System i

Sigurnost
Mapiranje identiteta u poduzeću

Verzija 6 Izdanje 1

System i

Sigurnost
Mapiranje identiteta u poduzeću

Verzija 6 Izdanje 1

Napomena

Prije korištenja ovih informacija i proizvoda koji podržavaju, pročitajte informacije u “Napomene”, na stranici 123.

Ovo izdanje se primjenjuje na verziju 6, izdanje 1, modifikaciju 0 za IBM i5/OS (broj proizvoda 5761–SS1) i na sva sljedeća izdanja i modifikacije dok se drukčije ne označi 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 poduzeću

Mapiranje identiteta u poduzeću (EIM) za System i platformu je i5/OS implementacija IBM infrastrukture koja omogućuje administratorima i razvijačima aplikacija rješavanje problema upravljanja s više korisničkih registara u cijelom poduzeću.

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

EIM vam omogućuje kreiranje sistema mapiranja identiteta, koji se zovu asocijacije, između različitih korisničkih identiteta u različitim korisničkim registrima za osobu u vašem poduzeću. EIM također omogućuje zajednički skup API-ja koji se mogu koristiti na svim platformama za razvoj aplikacija koje mogu koristiti mapiranje identiteta koje kreirate za gledanje odnosa među korisničkim identitetima. Dodatno, EIM možete koristiti zajedno s uslugom provjere autentičnosti mreže, i5/OS implementacijom Kerberosa, da omogućite okolinu jednostruke prijave.

EIM možete konfigurirati i njime upravljati preko System i Navigatora, System i grafičkog korisničkog sučelja. System i platforma koristi EIM da omogući i5/OS sučelja za provjeru autentičnosti uslugom provjere autentičnosti mreže. Aplikacije, kao i i5/OS, mogu prihvatiti Kerberos ulaznice i koristiti EIM da pronađu profil korisnika koji predstavlja istu osobu koju predstavlja i Kerberos ulaznica.

Da naučite više o tome kako EIM radi, o EIM konceptima i kako možete koristiti EIM u poduzeću pogledajte sljedeće:

Što je novo za V6R1

Pročitajte više o novim i značajno promijenjenim informacijama u zbirci poglavlja Mapiranje identiteta u poduzeću (EIM).

Nove ili poboljšane funkcije za EIM

- U prethodnim izdanjima i5/OS EIM je podržavao mapiranje na samo jedan identitet lokalnog korisnika po sistemu. U i5/OS V6R1, EIM podržava izbor između više mapiranja lokalnih korisničkih identiteta za isti sistem koristeći IP adresu ciljnog sistema za izbor ispravnog mapiranja lokalnog korisničkog identiteta na tom sistemu.

Dodatno, poglavlje Jednostruka prijava je ažurirano i osigurava dokumentaciju o primjeni EIM-a kao dijela okoline jednostruke prijave za smanjenje upravljanja lozinkom. Ovo poglavlje osigurava niz detaljnih scenarija s uobičajenim situacijama jednostruke prijave, uz detaljne upute konfiguracije za njihovu primjenu.

Kako vidjeti što je novo ili promijenjeno

Da bi vam pomogle vidjeti gdje su učinjene tehničke promjene, ove informacije koriste:

- Sliku  da označi gdje nova ili promijenjena informacija počinje.
- Sliku  da označi gdje nova ili promijenjena informacija završava.

Da nađete druge informacije o tome što je novo ili promijenjeno u ovom izdanju pogledajte Memorandum korisnicima.

PDF datoteka za Mapiranje identiteta u poduzeću

Možete pogledati i ispisati PDF datoteku s ovim informacijama.

Za pregled ili spuštanje PDF verzije ovog dokumenta izaberite Mapiranje identiteta u poduzeću (oko 1820 KB).

Možete pogledati ili spustiti PDF dokumente za sljedeća poglavlja:

- Usluge provjere autentičnosti mreže (oko 1398 KB) sadrži informacije kako konfigurirati uslugu provjere autentičnosti mreže zajedno s EIM-om za kreiranje okoline jednostruke prijave.
- IBM Tivoli Directory Server za i5/OS (LDAP) (oko 1700 KB) sadrži informacije kako konfigurirati LDAP poslužitelj koji možete koristiti kao EIM kontroler domene, zajedno s informacijama o naprednoj LDAP konfiguraciji.

Spremanje PDF datoteka

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

1. Desno kliknite PDF vezu u svom pretražitelju.
2. Kliknite na opciju koja sprema PDF lokalno.
3. Izaberite direktorij u koji želite spremiti PDF datoteku.
4. Kliknite **Save**.

Spuštanje Adobe Readera

Za pogled ili ispis ovih PDF dokumenata potreban vam je Adobe Reader instaliran na vašem sistemu. Besplatnu kopiju možete spustiti s Adobe Web stranice (www.adobe.com/products/acrobat/readstep.html) .

Pregled mapiranja identiteta u poduzeću

Mapiranje identiteta u poduzeću (EIM) vam može pomoći u rješavanju problema do kojih dolazi kada pokušavate upravljati s više od jednog korisničkog registra.

Današnje mrežno okruženje napravljeno je od kompleksne grupe sistema i aplikacija, rezultirajući iz potrebe za upravljanjem s više korisničkih registara. Bavljenje s višestrukim korisničkim registrima brzo raste u veliki administrativni problem koji utječe na korisnike, administratore i razvijače aplikacija. Prema tome, mnoge tvrtke se bore za sigurno upravljanje provjerom autentičnosti i autorizacije za sisteme i aplikacije. EIM administratorima i razvijačima aplikacija dozvoljava adresiranje ovog problema na jednostavniji i jeftiniji način u odnosu na prethodno rješenje.

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

Problem upravljanja višestrukim korisničkim registrima

Mnogi administratori upravljaju mrežama koje uključuju različite sisteme i poslužitelje, svaki s jedinstvenim načinom upravljanja korisnicima kroz različite korisničke registre. U ovim kompleksnim mrežama, administratori su odgovorni za upravljanje svakim korisničkim identitetom i lozinkom kroz višestruke sisteme. Dodatno, administratori često moraju sinkronizirati ove identitete i lozinke, a korisnici su opterećeni s pamćenjem višestrukih identiteta i lozinki i njihovim usklađivanjem. Opterećenost korisnika i administratora u ovom okruženju je pretjerana. Prema tome, administratori često utroše vrijedno vrijeme rješavajući problem neuspjelih pokušaja prijave i ponovnom postavljanju zaboravljenih lozinki umjesto upravljajući poduzećem.

Problem upravljanja višestrukim korisničkim registrima također utječe na razvijače aplikacije koji žele osigurati višestruko povezane ili heterogene aplikacije. Ovi razvijači razumiju da korisnici imaju važne poslovne podatke raspršene kroz mnoge različite tipove sistema, gdje svaki sistem posjeduje svoje vlastite korisničke registre. Nadalje,

razvijači moraju kreirati vlasničke korisničke registre i udružene sigurnosne semantike za njihove aplikacije. Iako ovo rješava problem za razvijača aplikacije, također i povećava opterećenje za korisnike i administratore.

Trenutni pristupi

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

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

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

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

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

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

EIM pristup

EIM nudi novi pristup za jeftina rješenja izgradnje za jednostavnije upravljanje višestrukim korisničkim registrima i korisničkim identitetima u heterogenoj okolini aplikacija s višestrukim razinama. EIM je arhitektura za opisivanje odnosa između individualaca ili cjelina (poput poslužitelja datoteka i poslužitelja ispisa) u poduzeću i mnogih identiteta koji ih u tom poduzeću predstavljaju. U dodatku, EIM osigurava skup API-ja koji dozvoljavaju aplikacijama da postavljaju pitanja o ovim odnosima.

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

EIM dozvoljava jedan-prema-više mapiranja (drugim riječima, jedan korisnik s više od jednog korisničkog identiteta u jednom korisničkom registru). Međutim, administrator ne mora imati specifična pojedinačna mapiranja za sve

korisničke identitete u korisničkom registru. EIM također omogućuje mapiranja više-na-jedan (drugim riječima, višestruki korisnici mapirani u jednostruki korisnički identitet u jednostrukom korisničkom registru).

Mogućnost mapiranja između korisničkih identiteta u različitim korisničkim registrima osigurava mnoge koristi. Primarno, to znači da aplikacije mogu imati fleksibilnost korištenja jednog korisničkog registra za provjeru autentičnosti dok koriste potpuno drugačiji korisnički registar za autorizaciju. Na primjer, administrator može mapirati identitet Windows korisnika u Kerberos registru na profil i5/OS korisnika u različitom registru korisnika za pristup i5/OS resursima za koje je profil i5/OS korisnika ovlašten.

EIM je otvorena arhitektura koju administratori mogu koristiti za predstavljanje odnosa mapiranja identiteta za bilo koji registar. Ne zahtijeva kopiranje postojećih podataka u novo spremište i pokušava održati obje kopije sinkroniziranim. Jedini novi podaci koje EIM predstavlja su informacije odnosa. EIM te podatke pohranjuje u LDAP direktorij, koji na jednom mjestu omogućuje fleksibilnost pri upravljanju podacima i sadrži kopije kada se program koristi. Konačno, EIM daje poduzećima i razvijačima aplikacija fleksibilnost za lagani rad u širokom rasponu okruženja s manje troška nego što je to moguće bez ove podrške.

EIM, korišten zajedno s uslugom provjere autentičnosti mreže, i5/OS implementacijom Kerberosa, pruža jednostruko rješenje prijave. Aplikacije mogu biti napisane tako da koriste GSS API-je i EIM za prihvaćanje Kerberos karata i da se mapiraju na drugi, pridruženi korisnički identitet u nekom drugom korisničkom registru. Asocijacija između korisničkih identiteta koji omogućuju mapiranje ovog identiteta može se postići kreiranjem asocijacija identifikatora koji indirektno pridružuju jedan korisnički identitet drugom kroz EIM identifikator ili kreiranjem asocijacija politika koje direktno pridružuju jedan korisnički identitet grupe s jednostrukim specifičnim korisničkim identitetom.

Upotreba mapiranja identiteta zahtijeva da administratori učine sljedeće:

1. Konfigurirajte EIM domenu u mreži. Za kreiranje kontrolera domene za domenu i za konfiguriranje pristupa domeni možete koristiti Čarobnjaka EIM konfiguracije. Kada koristite čarobnjaka možete izabrati kreirati novu EIM domenu i kreirati kontroler domene na lokalnom sistemu ili udaljenom sistemu. Ili, ako EIM domena već postoji, možete izabrati sudjelovati u postojećoj EIM domeni.
2. Odredite kojim je korisnicima koji su definirani za poslužitelj direktorija na kojem je smješten EIM kontroler domene dozvoljeno upravljanje ili pristup specifičnim informacijama u EIM domeni i pridružite ih odgovarajućim grupama EIM kontrole pristupa.
3. Kreirajte EIM definicije registra za one korisnike registra koji će sudjelovati u domeni. Iako možete definirati sve korisničke registre za EIM domenu, morate definirati korisničke registre za one aplikacije i operativne sisteme koji su EIM-omogućeni.
4. Ovisno o potrebama EIM implementacije, odredite koje od sljedećih zadataka treba izvesti za završavanje EIM konfiguracije:
   - Kreirajte EIM identifikator za svakog jedinstvenog korisnika u domeni i kreirajte asocijacije identifikatora za njih.
   - Kreirajte asocijacije politika.
   - Kreirajte kombinaciju istih.

   Srodne informacije

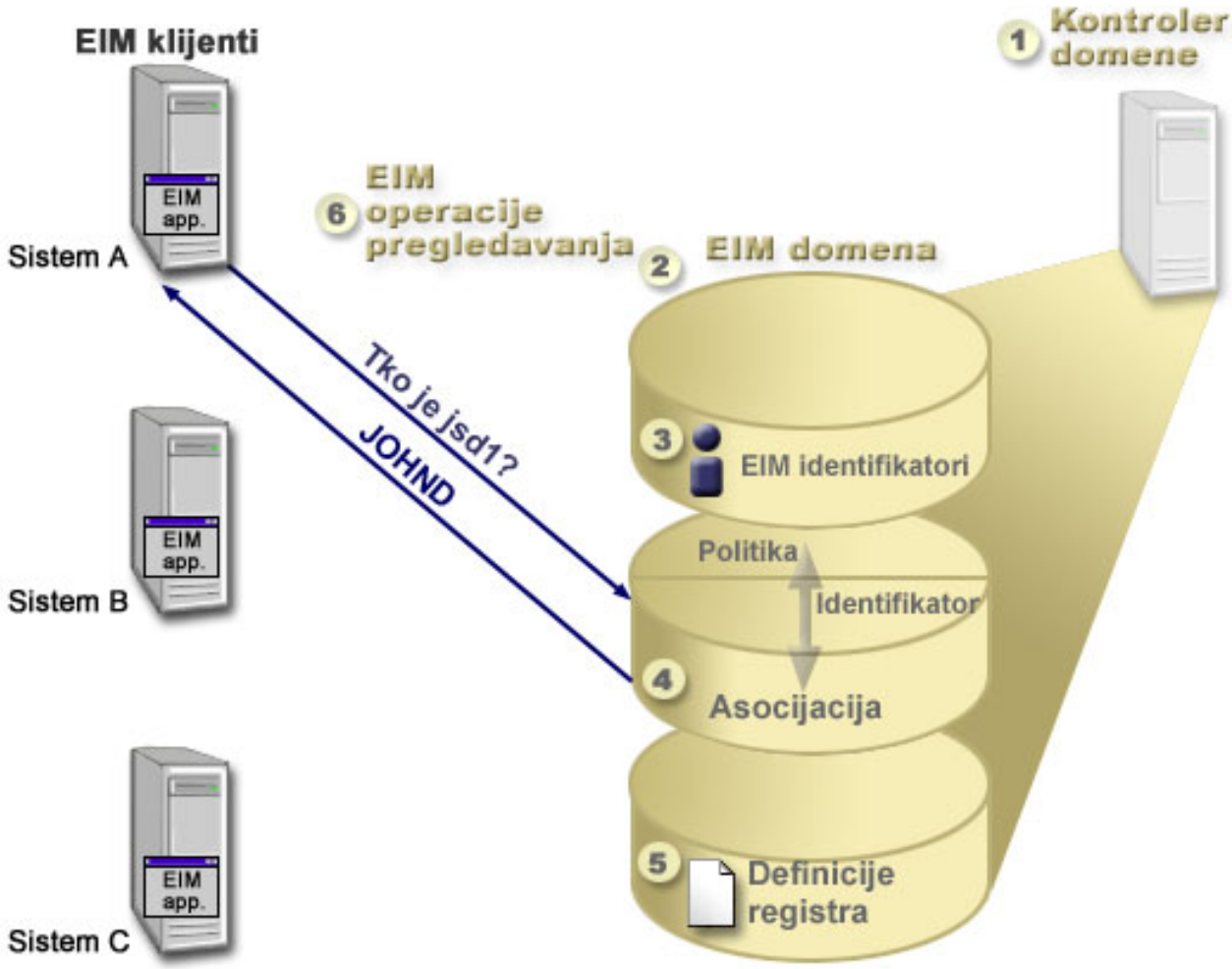
   Pregled jednostruke prijave

Koncepti Mapiranja identiteta u poduzeću

Konceptualno razumijevanje o tome kako radi Mapiranje identiteta u poduzeću (EIM) potrebno je za potpuno razumijevanje kako možete koristiti EIM u vašem poduzeću. Iako se konfiguracija i implementacija EIM API-ja mogu razlikovati između platformi poslužitelja, EIM koncepti su isti na svim IBM eServer platformama.

Slika 1 osigurava primjer EIM implementacije u poduzeću. Tri poslužitelja se ponašaju kao EIM klijenti i sadrže EIM-omogućene aplikacije koje zahtjevaju EIM podatke koji koriste EIM operacije pregledavanja 6 . Kontroler domene 1 pohranjuje informacije o EIM domeni 2 , što uključuje EIM identifikator 3 , asocijacije 4 između

ovih EIM identifikatora i korisničkih identiteta i EIM definicije registra 5 .



Slika 1. Primjer EIM implementacije

Pregledajte sljedeće informacije da naučite više o ovim EIM eServer konceptima:

Srodni koncepti

"LDAP koncepti za EIM" na stranici 46
EIM koristi LDAP poslužitelj kao kontroler domene za pohranu EIM podataka. Prema tome, morate razumjeti neke LDAP koncepte koji se odnose na konfiguriranje i upotrebu EIM-a u vašem poduzeću. Na primjer, možete koristiti LDAP razlikovno ime kao korisnički identitet za konfiguriranje EIM-a i provjere autentičnosti EIM kontrolera domene.

"Koncepti Mapiranja identiteta u poduzeću za i5/OS" na stranici 49
EIM možete primijeniti na bilo kojoj IBM eServer platformi. Ipak, kada EIM primjenjujete na System i model, morate računati na to da su neke od informacija specifične za System i primjenu.

Kontroler EIM domene

EIM kontroler domene je Lightweight Directory Access Protocol (LDAP) poslužitelj koji je konfiguriran za upravljanje jednom ili više EIM domena. EIM domenu čine svi EIM identifikatori, EIM asocijacije i korisnički registri koji su definirani u toj domeni. Sistemi (EIM klijenti) sudjeluju u EIM domeni korištenjem podataka domene za operacije EIM pregledavanja.

Trenutno možete konfigurirati IBM Tivoli Directory Server za i5/OS na nekim IBM eServer platformama da se ponaša kao EIM kontroler domene. Svaki sistem koji podržava EIM API-je može sudjelovati kao klijent u domeni. Ovi sistemi klijenata koriste EIM API-je za kontaktiranje EIM kontrolera domene radi izvedbe. Lokacija EIM klijenta određuje da li je kontroler EIM domene lokalni ili udaljeni sistem. Kontroler domene je *lokalni* ako se EIM klijent izvodi na istom sistemu kao i kontroler domene. Kontroler domene je *udaljeni* ako se EIM klijent izvodi na odvojenom sistemu od kontrolera domene.

Opaska: Ako planirate konfigurirati poslužitelj direktorija na udaljenom sistemu, poslužitelj direktorija mora omogućiti EIM podršku. EIM zahtjeva da je kontroler domene smješten na poslužitelju direktorija koji podržava verziju 3 Lightweight Directory Access Protocola (LDAP). Dodatno, proizvod poslužitelja direktorija mora biti konfiguriran tako da prihvaća EIM shemu. IBM Tivoli Directory Server za i5/OS osigurava ovu podršku.

Srodni koncepti

"EIM operacije pregledavanja" na stranici 26
Aplikacija ili operativni sistem koristi EIM API za izvođenje operacije pregledavanja tako da aplikacija ili operativni sistem mogu izvesti mapiranje s jednog identiteta korisnika u jednom registru na drugi identitet korisnika u drugom registru. EIM operacija pregledavanja je proces preko koje aplikacija ili operativni sistem pronalazi nepoznate pridružene korisničke identitete u određenom ciljnom registru tako da osigurava poznate i pouzdane informacije.

"LDAP shema i druga razmatranja za EIM" na stranici 48
Koristite ove informacije da saznate što je potrebno za rad poslužitelja direktorija s Mapiranjem identiteta u poduzeću (EIM).

EIM domena

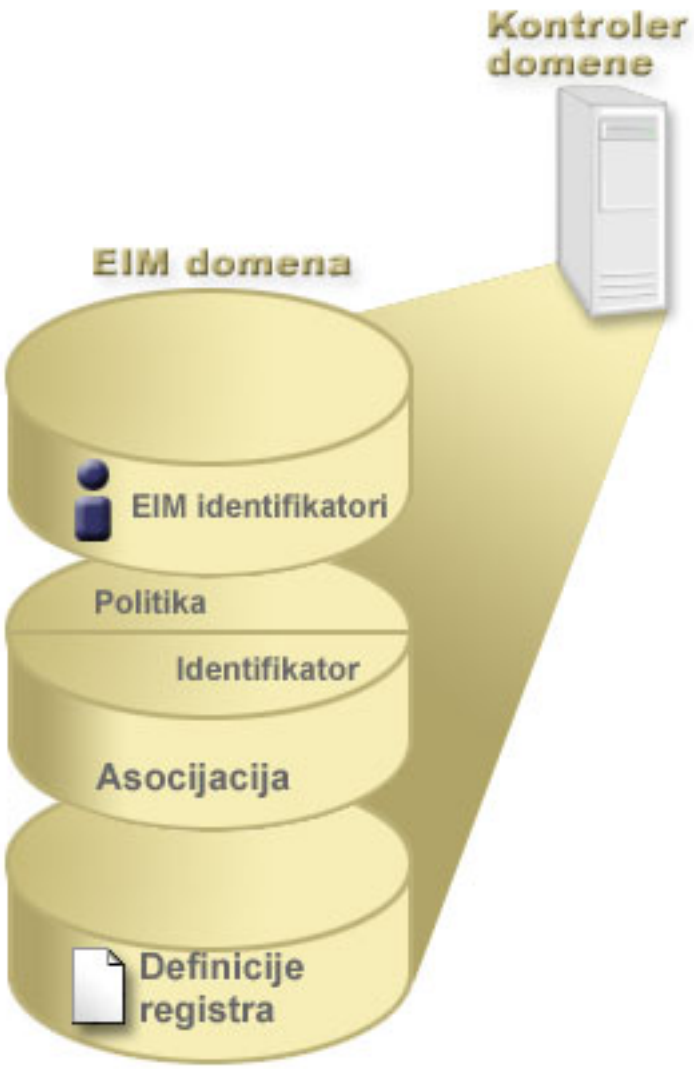
Domena Mapiranja identiteta u poduzeću (EIM) je direktorij u sklopu Lightweight Directory Access Protocol (LDAP) poslužitelja koji sadrži EIM podatke za poduzeće.

