mo∆e pro∆i puno vremena prije nego se popis identifikatora prika∆e. Za poboljšanje performanse kada imate veliki broj EIM identifikatora u domeni, mo∆ete prilagoditi pogled foldera **Identifikatora** ograni∆avanjem kriterija pretra∆ivanja koji se koristi za prikaz identifikatora. Desno kliknite na **Identifikatori**, izaberite **Prilagodi ovaj pogled... > Uklju∆i** i navedite kriterij prikazivanja koji ∆e se koristiti za generiranje popisa EIM identifikatora koji ∆e se uklju∆iti u pogled.
5. Izaberite EIM identifikator, desno kliknite na EIM identifikator i izaberite **Svojstva**.
6. Za prikaz popisa korisni∆kih identiteta za izabrani EIM identifikator izaberite stranicu **Asocijacije**.
7. Za kraj kliknite **OK**.

Prikaz svih asocijacija politike za domenu

Za prikaz svih asocijacija definiranih za domenu morate biti povezani s EIM domenom u kojoj ∆elite raditi i morate imati neku razinu "EIM kontrola pristupa" na stranici 33 da biste mogli izvesti ovaj zadatak. Mo∆ete pogledati sve asocijacije politike s bilo kojom razinom kontrole pristupa osim kontrole pristupa Administrator za izabrane registre. Ova razina kontrole pristupa omogu∆uje vam ispis i pogled samo onih asocijacija za registre za koje imate eksplicitno ovla∆tenje. Prema tome s ovom kontrolom pristupa ne mo∆ete ispisati ili pogledati niti jednu asocijaciju politike default domene, osim ako nemate kontrolu pristupa EIM operacija pregledavanja mapiranja.

Za prikaz svih asocijacija politike za domenu, izvedite sljede∆e korake:

1. Pro∆irite **Mre∆a > Mapiranje identiteta u poduze∆u > Upravljanje domenom**.
2. Desno kliknite EIM domenu u kojoj ∆elite raditi i izaberite **Politika mapiranja...**
   - Ako EIM domena s kojom ∆elite raditi nije ispisana u **Upravljanje domenom**, pogledajte "Dodavanje domene Mapiranja identiteta u poduze∆u u folder Upravljanja domenom" na stranici 78.
   - Ako trenutno niste povezani s EIM domenom u kojoj ∆elite raditi, pogledajte Povezivanje s EIM kontrolerom domene.
3. Izaberite stranicu za prikaz asocijacija politika definiranih za domenu, kao ∆to slijedi:

- Izaberite stranicu **Domena** za pogled asocijacija politike default domene definiranih za domenu i za provjeru je li asocijacija politike omogu⌂ena na razini registra.
- Izaberite stranicu **Registar** za pogled default asocijacija politike definiranih za domenu. Tako⌂er mo⌂ete pogledati na koje izvorne registre i ciljne registre utje⌂u asocijacije politike.
- Izaberite stranicu **Filter certifikata** za pogled asocijacija politike filtera certifikata definiranih i omogu⌂enih na razini registra.

4. Za kraj kliknite **OK**.

Prikaz svih asocijacija politike za definiciju registra

Za prikaz svih asocijacija politike definiranih za odre⌂eni registar morate biti povezani s EIM domenom u kojoj ⌂elite raditi i morate imati neku razinu "EIM kontrola pristupa" na stranici 33 da biste mogli izvesti ovaj zadatak. Mo⌂ete pogledati sve asocijacije politike s bilo kojom razinom kontrole pristupa osim kontrole pristupa Administrator za izabrane registre. Ova razina kontrole pristupa omogu⌂uje vam ispis i pogled samo onih asocijacija za registre za koje imate eksplicitno ovla⌂tenje. Prema tome s ovom kontrolom pristupa ne mo⌂ete ispisati ili pogledati niti jednu asocijaciju politike default domene, osim ako nemate kontrolu pristupa EIM operacija pregledavanja mapiranja.

Za prikaz svih asocijacija politike za definiciju registra, izvedite sljede⌂e korake:

1. Pro⌂irite **Mre⌂a > Mapiranje identiteta u poduze⌂u > Upravljanje domenom**.
2. Desno kliknite EIM domenu u kojoj ⌂elite raditi i izaberite **Korisni⌂ki registri** za prikaz ispisa definicija registra za domenu.
   - Ako EIM domena s kojom ⌂elite raditi nije ispisana u **Upravljanje domenom**, pogledajte "Dodavanje domene Mapiranja identiteta u poduze⌂u u folder Upravljanja domenom" na stranici 78.
   - Ako trenutno niste povezani s EIM domenom u kojoj ⌂elite raditi, pogledajte Povezivanje s EIM kontrolerom domene.
3. Desno kliknite definiciju registra u kojoj ⌂elite raditi i izaberite **Politika mapiranja...**
4. Izaberite stranicu za prikaz asocijacija politika definiranih za navedenu definiciju registra, kao ⌂to slijedi:
   - Izaberite stranicu **Domena** za pogled asocijacija politike default domene definiranih za registar.
   - Izaberite stranicu **Registar** za pogled default asocijacija politike registra definiranih i omogu⌂enih za registar.
   - Izaberite stranicu **Filter certifikata** za pogled asocijacija politika filtera certifikata definiranih i omogu⌂enih za registar.
5. Za kraj kliknite **OK**.

Brisanje asocijacije identifikatora

Za brisanje asocijacije identifikatora morate biti povezani s EIM domenom u kojoj ⌂elite raditi i morate imati "EIM kontrola pristupa" na stranici 33 koje treba tip asocijacije koju ⌂elite brisati.

Za brisanje izvorne ili administrativne asocijacije morate imati EIM kontrolu pristupa na jednoj od sljede⌂ih razina:

- Administrator identifikatora.
- EIM administrator.

Za brisanje ciljne asocijacije morate imati EIM kontrolu pristupa na jednoj od sljede⌂ih razina:

- Administrator registra.
- Administrator za izabrane registre (za definiciju registara koja se odnosi na korisni⌂ki registar koji sadr⌂i ciljni korisni⌂ki identitet).
- EIM administrator.

Za brisanje asocijacije identifikatora, izvedite sljede⌂e korake.

1. Pro⌂irite **Mre⌂a > Mapiranje identiteta u poduze⌂u > Upravljanje domenom**.
2. Izaberite EIM domenu u kojoj ⌂elite raditi.

- Ako EIM domena s kojom ∆elite raditi nije ispisana u **Upravljanje domenom**, pogledajte "Dodavanje domene Mapiranja identiteta u poduze∆u u folder Upravljanja domenom" na stranici 78.
- Ako trenutno niste povezani s EIM domenom u kojoj ∆elite raditi, pogledajte Povezivanje s EIM kontrolerom domene.

3. Pro∆irite EIM domenu na koju ste sada povezani.
4. Kliknite **Identifikatori**.

Bilješka: Ponekad kada poku∆ate pro∆iriti folder **Identifikatori** mo∆e pro∆i puno vremena prije nego se popis identifikatora prika∆e. Da poboljˆate performanse kada imate veliki broj EIM identifikatora u domeni, mo∆ete "Prilagodba pogleda identifikatora Mapiranja identiteta u poduze∆u" na stranici 90.