EIM domena je zbirka svih EIM identifikatora, EIM asocijacija i korisničkih registara koji su u toj domeni definirani kao i kontrole pristupa nad podacima. Sistemi (EIM klijenti) sudjeluju u domeni korištenjem domenskih podataka za EIM operacije pregledavanja.

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

Nasuprot tomu, EIM domena *odnosi* se na korisničke identitete, definirane u korisničkim registrima. EIM domena sadrži informacije o *odnosima* između identiteta u različitim korisničkim registrima (korisničko ime, tip registra i instanca registra) i stvarne ljude ili cjeline koje ovi identiteti predstavljaju.

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



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

EIM podaci uključuju:

Definicije EIM registra
Svaka EIM definicija registra koju kreirate predstavlja stvarni registar korisnika (i informacije o identitetima korisnika koje sadrži) koji postoji na sistemu unutar poduzeća. Jednom kada ste definirali specifični korisnički registar u EIM-u, taj korisnički registar može sudjelovati u EIM domeni. Možete kreirati dva tipa definicija registra, jedan tip se odnosi na korisničke registre sistema, a drugi se tip odnosi na korisničke registre aplikacija.

EIM identifikatori
Svaki identifikator EIM-a koji kreirate jednoznačno predstavlja osobu ili entitet (poput poslužitelja ispisa ili poslužitelja datoteka) unutar poduzeća. Možete kreirati EIM identifikator kada želite imati mapiranje s jednog na jedan među korisničkim identitetima koji pripadaju osobi ili cjelini kojoj odgovara EIM identifikator.

EIM asocijacije
EIM asocijacije koje kreirate predstavljaju odnose između identiteta korisnika. Asocijacije morate definirati tako da EIM klijenti mogu koristiti EIM API-je za uspješno izvođenje EIM operacija pregledavanja. Ove EIM operacije pregledavanja traže definirane asocijacije na EIM domeni. Postoje dva različita tipa asocijacija koje možete kreirati:

Asocijacije identifikatora

Asocijacije identifikatora vam dozvoljavaju da definirate odnos jedan-na-jedan između identiteta korisnika preko identifikatora EIM-a definiranog za individuu. Svaka EIM asocijacija identifikatora koju kreirate predstavlja jednostruki, specifični odnos između EIM identifikatora i pridruženog korisničkog identiteta unutar poduzeća. Asocijacije identifikatora omogućuju informacije koje vežu EIM identifikator za jedan određeni korisnički identitet u specifičnom korisničkom registru i za korisnika vam omogućuju kreiranje mapiranja identiteta jedan na jedan. Asocijacije identiteta su naročito korisne kada individue imaju identitete korisnika s posebnim ovlaštenjima i drugim povlasticama koje specifično želite kontrolirati kreirajući jedan-na-jedan mapiranja između njihovih identiteta korisnika.

Asocijacije politike

Asocijacije politike vam dozvoljavaju da definirate odnos između grupe korisničkih identiteta u jednom ili više registara korisnika i pojedinačnog identiteta korisnika u drugom registru korisnika. Svaka EIM asocijacija politike koju kreirate rezultira u mapiranju s više na jedan između izvorne grupe korisničkog identiteta u jednom korisničkom registru i jednostrukog ciljnog korisničkog identiteta. Tipično, asocijacije politike kreirate da mapirate grupu korisnika koji zahtijevaju istu razinu ovlaštenja na jednostruki identitet korisnika s tom razinom ovlaštenja.

Srodni koncepti

"Definicije EIM registra" na stranici 11
Definicija registra Mapiranja identiteta u poduzeću (EIM) je unos unutar EIM-a koji kreirate radi prikaza stvarnog korisničkog registra koji postoji na sistemu unutar poduzeća. Korisnički registar djeluje kao direktorij i sadrži listu važećih korisničkih identiteta za pojedinačni sistem ili aplikaciju.

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

"EIM operacije pregledavanja" na stranici 26
Aplikacija ili operativni sistem koristi EIM API za izvođenje operacije pregledavanja tako da aplikacija ili operativni sistem mogu izvesti mapiranje s jednog identiteta korisnika u jednom registru na drugi identitet korisnika u drugom registru. EIM operacija pregledavanja je proces preko koje aplikacija ili operativni sistem pronalazi nepoznate pridružene korisničke identitete u određenom ciljnom registru tako da osigurava poznate i pouzdane informacije.

EIM identifikator

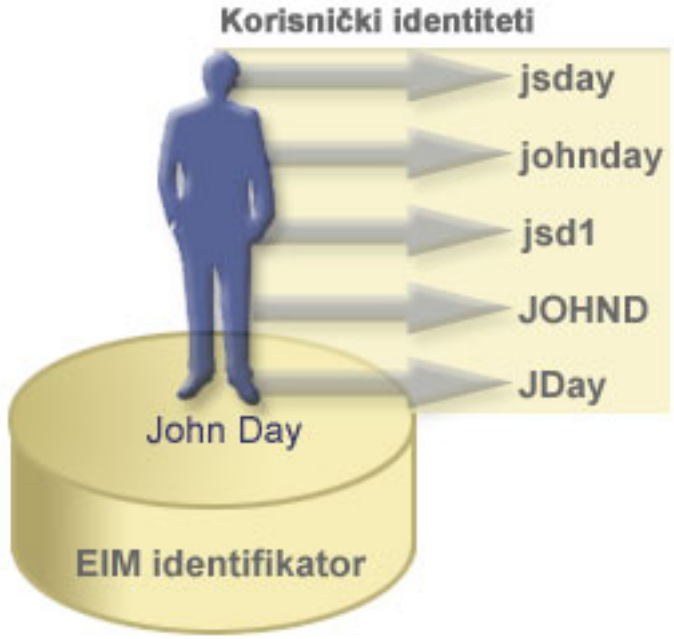
Identifikator Mapiranja identiteta u poduzeću (EIM) predstavlja osobu ili entitet u poduzeću. Tipična mreža sastoji se od različitih hardverskih platformi i aplikacija i njihovih udruženih korisničkih registara. Mnoge platforme i mnoge aplikacije koriste platformski specifične ili aplikacijski specifične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

EIM možete koristiti za kreiranje jedinstvenih EIM identifikatora za ljude ili cjeline u vašem poduzeću. Zatim možete kreirati asocijacije identifikatora ili mapirati identitete s jedan na jedan između EIM identifikatora i različitih korisničkih identiteta za osobe ili cjeline koje EIM identitet predstavlja. Ovaj proces olakšava izgradnju heterogenih aplikacija na više razina. Također postaje jednostavnija izgradnja i upotreba alata koji pojednostavljuju administraciju uključenu u upravljanje korisničkim identitetom koji osoba ili cjelina ima unutar poduzeća.

EIM identifikator koji predstavlja osobu

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

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

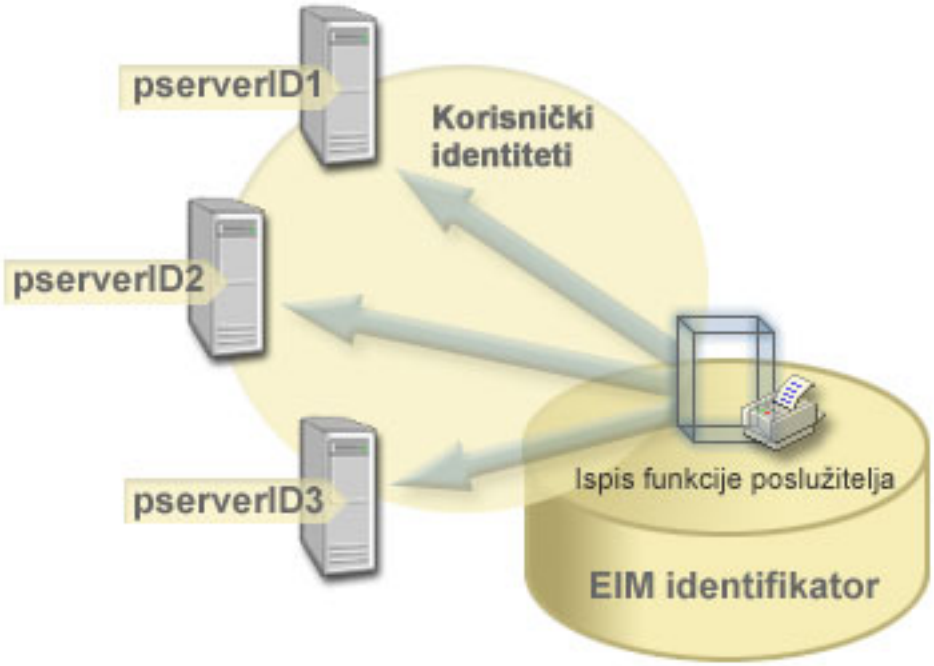


U EIM-u možete kreirati asocijacije koje definiraju odnose između John Day identifikatora i svakog od različitih korisničkih identiteta za *John Day*. Kreiranjem ovih asocijacija za definiranje ovih odnosa, vi i drugi možete pisati aplikacije koje koriste EIM API-je za traženje potrebnog, ali nepoznatog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

EIM identifikator koji predstavlja cjelinu

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

Slika 4: Odnos između EIM identifikatora koji predstavlja poslužiteljsku funkciju ispisa i različitih korisničkih identiteta za tu funkciju.



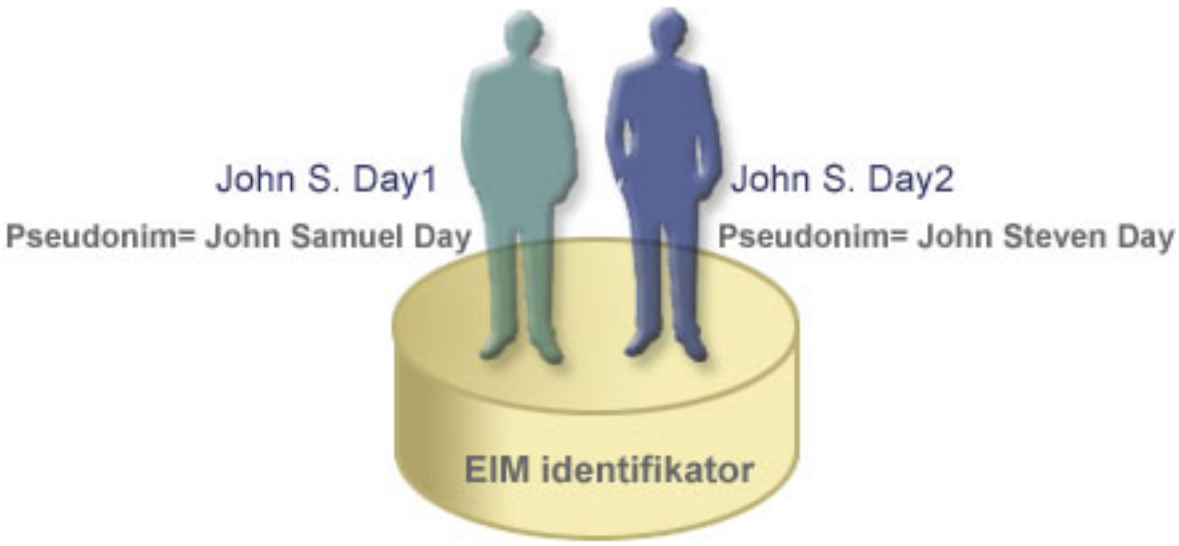
S EIM-om možete kreirati pojedinačni identifikator koji predstavlja poslužiteljsku funkciju ispisa unutar poduzeća. Kao što primjer pokazuje, EIM identifikator Poslužiteljska funkcija ispisa predstavlja stvarnu cjelinu poslužiteljske funkcije ispisa u poduzeću. Asocijacije su kreirane za definiranje odnosa između EIM identifikatora (Poslužiteljska funkcija ispisa) i svakog od korisničkih identiteta za tu funkciju (pserverID1, pserverID2 i pserverID3). Ove aplikacije dozvoljavaju razvijačima aplikacije da koriste EIM operacije pregledavanja za pronalaženje specifične poslužiteljske funkcije ispisa. Dobavljači aplikacije mogu tada lakše pisati distribuirane aplikacije koje upravljaju poslužiteljskom funkcijom ispisa unutar poduzeća.

EIM identifikatori i zamjensko ime

Imena EIM identifikatora moraju biti jedinstvena u EIM domeni. Zamjenska imena mogu pomoći u adresiranju situacija gdje korištenje jedinstvenih imena identifikatora može biti teško. Primjer korisnosti zamjenskih imena EIM identifikatora je u situaciji kada je nečije legalno ime različito od imena pod kojim je ta osoba poznata. Na primjer, različite individue unutar poduzeća mogu dijeliti isto ime, što može biti zbunjujuće ako koristite prava imena kao EIM identifikatore.

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

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



Korištenjem zamjenskih imena, EIM administrator može dobaviti dodatne informacije o pojedincu za svaki EIM identifikator. Svaki EIM identifikator može imati višestruka zamjenska imena za identificiranje kojeg *John S. Daya* EIM identifikator predstavlja. Na primjer, dodatna zamjenska imena mogu sadržavati korisnikov broj posla, broj odjela, naziv posla ili druge razlikovne atribute. U ovom primjeru zamjensko ime za John S. Day1 može biti John Samuel Day, a zamjensko ime za John S. Day2 može biti John Steven Day.

Informacije o zamjenskom imenu možete koristiti za pomoć prilikom lociranja određenog EIM identifikatora. Na primjer, aplikacija koja koristi EIM može navesti zamjensko ime koje koristi za pronalazak odgovarajućeg EIM identifikatora za aplikaciju. Administrator može to zamjensko ime dodati u EIM identifikator tako da aplikacija za EIM operacije može koristiti zamjensko ime umjesto jedinstvenog imena identifikatora. Aplikacija može ove informacije navesti prilikom korištenja API-ja Dohvat EIM ciljnih identiteta iz identifikatora (eimGetTargetFromIdentifier()) za izvedbu EIM operacije pregledavanja za pronalazak odgovarajućih korisničkih identiteta koji su mu potrebni.

Srodni koncepti

"EIM domena" na stranici 6
Domena Mapiranja identiteta u poduzeću (EIM) je direktorij u sklopu Lightweight Directory Access Protocol (LDAP) poslužitelja koji sadrži EIM podatke za poduzeće.

Definicije EIM registra

Definicija registra Mapiranja identiteta u poduzeću (EIM) je unos unutar EIM-a koji kreirate radi prikaza stvarnog korisničkog registra koji postoji na sistemu unutar poduzeća. Korisnički registar djeluje kao direktorij i sadrži listu važećih korisničkih identiteta za pojedinačni sistem ili aplikaciju.

Osnovni korisnički registar sadrži korisničke identitete i njihove lozinke. Jedan primjer korisničkog registra je z/OS Security Server Resource Access Control Facility (RACF) registar. Korisnički registri mogu sadržavati i druge informacije. Na primjer, Lightweight Directory Access Protocol (LDAP) direktorij sadrži vezana razlikovna imena, lozinke i kontrole pristupa podacima koji su spremljeni u LDAP-u. Drugi primjeri zajedničkih registara korisnika su principali u Kerberos području ili identiteti korisnika u domeni Aktivnog direktorija Windows-a i registar profila korisnika i5/OS-a

Također možete definirati korisničke registre koji postoje unutar drugih korisničkih registara. Neke aplikacije koriste podskup korisničkih identiteta unutar jedne instance korisničkog registra. Na primjer, registar z/OS Poslužitelja Sigurnosti (RACF) može sadržavati specifične korisničke registre koji su podskup korisnika unutar svih RACF korisničkih registara.

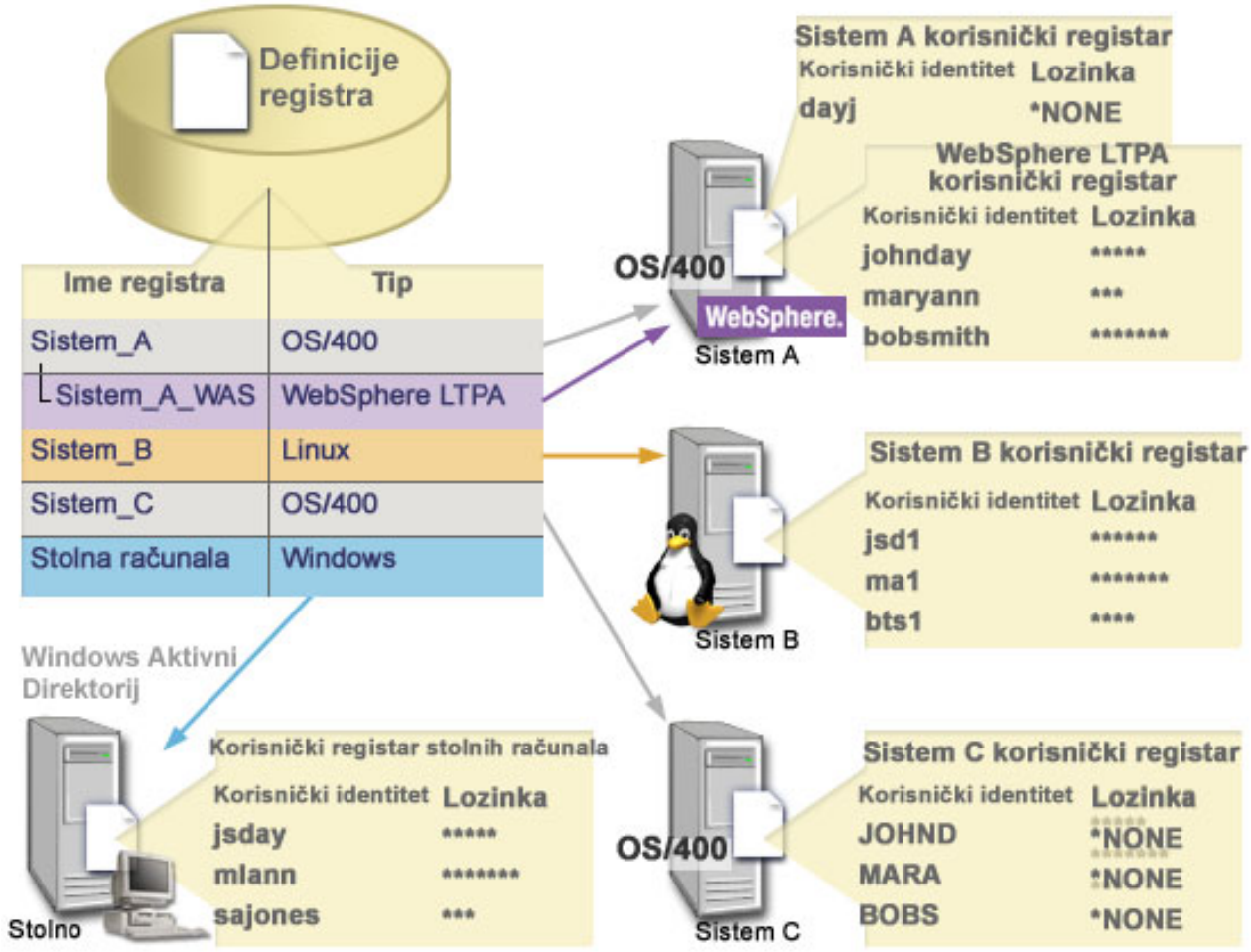
Definicije EIM registra osiguravaju informacije koje se odnose na korisničke registre u poduzeću. Administrator definira ove registre u EIM-u dobavljanjem sljedećih informacija:

- Jedinstveno, arbitrarno EIM ime registra. Svaka definicija registra predstavlja specifičnu instancu korisničkog registra. Prema tome, trebali biste izabrati ime definicije EIM registra koje vam pomaže u identificiranju pojedinačne instance korisničkog registra. Na primjer, mogli bi izabrati TCP/IP ime hosta za sistemski korisnički registar ili ime hosta kombinirano s imenom aplikacije za aplikacijski korisnički registar. Možete koristiti bilo koju kombinaciju alfanumeričkih znakova, naizmjenično koristiti velika i mala slova i prazna mjesta za kreiranje jedinstvenog imena EIM definicije registra.
- Tip korisničkog registra. Postoji broj unaprijed definiranih tipova korisničkih registara koje EIM omogućuje za pokrivanje većine operativnih korisničkih registara sistema. To uključuje:
  - AIX
  - Domino - dugo ime
  - Domino - kratko ime
  - Kerberos
  - Kerberos - osjetljiv na velika i mala slova
  - LDAP
  - - LDAP - kratko ime
  - Linux
  - Novell Directory Server
  - - Drugo
  - - Drugo - osjetljivo na velika i mala slova
  - i5/OS (ili OS/400)
  - Tivoli Upravitelj Pristupa
  - RACF
  - Windows - lokalni
  - Windows domena (Kerberos) (Ovaj tip je osjetljiv na velika i mala slova).
  - X.509

  Iako unaprijed definirani tipovi definicije registra pokrivaju većinu operativnih korisničkih registara, možda ćete trebati kreirati definiciju registra za koju EIM ne uključuje unaprijed definirane tipove registra. U ovoj situaciji imate dvije mogućnosti. Možete ili koristiti postojeću definiciju registra koja se podudara s karakteristikama vašeg korisničkog registra ili možete definirati privatni tip korisničkog 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 sadrži 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 pomaže pri identificiranju specifičnog pojavljivanja tipa korisničkog registra. Na primjer, IP adresa ili ime hosta često je dovoljno za mnoge tipove korisničkih registara. U ovom primjeru, administrator koristi System_A_WAS kao ime definicije registra aplikacije za identificiranje ove specifične instance WebSphere LTPA aplikacije. On također navodi da je registar sistema nadređen definiciji registra aplikacije System_A registar.

Slika 6: EIM definicije registra za pet korisničkih registara u poduzeću



Bilješka: Za daljnje smanjivanje potrebe za upravljanjem lozinkama korisnika, administrator na Slici 6 postavlja lozinke profila korisnika i5/OS-a na Sistemu A i Sistemu C na *NONE. Administrator u ovom slučaju konfigurira okolinu jednostruke prijave i jedine aplikacije s kojima radi njegov korisnik su EIM-omogućene aplikacije kao što je System i Navigator. Stoga, administrator želi ukloniti lozinke iz njihovih profila korisnika i5/OS-a tako da i korisnici i on imaju manje lozinki za upravljati.

Srodni koncepti

"EIM domena" na stranici 6
Domena Mapiranja identiteta u poduzeću (EIM) je direktorij u sklopu Lightweight Directory Access Protocol (LDAP) poslužitelja koji sadrži EIM podatke za poduzeće.

"Definiranje privatnog tipa korisničkog registra u EIM-u" na stranici 91
Kada kreirate definiciju registra Mapiranja identiteta u poduzeću (EIM), možete specificirati jedan od niza preddefiniranih tipova registara korisnika radi prikaza stvarnog registra korisnika koji postoji na sistemu unutar poduzeća.

Definicije registra sistema

Definicija registra sistema je unos koji kreirate u Mapiranju identiteta u poduzeću (EIM) da predstavlja i opisuje zasebni registar korisnika unutar radne stanice ili poslužitelja.

Možete kreirati definiciju EIM registra sistema za korisnički registar kada registar u poduzeću ima jedno od sljedećih obilježja:

- Registar je pružen od strane operacijskog sistema, poput AIX-a, i5/OS-a, ili proizvoda za upravljanje sigurnošću Resource Access Control Facility z/OS Poslužitelja sigurnosti (RACF).

- Registar sadrži korisničke identitete koji su jedinstveni specifičnim aplikacijama poput Lotus Notes.
- Registar sadrži distribuirane korisničke identitete kao što 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. Međutim, odvojene definicije registra dozvoljavaju da mapiranje podataka bude upravljano na aplikacijskoj osnovi. Odgovornost upravljanja aplikacijski specifičnih mapiranja može biti dodijeljeno administratoru za specifični registar.

Srodni zadaci

"Dodavanje definicije registra aplikacija" na stranici 89
Za kreiranje definicije registra aplikacije, morate biti povezani na domenu Mapiranja identiteta u poduzeću (EIM) na kojoj želite raditi i morate imati kontrolu pristupa EIM administratora.

Definicije registra aplikacije

Definicija registra aplikacije je unos u Mapiranju identiteta u poduzeću (EIM) koju kreirate da opisuje i predstavlja podskup identiteta korisnika koji su definirani u registru sistema. Ovi korisnički identiteti dijele zajednički skup atributa ili karakteristika koje im dozvoljavaju korištenje pojedinačne aplikacije ili skupa aplikacija.

Definicije registra aplikacije predstavljaju korisničke registre koji postoje unutar drugih korisničkih registara. Na primjer, registar z/OS Poslužitelja Sigurnosti (RACF) može sadržavati specifične korisničke registre koji su podskup korisnika unutar svih RACF korisničkih registara. Zbog ovog odnosa, morate navesti ime nadređenog registra sistema za bilo koju definiciju registra aplikacije koju ste kreirali.

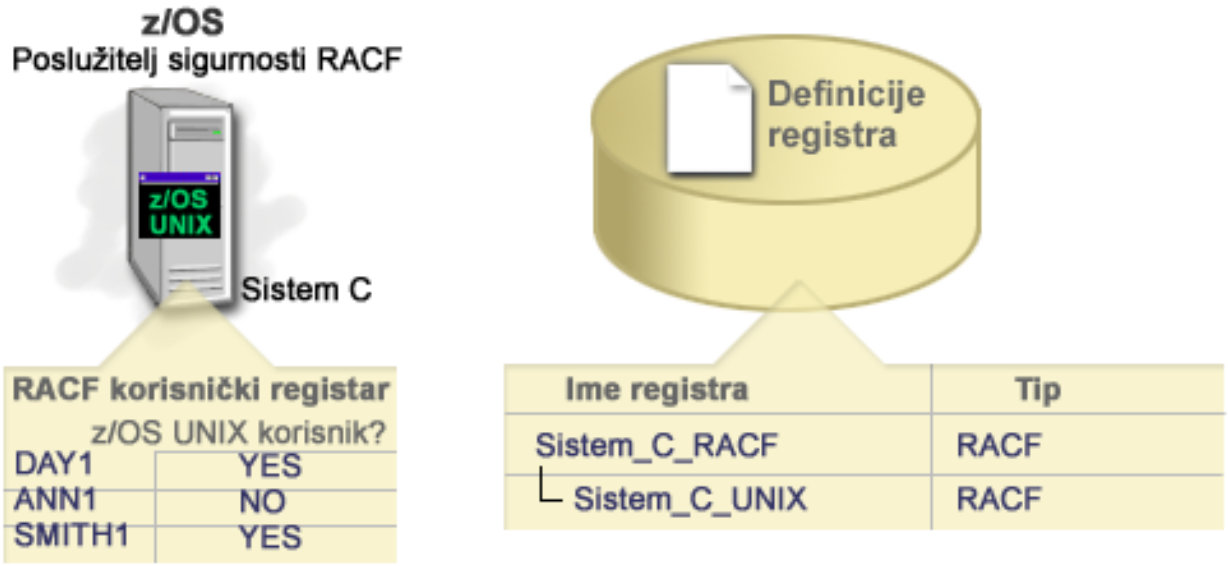
Možete kreirati EIM definiciju registra aplikacije za korisnički registar kada korisnički identiteti u registru imaju sljedeća obilježja:

- Korisnički identiteti za aplikaciju nisu spremljeni u korisničkom registru specifičnom za aplikaciju.
- Korisnički identiteti za aplikaciju pohranjeni su u registru sistema koji sadrži korisničke identitete za ostale aplikacije.

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

Na primjer, Slika 7 pokazuje kako je EIM administrator kreirao definiciju registra sistema za predstavljanje registra z/OS Poslužitelja Sigurnosti RACF. Administrator je također kreirao definiciju registra aplikacije da predstavlja identitete korisnika unutar RACF registra koji koriste z/OS(TM) UNIX sistemske usluge (z/OS UNIX). Sistem C sadrži RACF korisnički registar koji sadrži informacije za tri korisnička identiteta, DAY1, ANN1 i SMITH1. Dva od ovih identiteta korisnika (DAY1 i SMITH1) pristupaju z/OS UNIX na Sistemu C. Ti identiteti korisnika su ustvari 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 korisničkog registra. Administrator je također definirao System_C_UNIX za predstavljanje korisničkih identiteta koji imaju z/OS UNIX atribute.

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



Definicije registra grupe

Logičko grupiranje definicija registra vam dozvoljava da smanjite količinu posla koji morate obaviti za konfiguraciju EIM mapiranja. Možete upravljati definicijom registra grupe slično kao što upravljate pojedinačnom definicijom registra.

Svi članovi definicije registra grupe tipično sadrže najmanje jedan zajednički identitet korisnika na koji želite kreirati ciljnu ili izvorišnu asocijaciju. Grupiranjem članova možete kreirati samo jednu asocijaciju, umjesto višestrukih asocijacija, na definiciju registra grupe i identitet korisnika.

Na primjer, John Day se prijavi na svoj primarni sistem s korisničkim identitetom jday i koristi isti korisnički identitet, JOHND, na višestrukim sistemima. Prema tome, registar korisnika za svaki sistem sadrži korisnički identitet JOHND. Tipično, John Day kreira odijeljenu ciljnu asocijaciju od EIM identifikatora John Day na svaki od pojedinačnih registara korisnika koji sadrže korisnički identitet JOHND. Za smanjivanje količine posla kojeg mora obaviti za konfiguraciju EIM mapiranja, može kreirati jednu definiciju registra grupe sa svim registrima korisnika koji drže identitet korisnika JOHND kao članove grupe. On tada može kreirati jednostruku ciljnu asocijaciju iz EIM identifikatora John Day na definiciju registra grupe umjesto višestrukih ciljnih asocijacija od EIM identifikatora John Day na svaku od pojedinačnih definicija registra. Ova jednostruka ciljna asocijacija na definiciju registra grupe dozvoljava da se korisnički identitet John Daya jday mapira na korisnički identitet JOHND

Pročitajte sljedeće informacije o definicijama registra grupe:

- Svi članovi (pojedinačne definicije registra) definicije registra grupe moraju imati istu osjetljivost na velika i mala slova.
- Svi članovi (pojedinačne definicije registra) definicije registra grupe moraju biti definirani u EIM domeni prije nego ih možete dodati definiciji registra grupe.
- Definicija registra može biti član više od jedne grupe, ali bi trebali izbjegavati specificiranje pojedinačnog korisničkog registra kao člana više definicija registra grupe jer se može dogoditi da operacija pregledavanja vraća dvosmislene rezultate. Definicija registra grupe ne može biti član druge definicije registra grupe.

Srodni koncepti

“Primjeri operacije pregledavanja: Primjer 5” na stranici 35
Koristite ovaj primjer da saznate o operacijama pregledavanja koje vraćaju dvosmislene rezultate koji uključuju definicije registra grupe.

EIM asocijacije

Asocijacija Mapiranje identiteta u poduzeću (EIM) je unos koji možete kreirati u EIM domeni da definirate odnos između korisničkih identiteta u različitim korisničkim registrima. Tip asocijacije koju kreirate određuje je li definirani odnos direktan ili indirektan.

U EIM-u možete kreirati jedan od dva tipa asocijacija: asocijacije identifikatora i asocijacije politika. Asocijacije politika možete koristiti umjesto ili u kombinaciji s asocijacijama identifikatora. Način na koji koristite asocijacije ovisi o sveukupnom planu EIM implementacije.

Da biste naučili raditi s asocijacijama, pogledajte sljedeće informacije:

Informacije pregledavanja

Pomoću Mapiranja identiteta u poduzeću (EIM) možete osigurati opcijske podatke (nazivaju se informacije pregledavanja) za dalju identifikaciju ciljnog korisničkog identiteta. Taj ciljni korisnički identitet može biti specifičan 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 poboljšavanje traženja ciljnog korisničkog identiteta koji je objekt operacije. Podaci koje navedete za informacije pregledavanja odgovaraju dodatnim informacijskim parametrima korisničkog registra za te EIM API-je.

Informacija pregledavanja je potrebna samo kada operacija pregledavanja mapiranja može vratiti više od jedan ciljni korisnički identitet. Operacija pregledavanja mapiranja može vratiti višestruke korisničke registre kada postoji jedna ili više od sljedećih situacija:

- EIM identifikator ima višestruke individualne ciljne asocijacije na istom ciljnom registru.
- Više od jednog EIM identifikatora ima isti korisnički identitet naveden u izvornoj asocijaciji i svaki od tih EIM identifikatora ima ciljnu asocijaciju na istom ciljnom registru, iako korisnički identitet naveden za svaku ciljnu asocijaciju može biti različit.
- Više od jedne asocijacije politike default domene specificiraju isti ciljni registar.
- Više od jedne default asocijacije politike registra specificiraju isti izvorni registar i isti ciljni registar.
- Više od jedne asocijacije politike filtera certifikata specificiraju isti izvorni X.509 registar, filter certifikata i ciljni registar.

Bilješka: Operacija pregledavanja mapiranja koja vraća više od jednog identiteta ciljnog korisnika može stvoriti probleme EIM-omogućenim aplikacijama, uključujući i5/OS aplikacije i proizvode, koji nisu oblikovani za rukovanje ovim dvosmislenim rezultatima. Ipak, osnovne i5/OS aplikacije kao na primjer System i Access za Windows ne mogu koristiti informacije pregledavanja za razlikovanje između više ciljnih korisničkih identiteta vraćenih od strane operacije pregledavanja. Prema tome, možete razmotriti redefiniciju asocijacija za domenu da osigurate da operacija pregledavanja mapiranja može vratiti jednostruki ciljni identitet korisnika, da osigurate da osnovne i5/OS aplikacije mogu uspješno izvoditi operacije pregledavanja i mapirati identitete.

Informacije pregledavanja možete koristiti za izbjegavanje situacija u kojima je moguće da operacije pregledavanja mapiranja vrate više od jednog ciljnog korisničkog identiteta. Za sprečavanje da operacije pregledavanja mapiranja vraćaju višestruke korisničke ciljne identitete morate definirati jedinstvene informacije pregledavanja za svaki ciljni korisnički identitet u svakoj situaciji. Te se informacije pregledavanja moraju dati operaciji pregledavanja mapiranja da bi se osiguralo da operacija može vratiti jedinstveni ciljni korisnički identitet. U suprotnom, aplikacije koje ovise o EIM-u možda neće moći odrediti koji točno ciljni identitet upotrijebiti.

Na primjer, imate EIM identifikator imena John Day koji za Sistem A ima dva korisnička profila. Jedan od tih korisničkih profila je JDUSER za Sistem A, a drugi je JDSECADM koji ima posebna ovlaštenja administratora sigurnosti. Postoje dvije ciljne asocijacije za identifikator Johna Daya. Jedna od tih ciljnih asocijacije je za JDUSER korisnički identitet u ciljnom registru System_A i ima informacije pregledavanja od korisničkog ovlaštenja

navedenog za JDUSER. Druga je asocijacija za korisnički identitet JDSECADM u ciljnom registru System_A i ima informacije pregledavanja od službenika sigurnosti navedenog za JDSECADM.

Ako operacija pregledavanja mapiranja ne specificira nikakve informacije pregledavanja, operacija pregledavanja vraća korisničke identitete JDUSER i JDSECADM. Ako operacija pregledavanja mapiranja specificira informacije pregledavanja korisničkog ovlaštenja, operacija pregledavanja vraća samo korisnički identitet JDUSER. Ako operacija pregledavanja mapiranja specificira informacije službenika sigurnosti, operacija pregledavanja vraća samo korisnički identitet JDSECADM.

Bilješka: Ako obrišete zadnju ciljnu asocijaciju za korisnički identitet (bilo asocijaciju identifikatora ili asocijaciju politike), ciljni korisnički identitet i informacije pregledavanja također se brišu iz domene.

S obzirom da asocijacije politika certifikata i ostale asocijacije možete koristiti na mnoštvo preklapajućih načina, morate dobro razumjeti EIM podršku politike mapiranja i način rada operacija pregledavanja prije nego kreirate i koristite asocijacije politika certifikata.

Srodni koncepti

"Podrška politici mapiranja EIM i omogućivanje" na stranici 37
Podrška politike Mapiranja identiteta u poduzeću (EIM) dozvoljava vam korištenje asocijacija politike kao i određenih asocijacija identifikatora u nekoj EIM domeni. Asocijacije politika možete koristiti umjesto ili u kombinaciji s asocijacijama identifikatora.

"EIM operacije pregledavanja" na stranici 26
Aplikacija ili operativni sistem koristi EIM API za izvođenje operacije pregledavanja tako da aplikacija ili operativni sistem mogu izvesti mapiranje s jednog identiteta korisnika u jednom registru na drugi identitet korisnika u drugom registru. EIM operacija pregledavanja je proces preko koje aplikacija ili operativni sistem pronalazi nepoznate pridružene korisničke identitete u određenom ciljnom registru tako da osigurava poznate i pouzdane informacije.

"Asocijacije politika default domene" na stranici 21
Asocijacija politike default domene je jedan tip asocijacije politike koji možete koristiti za kreiranje mapiranja više-prema-jedan između identiteta korisnika.

"Asocijacije politika default registra" na stranici 23
Asocijacija politike default registra je jedan tip asocijacije politike koji možete koristiti za kreiranje mapiranja više-prema-jedan između identiteta korisnika.

Asocijacije identifikatora

EIM identifikator predstavlja određenu osobu ili cjelinu u poduzeću. EIM asocijacija identifikatora opisuje odnos između nekog EIM identifikatora i pojedinačnog jednostrukog korisničkog identiteta u korisničkom registru koji također predstavlja tu osobu. Kada kreirate asocijacije između EIM identifikatora i svih korisničkih identiteta osobe ili cjeline, tada osiguravate jedno, potpuno razumijevanje o tome kako ta osoba ili cjelina koristi resurse u poduzeću.

Korisnički identiteti mogu se koristiti za provjeru autentičnosti, autorizaciju ili oboje. *Provjera autentičnosti* je obrada provjeravanja da cjelina ili osoba koja dobavlja korisnički identitet ima pravo na pretpostavku tog identiteta. Provjera se često postiže prisiljavanjem osobe koja šalje korisnički identitet za dobavljanje tajnih ili privatnih informacija udruženih s korisničkim identitetom, kao što je lozinka. *Autorizacija* je obrada osiguravanja da ispravno ovlašteni korisnički identitet može izvoditi samo funkcije ili pristupati resursima za koje su identitetu dane povlastice. U prošlosti, gotovo sve aplikacije su bile prisiljene koristiti identitete u jednostrukom korisničkom registru i za provjeru autentičnosti i za ovlaštenje. Korištenjem operacija EIM pregledavanja, aplikacije sada mogu koristiti identitete u jednom korisničkom registru za provjeru autentičnosti dok koriste pridružene korisničke identitete u različitom korisničkom registru za ovlaštenje.

EIM identifikator osigurava neizravnu asocijaciju između onih korisničkih identiteta koji dozvoljavaju aplikacijama da nađu drugi korisnički identitet za neki EIM identifikator baziran na poznatom korisničkom identitetu. EIM osigurava API-je koji dozvoljavaju aplikacijama da pronađu nepoznati korisnički identitet u specifičnom (ciljnom) korisničkom registru dobavljanjem poznatog korisničkog identiteta u nekom drugom (izvornom) korisničkom registru. Taj se proces zove mapiranje identiteta.

U EIM-u administrator može definirati tri različita tipa asocijacija za opis odnosa između EIM identifikatora i korisničkog identiteta. Asocijacije identiteta mogu biti sljedećeg tipa: izvorne, ciljne ili administrativne. Tip asocijacije koji kreirate je baziran na načinu korištenja korisničkog identiteta. Na primjer, kreirate izvorne i ciljne asocijacije za one korisničke identitete za koje želite da sudjeluju u operacijama pregledavanja mapiranja. Tipično, ako se korisnički identitet koristi za provjeru autentičnosti, trebate kreirati za njega izvornu asocijaciju. Nakon toga kreirate ciljne asocijacije za one korisničke identitete koji se koriste za ovlaštenje.

Prije no što možete kreirati asocijaciju identifikatora, prvo morate kreirati odgovarajući EIM identifikator i odgovarajuću EIM definiciju registra za korisnički registar koji sadrži pridruženi korisnički identitet. Asocijacija definira vezu između EIM identifikatora i korisničkog identiteta korištenjem sljedećih informacija:

- Ime EIM identifikatora
- Ime korisničkog identiteta
- Ime definicije EIM registra
- Tip asocijacije
- Opcijski: informacije pregledavanja prema daljem identitetu ciljnog korisničkog identiteta u ciljnoj asocijaciji.

Izvorna asocijacija

Izvorna asocijacija dozvoljava korištenje korisničkog identiteta kao izvora u operaciji EIM pregledavanja za pronalaženje korisničkog identiteta koji je udružen s istim EIM identifikatorom.

Kada se koristi korisnički identitet za *provjeru autentičnosti*, taj korisnički identitet bi trebao imati izvornu asocijaciju s EIM identifikatorom. Na primjer, mogli ste kreirati izvornu asocijaciju za Kerberos principala zato, jer se taj oblik korisničkog identiteta koristi za provjeru autentičnosti. 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 vraćanje korisničkog identiteta kao rezultata operacije EIM pregledavanja. Korisnički identiteti koji predstavljaju krajnje korisnike normalno trebaju samo ciljnu asocijaciju.

Kada se korisnički identitet koristi za *autorizaciju*, a ne za provjeru autentičnosti, tada bi taj korisnički identitet trebao imati ciljnu asocijaciju s EIM identifikatorom. Na primjer, možda ste kreirali ciljnu asocijaciju za i5/OS korisnički profil jer ovaj oblik korisničkog identiteta određuje koje resurse i povlastice korisnik ima na specifičnoj System i platformi. 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 više ciljnih asocijacija za jednostruki EIM identifikator. Obično kreirate ciljnu asocijaciju za svaki korisnički identitet u korisničkom registru koju osoba može koristiti za ovlaštenje nad sistemom ili aplikacijom s kojom se podudara korisnički registar.