5. Desno kliknite EIM identifikator za koji ∆elite brisati asocijaciju i izaberite **Svojstva...**
6. Izaberite stranicu **Asocijacije** za prikaz trenutnih asocijacija za EIM identifikator.
7. Izaberite asocijaciju koju ∆elite brisati i kliknite **Ukloni** za brisanje asocijacije.

Bilješka: Nema potvrdnog prompta nakon ∆to kliknete **Ukloni**.

8. Za spremanje promjena kliknite **OK**.

Bilješka: Kada uklonite ciljnu asocijaciju bilo kakva operacija pregledavanja mapiranja u ciljni registar koji ovisi o kori∆tenju obrisane asocijacije mo∆da ne∆e uspjeti ako druge asocijacije (bilo asocijacije politike ili asocijacije identifikatora) ne postoje za taj zahva∆eni ciljni registar.

Jedini na∆in da se za EIM definira korisni∆ki identitet je kada navedete korisni∆ki identitet kao dio kreiranja asocijacije bilo asocijacije identifikatora ili asocijacije politike. Prema tome kada izbri∆ete zadnju ciljnu asocijaciju za korisni∆ki identitet (bilo uklanjanjem individualne ciljne asocijacije ili uklanjanjem asocijacije politike) taj korisni∆ki identitet nije vi∆e definiran u EIM-u. Prema tome gubi se ime korisni∆kog identiteta i bilo koje informacije pregledavanja za taj korisni∆ki identitet.

Brisanje asocijacije politike

Za brisanje asocijacije politike morate biti povezani s EIM domenom u kojoj ∆elite raditi i morate imati "EIM kontrola pristupa" na stranici 33 na jednoj od ovih razina:

- Administrator registra.
- EIM administrator.

Za brisanje asocijacije politike izvedite sljede∆e korake:

1. Pro∆irite **Mre∆a > Mapiranje identiteta u poduze∆u > Upravljanje domenom**.
2. Desno kliknite EIM domenu u kojoj ∆elite raditi i izaberite **Politika mapiranja...**
   - Ako EIM domena s kojom ∆elite raditi nije ispisana u **Upravljanje domenom**, pogledajte "Dodavanje domene Mapiranja identiteta u poduze∆u u folder Upravljanja domenom" na stranici 78.
   - Ako trenutno niste povezani s EIM domenom u kojoj ∆elite raditi, pogledajte Povezivanje s EIM kontrolerom domene.
3. Izaberite prikladnu stranicu za tip asocijacije politike koji ∆elite obrisati.
4. Na toj stranici izaberite odgovaraju∆u asocijaciju politike i kliknite **Ukloni**.

Bilješka: Nakon ∆to kliknete **Ukloni** od vas se ne tra∆i da akciju potvrdite.

5. Kliknite **OK** da iza∆ete iz dijaloga **Politika mapiranja** i spremite va∆e promjene.

Bilješka: Kada uklonite ciljnu asocijaciju politike, bilo kakve operacije pregledavanja mapiranja u ciljnom registru koje ovise o kori∆tenju obrisane asocijacije politike mo∆da ne∆e uspjeti ako druge asocijacije (bilo asocijacije politike ili asocijacije identifikatora) ne postoje za taj ciljni registar.

Jedini na⌂in da se za EIM definira korisni⌂ki identitet je kada navedete korisni⌂ki identitet kao dio kreiranja asocijacije bilo asocijacije identifikatora ili asocijacije politike. Prema tome kada izbri⌂ete zadnju ciljnu asocijaciju za korisni⌂ki identitet (bilo uklanjanjem individualne ciljne asocijacije ili uklanjanjem asocijacije politike) taj korisni⌂ki identitet nije vi⌂e definiran u EIM-u. Prema tome gubi se ime korisni⌂kog identiteta i bilo koje informacije pregledavanja za taj korisni⌂ki identitet.

Upravljanje EIM kontrolom korisni⌂kog pristupa

EIM korisnik je korisnik koji posjeduje "EIM kontrola pristupa" na stranici 33 baziranu na njegovom ⌂lanstvu u predefiniranim Lightweight Directory Access Protocol (LDAP) korisni⌂kim grupama. Specificiranjem EIM kontrole pristupa za korisnika dodaje se taj korisnik u odre⌂enu LDAP korisni⌂ku grupu. Svaka LDAP grupa ima ovla⌂tenje za izvo⌂enje raznolikih EIM administrativnih zadataka za tu domenu. Koje i kakve tipove administrativnih zadataka EIM korisnik mo⌂e izvesti, uklju⌂uju⌂i i operacije pregledavanja, odre⌂eno je grupom za kontrolu pristupa kojoj EIM korisnik pripada.

Samo korisnici, bilo s LDAP administratorskom kontrolom pristupa ili EIM administratorskom kontrolom pristupa, mogu dodati druge korisnike u grupu EIM kontrole pristupa ili mijenjati postavke kontrole pristupa za druge korisnike. Prije no ⌂to korisnik mo⌂e postati ⌂lan grupe za EIM kontrolu pristupa, taj se korisnik mora unijeti u poslu⌂itelja direktorija koji djeluje kao EIM kontroler domene. Tako⌂er, samo odre⌂eni tipovi korisnika mogu postati ⌂lanovi grupe za EIM kontrolu pristupa: Kerberos principali, razlikovna imena i OS/400 korisni⌂ki profili.

Bilješka: Da bi tip korisnika Kerberos principala bio dostupan u EIM-u, na sistemu mora biti konfigurirana usluga mre⌂ne provjere autenti⌂nosti. Da bi tip OS/400 korisni⌂kog profila bio dostupan u EIM-u, sufiks sistemskog objekta na poslu⌂itelju direktorija mora biti konfiguriran. Ovo omogu⌂uje poslu⌂itelju direktorija referenciranje OS/400 sistemskih objekata, poput OS/400 korisni⌂kih profila.

Za upravljanje kontrolom pristupa za postoje⌂eg korisnika poslu⌂itelja direktorija ili dodavanje postoje⌂eg korisnika direktorija u grupu EIM kontrole pristupa, izvedite sljede⌂e korake:

1. Pro⌂irite **Mre⌂a > Mapiranje identiteta u poduze⌂u > Upravljanje domenom**.
2. Izaberite EIM domenu u kojoj ⌂elite raditi.
   - Ako EIM domena s kojom ⌂elite raditi nije ispisana u **Upravljanje domenom**, pogledajte "Dodavanje domene Mapiranja identiteta u poduze⌂u u folder Upravljanja domenom" na stranici 78.
   - Ako trenutno niste povezani s EIM domenom u kojoj ⌂elite raditi, pogledajte Povezivanje s EIM kontrolerom domene.

     Bilješka: Osigurajte da se pove⌂ete na domenu s ovla⌂tenjem korisnika koji ima EIM ovla⌂tenje administratora.
3. Desno kliknite EIM domenu na kojoj ste spojeni i izaberite **Kontrola Pristupa...**
4. U dijalogu **Ure⌂ivanje EIM kontrole Pristupa**, izaberite **Tip korisnika** za prikaz polja potrebnih za dobavu identifikacijskih informacija za korisnika.
5. Unesite potrebne korisni⌂ke informacije za identifikaciju korisnika za kojeg ⌂elite da upravlja EIM kontrolom pristupa i kliknite **OK** za prikaz panela **Ure⌂ivanje EIM kontrole Pristupa**. Ako je potrebno kliknite **Pomo⌂** da odredite koje informacije navesti u odre⌂enom polju.
6. Izaberite jednu ili vi⌂e grupa **Kontrole pristupa** za korisnika i kliknite **OK** da dodate korisnika u izabrane grupe. Kliknite **Pomo⌂** za detaljnije informacije o tome koje ovla⌂tenje ima svaka grupa i za nau⌂iti o posebnim zahtjevima.
7. Nakon ⌂to osigurate potrebne informacije, za spremanje va⌂ih promjena kliknite **OK**.