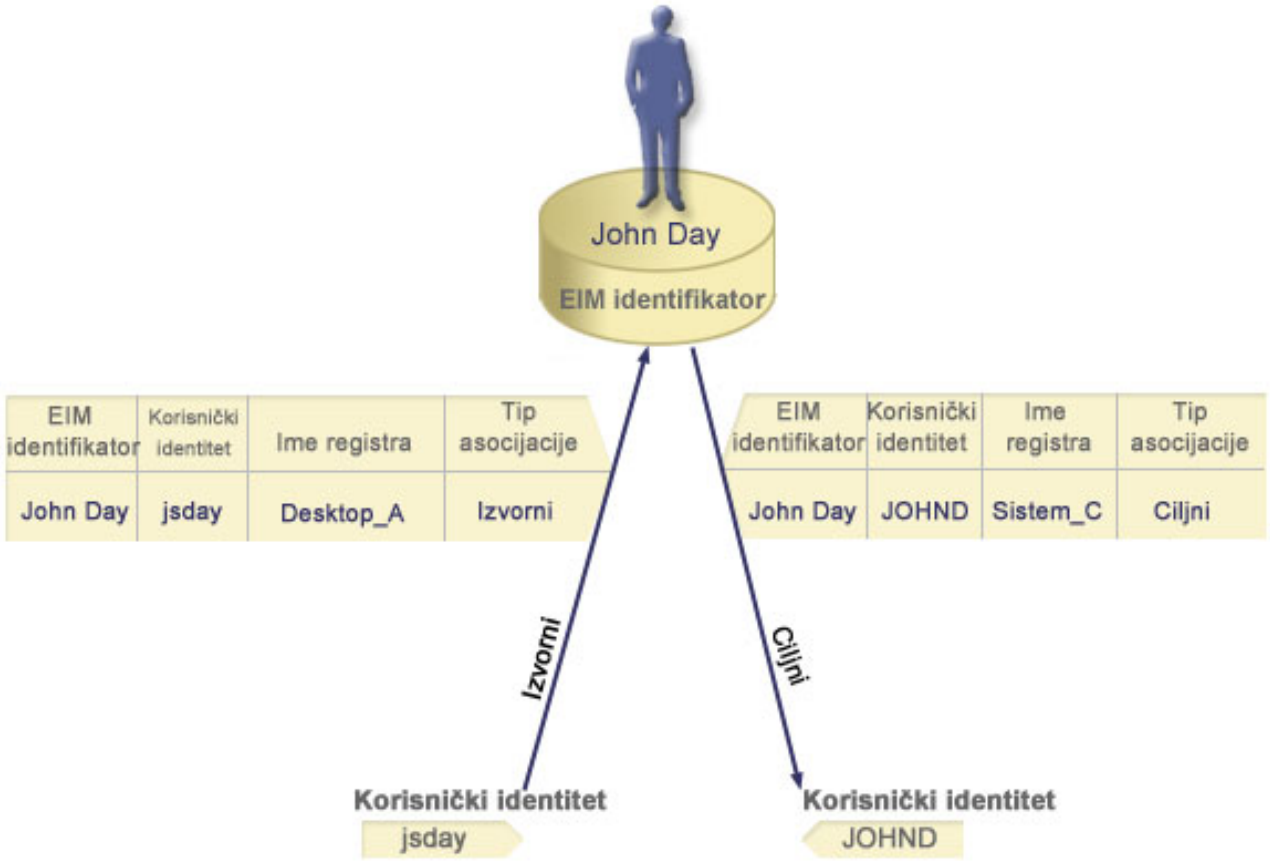
Na primjer, korisnici u vašem poduzeću obično se prijavljuju i provjeravaju autentičnost na Windows desktop računalima i pristupaju System i platformi radi izvođenja brojnih zadataka. Korisnici se na svoja desktop računala prijavljuju koristeći Kerberos principal, a na System i platformu se prijavljuju koristeći i5/OS korisnički profil. Vi želite kreirati okolinu jednostruke prijave kod koje se provjera autentičnosti korisnika na njihovim desktop računalima izvodi upotrebom Kerberos principala i više nije potrebna ručna provjera autentičnosti System i platforme.

Kako bi se taj cilj postigao, trebate kreirati izvornu asocijaciju za Kerberos principal za svakog korisnika i taj korisnikov EIM identifikator. Vi tada kreirate ciljnu asocijaciju za profil korisnika i5/OS-a za svakog korisnika i njegov EIM identifikator. Ovakva konfiguracija osigurava da i5/OS može izvesti operaciju pregledavanja mapiranja radi određivanja ispravnog korisničkog profila potrebnog korisniku koji pristupa System i platformi nakon njegove provjere

autentičnosti na njegovom računalu. i5/OS tada dozvoljava korisnički pristup resursima na poslužitelju osnovan na odgovarajućem profilu korisnika bez traženja da korisnik ručno potvrdi svoju autentičnost na poslužitelj.

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 između tog identifikatora i dva pridružena korisnička identiteta. Administrator kreira izvornu asocijaciju za jsday, Kerberos principal u Stolna računala korisničkom registru. Administrator također kreira ciljnu asocijaciju za JOHND, profil korisnika i5/OS-a u registru korisnika Sistem_C. Ove asocijacije dobavljaju značenja aplikacijama kako bi se dobio nepoznat korisnički identitet (ciljni, JOHND) baziran na poznatom korisničkom identitetu (izvorni, jsday) kao dio operacije EIM pregledavanja.

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



Za proširenje primjera, pretpostavite da EIM administrator shvati da John Day koristi isti profil korisnika i5/OS-a, jsd1, na pet različitih sistema. U toj situaciji, administrator mora kreirati šest asocijacija za EIM identifikator John Day da definira odnos između ovog identifikatora i pridruženog identiteta korisnika u pet registara korisnika: izvorišnu asocijaciju za johnday, Kerberos principal u registru korisnika Desktop_A i pet ciljnih asocijacija za jsd1, profil korisnika i5/OS-a u pet registara korisnika: Sistem_B, Sistem_C, Sistem_D, Sistem_E i Sistem_F. Za smanjivanje količine posla koji mora obaviti za konfiguriranje EIM mapiranja, EIM administrator kreira definiciju registra grupe. Članovi definicije registra grupe uključuju imena definicija registra Sistem_B, Sistem_C, Sistem_D, Sistem_E i Sistem_F. Grupiranje članova omogućuje administratoru da kreira jednu ciljnu asocijaciju na definiciju registra grupe i identitet korisnika, umjesto višestrukih asocijacija na pojedinačna imena definicije registra. Izvorišne i ciljne asocijacije pružaju načine za aplikacije da dobiju nepoznati identitet korisnika (ciljni, jsd1) u pet registara korisnika predstavljenih kao članova definicije registra grupe bazirane na poznatom identitetu korisnika (izvorišni, johnday), kao dio operacije pregledavanja EIM-a.

Za neke bi korisnike moglo biti potrebno kreirati i ciljnu i izvornu asocijaciju za isti korisnički identitet. Ovo je potrebno kada pojedinac koristi jedan sistem kao klijent i kao poslužitelj ili za pojedince koji se ponašaju kao administratori.

Bilješka: Korisnički identiteti koji predstavljaju tipične korisnike normalno trebaju samo ciljnu asocijaciju.

Za neke bi korisnike moglo biti potrebno kreirati i ciljnu i izvornu asocijaciju za isti korisnički identitet. Ovo je potrebno kada pojedinac koristi jedan sistem kao klijent i kao poslužitelj ili za pojedince koji se ponašaju kao administratori.

Na primjer, administrator koristi funkciju Središnje upravljanje u System i Navigator za upravljanje središnjim sistemom na nekoliko krajnjih sistema. Administrator izvodi raznolike funkcije i te funkcije mogu biti na središnjem sistemu ili na krajnjem sistemu. U toj bi situaciji kreirali i izvornu asocijaciju i ciljnu asocijaciju za sve administratorske korisničke identitete na svim sistemima. To osigurava da, kojigod sistem administrator koristi za izvorni pristup na jedno od ostalih sistema, korišteni se korisnički identitet za izvorni pristup na drugi sistem može mapirati u prikladan korisnički identitet za sljedeći sistem kojemu administrator pristupa.

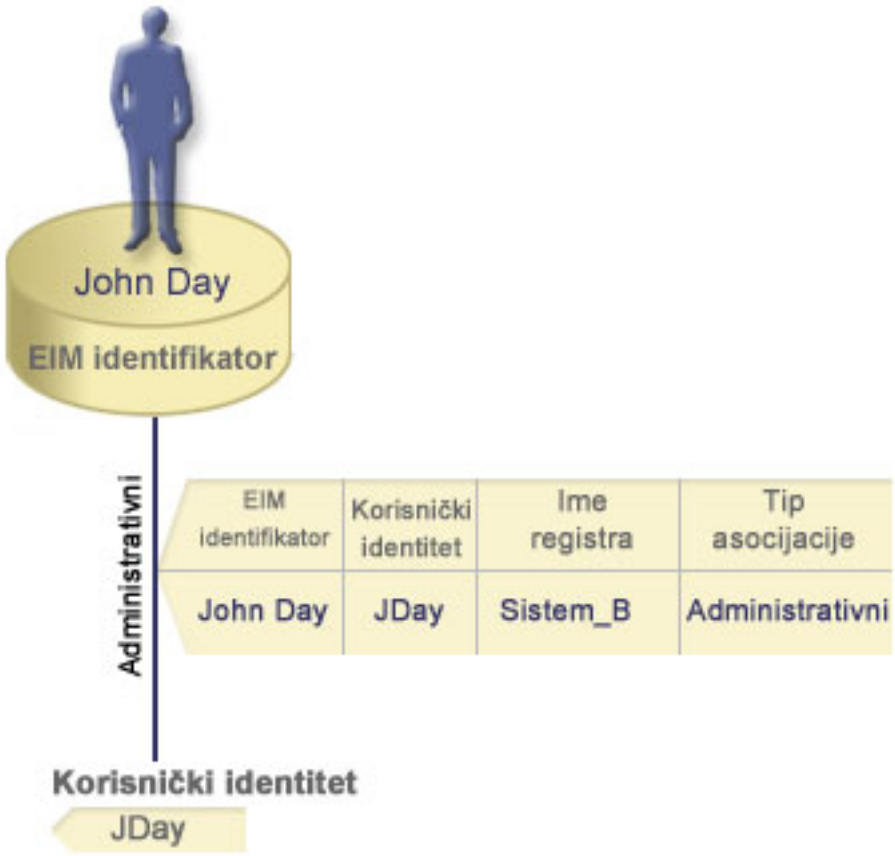
Administrativna asocijacija

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

U skladu s posebnom prirodom administracijskih asocijacija, ovaj tip asocijacija ne može sudjelovati u operacijama EIM pregledavanja mapiranja. Kao posljedica, operacija EIM pregledavanja koja dobavlja izvorni korisnički identitet s administracijskom asocijacijom ne vraća rezultate. Slično, korisnički identitet s administrativnom asocijacijom nikad se ne vraća kao rezultat operacije EIM pregledavanja.

Slika 7 prikazuje primjer administrativne asocijacije. U ovom primjeru, zaposlenik pod imenom John Day ima korisnički identitet John_Day na Sistemu A i korisnički identitet JDay na Sistemu B koji je sistem s visokom sigurnošću. Sistemski administrator želi osigurati provjeru autentičnosti korisnika na Sistemu B korištenjem samo lokalnog korisničkog registra ovog sistema. Administrator ne želi dozvoliti aplikaciji da ovlasti John Day na sistemu upotrebom nekog drugog mehanizma provjere autentičnosti. Korištenjem administrativne asocijacije za JDay korisnički identitet na Sistemu B, EIM administrator može vidjeti da John Day posjeduje račun na Sistemu B, ali EIM ne vraća informacije o JDay identitetu kod operacije EIM pregledavanja. Čak i ako aplikacije postoje na ovom sistemu koji koristi operacije EIM pregledavanja, one ne mogu pronaći korisničke identitete koji imaju administrativne asocijacije.

Slika 7: EIM administracijska asocijacija za EIM identifikator John Day



Asocijacije politike

Politika Mapiranja identiteta u poduzeću (EIM) dozvoljava EIM administratoru da kreira i koristi asocijacije politike za definiranje odnosa između višestrukih identiteta korisnika u jednom ili više registara korisnika i identiteta jednog korisnika u drugom registru korisnika.

Asocijacije politike koriste podršku politike EIM mapiranja za kreiranje više-prema-jedan mapiranja između korisničkih identiteta bez uključivanja EIM identifikatora. Asocijacije politike možete koristiti umjesto ili u kombinaciji s asocijacijama identifikatora koje osiguravaju jedan-prema-jedan mapiranje između EIM identifikatora i jednostrukog korisničkog identiteta.

Asocijacija politike utječe samo na one korisničke identitete za koje određene pojedinačne EIM asocijacije ne postoje. Kada određene asocijacije identifikatora postoje između EIM identifikatora i korisničkih identiteta, tada se ciljni korisnički identitet iz asocijacije identifikatora vraća aplikaciji s izvođenjem operacije pregledavanja, čak ako asocijacija politike postoji i ako je korištenje asocijacije politike omogućeno.

Možete kreirati tri različita tipa asocijacije politike:

Srodni koncepti

“EIM operacije pregledavanja” na stranici 26
Aplikacija ili operativni sistem koristi EIM API za izvođenje operacije pregledavanja tako da aplikacija ili operativni sistem mogu izvesti mapiranje s jednog identiteta korisnika u jednom registru na drugi identitet korisnika u drugom registru. EIM operacija pregledavanja je proces preko koje aplikacija ili operativni sistem pronalazi nepoznate pridružene korisničke identitete u određenom ciljnom registru tako da osigurava poznate i pouzdane informacije.

Asocijacije politika default domene:

Asocijacija politike default domene je jedan tip asocijacije politike koji možete koristiti za kreiranje mapiranja više-prema-jedan između identiteta korisnika.

Možete koristiti asocijaciju politike default domene za mapiranje izvornog skupa višestrukih korisničkih identiteta (u ovom slučaju, svi korisnici u domeni) u jednostruki ciljni korisnički identitet u određenom ciljnom korisničkom registru. U asocijaciji politike default domene, svi su korisnici u domeni izvor asocijacije politike i mapiraju se u jednostruki ciljni registar i ciljni korisnički identitet.

Da biste koristili asocijacije politike default domene, morate omogućiti pregledavanje mapiranja upotrebom asocijacija politike za domenu. Morate također omogućiti pregledavanje mapiranja za ciljni korisnički registar asocijacije politike. Kada konfigurirate ovu mogućnost, registri korisnika u asocijaciji politike mogu sudjelovati u operacijama pregledavanja mapiranja.

Asocijacija politike default domene ima učinak 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 korisnički identiteti u domeni mapirani u pojedinačni identitet ciljnog korisnika kako je specificirano asocijacijom politike default domene.

Na primjer, možete kreirati asocijaciju politike default domene s ciljnim korisničkim identitetom John_Day u ciljnom registru Registry_xyz, a da niste kreirali nikakve asocijacije identifikatora ili druge asocijacije politike koje se mapiraju u ovaj korisnički 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 korisničke identitete u domeni koji nemaju za njih definirane druge asocijacije.

Možete definirati ove dvije stvari za asocijaciju politike default domene:

- **Ciljni registar**. Specificirani ciljni registar je ime definicije registra Mapiranja identiteta u poduzeću (EIM) koji sadrži korisnički identitet u koji se trebaju mapirati svi korisnički identiteti u domeni.
- **Ciljni korisnik**. Ciljni korisnik je ime korisničkog identiteta koje se vraća kao cilj operacije EIM pregledavanja mapiranja bazirane na ovoj asocijaciji politike.

Možete definirati default asocijaciju politike domene za svaki registar u domeni. Ako se dvije ili više asocijacija politike domene odnose na isti ciljni registar, morate definirati jedinstvene informacije pregledavanja za svaku od tih asocijacija politike da osigurate da ih operacije pregledavanja mapiranja mogu razlikovati. Inače, operacije pregledavanja mapiranja mogu vratiti višestruke ciljne korisničke identitete. Rezultat ovih dvosmislenih rezultata je da aplikacija koja ovisi o EIM-u neće moći odrediti koji točno ciljni identitet treba koristiti.

S obzirom da asocijacije politika možete koristiti na mnoštvo preklapajućih načina, morate dobro razumjeti EIM podršku politike mapiranja i način rada operacija pregledavanja prije nego kreirate i koristite asocijacije politika.

Bilješka: Možda ćete htjeti kreirati defaultnu asocijaciju politike domene s ciljnim identitetom korisnika koji postoji unutar definicije registra grupe. Svi korisnici u domeni su izvor asocijacije politike i mapirani su u ciljni identitet korisnika u ciljnoj definiciji registra grupe. Identitet korisnika koji definirate u defaultnoj asocijaciji politike domene postoji unutar članova definicije registra grupe.

Na primjer, John Day koristi isti profil i5/OS korisnika, John_Day, na pet različitih sistema: Sistemu B, Sistemu C, Sistemu D, Sistemu E i Sistemu F. Za smanjivanje količine posla koji mora obaviti za konfiguraciju EIM mapiranja, EIM administrator kreira definiciju registra grupe nazvanu Grupa_1. Članovi definicije registra grupe uključuju imena definicija registra grupe Sistem_B, Sistem_C, Sistem_D, Sistem_E i Sistem_F. Grupiranje članova omogućuje administratoru da kreira jednostruku ciljnu asocijaciju na definiciju registra grupe i identitet korisnika, umjesto višestrukih asocijacija na pojedinačne definicije registra.

EIM administrator kreira defaultnu asocijaciju politike domene s ciljnim identitetom korisnika John_Day u ciljnom registru Grupa_1. U ovom slučaju, ne vrijede druge specifične asocijacije identifikatora ili asocijacije politike. Prema tome, kada je navedena Grupa_1 kao ciljni registar u operacijama pregledavanja,

politika defaultne domene osigurava da se ciljni identitet korisnika John_Day vrati za sve identitete korisnika u domeni koji nemaju definirane asocijacije specifičnih identifikatora.

Srodni koncepti

"Informacije pregledavanja" na stranici 16
Pomoću Mapiranja identiteta u poduzeću (EIM) možete osigurati opcijske podatke (nazivaju se informacije pregledavanja) za dalju identifikaciju ciljnog korisničkog identiteta. Taj ciljni korisnički identitet može biti specifičan u asocijaciji identifikatora ili u asocijaciji politike.

"Podrška politici mapiranja EIM i omogućivanje" na stranici 37
Podrška politike Mapiranja identiteta u poduzeću (EIM) dozvoljava vam korištenje asocijacija politike kao i određenih asocijacija identifikatora u nekoj EIM domeni. Asocijacije politika možete koristiti umjesto ili u kombinaciji s asocijacijama identifikatora.

Asocijacije politika default registra:

Asocijacija politike default registra je jedan tip asocijacije politike koji možete koristiti za kreiranje mapiranja više-prema-jedan između identiteta korisnika.

Možete koristiti asocijaciju politike default registra za mapiranje izvornog skupa višestrukih korisničkih identiteta (u ovom slučaju onih u jednostrukom registru) u jednostruki ciljni korisnički identitet u određenom ciljnom korisničkom 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 omogućiti pregledavanje mapiranja upotrebom asocijacija politike za domenu. Morate također omogućiti pregledavanje mapiranja za izvorni registar i omogućiti pregledavanje mapiranja i korištenje asocijacija politike za ciljni registar korisnika asocijacije politike. Kada konfigurirate ovu mogućnost, registri korisnika u asocijaciji politike mogu sudjelovati u operacijama pregledavanja mapiranja.

Asocijacija politike default registra ima učinak 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 korisnički identiteti u izvornom registru mapirani u pojedinačni identitet ciljnog korisnika kako je specificirano asocijacijom politike default registra.

Na primjer, možete kreirati asocijaciju politike default registra koja ima izvorni registar my_realm.com, što su principali u specifičnom Kerberos području. Za ovu asocijaciju politike, također navodite ciljni identitet korisnika general_user1 u ciljnom registru i5/OS_system_reg, koji je specifični korisnički profil u i5/OS registru korisnika. U tom slučaju, niste kreirali nikakve asocijacije identifikatora ili asocijacije politike koje se primjenjuju na bilo koje identitete korisnika u izvornom registru. Prema tome, kada je navedeno i5/OS_system_reg kao ciljni registar i my_realm.com naveden kao izvorišni registar u operacijama pregledavanja, defaultna asocijacija politike registra osigurava da se ciljni identitet korisnika general_user1 vrati za sve identitete korisnika u my_realm.com koji nemaju definirane asocijacije specifičnih identifikatora ili asocijacije politike filtera certifikata.

Možete specificirati ove tri stvari za definiranje asocijacije politike default registra:

- **Izvorni registar**. Ovo je definicija registra koju želite da koristi asocijacija politike kao izvor mapiranja. Svi korisnički identiteti u izvornom korisničkom registru se trebaju mapirati u specifičnog ciljnog korisnika asocijacije politike.
- **Ciljni registar**. Specificirani ciljni registar je ime definicije registra Mapiranja identiteta u poduzeću (EIM). Ciljni registar mora sadržavati ciljni korisnički identitet u kojeg se svi korisnički identiteti u izvornom registru mapiraju.
- **Ciljni korisnik**. Ciljni korisnik je ime korisničkog identiteta koje se vraća kao cilj operacije EIM pregledavanja mapiranja bazirane na ovoj asocijaciji politike.

Možete definirati više od jedne asocijacije politike default registra. Ako se dvije ili više asocijacija politike s istim izvornim registrom odnose na isti ciljni registar, morate definirati jedinstvene informacije pregledavanja za svaku od tih asocijacija politike da osigurate da ih operacije pregledavanja mapiranja mogu razlikovati. Inače, operacije pregledavanja mapiranja mogu vratiti višestruke ciljne korisničke identitete. Rezultat ovih dvosmislenih rezultata je da aplikacija koja ovisi o EIM-u neće moći odrediti koji točno ciljni identitet treba koristiti.

S obzirom da asocijacije politika možete koristiti na mnoštvo preklapajućih načina, morate dobro razumjeti EIM podršku politike mapiranja i način rada operacija pregledavanja prije nego kreirate i koristite asocijacije politika.

Bilješka: Možda ćete htjeti kreirati defaultnu asocijaciju politike registra s ciljnim identitetom korisnika koji postoji unutar definicije registra grupe. Svi korisnici u izvorišnom registru korisnika su izvor asocijacije politike i mapirani su u ciljni identitet korisnika u ciljnoj definiciji registra grupe. Identitet korisnika koji definirate u defaultnoj asocijaciji politike registra postoji unutar članova definicije registra grupe.

Na primjer, John Day koristi isti i5/OS profil korisnika, John_Day, na pet različitih sistema: Sistem_B, Sistem_C, Sistem_D, Sistem_E i Sistem_F. Za smanjenje količine posla kojeg on mora obaviti za konfiguriranje EIM mapiranja, EIM administrator kreira definiciju registra grupe nazvanu Grupa_1. Članovi definicije registra grupe uključuju imena definicija registra Sistem_B, Sistem_C, Sistem_D, Sistem_E i Sistem_F. Grupiranje članova omogućuje administratoru da kreira jednu ciljnu asocijaciju na definiciju registra grupe i identitet korisnika, umjesto višestrukih asocijacija na pojedinačne definicije registra.

EIM administrator kreira defaultnu asocijaciju politike registra koja ima izvorišni registar my_realm.com, koji su principali u specifičnom Kerberos području. Za tu asocijaciju politike, on također navodi ciljni identitet korisnika John_Day u ciljnom registru Grupa_1. U ovom slučaju, ne primjenjuje se niti jedna druga asocijacija identifikatora ili politike. Prema tome, kada je navedena Grupa_1 kao ciljni registar i my_realm.com naveden kao izvorišni registar u operacijama pregledavanja, defaultna asocijacija politike registra osigurava da se ciljni identitet korisnika John_Day vrati za sve identitete korisnika u my_realm.com koji nemaju definirane asocijacije specifičnih identifikatora.

Srodni koncepti

“Informacije pregledavanja” na stranici 16
Pomoću Mapiranja identiteta u poduzeću (EIM) možete osigurati opcijske podatke (nazivaju se informacije pregledavanja) za dalju identifikaciju ciljnog korisničkog identiteta. Taj ciljni korisnički identitet može biti specifičan u asocijaciji identifikatora ili u asocijaciji politike.

“Podrška politici mapiranja EIM i omogućivanje” na stranici 37
Podrška politike Mapiranja identiteta u poduzeću (EIM) dozvoljava vam korištenje asocijacija politike kao i određenih asocijacija identifikatora u nekoj EIM domeni. Asocijacije politika možete koristiti umjesto ili u kombinaciji s asocijacijama identifikatora.

Asocijacije politika filtera certifikata:

Asocijacija politike filtera certifikata je jedan tip asocijacije politike koji možete koristiti za kreiranje mapiranja više-prema-jedan između identiteta korisnika. Možete koristiti asocijaciju politike filtera certifikata za mapiranje izvornog skupa certifikata u jednostruki ciljni korisnički identitet u određenom ciljnom korisničkom registru.

U asocijaciji politike filtera certifikata u jednostrukom X.509 registru kao izvor asocijacije politike određujete 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 možete u registru navesti podskup certifikata. Filter certifikata koji specificirate za asocijaciju politike određuje njegovo područje djelovanja.

Bilješka: Kreirajte i koristite default asocijaciju politike registra kada želite sve certifikate iz X.509 korisničkog registra mapirati u jednostruki ciljni korisnički identitet.

Da biste koristili asocijacije politike filtera certifikata, morate omogućiti pregledavanje mapiranja upotrebom asocijacija za domenu. Morate također omogućiti pregledavanje mapiranja za izvorni registar i omogućiti pregledavanje mapiranja i korištenje asocijacija politike za ciljni registar korisnika asocijacije politike. Kada konfigurirate ovu mogućnost, registri korisnika u asocijaciji politike mogu sudjelovati u operacijama pregledavanja mapiranja.

Kada je digitalni certifikat izvorni identitet korisnika u operaciji pregledavanja mapiranja u Mapiranju identiteta u poduzeću (EIM) (nakon što zahtijevajuća aplikacija upotrijebi eimFormatUserIdentity() EIM API za formatiranje imena identiteta korisnika), EIM najprije provjerava da li postoji asocijacija identifikatora između EIM identifikatora i navedenog identiteta korisnika. Ako ne postoji, EIM tada uspoređuje DN informacije u certifikatu s DN ili djelomičnim DN informacijama specificiranim u filteru asocijacije politike. Ako DN informacije u certifikatu zadovoljavaju kriterij u filteru, EIM vraća 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 pojedinačni identitet ciljnog korisnika kako je specificirano asocijacijom politike filtera certifikata.

Na primjer, možete kreirati asocijaciju politike filtera certifikata koja ima izvorni registar certificates.x509. Ovaj registar sadrži certifikate za sve zaposlenike poduzeća, uključujući certifikate koje upravitelji odjela upravljanja ljudskim resursima koriste za pristup određenim privatnim internim Web stranicama i ostalim resursima kojima pristupaju preko System i modela. Za ovu asocijaciju politike, također navodite ciljni identitet korisnika hr_managers u ciljnom registru system_abc koji je specifični korisnički profil u i5/OS registru korisnika. 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 slučaju, 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 specifične asocijacije identifikatora.

Trebate specificirati sljedeće informacije za definiranje asocijacije politike filtera certifikata:

- **Izvorni registar**. Definicija izvornog registra koju ste specificirali mora biti X.509 tipa korisničkog registra. Politika filtera certifikata kreira asocijaciju između identiteta korisnika u ovom X.509 korisničkom registru i pojedinačnog specifičnog ciljnog korisničkog identiteta. Asocijacija se primjenjuje samo na one korisničke identitete u registru koji zadovoljavaju kriterije filtera certifikata koji ste specificirali za ovu politiku.
- **Filter certifikata**. Filter certifikata definira skup sličnih atributa certifikata korisnika. Asocijacija politike filtera certifikata mapira sve certifikate s tako definiranim atributima u X.509 korisničkom registru u specifični ciljni korisnički identitet. Trebate specificirati filter baziran na kombinaciji Razlikovnog imena naslova (SDN) i Razlikovnog imena izdavača (IDN) koji se podudara s certifikatima koje želite koristiti kao izvor mapiranja. Filter certifikata koji ste specificirali za politiku mora već postojati u EIM domeni.
- **Ciljni registar**. Definicija ciljnog registra koju ste specificirali je korisnički registar koji sadrži korisničke identitete u koje želite mapirati certifikate koji se podudaraju s filterom certifikata.
- **Ciljni korisnik**. Ciljni korisnik je ime korisničkog identiteta koji je vraćen kao cilj iz operacije EIM pregledavanja mapiranja baziran na asocijaciji politike.

S obzirom da asocijacije politika certifikata i ostale asocijacije možete koristiti na mnoštvo preklapajućih načina, morate dobro razumjeti EIM podršku politike mapiranja i način rada operacija pregledavanja prije nego kreirate i koristite asocijacije politika certifikata.

Bilješka: Možda ćete htjeti kreirati asocijaciju politike filtera certifikata s ciljnim identitetom korisnika koji postoji unutar definicije registra grupe. Korisnici u izvorišnom registru koji udovoljavaju kriterijima navedenim filterom certifikata su izvor asocijacije politike i mapiraju se na ciljni identitet korisnika u ciljnoj definiciji registra grupe. Identitet korisnika koji definirate u asocijaciji politike filtera certifikata postoji unutar članova definicije registra grupe.

Na primjer, John Day koristi isti profil i5/OS korisnika, John_Day, na pet različitih sistema: Sistem B, Sistem C, Sistem D, Sistem E i Sistem F. Da smanji količinu posla koju mora obaviti da konfigurira EIM mapiranje, EIM administrator kreira definiciju registra grupe. Članovi definicije registra grupe uključuju imena definicija registra grupe Sistem_B, Sistem_C, Sistem_D, Sistem_E i Sistem_F. Grupiranje članova omogućuje administratoru da kreira jednostruku ciljnu asocijaciju na definiciju registra grupe i identitet korisnika, umjesto višestrukih asocijacija na pojedinačne definicije registra.

EIM administrator kreira asocijaciju politike filtera certifikata gdje definira podskup certifikata unutar pojedinačnog X.509 registra kao izvor asocijacije politike. On navodi ciljni identitet korisnika John_Day u ciljnom registru Grupa_1. U ovom slučaju, ne primjenjuje se niti jedna druga specifična asocijacija identifikatora ili druga asocijacija politike filtera certifikata. Prema tome, kada se Grupa_1 navede kao ciljni registar u operacijama pregledavanja, svi certifikati u izvorišnom X.509 registru koji udovoljavaju kriterijima filtera certifikata se mapiraju na navedeni ciljni identitet korisnika.

Filteri certifikata:

Filter certifikata definira skup sličnih atributa certifikata razlikovnog imena za grupu korisničkih certifikata u X.509 izvornom registru korisnika. Filter certifikata možete koristiti kao osnovu asocijacija politika filtera certifikata.

Filter certifikata u asocijaciji politike određuje koji certifikat u specificiranom izvornom X.509 registru mapirati u specificiranog ciljnog korisnika. Oni certifikati koji imaju informacije DN naslova i DN izdavača koje zadovoljavaju kriterij filtera se mapiraju na navedenog ciljnog korisnika tijekom operacija pregledavanja Mapiranja identiteta u poduzeću (EIM).

Na primjer, možete 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 više od jednog filtera certifikata kod kojeg certifikat zadovoljava kriterije, prednost ima specifičnija 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 specifičniji 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 specifičniji filter certifikata zbog boljeg podudaranja certifikata s njegovim kriterijima.

Od sljedećeg možete specificirati jedno ili oboje za definiranje filtera certifikata:

- Razlikovno ime naslova (SDN). Potpuni ili djelomični DN koji ste specificirali za filter mora odgovarati dijelu DN naslova od digitalnog certifikata što opisuje vlasnika certifikata. Možete dobaviti potpuni niz znakova DN naslova ili možete dobaviti jedan ili više djelomičnih DN-ova koji obuhvaćaju potpuni SDN.
- Razlikovno ime izdavača (IDN). Potpuni ili djelomični DN koji ste specificirali za filter mora odgovarati dijelu DN izdavača od digitalnog certifikata što opisuje Izdavača certifikata koji je izdao certifikat. Možete dobaviti potpuni niz znakova DN izdavača ili možete dobaviti jedan ili više djelomičnih DN-ova koji bi mogli obuhvatiti potpuni IDN.

Nekoliko je metoda koje možete koristiti za kreiranje filtera certifikata, uključujući upotrebu API-ja Format EIM filtera politike (eimFormatPolicyFilter) za generiranje filtera certifikata upotrebom certifikata kao predloška za kreiranje potrebnih DN-ova u ispravnom poretku i formatu za SDN i IDN.

Srodni koncepti

“Razlikovno ime” na stranici 46
Razlikovno ime (DN) je unos LDAP-a koji jednoznačno identificira i opisuje unos u (LDAP) poslužitelju direktorija. Vi koristite Čarobnjaka konfiguracije Mapiranja identiteta u poduzeću (EIM) za konfiguriranje poslužitelja direktorija za pohranu informacija domene EIM-a. Budući da EIM koristi poslužitelja direktorija za pohranu EIM podataka, možete koristiti razlikovna imena kao imena za provjeru autentičnosti na EIM kontroleru domene.

Srodne informacije

API Format filtera EIM politike (eimFormatPolicyFilter)

EIM operacije pregledavanja

Aplikacija ili operativni sistem koristi EIM API za izvođenje operacije pregledavanja tako da aplikacija ili operativni sistem mogu izvesti mapiranje s jednog identiteta korisnika u jednom registru na drugi identitet korisnika u drugom registru. EIM operacija pregledavanja je proces preko koje aplikacija ili operativni sistem pronalazi nepoznate pridružene korisničke identitete u određenom 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 može izvesti jedan od dva tipa EIM operacija pregledavanja na osnovu tipa informacija koje aplikacija dobavlja kao izvor EIM operacije pregledavanja: korisnički identitet ili EIM identifikator.

Kada aplikacije ili operativni sistemi koriste eimGetTargetFromSource() API za dobivanje ciljnog korisničkog identiteta za dani ciljni registar, moraju osigurati *korisnički identitet kao cilj* operacije pregledavanja. Da bi se koristio kao izvor u EIM operaciji pregledavanja, korisnički 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:

- Korisnički identitet kao izvor ili početnu točku operacije.
- Ime EIM definicije registra za izvorni korisnički identitet.
- Ime EIM definicije registra koje je cilj EIM operacije pregledavanja. Ova definicija registra opisuje korisnički registar koji sadrži korisnički identitet koji aplikacija traži.

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

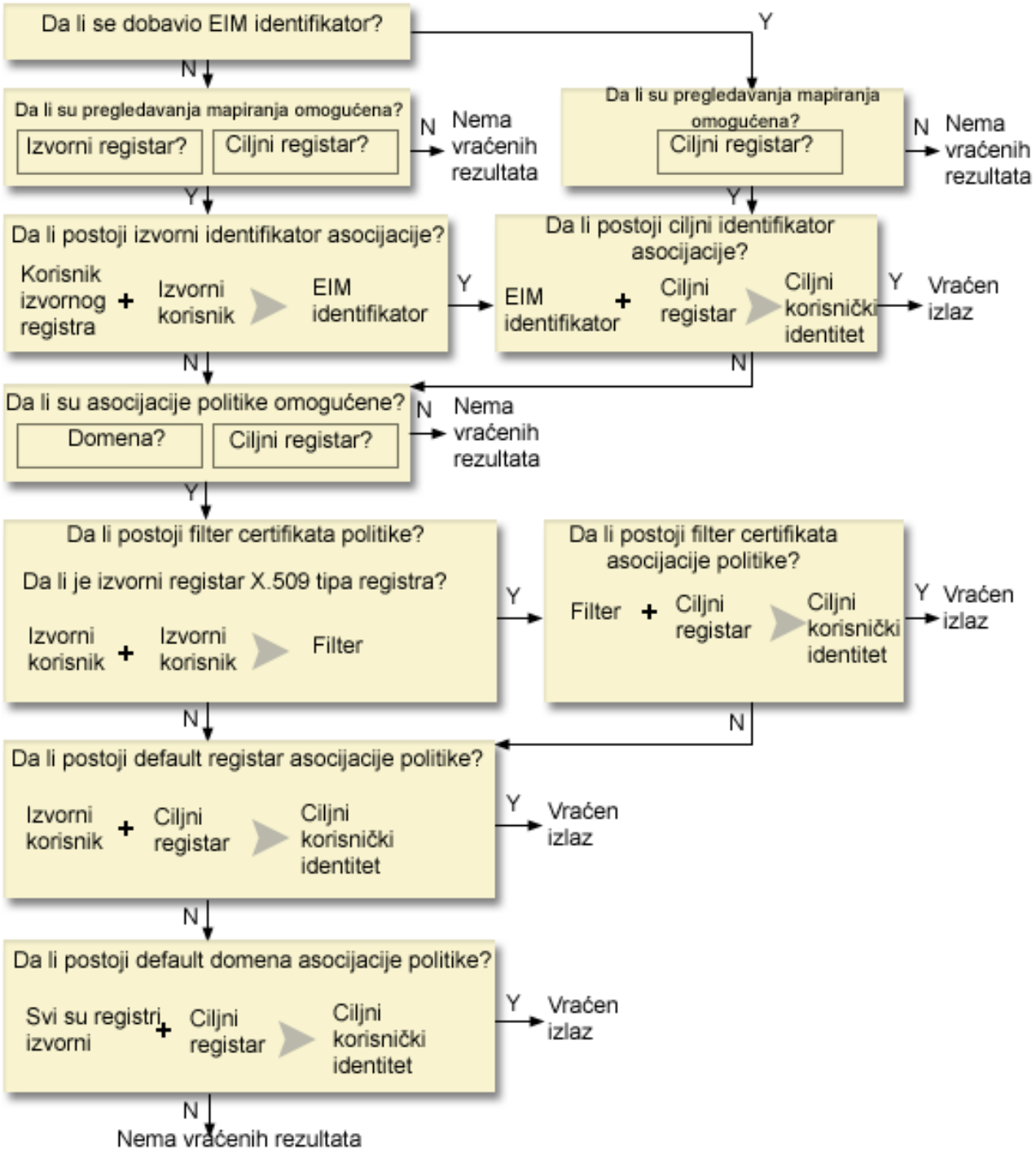
- EIM identifikator kao izvor ili početnu točku operacije.
- Ime EIM definicije registra koje je cilj EIM operacije pregledavanja. Ova definicija registra opisuje korisnički registar koji sadrži korisnički identitet koji aplikacija traži.

Da bi korisnički identitet bio vraćen kao cilj bilo kojeg tipa EIM operacije pregledavanja, korisnički identitet mora za njega imati definiranu ciljnu asocijaciju. Ova ciljna asocijacija može biti u obliku asocijacije identifikatora ili asocijacije politike.

Osigurana se informacija daje EIM-u i EIM operacija pretraživanja traži i vraća bilo koji ciljni korisnički identitet pretražujući EIM podatke sljedećim redoslijedom kao što prikazuje slika 10:

1. Ciljna asocijacija identifikatora za EIM identifikator. EIM identifikator se identificira na jedan od dva načina: osigurava ga eimGetTargetFromIdentifier() API. ili se EIM identifikator određuje 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 općenite obrade



Bilješka: U sljedećem dijagramu, operacije pregledavanja najprije provjeravaju pojedinačnu definiciju registra, poput navedenog izvorišnog ili ciljnog registra. Ako operacije pregledavanja ne uspiju pronaći mapiranje koristeći pojedinačnu definiciju registra, određuje se da li je pojedinačna definicija registra član definicije registra grupe. Ako je član definicije registra grupe, operacija pregledavanja provjerava definiciju registra grupe da udovolji zahtjevu pregleda mapiranja.

Pretraga operacije pregledavanja teče na sljedeći način:

1. Operacija pregledavanja provjerava jesu li pregledavanja mapiranja omogućena. Operacija pregledavanja određuje jesu li pregledavanja mapiranja omogućena za navedeni izvorni registar, navedeni ciljni registar ili oba navedena registra. Ako pregledavanje mapiranja nije omogućeno za jedan ili oba registra, tada operacija pregledavanja završava vraćajući ciljni korisnički identitet.
2. Operacija pregledavanja provjerava postoje li asocijacije identifikatora koje odgovaraju kriterijima pregledavanja. Ako je omogućen EIM identifikator, operacija pregledavanja koristi navedeno ime EIM identifikatora. Inače, operacija pregledavanja provjerava postoji li specifična izvorna asocijacija identifikatora koja odgovara osiguranom izvornom korisničkom identitetu i izvornom registru. Ako postoji, operacija pregledavanja ju koristi za određivanje odgovarajućeg imena EIM identifikatora. Operacija pregledavanja tada koristi ime EIM identifikatora za pretraživanje ciljnih asocijacija identifikatora za EIM identifikator koji odgovara navedenom imenu ciljne EIM definicije registra. Ako postoji ciljna asocijacija identifikatora koja odgovara, operacija pregledavanja vraća ciljni korisnički identitet definiran u ciljnoj asocijaciji.
3. Operacija pregledavanja provjerava je li korištenje asocijacija politika omogućeno. Operacija pregledavanja provjerava je li domena omogućena kako bi mogla dopustiti pregledavanje mapiranja upotrebom asocijacija politike. Operacija pregledavanja također provjerava je li ciljni registar omogućen za korištenje asocijacija politike. Ako domena nije omogućena za asocijacije politika ili registar nije omogućen za asocijacije politika, tada operacija pregledavanja završava bez vraćanja ciljnog korisničkog identiteta.
4. Operacija pregledavanja traži 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 podudarajuća asocijacija politike i postoje certifikati koji zadovoljavaju kriterij filtera certifikata, operacija mapiranja vraća odgovarajući ciljni korisnički identitet za tu asocijaciju politike.
5. Operacija pregledavanja traži default asocijacije politike registra. Operacija pregledavanja provjerava postoji li default asocijacija politike registra koja odgovara izvornim i ciljnim imenima definicije registra. Postoji li podudarajuća asocijacija politike, operacija pregledavanja vraća odgovarajući ciljni korisnički identitet za tu asocijaciju politika.
6. Operacija pregledavanja traži asocijacije politike default domene. Operacija pregledavanja provjerava postoji li asocijacija politike default domene koja je definirana za ciljnu definiciju registra. Postoji li podudarajuća asocijacija politike, operacija pregledavanja vraća pridruženi ciljni korisnički identitet za tu asocijaciju politika.
7. Operacija pregledavanja ne može vratiti nikakav rezultat.

Da saznate više o operacijama pregledavanja Mapiranja identiteta u poduzeću, pogledajte sljedeće primjere:

Srodni koncepti

"EIM domena" na stranici 6
Domena Mapiranja identiteta u poduzeću (EIM) je direktorij u sklopu Lightweight Directory Access Protocol (LDAP) poslužitelja koji sadrži EIM podatke za poduzeće.

"Asocijacije politike" na stranici 21
Politika Mapiranja identiteta u poduzeću (EIM) dozvoljava EIM administratoru da kreira i koristi asocijacije politike za definiranje odnosa između višestrukih identiteta korisnika u jednom ili više registara korisnika i identiteta jednog korisnika u drugom registru korisnika.

"Kontroler EIM domene" na stranici 5
EIM kontroler domene je Lightweight Directory Access Protocol (LDAP) poslužitelj koji je konfiguriran za upravljanje jednom ili više EIM domena. EIM domenu čine svi EIM identifikatori, EIM asocijacije i korisnički registri koji su definirani u toj domeni. Sistemi (EIM klijenti) sudjeluju u EIM domeni korištenjem podataka domene za operacije EIM pregledavanja.