Upravljanje svojstvima EIM konfiguracije

Za va⌂ poslu⌂itelj mo⌂ete upravljati nekoliko razli⌂itim svojstvima EIM konfiguracije. Tipi⌂no, to ne trebate ⌂esto ⌂initi. Me⌂utim, postoje situacije koje zahtijevaju promjene na svojstvima konfiguracije. Na primjer, ako vam se sistem sru⌂i i trebate ponovno kreirati va⌂a svojstva EIM konfiguracije mo⌂ete ili ponovno pokrenuti ⌂arobnjaka EIM

konfiguracije ili ovdje promijeniti svojstva. Drugi primjer je kada izaberete ne kreirati definicije registra za lokalne registre kada pokre⌂ete ⌂arobnjaka EIM konfiguracije tada ovdje mo⌂ete a⌂urirati informacije definicije registra.

Svojstva koja mo⌂ete promijeniti uklju⌂uju:

- EIM domenu u kojoj poslu⌂itelj sudjeluje.
- Informacije povezivanja za EIM kontroler domene.
- Korisni⌂ki identitet koji sistem koristi za izvo⌂enje EIM operacija na ra⌂un funkcija operativnog sistema.
- Imena definicije registra koja se odnose na stvarne korisni⌂ke registre koje sistem mo⌂e koristiti prilikom izvo⌂enja EIM operacije u ime funkcija operativnog sistema. Ta imena definicije registara odnose se na lokalne korisni⌂ke registre koje kreirate kada pokrenete ⌂arobnjaka EIM konfiguracije.

  Bilješka: Ako izaberete ne kreirati imena lokalne definicije registra kada pokrenete ⌂arobnjaka EIM konfiguracije zato, jer su registri ve⌂ definirani na EIM domeni ili, jer ste ih izabrali kasnije definirati na domeni, morate ovdje a⌂urirati svojstva konfiguracije sistema s tim imenima definicije registra. Sistem te informacije definicije registra treba za izvo⌂enje EIM operacija za funkcije operativnog sistema.

Za promjenu EIM svojstava konfiguracije morate imati ova posebna ovla⌂tenja:

- Administrator sigurnosti (*SECADM).
- Svi objekti (*ALLOBJ).

Za promjenu EIM svojstava konfiguracije za va⌂ iSeries poslu⌂itelj, izvedite sljede⌂e korake:

1. Pro⌂irite **Mre⌂a > Mapiranje identiteta u poduze⌂u**.
2. Desno kliknite **Konfiguracija** i izaberite **Svojstva**.
3. Napravite promjene na EIM informacijama konfiguracije.
4. Za odre⌂ivanje koje informacije navesti u svakom polju dijaloga kliknite **Pomo⌂**.
5. Kliknite **Provjeri konfiguraciju** da osigurate da sve navedene informacije omogu⌂uju sistemu da uspje⌂no uspostavi vezu s EIM kontrolerom domene.
6. Za spremanje promjena kliknite **OK**.

Bilješka: Ako niste koristili ⌂arobnjaka EIM konfiguracije za kreiranje domene ili spajanje na domenu, ne poku⌂avajte kreirati EIM konfiguraciju ru⌂nim specificiranjem svojstava konfiguracije. Upotrebom ⌂arobnjaka za kreiranje osnovne EIM konfiguracije mo⌂ete sprije⌂iti mogu⌂e konfiguracijske probleme, jer ⌂arobnjak ⌂ini vi⌂e od samog konfiguriranja tih svojstava.

API-ji Mapiranja identiteta u poduze⌂u

Mapiranje identiteta u poduze⌂u (EIM) dobavlja mehanizme upravljanja korisni⌂kim identitetom preko razli⌂itih platformi. EIM ima vi⌂estruka su⌂elja aplikativnog programiranja (API-je) koje aplikacija mo⌂e koristiti za vo⌂enje EIM operacija u koristi aplikacije ili aplikacijskog korisnika. Mo⌂ete koristiti ove API-je za vo⌂enje operacija pregledavanja mapiranja identiteta, vo⌂enje razli⌂itih EIM funkcija upravljanja i konfiguracije, kao i promjene informacija i sposobnosti upita. Svaki od tih API-ija su podr⌂ani preko IBM platformi.

EIM API-ji spadaju u vi⌂e kategorija kako slijedi:

- Operacije EIM rukovanja i povezivanja
- Administracija EIM domene
- Operacije registra
- Operacije EIM identifikatora
- Upravljanje EIM asocijacijama
- Operacije EIM pregledavanja mapiranja
- Upravljanje EIM ovla⌂tenjem

Aplikacije koje koriste ove API-je za upravljanje ili upotrebu EIM informacija u EIM domeni tipi⌂no se odnose na sljede⌂i programerski model:

1. Dohvat EIM hvati⌂ta
2. Povezivanje na EIM domenu
3. Normalna obrada podataka
4. Upotreba API-ja EIM administracije ili EIM operacije pregleda mapiranja identiteta
5. Normalna obrada podataka
6. Prije zavr⌂etka, uni⌂ti EIM hvati⌂te

Za detaljne informacije i potpune liste dostupnih EIM API-ija za iSeries poslu⌂itelj, pogledajte poglavlje API-ji Mapiranja identiteta u poduze⌂u (EIM).

Rje⌂avanje problema Mapiranja identiteta u poduze⌂u

Mapiranja identiteta u poduze⌂u (EIM) je sastavljeno od vi⌂estrukih tehnologija i mno⌂tva aplikacija i funkcija. Prema tome, problemi se mogu dogoditi u mnogim podru⌂jima. Sljede⌂e informacije opisuju neke uobi⌂ajene probleme i pogre⌂ke na koje mo⌂ete nai⌂i kada upotrebljavate EIM i neke sugestije kako ispraviti te pogre⌂ke i probleme.

- "Rje⌂avanje problema s povezivanjem kontrolera domene"
- "Rje⌂avanje op⌂enitih EIM konfiguracijskih problema i problema domene" na stranici 107
- "Rje⌂avanje problema Mapiranja identiteta u poduze⌂u: problemi mapiranja" na stranici 109

Ako koristite EIM za omogu⌂avanje okoline jednostruke prijave, mo⌂da ⌂ete htjeti pogledati Rje⌂avanje problema konfiguracije jednostruke prijave u poglavlju Jednostruka prijava da biste nau⌂ili vi⌂e o savjetima za rje⌂avanje problema.

Rje⌂avanje problema s povezivanjem kontrolera domene

Velik broj faktora mo⌂e pridonijeti problemima povezivanja kod poku⌂aja povezivanja na kontroler domene. Koristite sljede⌂u tablicu za odre⌂ivanje kako rije⌂iti potencijalne probleme povezivanja kontrolera domene.

Tablica 27. Uobi⌂ajeni problemi i rje⌂enja povezivanja EIM kontrolera domene

Mogu⌂i problem	Mogu⌂a rje⌂enja
Ne mo⌂ete se spojiti na kontroler domene kad koristite iSeries Navigator za upravljanje EIM-om.	Informacije veze kontrolera domene mogu biti neispravno navedene za domenu kojom ⌂elite upravljati. Izvedite sljede⌂e korake za provjeru informacija veze domene: • Pro⌂irite **Mre⌂a-->Mapiranje identiteta u poduze⌂u-->Mre⌂a->Upravljanje domenom**. Desno kliknite domenu kojom ⌂elite upravljati i izaberite **Svojstva**. • Provjerite da je ime **Kontrolera domene** ispravno i da je **Nadre⌂eni DN** ispravno naveden. • Provjerite da su informacije za **Vezu** za kontroler domene ispravne. Provjerite da je broj **Porta** ispravan. Ako je izabrano **Koristi sigurnu vezu (SSL ili TLS)** poslu⌂itelj direktorija mora biti konfiguriran za kori⌂tenje SSL-a. Kliknite **Provjeri vezu** da provjerite da mo⌂ete koristiti navedene informacije za uspje⌂nu uspostavu veze s kontrolerom domene. • Provjerite da su korisni⌂ke informacije u panelu **Povezivanje na kontroler domene** ispravne.

Tablica 27. Uobi⌂ajeni problemi i rje⌂enja povezivanja EIM kontrolera domene (nastavak)

Mogu⌂i problem	Mogu⌂a rje⌂enja
Operativni sistem ili aplikacije ne mogu se spojiti na kontroler domene za pristup EIM podacima. Na primjer, ne uspijevaju operacije EIM pregledavanja mapiranja koje su izvedene za sistem. To se mo⌂e de⌂avati, jer je EIM konfiguracija na sistemu ili sistemima neispravna.	Provjerite va⌂u EIM konfiguraciju. Pro⌂irite **Mre⌂a-->Mapiranje identiteta u poduze⌂u-->Konfiguracija** na sistemu na kojem poku⌂avate provjeriti autenti⌂nost. Desno kliknite folder **Konfiguracija** i izaberite **Svojstva** i provjerite sljede⌂e: • Stranica **Domena**: – Ispravnost imena kontrolera domene i brojeva porta. – Kliknite **Provjeri konfiguraciju** da provjerite da je kontroler domene aktivan. – Ispravnost navedenog imena lokalnog registra – Ispravnost imena Kerberos registra – Provjerite da je izabrano **Omogu⌂i EIM operacije za ovaj sistem**. • Stranica **Korisnik sistema**: – Da li navedeni korisnik ima dostatnu EIM kontrolu pristupa za izvo⌂enje pregledavanja mapiranja i lozinka je va⌂e⌂a za korisnika. Pogledajte online pomo⌂ da nau⌂ite vi⌂e o razli⌂itim tipovima korisni⌂kih vjerodajnica. **Bilješka:** Ako ste lozinku promijenili za specifi⌂nog sistemskog korisnika u poslu⌂itelju direktorija, lozinku morate tako⌂er i ovdje promijeniti. Ako te lozinke ne odgovaraju, tada korisnik sistema ne mo⌂e izvesti EIM funkcije za operativni sistem i operacija pregledavanja mapiranja ne⌂e uspjeti. – Kliknite **Provjeri vezu** da potvrdite da su navedene korisni⌂ke informacije ispravne.
Izgleda da su informacije konfiguracije ispravne, ali ne mo⌂ete se spojiti na kontroler domene.	• Provjerite da li je aktivan poslu⌂itelj direktorija koji djeluje kao EIM kontroler domene. Ako je kontroler domene iSeries poslu⌂itelj, mo⌂ete koristiti iSeries Navigator i slijediti ove korake: 1. Pro⌂irite **Mre⌂a > Poslu⌂itelj > TCP/IP**. 2. Provjerite da poslu⌂itelj direktorija ima stanje **Pokrenut**. Ako je poslu⌂itelj zaustavljen, desno kliknite na **Poslu⌂itelj direktorija** i izaberite **Pokreni...**

Nakon ⌂to se provjerili informacije veze i da je poslu⌂itelj direktorija aktivan, poku⌂ajte se povezati na kontroler domene tako da slijedite ove korake:

1. Pro⌂irite **Mre⌂a > Mapiranje identiteta u poduze⌂u > Upravljanje domenom**.
2. Desno kliknite na EIM domenu na koju se ⌂elite povezati i izaberite **Povezivanje...**.
3. Specificirajte tip korisnika i potrebne korisni⌂ke informacije koje bi se trebale koristiti za povezivanje na kontroler EIM domene.
4. Kliknite**OK**.

Rje⌂avanje op⌂enitih EIM konfiguracijskih problema i problema domene

Postoji veliki broj op⌂enitih problema na koje mo⌂ete nai⌂i kada konfigurirate EIM za va⌂ sistem, kao i problemi na koje mo⌂ete nai⌂i kada pristupate EIM domeni. Koristite sljede⌂u tablicu da nau⌂ite vi⌂e o nekim uobi⌂ajenim problemima i potencijalnim rje⌂enjima koje mo⌂ete koristiti za rje⌂avanje ovih problema.