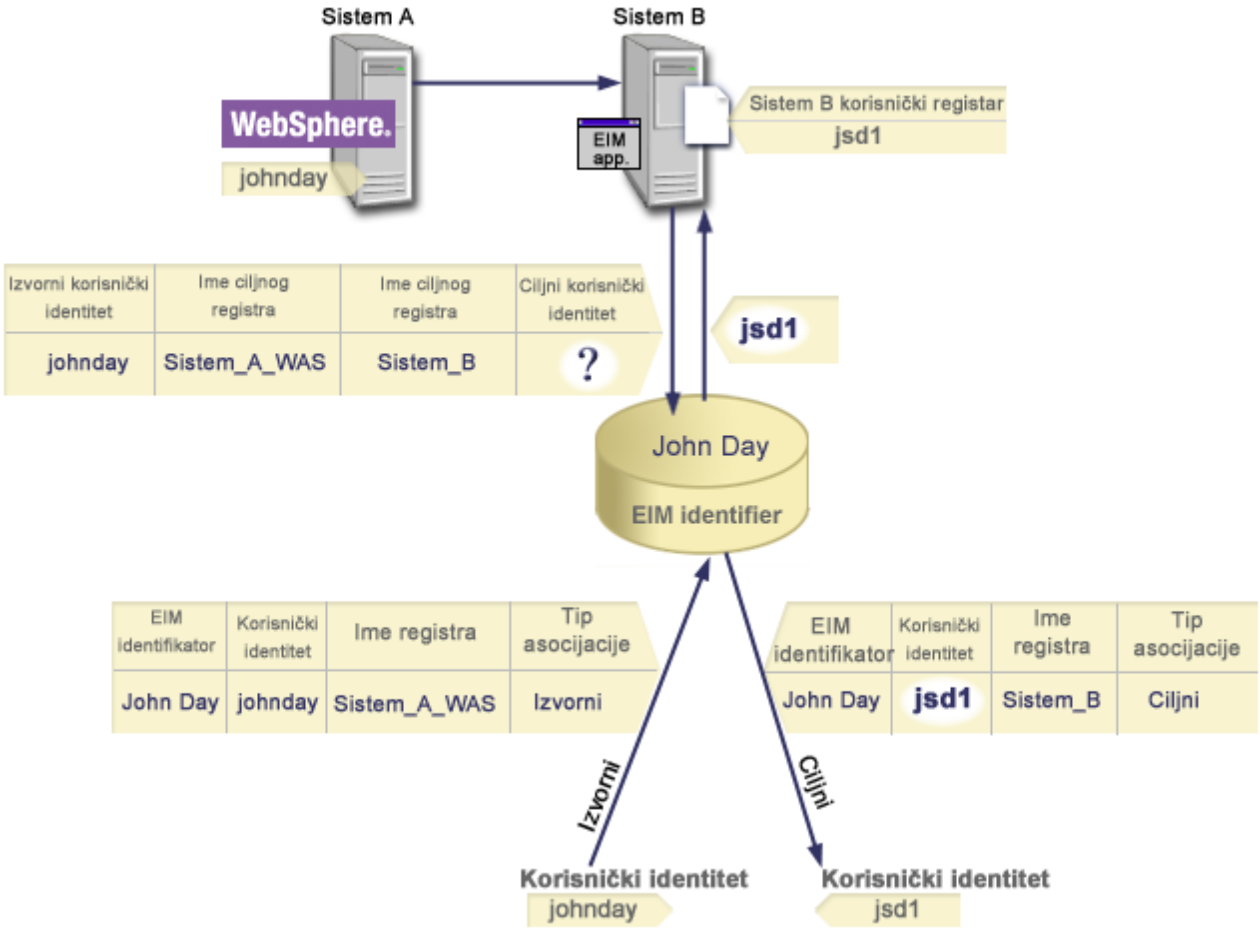
"Informacije pregledavanja" na stranici 16
Pomoću Mapiranja identiteta u poduzeću (EIM) možete osigurati opcijske podatke (nazivaju se informacije pregledavanja) za dalju identifikaciju ciljnog korisničkog identiteta. Taj ciljni korisnički identitet može biti specifičan u asocijaciji identifikatora ili u asocijaciji politike.

Primjeri operacije pregledavanja: Primjer 1

Koristite ovaj primjer da saznate kako radi dijagram pretrage za operaciju pretrage koja vraća ciljni identitet korisnika iz određenih asocijacija identifikatora baziranih na poznatom identitetu korisnika.

Na Slici 11, identitet korisnika johnday potvrđuje autentičnost na Aplikacijskom poslužitelju WebSphere-u koristeći Lightweight Third-Party Authentication (LPTA) na Sistemu A. Aplikacijski poslužitelj WebSphere na Sistemu A zove integrirani program na Sistemu B da pristupi podacima Sistemu B. Integrirani program koristi API Mapiranja identiteta u poduzeću (EIM) za izvođenje operacije pregledavanja EIM-a bazirano na korisničkom identitetu na Sistemu A kao izvoru operacije. Aplikacija dobavlja sljedeće informacije za izvođenje operacije: johnday kao izvorni korisnički identitet, System_A_WAS kao izvorno ime definicije EIM registra i System_B kao ciljno ime definicije EIM registra. Ove 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 traže ciljnu asocijaciju identifikatora za ovaj identifikator koja se podudara s ciljnim imenom EIM definicije registra za System_B. Kada je pronađena podudarajuća ciljna asocijacija EIM operacija pregledavanja aplikaciji vraća jsd1 korisnički identitet.

Slika 11: EIM operacija pregledavanja vraća ciljni korisnički identitet iz određene asocijacije identifikatora zasnovane na poznatom korisničkom identitetu johnday



Primjeri operacije pregledavanja: Primjer 2

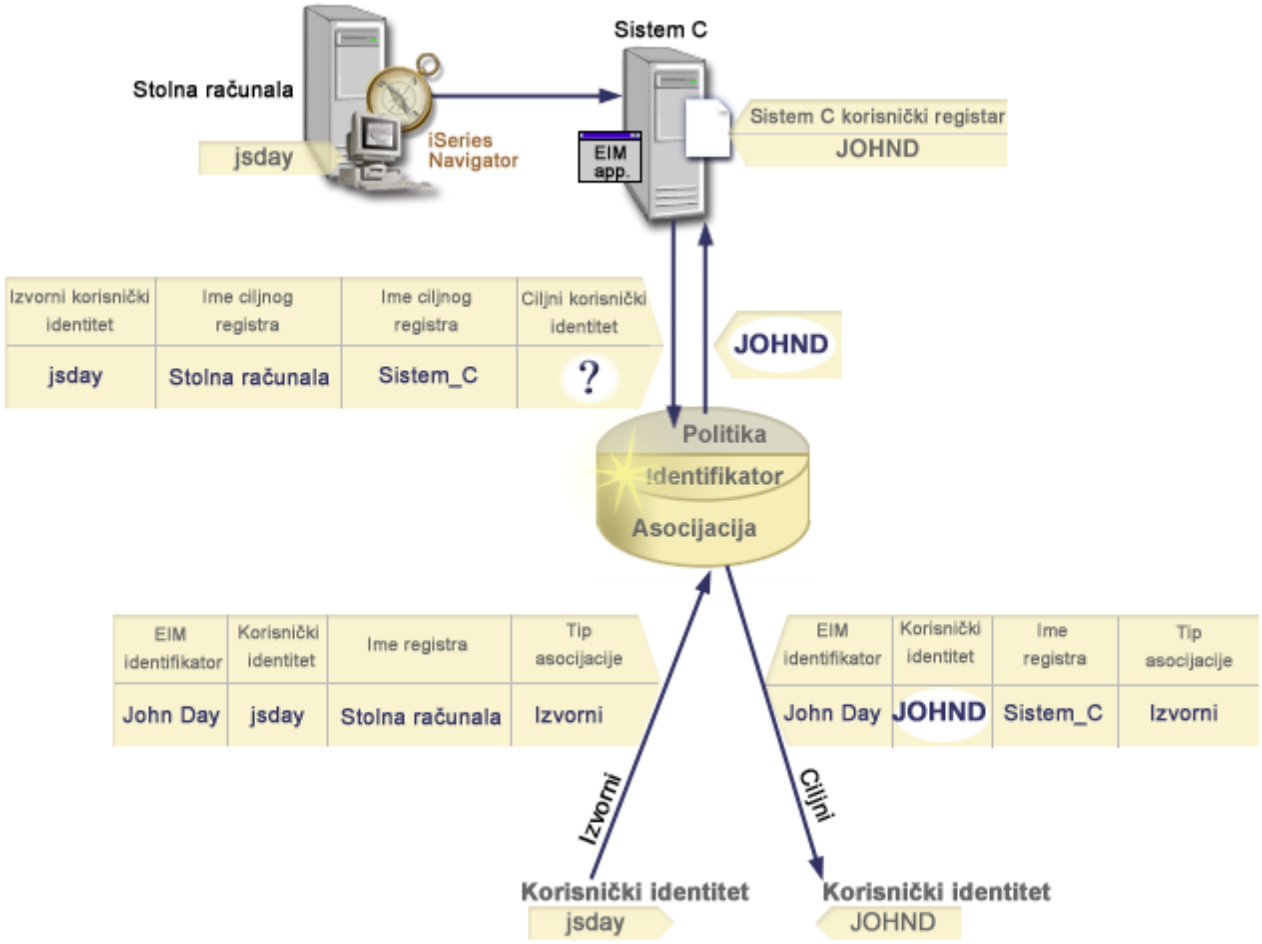
Koristite ovaj primjer da saznate kako radi dijagram pretrage za operaciju pretrage koja vraća ciljni identitet korisnika iz određenih asocijacija identifikatora baziranih na poznatom Kerberos principalu.

Na Slici 12, administrator želi mapirati Windows korisnika u Windows registru Aktivnog direktorija na profil i5/OS korisnika. Kerberos je metoda provjere autentičnosti koju Windows koristi i ime registra Windows Aktivnog direktorija kako ga je administrator definirao u EIM-u je Desktopi. Korisnički identitet iz kojeg administrator želi mapirati je Kerberos principal imena jsday. Ime registrai5/OS-a kako ga je administrator definirao u EIM-u je Sistem_C i identitet korisnika na kojeg administrator želi mapirati je profil korisnika imenovan 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 Desktopi.
- Ciljna asocijacija za profil i5/OS korisnika nazvana JOHND u registru Sistem_C.

Slika 12: EIM operacija pregledavanja vraća ciljni korisnički identitet iz određenih asocijacija identifikatora zasnovanih na poznatom Kerberos principalu jsday



Ova konfiguracija dozvoljava da operacija pregledavanja mapiranja mapira od Kerberos principala na profil korisnika i5/OS-a kako slijedi:

Izvorni korisnički identitet i registar	**--->**	**EIM identifikator**	**--->**	**Ciljni korisnički identitet**
jsday u registru Desktopi	--->	John Day	--->	JOHND (u registru System_C)

Pretraga operacije pregledavanja teče na sljedeći način:

1. Korisnik jsday prijavljuje se i provjeru autentičnosti radi Windows upotrebom njegovih Kerberos principala u Windows Aktivni direktorij registru Desktopi.
2. Korisnik otvara System i Navigator za pristup podataka na System_C.
3. i5/OS koristi EIM API za obavljanje operacije pregledavanja EIM-a s izvorišnim identitetom korisnika jsday, izvorišnim registrom Desktopi i ciljnim registrom Sistem_C.
4. EIM operacija pregledavanja provjerava jesu li omogućeni pregledi mapiranja za izvorni registar Desktopi i ciljni registar System_C. Jesu.
5. Operacija pregledavanja traži određenu izvornu asocijaciju identifikatora koja se podudara s navedenim izvornim korisničkim identitetom jsday iz izvornog registra Desktopi.
6. Operacija pregledavanja koristi podudarajuću izvornu asocijaciju identifikatora za određivanje odgovarajućeg imena EIM identifikatora koji je John Day.
7. Operacija pregledavanja koristi to ime EIM identifikatora za traženje 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 korisnički identitet JOHND vraća kao definiran u ciljnoj asocijaciji.
9. Uz dovršetak operacije pregledavanja mapiranja, System i Navigator započinje izvođenje pod korisničkim profilom JOHND. Ovlaštenje korisnika za pristup resursima i izvođenje akcija unutar System i Navigator određeno je ovlaštenjem definiranim za korisnički profil JOHND, umjesto ovlaštenjima definiranim za korisnički profil jsday.

Primjeri operacije pregledavanja: Primjer 3

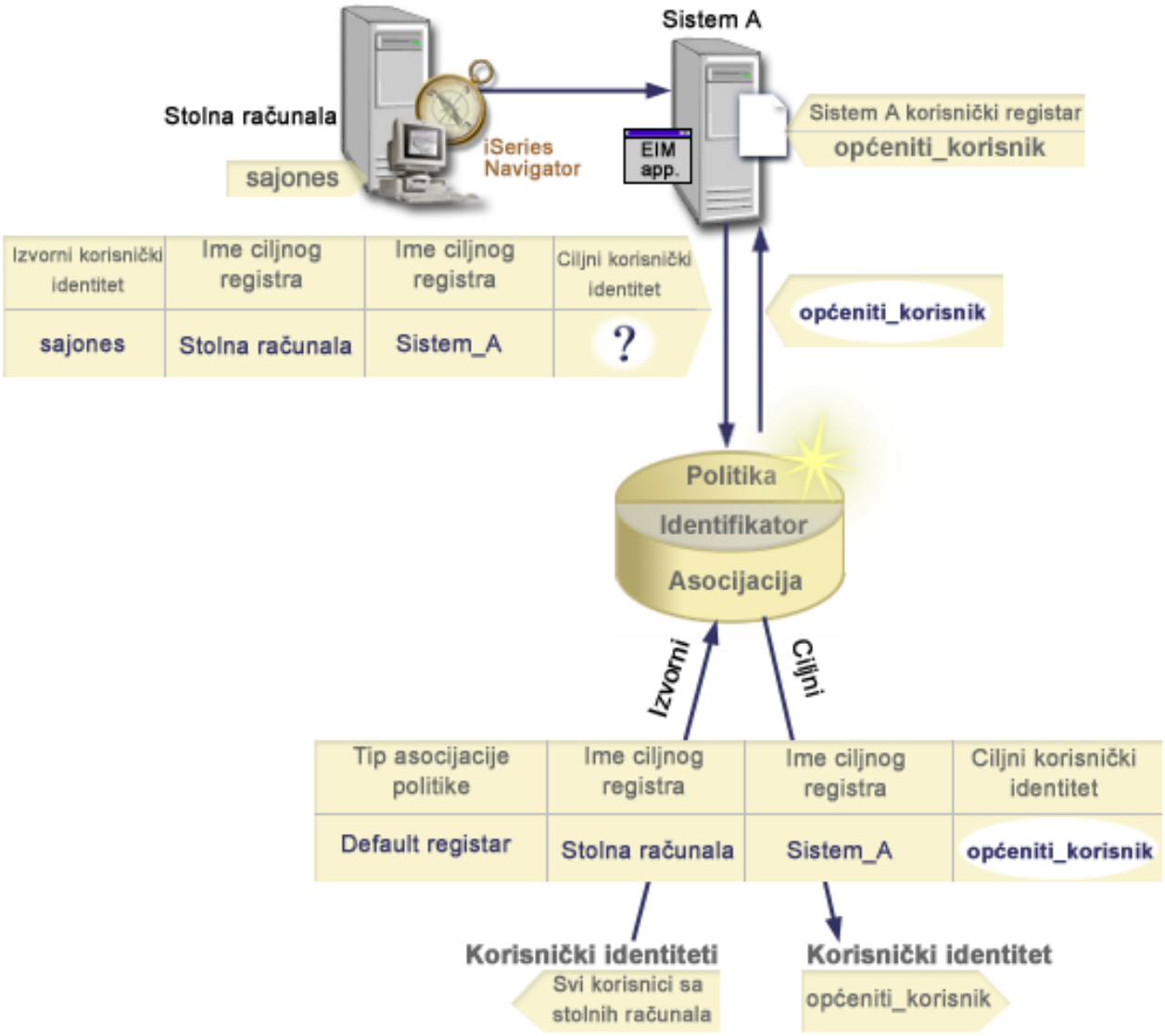
Koristite ovaj primjer da saznate kako radi dijagram pretrage za operaciju pretrage koja vraća ciljni identitet korisnika iz asocijacije politike defaultnog registra.

Na slici 13, administrator želi mapirati sve korisnike radnih stanica u registru Aktivnog direktorija Windows-a na jednostruki profil korisnika i5/OS-a nazvan general_user u registru i5/OS-a kojeg je nazvao Sistem_A u Mapiranju identiteta u poduzeću (EIM). Kerberos je metoda provjere autentičnosti koju koriste Windows-i i ime registra Aktivnog direktorija Windows-a kako ga je administrator definirao u EIM-u je Desktopi. Jedan od korisničkih identiteta iz kojeg administrator želi mapirati je Kerberos principal s imenom sajones.

Administrator kreira default asocijaciju politike registra sa sljedećim informacijama:

- Izvorni registar od Desktopi.
- Ciljni registar od System_A.
- Ciljni korisnički identitet od general_user.

Slika 13: Operacija pregledavanja vraća ciljni korisnički identitet iz default asocijacije politike registra.



Ova konfiguracija dozvoljava operaciji pregledavanja da mapira sve Kerberos principale u registru Desktopi, uključujući sajones principal, na profil korisnika i5/OS-a nazvan general_user kako slijedi:

Izvorni korisnički identitet i registar	**--->**	**Defaultna asocijacija politike registra**	**--->**	**Ciljni korisnički identitet**
sajones u Desktopi registru	--->	Defaultna asocijacija politike registra	--->	general_user (u System_A registru)

Pretraga operacije pregledavanja teče na sljedeći način:

1. Korisnik sajones prijavljuje se i njegovu autentičnost provjerava Windows stolno računalo upotrebom Kerberos principala iz Desktopi registra.
2. Korisnik otvara System i Navigator za pristup podacima na Sistemu A.
3. i5/OS koristi EIM API za obavljanje operacije pregledavanja EIM-a s izvorišnim identitetom korisnika sajones, izvorišnim registrom Desktopi i ciljnim registrom Sistem_A.
4. EIM operacija pregledavanja provjerava jesu li pregledavanja mapiranja omogućena za izvorni registar Desktopi i ciljni registar System_A. Jesu.

5. Operacija pregledavanja traži određenu izvornu asocijaciju identifikatora koja se podudara s navedenim izvornim korisničkim identitetom sajones iz izvornog registra Desktopi. Ne pronalazi podudarajuću asocijaciju identifikatora.
6. Operacija pregledavanja provjerava je li domena omogućena za upotrebu asocijacija politika. Jest.
7. Operacija pregledavanja provjerava je li ciljni registar (System_A) omogućen za upotrebu asocijacija politika. Jest.
8. Operacija pregledavanja provjerava je li izvorni registar (Desktopi) X.509 registar. Nije.
9. Operacija pregledavanja provjerava postoji li default asocijacija politike registra koja odgovara imenu definicije izvornog registra (Desktopi) i imenu definicije ciljnog registra (System_A).
10. Operacija pregledavanja određuje da postoji i kao ciljni korisnički identitet vraća general_user.

Ponekad EIM operacija pregledavanja vraća dvosmislene rezultate. Ovo se može desiti, na primjer, kada se više od jednog ciljnog korisničkog identiteta podudara s navedenim kriterijem operacije pregledavanja. Neke EIM-omogućene aplikacije, uključujući i5/OS aplikacije i proizvode nisu oblikovane da rukuju ovim dvosmislenim rezultatima i mogu ne uspjeti ili dati neočekivane rezultate. Možda ćete trebati poduzeti neke mjere da riješite tu situaciju. Na primjer, morat ćete promijeniti EIM konfiguraciju ili definirati informacije pregledavanja za svaki ciljni korisnički identitet da spriječite višestruka podudaranja ciljnih korisničkih identiteta. Također, možete testirati mapiranja da odredite da li promjene koje ste napravili rade prema očekivanjima.

Primjeri operacije pregledavanja: Primjer 4

Koristite ovaj primjer da saznate kako radi dijagram pretrage za operaciju pretrage koja vraća ciljni identitet korisnika u registru korisnika koji je član definicije registra grupe.

Administrator želi mapirati Windows korisnika na profil i5/OS korisnika. Kerberos je način provjere autentičnosti koji koriste Windows-i i ime Kerberos registra kako ga je administrator definirao u Mapiranju identiteta u poduzeću (EIM) je Desktop_A. Identitet korisnika od kojeg administrator želi mapirati je Kerberos principal imenovan jday. Ime definicije registra i5/OS-a kako ga je definirao administrator u EIM-u je Grupa_1 i identitet korisnika na koji administrator želi mapirati je profil korisnika nazvan JOHND koji postoji u tri pojedinačna registra: Sistem_B, Sistem_C i Sistem_D. Svaki od pojedinačnih registara je član definicije registra grupe Grupa_1.

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

- Izvorišna asocijacija za Kerberos principal nazvana jday u Desktop_A registru.
- Ciljna asocijacija za profil i5/OS korisnika nazvana JOHND u registru Grupa_1 .

Ova konfiguracija dozvoljava da operacija pregledavanja mapiranja mapira od Kerberos principala na profil korisnika i5/OS-a kako slijedi:

Izvorni korisnički identitet i registar	**--->**	**EIM identifikator**	**--->**	**Ciljni korisnički identitet**
jday u Desktop_A registru	--->	John Day	--->	JOHND (u Grupa_1 definiciji registra grupe)

Pretraga operacije pregledavanja teče na sljedeći način:

1. Korisnik (jday) se prijavljuje i provjerava autentičnost na Windows-e na Desktop_A.
2. Korisnik otvara System i Navigator za pristup podacima na System_B.
3. i5/OS koristi EIM API za obavljanje operacije pregledavanja EIM-a s izvorišnim identitetom korisnika jday, izvorišnim registrom Desktop_A i ciljnim registrom Sistem_B.
4. Operacija pregledavanja EIM-a provjerava da li su pregledi mapiranja omogućeni za izvorišni registar (Desktop_A) i ciljni registar (Sistem_B).
5. Operacija pregledavanja provjerava specifične asocijacije pojedinačnih izvora koji se podudaraju s dobavljenim izvorišnim identitetom korisnika jday u izvorišnom registru Desktop_A.