Tablica 28. Uobi⌂ajeni problemi i rje⌂enja EIM konfiguracije i domene

Mogu⌂i problem	Mogu⌂a rje⌂enja
Izgleda da ⌂arobnjak EIM konfiguracije visi za vrijeme obrade **Zavr⌂etka**.	⌂arobnjak mo⌂da ⌂eka da se kontroler domene pokrene. Provjerite da se u toku pokretanja poslu⌂itelja direktorija nisu pojavile pogre⌂ke. Za iSeries poslu⌂itelje, provjerite dnevnik posla za posao QDIRSRV u podsistemu QSYSWRK. Da provjerite dnevnik posla, pratite ove korake: 1. U iSeries Navigatoru, pro⌂irite **Upravljanje poslom > Podsistemi > Qsyswrk**. 2. Desno kliknite na **Qdirsrv** i izaberite **Dnevnik posla**.
Za vrijeme upotrebe ⌂arobnjaka EIM konfiguracije za kreiranje domene na udaljenom sistemu, primili ste sljede⌂u poruku o gre⌂ci: ″Nadre⌂eno razlikovno ime (DN) koje ste unijeli, nije va⌂e⌂e″. DN mora postojati na udaljenom poslu⌂itelju direktorija. Navedite ili izaberite novi ili postoje⌂i nadre⌂eni DN.	Nadre⌂eni DN naveden za udaljenu domenu ne postoji. Pogledajte "Kreiranje i spajanje nove udaljene domene" na stranici 66 za nau⌂iti vi⌂e o tome kako koristiti ⌂arobnjaka EIM konfiguracije. Tako⌂er, pogledajte online pomo⌂ za detaljne informacije o specificiranju nadre⌂enog DN-a kada kreirate domenu.
Primili ste poruku koja ukazuje da EIM domena ne postoji.	Ako niste kreirali EIM domenu, koristite ⌂arobnjaka za EIM konfiguraciju. Ovaj ⌂arobnjak za vas kreira EIM domenu ili vam omogu⌂uje konfiguriranje postoje⌂e EIM domene. Ako ste kreirali EIM domenu, osigurajte da je navedeni korisnik ⌂lan neke "EIM kontrola pristupa" na stranici 33 grupe s dostatnim ovla⌂tenjima da joj pristupi.
Primili ste poruku koja ukazuje da EIM objekt (identifikator, registar, asocijacija, asocijacija politike ili filter certifikata) nije prona⌂en ili da nemate ovla⌂tenja na EIM podacima.	Provjerite da EIM objekt postoji i je li naveden korisnik ⌂lan neke "EIM kontrola pristupa" na stranici 33 grupe s dostatnim ovla⌂tenjima za taj objekt.
Kada pro⌂irite folder **Identifikatori** pro⌂e puno vremena prije nego se poka⌂e popis identifikatora.	Ovo se mo⌂e desiti ako u domeni postoji veliki broj EIM identifikatora. Da biste to rije⌂ili, mo⌂ete prilagoditi pogled foldera **Identifikatori** tako da ograni⌂ite kriterije pretra⌂ivanja za prikaz identifikatora. Da prilagodite pogled EIM identifikatora, pratite ove korake: 1. U iSeries Navigatoru, pro⌂irite **Mre⌂a > Mapiranje identiteta u poduze⌂u > Upravljanje domenom**. 2. Pro⌂irite EIM domenu u kojoj ⌂elite prikazati EIM identifikatore. 3. Desno kliknite **Identifikatori** pa izaberite **Prilagodi ovaj pogled > Uklju⌂i...**. 4. Navedite kriterij prikaza koji ⌂e se koristiti za generiranje popisa EIM identifikatora koji ⌂e se uklju⌂iti u pogled. **Bilješka:** Kao generi⌂ki znak mo⌂ete koristiti zvjezdicu (*). 5. Kliknite**OK**. Kada sljede⌂i put kliknete **Identifikatori**, prikazuju se samo oni EIM identifikatori koji odgovaraju kriteriju koji ste naveli.
Prilikom upravljanja EIM-om pomo⌂u iSeries Navigatora, primili ste pogre⌂ku koja ukazuje da EIM nadimak nije vi⌂e va⌂e⌂i.	Veza s kontrolerom domene je izgubljena. Da se ponovno pove⌂ete na kontroler domene, pratite ove korake: 1. U iSeries Navigatoru, pro⌂irite **Mre⌂a > Mapiranje identiteta u poduze⌂u > Upravljanje domenom**. 2. Desno kliknite domenu s kojom ⌂elite raditi i izaberite **Ponovno spajanje...**. 3. Specificirajte informacije povezivanja. 4. Kliknite**OK**.

Tablica 28. Uobi⌂ajeni problemi i rje⌂enja EIM konfiguracije i domene (nastavak)

Mogu⌂i problem	Mogu⌂a rje⌂enja
Kada koristite Kerberos protokol za provjeru autenti⌂nosti s EIM-om, dijagnosti⌂ka se poruka CPD3E3F pi⌂e u dnevnik posla.	Ova je poruka generirana kad god ne uspije provjera autenti⌂nosti ili operacija pregledavanja mapiranja. Dijagnosti⌂ke poruke sadr⌂e glavne i manje va⌂ne kodove stanja za ozna⌂avanje gdje se desio problem. Naj⌂e⌂e gre⌂ke su dokumentirane u poruci zajedno s obnavljanjem. Pogledajte informacije pomo⌂i pridru⌂ene dijagnosti⌂koj poruci za pokretanje ispravljanja gre⌂aka u problemu. Tako⌂er vam mo⌂e biti od pomo⌂i pogledati Rje⌂avanje problema konfiguracije jednostruke prijave.

Rje⌂avanje problema Mapiranja identiteta u poduze⌂u: problemi mapiranja

Postoje brojni uobi⌂ajeni problemi koji mogu prouzro⌂iti potpuni neuspjeh mapiranja u Mapiranju identiteta u poduze⌂u (EIM) ili neo⌂ekivani rad. Koristite se sljede⌂om tablicom za pronalazak informacija o problemu koji je uzrok neuspjehu EIM mapiranja i mogu⌂ih rje⌂enja tog problema. Ako ne uspije EIM mapiranje, trebat ⌂ete prou⌂iti svako rje⌂enje u tablici kako bi osigurali pronalazak i rje⌂enje jednog ili vi⌂e problema koji su uzrok neuspjeha mapiranja.

Tablica 29. Uobi⌂ajeni problemi i rje⌂enja EIM mapiranja

Mogu⌂i problem	Mogu⌂a rje⌂enja
Informacije povezivanja za kontroler domene mo⌂da nisu ispravne ili kontroler domene mo⌂da nije aktivan.	Pogledajte Probleme povezivanja kontrolera domene za nau⌂iti kako provjeriti informacije povezivanja za kontroler domene i kako provjeriti da je kontroler domene aktivan.
Operacije pregledavanja EIM mapiranja koje su se izvodile za sistem ne uspijevaju. To se de⌂ava zbog pogre⌂ne EIM konfiguracije na sistemu ili sistemima.	Provjerite va⌂u EIM konfiguraciju. Pro⌂irite **Mre⌂a-->Mapiranje identiteta u poduze⌂u-->Konfiguracija** na sistemu na kojemu poku⌂avate provjeriti autenti⌂nost. Desno kliknite folder **Konfiguracija** i izaberite **Svojstva** i provjerite sljede⌂e: • **Domena** stranica: – Ime kontrolera domene i brojevi porta ispravni su. – Kliknite **Provjeri konfiguraciju** da provjerite da je kontroler domene aktivan. – Ime lokalnog registra je neispravno navedeno. – Ime Kerberos registra je neispravno navedeno. – Provjerite da je izabrano **Za ovaj sistem omogu⌂i EIM operacije**. • **Korisnik sistema** stranica: – Navedeni korisnik ima dostatnu EIM kontrolu pristupa za izvo⌂enje pregledavanja mapiranja, a lozinka je va⌂e⌂a za korisnika. Pogledajte online pomo⌂ da nau⌂ite vi⌂e o razli⌂itim tipovima korisni⌂kih vjerodajnica. **Bilješka:** Ako ste lozinku promijenili za specifi⌂nog sistemskog korisnika u poslu⌂itelju direktorija, lozinku morate tako⌂er i ovdje promijeniti. Ako te lozinke ne odgovaraju, tada korisnik sistema ne mo⌂e izvesti EIM funkcije za operativni sistem i operacije pregledavanja mapiranja ne⌂e uspjeti. – Kliknite **Provjeri vezu** da potvrdite da su navedene korisni⌂ke informacije ispravne.