6. Operacija pregledavanja koristi izvorišnu asocijaciju koja se podudara da odredi odgovarajuće ime EIM identifikatora, koje je John Day.
7. Operacija pregledavanja koristi to ime EIM identifikatora za traženje pojedinačne ciljne asocijacije za EIM identifikator koja se podudara s navedenim ciljnim imenom definicije registra EIM-a Sistem_B. (Ne postoji niti jedna.)
8. Operacija pregledavanja provjerava da li je izvorišni registar (Desktop_A) član neke definicije registra grupe. (Nije.)
9. Operacija pregledavanja provjerava da li je ciljni registar (Sistem_B) član neke definicije registra grupe. Član je definicije registra grupe Grupa_1.
10. Operacija pregledavanja koristi ime EIM identifikatora za traženje pojedinačne ciljne asocijacije za EIM identifikator koja se podudara s navedenim ciljnim imenom definicije registra EIM-a Grupa_1.
11. Postoji takva pojedinačna ciljna asocijacija i operacija pregledavanja vraća ciljni identitet korisnika JOHND kako je definiran u ciljnoj asocijaciji.

Bilješka: U nekim slučajevima EIM operacija pregledavanja vraća dvosmislene rezultate kada se više od jednog ciljnog identiteta korisnika podudara s navedenim kriterijem operacije pregledavanja. S obzirom da EIM ne može vratiti jedan ciljni korisnički identitet, EIM-omogućene aplikacije (uključujući i5/OS aplikacije i proizvode koji nisu oblikovani za rukovanje ovim dvosmislenim rezultatima) mogu biti neuspješne ili mogu vratiti neočekivane rezultate. Možda ćete trebati poduzeti neke mjere da riješite tu situaciju. Na primjer, morat ćete promijeniti EIM konfiguraciju ili definirati informacije pregledavanja za svaki ciljni korisnički identitet da spriječite višestruka podudaranja ciljnih korisničkih identiteta. Možete testirati mapiranja da odredite da li promjene koje ste napravili rade prema očekivanjima.

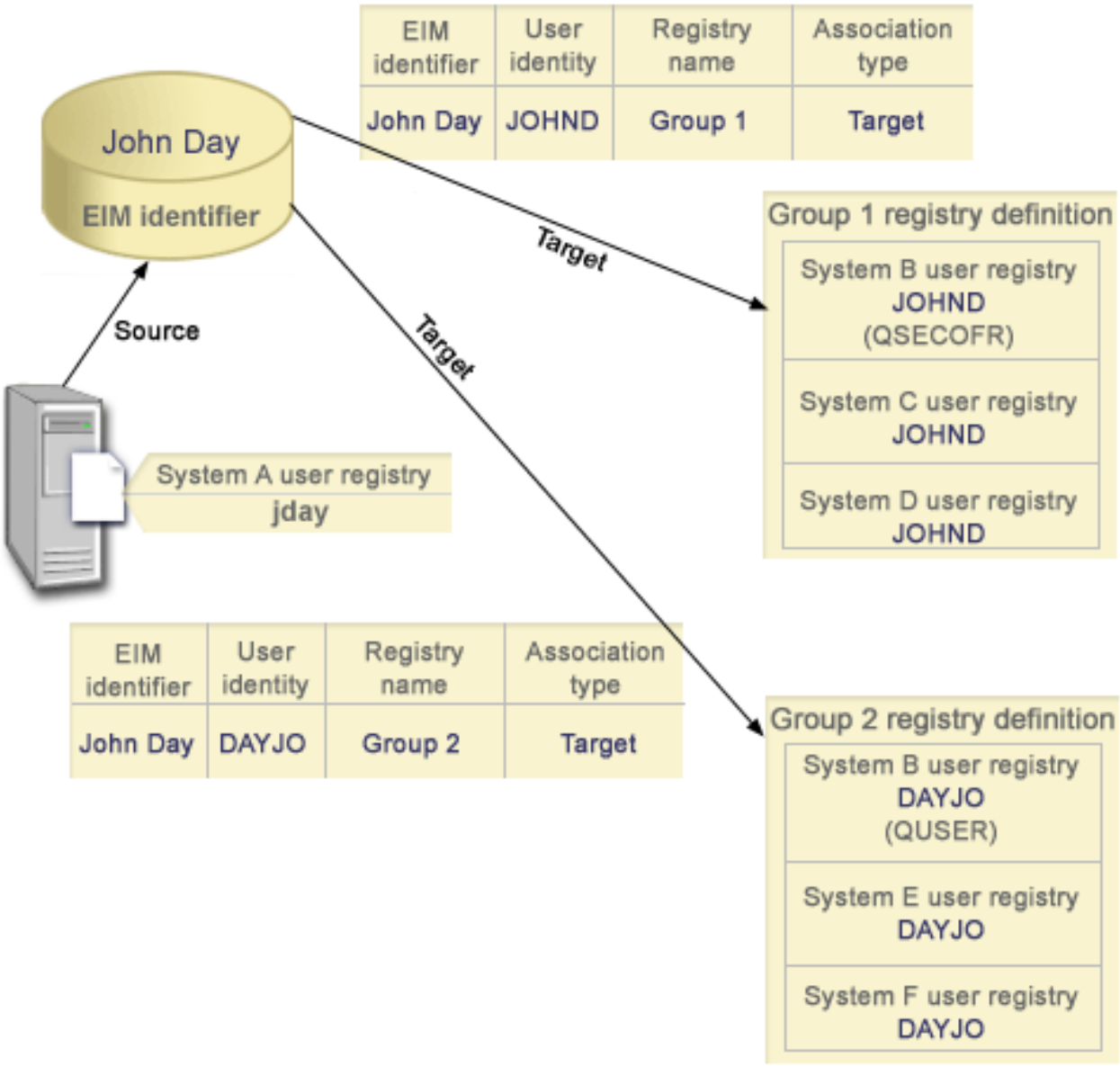
Primjeri operacije pregledavanja: Primjer 5

Koristite ovaj primjer da saznate o operacijama pregledavanja koje vraćaju dvosmislene rezultate koji uključuju definicije registra grupe.

U nekim slučajevima operacija pregledavanja mapiranja vraća dvosmislene rezultate kada se više od jednog ciljnog identiteta korisnika podudara s navedenim kriterijem pregledavanja. Stoga što situacija s dvosmislenim rezultatima može uzrokovati neuspjeh ili neočekivane rezultate aplikacija koje koriste EIM, morate poduzeti akcije da spriječite ili riješite situaciju.

Posebno, budite svjesni da operacije pregledavanja mogu vratiti dvosmislene rezultate kada navedete pojedinačnu definiciju registra korisnika kao člana više od jedne definicije registra grupe. Ako je pojedinačna definicija registra korisnika član višestrukih definicija registra grupe i vi kreirate pojedinačne asocijacije EIM identifikatora ili asocijacije politike koje koriste definiciju registra grupe bilo kao izvorišni ili ciljni registar, operacije pregledavanja mogu vratiti dvosmislene rezultate. Na primjer, mogli biste koristiti dva različita identiteta korisnika za dva različita sistemska zadatka koja izvodite: izvodite zadatke kao administrator sigurnosti koji zahtijevaju identitet korisnika s QSECOFR ovlaštenjem i izvodite tipične korisničke zadatke koji zahtijevaju identitet korisnika s QUSER ovlaštenjem. Ako se oba vaša korisnička identiteta nalaze unutar pojedinačnog registra korisnika koji je član dviju različitih definicija registra grupe i kreirate asocijacije ciljnih identiteta za oba ciljna identiteta korisnika, operacije pregledavanja pronalaze oba ciljna identiteta korisnika i posljedično vraćaju dvosmislene rezultate.

Sljedeći primjer opisuje kako se ovaj problem može pojaviti kada navedete pojedinačni registar korisnika kao člana dviju definicija registra grupe i navedete jednu od definicija registra grupe kao ciljni registar u dvije asocijacije pojedinačnih EIM identifikatora.



Primjer:

John Day ima sljedeće korisničke identitete unutar definicije registra sistema nazvane Sistem B registar korisnika:

- JOHND
- DAYJO

Sistem B registar korisnika je član sljedećih definicija registra grupe:

- Grupa 1
- Grupa 2

EIM identifikator John Day ima dvije ciljne asocijacije sa sljedećim specifikacijama:

- Ciljna asocijacija: Ciljni registar je Grupa 1 koji sadrži korisnički identitet JOHND u Sistem B registru korisnika.
- Ciljna asocijacija: Ciljni registar je Grupa 2 koji sadrži korisnički identitet DAYJO u Sistem B registru korisnika.

U ovoj situaciji, operacija pregledavanja mapiranja vraća dvosmislene rezultate jer se više od jednog ciljnog korisničkog identiteta podudara s navedenim kriterijem pregledavanja; oba korisnička identiteta (JOHND i DAYOJO) se podudaraju s navedenim kriterijem pregledavanja.

Slično, operacije pregledavanja mapiranja mogu vratiti dvosmislene rezultate ako kreirate dvije asocijacije politike (umjesto asocijacija pojedinačnih identifikatora EIM-a) koje koriste definicije registra grupe kao ciljne registre.

Da spriječite da operacije pregledavanja vraćaju dvosmislene rezultate koji uključuju definicije registra grupe, razmotrite sljedeće upute:

- Ne navodite pojedinačni registar korisnika kao člana više od jedne definicije registra grupe.
- Koristite oprez kada kreirate asocijacije pojedinačnih EIM identifikatora ili asocijacije politike koje koriste definicije registra grupe bilo kao izvorišni ili ciljni registar. Provjerite da definicija registra grupe nije član više od jedne definicije registra grupe. Budite svjesni da ako je član ciljne definicije registra grupe također član neke druge definicije registra grupe, operacije pregledavanja mogu vratiti dvosmislene rezultate.
- Ako imate situaciju dvosmislenih rezultata gdje ste naveli pojedinačnu definiciju registra grupe kao člana višestrukih definicija registra grupe i kreirate asocijaciju pojedinačnih identifikatora ili asocijaciju politike koja koristi jednu od tih definicija registra grupe bilo kao izvorišni registar ili ciljni registar, možete definirati jedinstvene informacije pregledavanja za svaki ciljni identitet korisnika u svakoj asocijaciji kako bi dalje pročistili potragu.

Mogli biste definirati sljedeće informacije pregledavanja za svaki ciljni korisnički identitet u primjeru o John Day:

- Za JOHND: Definirajte Administrator kao informaciju pregledavanja
- Za DAYJO: Definirajte Korisnik kao informaciju pregledavanja

Ipak, osnovne i5/OS aplikacije kao na primjer System i Access za Windows ne mogu koristiti informacije pregledavanja za razlikovanje između više ciljnih korisničkih identiteta vraćenih od strane operacije pregledavanja. Prema tome, možete razmotriti redefiniciju asocijacija za domenu da osigurate da operacija pregledavanja mapiranja može vratiti jednostruki ciljni identitet korisnika, da osigurate da osnovne i5/OS aplikacije mogu uspješno izvoditi operacije pregledavanja i mapirati identitete.

Srodni koncepti

"Definicije registra grupe" na stranici 15
Logičko grupiranje definicija registra vam dozvoljava da smanjite količinu posla koji morate obaviti za konfiguraciju EIM mapiranja. Možete upravljati definicijom registra grupe slično kao što upravljate pojedinačnom definicijom registra.

Podrška politici mapiranja EIM i omogućivanje

Podrška politike Mapiranja identiteta u poduzeću (EIM) dozvoljava vam korištenje asocijacija politike kao i određenih asocijacija identifikatora u nekoj EIM domeni. Asocijacije politika možete koristiti umjesto ili u kombinaciji s asocijacijama identifikatora.

Podrška politike EIM mapiranja osigurava značenja omogućavanja i onemogućavanja korištenja asocijacija politike za cijelu domenu kao i za svaki specifični ciljni korisnički registar. EIM vam također dozvoljava da postavite da li određeni registar može sudjelovati općenito u operacijama pregledavanja mapiranja. Kao posljedica, možete koristiti podršku politike mapiranja za precizniju kontrolu kako operacije pregledavanja mapiranja vraćaju rezultate.

Default postavka za EIM domenu je da su pregledavanja mapiranja koja koriste asocijacije politike onemogućena za domenu. Kada je onemogućeno korištenje asocijacija politike za domenu, sve operacije pregledavanja mapiranja za domenu vraćaju rezultate korištenjem samo određenih asocijacija identifikatora između korisničkih identiteta i EIM identifikatora.

Default postavke za svaki pojedinačni registar su takve da je sudjelovanje pregledavanja mapiranja omogućeno, a korištenje asocijacija politike onemogućeno. Kada omogućite korištenje asocijacija politike za pojedinačni ciljni registar, trebate također osigurati da je ta postavka omogućena za domenu.

Možete konfigurirati sudjelovanje pregledavanja mapiranja i korištenje asocijacija politike za svaki registar na jedan od tri načina:

- Operacije pregledavanja mapiranja se ne mogu u potpunosti koristiti za određeni registar. Drugim riječima, neka aplikacija koja izvodi operaciju pregledavanja mapiranja uključujući taj registar neće uspjeti vratiti rezultate.
- Operacije pregledavanja mapiranja mogu koristiti određene asocijacije identifikatora između samo korisničkih identiteta i EIM identifikatora. Pregledavanja mapiranja su omogućena za registar, ali je zato korištenje asocijacija politike onemogućeno za registar.
- Operacije pregledavanja mapiranja mogu koristiti određene asocijacije identifikatora kada postoje i asocijacije politike kada određene asocijacije identifikatora ne postoje (sve su postavke omogućene).

Srodni koncepti

"Informacije pregledavanja" na stranici 16
Pomoću Mapiranja identiteta u poduzeću (EIM) možete osigurati opcijske podatke (nazivaju se informacije pregledavanja) za dalju identifikaciju ciljnog korisničkog identiteta. Taj ciljni korisnički identitet može biti specifičan u asocijaciji identifikatora ili u asocijaciji politike.

"Asocijacije politika default domene" na stranici 21
Asocijacija politike default domene je jedan tip asocijacije politike koji možete koristiti za kreiranje mapiranja više-prema-jedan između identiteta korisnika.

"Asocijacije politika default registra" na stranici 23
Asocijacija politike default registra je jedan tip asocijacije politike koji možete koristiti za kreiranje mapiranja više-prema-jedan između identiteta korisnika.

"Kreiranje asocijacije politike" na stranici 99
Asocijacija politike je sredstvo za direktno definiranje odnosa između višestrukih korisničkih identiteta u jednom ili više registara i individualnog ciljnog korisničkog identiteta u drugom registru.

Srodni zadaci

"Omogućavanje asocijacija politike za domenu" na stranici 85
Asocijacija politike pruža načine kreiranja više-na-jedan mapiranja u situacijama gdje asocijacije između identiteta korisnika i identifikatora Mapiranja identiteta u poduzeću (EIM) ne postoje.

"Omogućavanje podrške pregledavanja mapiranja i upotrebe asocijacije politika za ciljni registar" na stranici 92
Podrška politike Mapiranja identiteta u poduzeću (EIM) vam dozvoljava upotrebu asocijacija politike kao načina za kreiranje više-na-jedan mapiranja u situacijama gdje ne postoje asocijacije između korisničkih identiteta i EIM identifikatora. Asocijaciju politike možete koristiti za mapiranje izvornog skupa višestrukih korisničkih identiteta (umjesto jednostrukog korisničkog identiteta) na jednostruki ciljni korisnički identitet u određenom ciljnom korisničkom registru.

EIM kontrola pristupa

Korisnik Mapiranja identiteta u poduzeću (EIM) je korisnik koji posjeduje kontrolu pristupa EIM-u baziranu na njegovom članstvu u preddefiniranoj korisničkoj grupi Lightweight Directory Access Protocol (LDAP) za specifičnu domenu.

Specificiranjem EIM kontrole pristupa za korisnika dodaje se taj korisnik u određenu LDAP korisničku grupu za određenu domenu. Svaka LDAP grupa ima ovlaštenje za izvođenje određenih EIM administrativnih zadataka za tu domenu. Koje i kakve tipove administrativnih zadataka, uključujući operacije pregledavanja, EIM korisnik može izvesti određeno je grupom za kontrolu pristupa kojoj EIM korisnik pripada.

Bilješka: Za konfiguriranje EIM-a morate dokazati da ste pouzdani unutar cijele mreže a ne samo na određenom sistemu. Ovlaštenje za konfiguriranje EIM-a nije bazirano na vašem ovlaštenju profila korisnika i5/OS-a, nego na vašem ovlaštenju kontrole pristupa EIM-u. EIM je mrežni resurs, ne resurs za bilo koji određeni sistem; prema tome, EIM ne prepoznaje i5/OS-specifična posebna ovlaštenja poput *ALLOBJ i *SECADM za konfiguraciju. Jednom kada je EIM konfiguriran, međutim, ovlaštenje za izvođenje zadataka može biti bazirano na različitim tipovima korisnika, uključujući profile korisnika i5/OS-a. Na primjer, IBM Tivoli Directory Server za i5/OS tretira i5/OS profile s *ALLOBJ i *IOSYSCFG posebnim ovlaštenjima kao administratore direktorija.

Samo korisnici s administratorskom EIM kontrolom pristupa mogu dodati druge korisnike u grupu za EIM kontrolu pristupa ili mijenjati ostale korisničke postavke kontrole pristupa. Da bi korisnik mogao postati članom grupe EIM kontrole pristupa on mora imati unos u poslužitelju direktorija koji djeluje kao kontroler EIM domene. Također, samo određeni tipovi korisnika mogu biti članovi grupe EIM kontrole pristupa. Identitet korisnika može biti u obliku Kerberos principala, razlikovnog imena LDAP-a ili profila korisnika i5/OS-a tako dugo dok je identitet korisnika definiran na poslužitelju direktorija.

Opaska: Da biste imali tip korisnika Kerberos principala dostupan u EIM-u, na sistemu mora biti konfigurirana usluga provjere autentičnosti mreže. Da tip profila korisnika i5/OS-a bude dostupno u EIM-u, morate konfigurirati sufiks objekta sistema na poslužitelju direktorija. To dozvoljava poslužitelju direktorija da referencira objekte i5/OS sistema, poput profila korisnika i5/OS-a.

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

Administrator Lightweight Directory Access Protokola (LDAP)

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 može izvesti sljedeće 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.
- Omogućiti i onemogućiti korištenje asocijacija politika za domenu.
- Omogućiti i onemogućiti pregledavanja mapiranja za registar.
- Omogućiti i onemogućiti korištenje asocijacija politika za registar.
- Izvoditi EIM operacije pregledavanja.
- Dohvaćati asocijacije identifikatora, asocijacije politika, filtere certifikata, EIM identifikatore i EIM definicije registara.
- Dodavati, uklanjati i ispisivati informacije EIM kontrole pristupa.
- Promijeniti i ukloniti informacije vjerodajnica za korisnika registra.

EIM administrator

Članstvo u ovoj grupi kontrole pristupa omogućava korisniku upravljanje svim EIM podacima unutar EIM domene. Korisnik s ovom kontrolom pristupa može izvesti sljedeće 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.
- Omogućiti i onemogućiti korištenje asocijacija politika za domenu.
- Omogućiti i onemogućiti pregledavanja mapiranja za registar.
- Omogućiti i onemogućiti korištenje asocijacija politika za registar.
- Izvoditi EIM operacije pregledavanja.

- Dohvaćati asocijacije identifikatora, asocijacije politika, filtere certifikata, EIM identifikatore i EIM definicije registara.
- Dodavati, uklanjati i ispisivati informacije EIM kontrole pristupa.
- Promijeniti i ukloniti informacije vjerodajnica za korisnika registra.

Administrator identifikatora

Članstvo u ovoj grupi kontrole pristupa omogućava korisniku dodavanje i mijenjanje EIM identifikatora i upravljanje izvornim i administrativnim asocijacijama. Korisnik s ovom kontrolom pristupa može izvesti sljedeće funkcije:

- Kreirati EIM identifikatore.
- Kreirati i ukloniti izvorne asocijacije.
- Kreirati i ukloniti administrativne asocijacije.
- Izvoditi EIM operacije pregledavanja.
- Dohvaćati asocijacije identifikatora, asocijacije politika, filtere certifikata, EIM identifikatore i EIM definicije registara.

EIM operacije mapiranja

Članstvo u ovoj grupi kontrole pristupa omogućava korisniku izvođenje EIM operacija pregledavanja mapiranja. Korisnik s ovom kontrolom pristupa može izvesti sljedeće funkcije:

- Izvoditi EIM operacije pregledavanja.
- Dohvaćati asocijacije identifikatora, asocijacije politika, filtere certifikata, EIM identifikatore i EIM definicije registara.

Administrator registra

Članstvo u ovoj grupi kontrole pristupa omogućava korisniku upravljanje definicijama EIM registra. Korisnik s ovom kontrolom pristupa može izvesti sljedeće funkcije:

- Dodati i ukloniti ciljne asocijacije.
- Kreirati i ukloniti asocijacije politika.
- Kreirati i ukloniti filtere certifikata.
- Omogućiti i onemogućiti pregledavanja mapiranja za registar.
- Omogućiti i onemogućiti korištenje asocijacija politika za registar.
- Izvoditi EIM operacije pregledavanja.
- Dohvaćati asocijacije identifikatora, asocijacije politika, filtere certifikata, EIM identifikatore i EIM definicije registara.

Administrator za izabrane registre

Članstvo u ovoj grupi kontrole pristupa korisniku omogućuje upravljanje EIM informacijama samo za određenu definiciju korisničkog registra (poput Registry_X). Članstvo u ovoj grupi kontrole pristupa također omogućuje korisniku dodavanje i uklanjanje ciljnih asocijacija samo za određenu definiciju korisničkog registra. Za potpunu prednost operacija pregledavanja mapiranja i asocijacija politike, korisnik s ovom kontrolom pristupa također treba imati kontrolu pristupa **EIM operacije mapiranja**. Ova kontrola pristupa omogućuje korisniku izvođenje sljedeće funkcije za određene ovlaštene 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.
- Omogućavanje i onemogućavanje pregledavanja mapiranja samo za navedene definicije registara.