Tablica 29. Uobi⌂ajeni problemi i rje⌂enja EIM mapiranja (nastavak)

Mogu⌂i problem	Mogu⌂a rje⌂enja
Operacija pregledavanja mapiranja mo⌂e vra⌂ati vi⌂estruke ciljne korisni⌂ke identitete. Ovo se mo⌂e desiti kada postoji jedna ili vi⌂e sljede⌂ih situacija: • EIM identifikatora ima vi⌂estruke individualne ciljne asocijacije na istom ciljnom registru. • Vi⌂e od jednog EIM identifikatora ima isti korisni⌂ki identitet naveden u izvornoj asocijaciji i svaki od tih EIM identifikatora ima ciljnu asocijaciju na istom ciljnom registru, iako korisni⌂ki identitet naveden za svaku ciljnu asocijaciju mo⌂e biti razli⌂it. • Vi⌂e od jedne default asocijacije politike domene specificira isti ciljni registar. • Vi⌂e od jedne default asocijacije politike registra specificira isti izvorni registar i isti ciljni registar. • Vi⌂e od jedne asocijacije politike filtera certifikata specificira isti izvorni X.509 registar, filter certifikata i ciljni registar.	Koristite "Testiranje EIM mapiranja" na stranici 79 funkciju za provjeru da li se odre⌂eni izvorni korisni⌂ki identitet mapira ispravno u prikladan ciljni korisni⌂ki identitet. Kako ⌂ete ispraviti problem ovisi o rezultatima koje dobijete iz testiranja, kako slijede: • Test vra⌂a ne⌂eljene vi⌂estruke ciljne identitete. To ukazuje da konfiguracija asocijacije za domenu nije ispravna zbog jednog od sljede⌂eg: – Ciljna ili izvorna asocijacija nije ispravno konfigurirana za EIM identifikator. Na primjer, ne postoji izvorna asocijacija za Kerberos principal (ili windows korisnika) ili je neispravna. Ili, ciljna asocijacija navodi neto⌂ni korisni⌂ki identitet. Prika⌂ite sve asocijacije identifikatora za EIM identifikator da provjerite asocijacije za specifi⌂ni identifikator. – Asocijacija politike nije ispravno konfigurirana. Prika⌂ite sve asocijacije politika za domenu da provjerite izvorne i ciljne informacije za sve asocijacije politike definirane u domeni. • Test vra⌂a vi⌂estruke ciljne korisni⌂ke identitete i ti su rezultati prikladni za na⌂in na koji ste konfigurirali asocijacije. Ako je ovo slu⌂aj, tada trebate specificirati informacije pregledavanja za svaki ciljni korisni⌂ki identitet kako bi osigurali da operacija pregledavanja vra⌂a jednostruki ciljni korisni⌂ki identitet umjesto svih mogu⌂ih korisni⌂kih identiteta. Pogledajte Dodavanja informacije pregledavanja u ciljni korisni⌂ki identitet. **Bilješka:** Ovaj pristup radi samo ako je aplikacija omogu⌂ena za kori⌂tenje informacije pregledavanja. Me⌂utim, osnovne OS/400 aplikacije poput iSeries Access-a za Windows ne mogu koristiti informacije pregledavanja za razlikovanje vi⌂estrukih ciljnih korisni⌂kih identiteta koje vra⌂a operacija pregledavanja. Prema tome, trebate razmotriti ponovno definiranje asocijacija za domenu kako bi osigurali da operacija pregledavanja mapiranja mo⌂e vratiti jednostruki ciljni korisni⌂ki identitet koji osigurava da osnovne OS/400 aplikacije mogu uspje⌂no izvesti operacije pregledavanja i mapirati identitete.

Tablica 29. Uobi⌂ajeni problemi i rje⌂enja EIM mapiranja (nastavak)

Mogu⌂i problem	Mogu⌂a rje⌂enja
Operacije EIM pregledavanja ne vra⌂aju rezultate, a asocijacije su konfigurirane za domenu.	Koristite "Testiranje EIM mapiranja" na stranici 79 funkciju za provjeru da li se odre⌂eni izvorni korisni⌂ki identitet mapira ispravno u prikladan ciljni korisni⌂ki identitet. Provjerite da ste za test osigurali ispravne informacije. Ako su informacije ispravne i test ne vra⌂a rezultate, tada problem mo⌂e biti uzrokovan jednim od sljede⌂eg: • Konfiguracija asocijacije je pogre⌂na. Provjerite va⌂u konfiguraciju asocijacije kori⌂tenjem informacija o rje⌂avanju problema iz prethodnog ulaza. • Podr⌂ka asocijacije politike nije omogu⌂ena na razini domene. Trebat ⌂ete omogu⌂iti asocijacije politike za domenu. • Podr⌂ka pregledavanja mapiranja ili podr⌂ka asocijacije politike nije omogu⌂ena na individualnoj razini registra. Mo⌂da ⌂ete morati omogu⌂iti podr⌂ku pregledavanja mapiranja i kori⌂tenje asocijacija politike za ciljni registar. • Definicija registra i korisni⌂ki identitet ne podudaraju se zbog osjetljivosti na velika i mala slova. Registar mo⌂ete obrisati i ponovno kreirati ili izbrisati i ponovno kreirati asocijaciju s ispravnom veli⌂inom slova.

Sli⌂ne informacije za Mapiranje identiteta u poduze⌂u

Mo⌂da ⌂ete htjeti nau⌂iti o ostalim tehnologijama koje se odnose na Mapiranje identiteta u poduze⌂u (EIM). Sljede⌂a poglavlja Informacijskog Centra poma⌂u vam u razumijevanju ovih srodnih tehnologija:

- **Jednostruka prijava** Ovo poglavlje daje informacije o tome kako konfigurirati i upravljati okolinom jednostruke prijave za va⌂e poduze⌂e, uklju⌂uju⌂i mno⌂tvo scenarija koje mo⌂ete koristiti za odre⌂ivanje kako jednostruka prijava mo⌂e koristiti va⌂em poduze⌂u.
- **Usluga mre⌂ne provjere autenti⌂nosti** Ovo poglavlje pru⌂a konfiguracijske informacije i ostale informacije o kori⌂tenju usluge mre⌂ne provjere autenti⌂nosti, iSeries implementacije Kerberos protokola. Kada konfigurirate uslugu mre⌂ne provjere autenti⌂nosti za rad u konjukciji s EIM-om, mo⌂ete kreirati okolinu jednostruke prijave za va⌂e poduze⌂e.
- **IBM Poslu⌂itelj direktorija za iSeries (LDAP)** Ovo poglavlje daje konfiguracijske i konceptualne informacije za IBM Poslu⌂itelja direktorija za iSeries (LDAP). EIM mo⌂e poslu⌂itelja direktorija koristiti tako da djeluje poput hosta za EIM kontrolera domene i pohranjivanje podataka EIM domene.

Termini i uvjeti za spu⌂tanje i ispis informacija

Dozvole za upotrebu informacija koje ste izabrali za spu⌂tanje dodjeljuju se prema sljede⌂im terminima i uvjetima i nakon va⌂eg prihva⌂anja.

Osobna upotreba: Mo⌂ete reproducirati ove informacije za va⌂u osobnu, nekomercijalnu upotrebu, uz osiguranje da su sve napomene o vlasni⌂tvu sa⌂uvane. Ne smijete distribuirati, prikazivati ili raditi izvedena djela iz ovih informacija, ili bilo kojeg njihovog dijela, bez izri⌂ite suglasnosti IBM-a.

Komercijalna upotreba: Mo⌂ete reproducirati, distribuirati i prikazivati ove informacije isklju⌂ivo unutar va⌂eg poduze⌂a, uz osiguranje da su sve napomene o vlasni⌂tvu sa⌂uvane. Ne smijete izra⌂ivati izvedene radove iz ovih informacija ili reproducirati, distribuirati ili prikazivati ove informacije ili bilo koji njihov dio izvan va⌂eg poduze⌂a, bez izri⌂ite dozvole IBM-a.

Osim kako je izri⌂ito dodijeljeno u ovoj dozvoli, nisu dane nikakve dozvole, licence ili prava, niti izri⌂ita niti posredna, na informacije ili bilo koje podatke, softver ili bilo koje drugo intelektualno vlasni⌂tvo sadr⌂ano unutar.

IBM rezervira pravo da bilo kad, po vlastitom nahoΔenju, povuΔe ovdje dodijeljene dozvole, ako je upotreba informacija Δtetna za njegove interese ili je ustanovljeno od strane IBM-a da gornje upute nisu bile ispravno slijeΔene.

Ne smijete spustiti, eksportirati ili reeksportirati ove informacije, osim kod potpune usklaΔenosti sa svim primjenjivim zakonima i propisima, ukljuΔujuΔi sve zakone i propise o izvozu Sjedinjenih DrΔava. IBM NE DAJE NIKAKVA JAMSTVA NA SADRΔAJ OVIH INFORMACIJA. INFORMACIJE SE DAJU ″KAKVE JESU″ I BEZ JAMSTAVA BILO KOJE VRSTE, IZRAVNIH ILI POSREDNIH, UKLJUΔUJUΔI, ALI NE OGRANIΔAVAJUΔI SE NA, POSREDNA JAMSTVA PROĐE NA TRΔIΔTU, NEKRΔENJA I PRIKLADNOSTI ZA ODREĐENU SVRHU.

Svi materijali su autorsko pravo od IBM Corporation.

SpuΔtanjem i ispisom informacija s ove stranice, naznaΔili ste da se slaΔete s ovim terminima i uvjetima.

Dodatak. Napomene

Ove informacije su razvijene za proizvode i usluge koji se nude u SAD.

IBM možda ne nudi proizvode, usluge ili dodatke koji su opisani u ovom dokumentu u drugim zemljama. Posavjetujte se sa svojim lokalnim IBM predstavnikom radi informacija o tome koji su proizvodi i usluge trenutno dostupni u vašem području. Bilo koje upućivanje na IBM proizvod, program ili uslugu nema namjeru tvrditi ili implicirati da se može koristiti samo taj IBM proizvod, program ili usluga. Umjesto toga se može koristiti bilo koji funkcionalno ekvivalentan proizvod, program ili usluga, koji ne narušava neko IBM intelektualno vlasništvo. Međutim, na korisniku je odgovornost da procijeni i verificira operacije bilo kojeg ne-IBM proizvoda, programa ili usluge.

IBM može imati patente ili molbe za patentiranje u stanju čekanja koji pokrivaju temu koja je opisana u ovom dokumentu. Posjedovanje ovog dokumenta vam ne daje nikakve licence na ove patente. Upite o licenci možete u pisanom obliku poslati na:

| IBM Director of Licensing
| IBM Corporation
| North Castle Drive
| Armonk, NY 10504-1785
| U.S.A.

Za upite o licenci koji se odnose na dvo-bajtne (DBCS) informacije, kontaktirajte IBM Odjel za intelektualno vlasništvo u vašoj zemlji ili pošaljite upite u pisanom obliku na:

| IBM World Trade Asia Corporation
| Licensing
| 2-31 Roppongi 3-chome, Minato-ku
| Tokyo 106-0032, Japan

Sljedeći odlomak se ne primjenjuje na Ujedinjeno Kraljevstvo ili bilo koju drugu zemlju gdje su takve izjave nekonzistentne s lokalnim zakonima: INTERNATIONAL BUSINESS MACHINES CORPORATION DAJE OVU PUBLIKACIJU “KAKVA JE ”, BEZ IKAKVIH JAMSTAVA, BILO IZRAVNIH ILI POSREDNIH, UKLJUČUJUĆI, ALI NE OGRANIČAVAJUĆI SE NA, UKLJUČENA JAMSTVA O NE-POVREĐIVANJU, PROĐI NA TRŽIŠTU ILI SPOSOBNOSTI ZA ODREĐENU SVRHU. Neke zemlje ne dozvoljavaju odricanje od izravnih ili posrednih jamstava u određenim transakcijama, zbog toga, se ova izjava možda ne odnosi na vas.

Ove informacije mogu sadržavati tehničke netočnosti ili tipografske pogreške. Promjene se povremeno rade u ovim informacijama; te promjene će biti uključene u nova izdanja publikacije. IBM može bilo kada i bez obavijesti učiniti poboljšanja i/ili promjene u proizvodima i/ili programima opisanim u ovoj publikaciji.

Bilo koje upućivanje u ovim informacijama na ne-IBM Web stranice, služi samo kao pomoć i ni na kakav način ne služi za promicanje tih Web stranica. Materijali na tim Web stranicama nisu dio materijala za ovaj IBM proizvod i te Web stranice koristite na vlastiti rizik.

| IBM može koristiti ili distribuirati sve informacije koje vi dobavite, na bilo koji način za koji smatra da je prikladan i
| bez ikakvih obveza prema vama.

Vlasnici licence za ovaj program, koji žele imati informacije o njemu u svrhu omogućavanja: (i) izmjene informacija između neovisno kreiranih programa i drugih programa (uključujući i ovaj) i (ii) uzajamne upotrebe informacija koje su bile izmijenjene, trebaju kontaktirati:

| IBM Corporation
| Software Interoperability Coordinator, Department 49XA
| 3605 Highway 52 N

Rochester, MN 55901
U.S.A.

Takve informacije mogu biti dostupne, uz odgovarajuće termine i uvjete, uključujući u nekim slučajevima i plaćanje pristojbe.

Licencni program koji je opisan u ovim informacijama i sav licencni materijal dostupan za njega, IBM osigurava pod uvjetima IBM Korisničkog ugovora, IBM međunarodnog ugovora o programskim licencama, IBM Ugovora o licenci za strojni kod ili sličnog ugovora između nas.

Svi podaci o izvedbi koji su ovdje sadržani su utvrđeni u kontroliranoj okolini. Stoga, rezultati koji su dobavljeni u drugim operacijskim okolinama mogu značajno varirati. Neka mjerenja su možda bila izvedena na sistemima na razvojnoj razini i ne postoji nikakvo jamstvo da će ta mjerenja biti ista na općenito dostupnim sistemima. Osim toga, neka mjerenja su možda bila procijenjena pomoću ekstrapolacije. Stvarni rezultati se mogu razlikovati. Korisnici ovog dokumenta bi trebali verificirati primjenljive podatke za njihovo određeno okruženje.

Informacije koje se tiču ne-IBM proizvoda su dobivene od dobavljača tih proizvoda, njihovih objavljenih najava ili drugih dostupnih javnih izvora. IBM nije testirao te proizvode i ne može potvrditi koliko su točne tvrdnje o performansama, kompatibilnosti ili druge tvrdnje koje se odnose na ne-IBM proizvode. Pitanja o sposobnostima ne-IBM proizvoda bi trebala biti adresirana na dobavljače tih proizvoda.

Sve izjave koje se odnose na buduća usmjerenja ili namjere IBM-a su podložne promjenama i mogu se povući bez najave, a predstavljaju samo ciljeve i težnje.

Sve IBM-ove prikazane cijene su IBM-ove maloprodajne cijene, trenutne su i podložne su izmjenama bez prethodnog upozorenja. Cijene zastupnika mogu odstupati.

Ove su informacije samo za svrhu planiranja. Ove informacije su podložne izmjenama prije no što opisani proizvodi postanu dostupni.

Ove informacije sadrže primjere podataka i izvještaja koji se koriste u svakodnevnom poslovanju. Za njihovu što je moguće bolju ilustraciju, primjeri uključuju imena pojedinaca, poduzeća, brandova i proizvoda. Sva ta imena su izmišljena i bilo kakva sličnost s imenima i adresama koje koristi stvarno poslovno poduzeće je sasvim slučajna.

LICENCA O AUTORSKOM PRAVU:

Ove informacije sadrže primjere aplikacijskih programa u izvornom jeziku koji ilustriraju programerske tehnike na različitim operacijskim platformama. Možete kopirati, modificirati i distribuirati primjere programa u bilo kakvom obliku bez potrebe za plaćanjem IBM-u za potrebe razvoja, korištenja, reklamiranja ili distribuiranja aplikacijskih programa prilagođenih sučelju aplikativnog programiranja za operacijske platforme za koje su primjeri programa i napisani. Ti primjeri nisu u potpunosti testirani pod svim uvjetima. IBM zbog toga ne može jamčiti ili potvrditi pouzdanost, upotrebljivost ili funkcioniranje tih programa.

PODLOŽNO BILO KOJIM ZAKONSKIM JAMSTVIMA KOJA SE NE MOGU ISKLJUČITI, IBM, NJEGOVI RAZVIJAČI PROGRAMA I DOBAVLJAČI NE DAJU JAMSTVA ILI UVJETE, IZRIČITE ILI POSREDNE, UKLJUČUJUĆI, ALI NE OGRANIČAVAJUĆI SE NA, POSREDNA JAMSTVA ILI UVJETE ZA PROĐU NA TRŽIŠTU, SPOSOBNOSTI ZA ODREĐENU SVRHU I NE-KRŠENJE, VEZANO UZ PROGRAM ILI TEHNIČKU PODRŠKU, UKOLIKO POSTOJE.

IBM, RAZVIJAČI PROGRAMA ILI DOBAVLJAČI NISU NITI U KOJIM UVJETIMA ODGOVORNI ZA BILO ŠTO OD SLJEDEĆEG, ČAK I AKO SU OBAVIJEŠTENI O TAKVOJ MOGUĆNOSTI:

1. GUBITAK ILI OŠTEĆENJE PODATAKA;
2. POSEBNE, SLUČAJNE ILI NEIZRAVNE ŠTETE, ILI EKONOMSKE POSLJEDIČNE ŠTETE; ILI
3. GUBITAK PROFITA, POSLA, ZARADE, DOBROG GLASA ILI UŠTEDE.

| NEKA ZAKONODAVSTVA NE DOZVOLJAVAJU ISKLJUČENJE ILI OGRANIČENJE SLUČAJNIH ILI
| POSLJEDIČNIH ŠTETA, TAKO DA SE GORNJA OGRANIČENJA MOŽDA NE ODNOSE NA VAS.

Svaka kopija ili dio tih primjera programa ili bilo kakav izvedeni rad, mora uključivati napomenu o autorskom pravu kako slijedi:

Ako gledate nepostojanu kopiju ovih informacija, fotografije i ilustracije u boji se možda neće vidjeti.

Zaštitni znaci

Sljedeći termini su zaštitni znaci International Business Machines Corporation u Sjedinjenim Državama, drugim zemljama ili oboje:

AIX
Distributed Relational Database Architecture
Domino
DRDA
e(logo)server
eServer
IBM
iSeries
OS/400
pSeries
RACF
RDN
Tivoli
WebSphere
xSeries
z/OS
zSeries

| Lotus, Lotus Notes, Freelance i WordPro su zaštitni znaci International Business Machines Corporation i Lotus
| Development Corporation u Sjedinjenim Državama, drugim zemljama ili oboje.

Microsoft, Windows, Windows NT i Windows logo su zaštitni znaci Microsoft Corporation u Sjedinjenim Državama, drugim zemljama ili oboje.

UNIX je registrirani zaštitni znak The Open Group u Sjedinjenim Državama i drugim zemljama.

Druga imena poduzeća, proizvoda i usluga mogu biti zaštitni znaci ili trgovački znaci drugih.

Termini i uvjeti za spu⌂tanje i ispis informacija

| Dozvole za upotrebu informacija koje ste izabrali za spu⌂tanje dodjeljuju se prema sljede⌂im terminima i uvjetima i
| nakon va⌂eg prihva⌂anja.

| **Osobna upotreba:** Mo⌂ete reproducirati ove informacije za va⌂u osobnu, nekomercijalnu upotrebu, uz osiguranje da
| su sve napomene o vlasni⌂tvu sa⌂uvane. Ne smijete distribuirati, prikazivati ili raditi izvedena djela iz ovih
| informacija, ili bilo kojeg njihovog dijela, bez izri⌂ite suglasnosti IBM-a.

Komercijalna upotreba: Mo⌂ete reproducirati, distribuirati i prikazivati ove informacije isklju⌂ivo unutar va⌂eg poduze⌂a, uz osiguranje da su sve napomene o vlasni⌂tvu sa⌂uvane. Ne smijete izra⌂ivati izvedene radove iz ovih informacija ili reproducirati, distribuirati ili prikazivati ove informacije ili bilo koji njihov dio izvan va⌂eg poduze⌂a, bez izri⌂ite dozvole IBM-a.

Osim kako je izri⌂ito dodijeljeno u ovoj dozvoli, nisu dane nikakve dozvole, licence ili prava, niti izri⌂ita niti posredna, na informacije ili bilo koje podatke, softver ili bilo koje drugo intelektualno vlasni⌂tvo sadr⌂ano unutar.

IBM rezervira pravo da bilo kad, po vlastitom naho⌂enju, povu⌂e ovdje dodijeljene dozvole, ako je upotreba informacija ⌂tetna za njegove interese ili je ustanovljeno od strane IBM-a da gornje upute nisu bile ispravno slije⌂ene.

Ne smijete spustiti, eksportirati ili reeksportirati ove informacije, osim kod potpune uskla⌂enosti sa svim primjenjivim zakonima i propisima, uklju⌂uju⌂i sve zakone i propise o izvozu Sjedinjenih Dr⌂ava. IBM NE DAJE NIKAKVA JAMSTVA NA SADR⌂AJ OVIH INFORMACIJA. INFORMACIJE SE DAJU ″KAKVE JESU″ I BEZ JAMSTAVA BILO KOJE VRSTE, IZRAVNIH ILI POSREDNIH, UKLJU⌂UJU⌂I, ALI NE OGRANI⌂AVAJU⌂I SE NA, POSREDNA JAMSTVA PROĐE NA TR⌂I⌂TU, NEKR⌂ENJA I PRIKLADNOSTI ZA ODREĐENU SVRHU.

Svi materijali su autorsko pravo od IBM Corporation.

Spu⌂tanjem i ispisom informacija s ove stranice, nazna⌂ili ste da se sla⌂ete s ovim terminima i uvjetima.

Tiskano u Hrvatskoj