- Omogućavanje i onemogućavanje korištenje asocijacija politika samo za navedene definicije registara.
- Dohvaćanje EIM identifikatora.
- Dohvaćanje asocijacije identifikatora i filtera certifikata samo za navedene definicije registara.
- Dohvaćanje informacija EIM definicije registara samo za navedene definicije registara.

Bilješka: Ako je navedena definicija registra definicija registra grupe, korisnik s Administrator za kontrolu pristupa izabranih registara ima administratorski pristup jedino grupi, ne i članovima grupe.

Korisnik koji ima kontrolu pristupa **Administrator za izabrane registre** i kontrolu pristupa **EIM operacije pregledavanja mapiranja** dobiva mogućnost izvođenja sljedećih funkcija:

- Dodavanje i uklanjanje asocijacija politike samo za navedene registre.
- Izvoditi EIM operacije pregledavanja.
- Dohvaćati sve asocijacije identifikatora, asocijacije politika, filtere certifikata, EIM identifikatore i EIM definicije registara.

Pregledavanje vjerodajnica

Ova grupa kontrole pristupa dozvoljava korisniku da dohvati informacije o vjerodajnicama, poput lozinki.

Ako korisnik s ovom kontrolom pristupa želi izvesti dodatnu operaciju EIM-a, on mora biti član grupe kontrole pristupa koja pruža ovlaštenje za željenu operaciju EIM-a. Na primjer, ako korisnik s ovom kontrolom pristupa želi dohvatiti ciljnu asocijaciju iz izvorišne asocijacije, on mora biti član jedne od sljedećih grupa kontrole pristupa:

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

Srodni koncepti

“Razmatranja i5/OS profila korisnika za EIM” na stranici 49
Mogućnost izvođenja zadataka u Mapiranju identiteta u poduzeću (EIM) se ne zasniva na ovlaštenju vašeg i5/OS korisničkog profila, već na vašem ovlaštenju kontrole pristupa EIM-u.

“Identifikacija potrebnih sposobnosti i uloga” na stranici 53
Mapiranje identiteta u poduzeću (EIM) je oblikovano tako da jedna osoba može jednostavno biti odgovorna za konfiguriranje i administriranje u maloj organizaciji. Ili u većim organizacijama, možda želite imati veći broj različitih pojedinaca koji rukuju tim odgovornostima.

Srodni zadaci

“Upravljanje EIM kontrole pristupa korisnika” na stranici 111
Korisnik Mapiranja identiteta u poduzeću (EIM) je korisnik koji posjeduje kontrolu pristupa EIM-u baziranu na njegovom članstvu u preddefiniranim korisničkim grupama Lightweight Directory Access Protocol (LDAP). Specificiranjem EIM kontrole pristupa za korisnika dodaje se taj korisnik u određenu LDAP korisničku grupu.

EIM grupa kontrole pristupa: API ovlaštenje

Ove informacije prikazuju tablice koje su organizirane prema operaciji Mapiranja identiteta u poduzeću (EIM) koju izvodi API.

Svaka od sljedećih tablica prikazuje svaki EIM API, različite grupe kontrole pristupa EIM i ima li grupa kontrole pristupa ovlaštenje za izvođenje određenih EIM funkcija.

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	-	-	-	-

Tablica 1. Rad s domenama (nastavak)

EIM API	LDAP administrator	EIM administrator	Administrator identifikatora	EIM pregledavanje mapiranja	Administrator registra	Administrator za izabrani registar
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
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-je postoje četiri parametara koja određuju tip asocijacije koja se ili dodala ili uklonila. Ovlaštenje za ove API-je se razlikuje na osnovu tipa asocijacije specificirane u ovim parametrima. U sljedećoj tablici uključen 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

Tablica 4. Rad s asocijacijama identifikatora (nastavak). Za eimAddAssociation() i eimRemoveAssociation() API-je postoje četiri parametara koja određuju tip asocijacije koja se ili dodala ili uklonila. Ovlaštenje za ove API-je se razlikuje na osnovu tipa asocijacije specificirane u ovim parametrima. U sljedećoj tablici uključen 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
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
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 EIM: ovlaštenje EIM zadatka

Ove informacije prikazuju tablicu koja objašnjava odnose među različitim grupama kontrole pristupa Mapiranju identiteta u poduzeću (EIM) i zadatke EIM-a koje mogu izvoditi.

Premda LDAP administrator nije ispisan u tablici, ta je razina kontrole pristupa potrebna za kreiranje nove EIM domene. Također, 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	Pregledavanje vjerodajnica
Kreiranje domene	-	-	-	-	-	
Brisanje domene	X	-	-	-	-	
Modificiranje domene	X	-	-	-	-	
Omogućavanje/ Onemogućavanje asocijacija politike za domenu	X	-	-	-	-	
Traženje domena	X	-	-	-	-	
Dodavanje sistemskog registra	X	-	-	-	-	
Dodavanje aplikacijskog registra	X	-	-	-	-	
Uklanjanje registra	X	-	-	-	-	
Modificiranje registra	X	-	-	X	X	
Omogućavanje/ Onemogućavanje pregledavanje mapiranja za registar	X	-	-	X	X	
Omogućavanje/ Onemogućavanje asocijacija politike za registar	X	-	-	X	X	
Traženje registara	X	X	X	X	X	
Dodavanje identifikatora	X	X	-	-	-	
Uklanjanje identifikatora	X	-	-	-	-	
Modificiranje identifikatora	X	X	-	-	-	
Traženje identifikatora	X	X	X	X	X	
Dohvat pridruženih identifikatora	X	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	Pregledavanje vjerodajnica
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	
Traženje filtera certifikata	X	X	X	X	X	
Traženje asocijacija	X	X	X	X	X	
Traženje asocijacija politike	X	X	X	X	X	
Dohvat ciljne asocijacije iz izvorne asocijacije	X	X	X	X	-	
Dohvat ciljne asocijacije iz identifikatora	X	X	X	X	X	
Modificiranje korisnika registra	X	-	-	X	X	
Traženje korisnika registra	X	X	X	X	X	
Modificiranje pseudonima registra	X	-	-	X	X	
Traženje pseudonima registra	X	X	X	X	X	
Dohvat registra iz pseudonima	X	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	Pregledavanje vjerodajnica
Dodavanje/ Uklanjanje EIM kontrole pristupa	X	-	-	-	-	
Prikaz članova grupe kontrole pristupa	X	-	-	-	-	
Prikaz EIM kontrole pristupa za specificiranog korisnika	X	-	-	-	-	
Upit u EIM kontrolu pristupa	X	-	-	-	-	
Promjena vjerodajnice	X	-	-	-	-	-
Dohvat vjerodajnice	X	-	-	-	-	X
1 - Ako je navedena definicija registra definicija registra grupe, korisnik s Administrator za kontrolu pristupa izabranih registara ima administratorski pristup jedino grupi, ne i članovima grupe.						

LDAP koncepti za EIM

EIM koristi LDAP poslužitelj kao kontroler domene za pohranu EIM podataka. Prema tome, morate razumjeti neke LDAP koncepte koji se odnose na konfiguriranje i upotrebu EIM-a u vašem poduzeću. Na primjer, možete koristiti LDAP razlikovno ime kao korisnički identitet za konfiguriranje EIM-a i provjere autentičnosti EIM kontrolera domene.

Da bolje razumijete konfiguriranje i upotrebu EIM-a, morate razumjeti sljedeće LDAP koncepte:

Srodni koncepti

“Koncepti Mapiranja identiteta u poduzeću” na stranici 4
Konceptualno razumijevanje o tome kako radi Mapiranje identiteta u poduzeću (EIM) potrebno je za potpuno razumijevanje kako možete koristiti EIM u vašem poduzeću. Iako se konfiguracija i implementacija EIM API-ja mogu razlikovati između platformi poslužitelja, EIM koncepti su isti na svim IBM eServer platformama.

Razlikovno ime

Razlikovno ime (DN) je unos LDAP-a koji jednoznačno identificira i opisuje unos u (LDAP) poslužitelju direktorija. Vi koristite Čarobnjaka konfiguracije Mapiranja identiteta u poduzeću (EIM) za konfiguriranje poslužitelja direktorija za pohranu informacija domene EIM-a. Budući da EIM koristi poslužitelja direktorija za pohranu EIM podataka, možete koristiti razlikovna imena kao imena za provjeru autentičnosti 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 zovemo njegovim nadređenim razlikovnim imenom. U ovom primjeru, cn=Tim Jones imenuje unos, tako da je to RDN. o=IBM, c=US je nadređeno DN za cn=Tim Jones.

S obzirom da EIM koristi poslužitelj direktorija za pohranu EIM podataka, razlikovno ime možete koristiti za identitet korisnika koji se prijavljuje i provjerava autentičnost na kontroleru domene. Također možete koristiti razlikovno ime za identitet korisnika koji konfigurira EIM za vašu System i platformu. Na primjer, možete koristiti razlikovno ime kada radite sljedeće:

- Konfigurirate poslužitelj direktorija da djeluje kao EIM kontroler domene. Ovo učinite tako da kreirate i koristite razlikovno ime koje identificira LDAP administratora za poslužitelja direktorija. Ako poslužitelj direktorija nije prethodno konfiguriran, poslužitelj direktorija možete konfigurirati kada koristite čarobnjaka EIM konfiguracije za kreiranje i spajanje nove domene.
- Koristite EIM Čarobnjaka konfiguracije za izbor tipa korisničkog identiteta koji bi čarobnjak trebao koristiti u povezivanju na kontroler EIM domene. Razlikovno ime je jedno od korisničkih tipova koje izaberete. Razlikovno ime mora predstavljati korisnika koji ima ovlaštenja za kreiranje objekata u lokalnom prostoru imena poslužitelja direktorija.
- Koristite EIM Čarobnjaka konfiguracije za izbor tipa korisnika za izvođenje EIM operacija u ime funkcija operativnog sistema. Ove operacije uključuju operacije pregledavanja mapiranja i brisanje asocijacija kada se briše lokalni profil i5/OS korisnika. Razlikovno ime je jedno od korisničkih tipova koje izaberete.
- Povezivanja na kontroler domene za administraciju EIM-a, na primjer, za upravljanje registrima i identifikatorima te za izvođenje 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 izdavača ili certifikat za specificiranje kriterija koje filter koristi za određivanje na koje certifikate utječe asocijacija politike.

Srodni koncepti

"Nadređeno razlikovno ime"
Nadređeno razlikovno ime (DN) je unos u Lightweight Directory Access Protocol (LDAP) imenskom prostoru poslužitelja direktorija. Unosi LDAP poslužitelja svrstani su u hijerarhijskoj strukturi koja može odražavati političke, geografske, organizacijske ili domenske granice. Razlikovno ime se smatra nadređenim DN-om, kad je DN unos direktorija izravno superioran danom DN-u.

"Filteri certifikata" na stranici 26
Filter certifikata definira skup sličnih atributa certifikata razlikovnog imena za grupu korisničkih certifikata u X.509 izvornom registru korisnika. Filter certifikata možete koristiti kao osnovu asocijacija politika filtera certifikata.

Srodne informacije

Koncepti poslužitelja direktorija

Nadređeno razlikovno ime

Nadređeno razlikovno ime (DN) je unos u Lightweight Directory Access Protocol (LDAP) imenskom prostoru poslužitelja direktorija. Unosi LDAP poslužitelja svrstani su u hijerarhijskoj strukturi koja može odražavati političke, geografske, organizacijske ili domenske granice. Razlikovno ime se smatra nadređenim 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 nadređenom razlikovnom imenu. U ovom primjeru, cn=Tim Jones imenuje unos, tako da je to RDN. o=IBM, c=US je nadređeno DN za cn=Tim Jones.

Mapiranje identiteta u poduzeću (EIM) koristi poslužitelj direktorija kao kontroler domene za pohranu EIM podataka domene. Nadređeni DN u kombinaciji s imenom EIM domene određuje smještaj EIM podataka domene u imenskom prostoru poslužitelja direktorija. Kada za kreiranje i spajanje na novu domenu koristite čarobnjaka za EIM konfiguraciju, možete izabrati da specificirate nadređeni DN za domenu koju kreirate. Upotrebom nadređenog DN-a možete odrediti gdje u LDAP imenskom prostoru EIM podaci trebaju prebivati za domenu. Kada ne navedete nadređeni DN, EIM podaci prebivaju na svom vlastitom sufiksu u imenskom prostoru i default lokacija EIM podataka domene je ibm-eimDomainName=EIM.

Srodni koncepti

"Razlikovno ime" na stranici 46
Razlikovno ime (DN) je unos LDAP-a koji jednoznačno identificira i opisuje unos u (LDAP) poslužitelju direktorija. Vi koristite Čarobnjaka konfiguracije Mapiranja identiteta u poduzeću (EIM) za konfiguriranje poslužitelja direktorija za pohranu informacija domene EIM-a. Budući da EIM koristi poslužitelja direktorija za pohranu EIM podataka, možete koristiti razlikovna imena kao imena za provjeru autentičnosti na EIM kontroleru domene.

Srodne informacije

Koncepti poslužitelja direktorija

LDAP shema i druga razmatranja za EIM

Koristite ove informacije da saznate što je potrebno za rad poslužitelja direktorija s Mapiranjem identiteta u poduzeću (EIM).

EIM zahtijeva da poslužitelj direktorija koji podržava Lighweight Directory Protocol (LDAP) verziju 3 bude host kontroleru domene. Dodatno, proizvod poslužitelja direktorija mora biti sposoban prihvatiti EIM shemu i razumjeti sljedeće atribute i klase objekata:

- Atribut ibm-entryUUID.
- ibmattributetypes:
  - acIEntry
  - acIPropagate
  - acISource
  - entryOwner
  - ownerPropagate
  - ownerSource
- EIM atributi, uključujući tri nova atributa za podršku 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, uključujući tri nove klase za podršku asocijaciji politike:
  - ibm-eimApplicationRegistry
  - ibm-eimDomain
  - ibm-eimIdentifier
  - ibm-eimRegistry
  - ibm-eimRegistryUser
  - ibm-eimSourceRelationship
  - ibm-eimSystemRegsitry
  - ibm-eimTargetRelationship
  - ibm-eimFilterPolicy
  - ibm-eimDefaultPolicy
  - ibm-eimPolicyListAux

Srodni koncepti

"Kontroler EIM domene" na stranici 5
EIM kontroler domene je Lightweight Directory Access Protocol (LDAP) poslužitelj koji je konfiguriran za upravljanje jednom ili više EIM domena. EIM domenu čine svi EIM identifikatori, EIM asocijacije i korisnički registri koji su definirani u toj domeni. Sistemi (EIM klijenti) sudjeluju u EIM domeni korištenjem podataka domene za operacije EIM pregledavanja.

Koncepti Mapiranja identiteta u poduzeću za i5/OS

EIM možete primijeniti na bilo kojoj IBM eServer platformi. Ipak, kada EIM primjenjujete na System i model, morate računati na to da su neke od informacija specifične za System i primjenu.

Pregledajte sljedeće informacije da naučite više o i5/OS aplikacijama koje su omogućene za EIM, razmatranja o korisničkim profilima i ostala poglavlja koja vam mogu pomoći u učinkovitom korištenju EIM-a na System i platformi:

Srodni koncepti

"Koncepti Mapiranja identiteta u poduzeću" na stranici 4
Konceptualno razumijevanje o tome kako radi Mapiranje identiteta u poduzeću (EIM) potrebno je za potpuno razumijevanje kako možete koristiti EIM u vašem poduzeću. Iako se konfiguracija i implementacija EIM API-ja mogu razlikovati između platformi poslužitelja, EIM koncepti su isti na svim IBM eServer platformama.

Razmatranja i5/OS profila korisnika za EIM

Mogućnost izvođenja zadataka u Mapiranju identiteta u poduzeću (EIM) se ne zasniva na ovlaštenju vašeg i5/OS korisničkog profila, već na vašem ovlaštenju kontrole pristupa EIM-u.

Potrebno je izvesti nekoliko dodatnih zadataka za postavljanje i5/OS za upotrebu EIM-a. Ti dodatni zadaci zahtijevaju da imate profil korisnika i5/OS-a s odgovarajućim posebnim ovlaštenjima.

Za postav i5/OS za upotrebu EIM-a koristeći System i Navigator, vaš korisnički profil mora imati sljedeća posebna ovlaštenja:

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

Poboljšanje naredbi profila korisnikai5/OS-a za EIM identifikatore

Jednom kada konfigurirate EIM za vaš sistem, novi parametar EIMASSOC možete iskoristiti za obje naredbe, naredbu Kreiraj korisnički profil (CRTUSRPRF) i naredbu Promijeni korisnički profil (CHGUSRPRF). Ovaj parametar možete koristiti za definiranje asocijacija EIM identifikatora za određeni korisnički profil lokalnog registra.

Kada koristite taj parametar, možete specificirati sljedeće informacije:

- Ime EIM identifikatora, što može biti novo ime ili već postojeće ime identifikatora.
- Opcijska akcija za asocijaciju što može 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 postojeće 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 može biti ciljni, izvorni ili i ciljni i izvorni ili je to administrativna asocijacija.
- Da li kreirati specificirani EIM identifikator ako već ne postoji.

Obično kreirate ciljnu asocijaciju za i5/OS profil, posebno u okolini jednostruke prijave. Nakon što koristite naredbu kreiranja potrebne ciljne asocijacije za korisnički profil (i EIM identifikator ako je potrebno), možda trebate kreirati i

odgovarajuću izvornu asocijaciju. Za kreiranje ciljne asocijacije za drugi korisnički identitet možete koristiti System i Navigator, na primjer za Kerberos principal pomoću kojeg se korisnik prijavljuje na mrežu.

Kada ste konfigurirali EIM na sistemu, specificirali ste korisnički identitet i lozinku koju će sistem koristiti kada izvodi EIM operacije za operacijski sistem. Ovaj korisnički identitet mora imati ovlaštenje kontrole pristupa EIM-u koje omogućuje kreiranje identifikatora i dodavanje asocijacija.

Lozinke i EIM profila i5/OS korisnika

Kao administrator, vaš primarni cilj za konfiguriranje EIM-a kao dijela okoline jednostruke prijave je smanjenje količine upravljanja korisničkim lozinkama koju morate izvesti za tipične krajnje korisnike u vašem poduzeću. Korištenjem mapiranja identiteta koje osigurava EIM u kombinaciji s Kerberos provjerom autentičnosti, znate da će vam korisnici izvoditi manje prijava i pamtiti i upravljati manjim brojem lozinki. Od toga imate koristi, jer imate manji broj poziva za rješavanje problema od mapiranih korisničkih identiteta kao što su pozivi za reset tih lozinki kada ih korisnici zaborave. Svakako, uloge lozinka sigurnosne politike su stalno djelotvorne i vi morate stalno upravljati tim korisničkim profilima za korisnike kada god istekne lozinka.

Za dalje prednosti vaše okoline jednostruke prijave, razmotrite promjenu postavki lozinke za one korisničke profile koji predstavljaju cilj mapiranja identiteta. Kao cilj mapiranja identiteta korisnik više ne treba osigurati lozinku za korisnički profil kada pristupa System i platformi ili EIM-omogućenom i5/OS resursu. Za najčešće korisnike, možete promijeniti postavke lozinke na *NONE tako da se ne mora koristiti lozinka s korisničkim profilom. Vlasnik korisničkog profila više ne treba lozinku zbog mapiranja identiteta kod jednostruke prijave. Postavljanjem lozinke na *NONE dobivate dodatnu pogodnost, jer vi i vaši korisnici više ne morate upravljati istekom lozinke; dodatno, ovaj profil nitko ne može koristiti za izravnu prijavu na System i platformu, ili za pristup EIM-omogućenim i5/OS resursima. Ipak, možda će vam više odgovarati da i dalje administratori imaju lozinke za svoje korisničke profile u slučaju da nekada zatrebaju prijavu izravno na System i platformu. Na primjer, ako vaš EIM kontroler domene nije funkcionalan i ako ne može doći do mapiranja identiteta, administrator treba imati mogućnost izravne prijave na System i platformu sve dok se ne riješe problemi s kontrolerom domene.

Srodni koncepti

“EIM kontrola pristupa” na stranici 38
Korisnik Mapiranja identiteta u poduzeću (EIM) je korisnik koji posjeduje kontrolu pristupa EIM-u baziranu na njegovom članstvu u preddefiniranoj korisničkoj grupi Lightweight Directory Access Protocol (LDAP) za specifičnu domenu.

Srodne informacije

Naredba Kreiranje profila korisnika (CRTUSRPRF)

i5/OS revidiranje za EIM

Važno je uzeti u obzir koju reviziju obavljate za vaš ukupni sigurnosni plan.

Kada konfigurirate i koristite Mapiranje identiteta u poduzeću (EIM), možda ćete htjeti konfigurirati podršku za reviziju za direktorij poslužitelja kako biste osigurali da vam se dobavi prikladna razina pouzdanosti koju vaša sigurnosna politika treba. Na primjer, podrška za reviziju može biti korisna kod određivanja koji je od korisnika mapiranih od strane asocijacije politike izveo akciju na vašem sistemu, ili promijenio objekt.

Srodne informacije

Revizija poslužitelja direktorija

EIM omogućene aplikacije za i5/OS

EIM može koristiti niz i5/OS aplikacija.

Sljedeće i5/OS aplikacije mogu biti konfigurirane da koriste Mapiranje identiteta u poduzeću (EIM):

- i5/OS glavni poslužitelji (trenutno ih koriste System i Access za Windows
- i System i Navigator)
- Telnet Poslužitelj (trenutno ga koriste PC5250 i IBM Websphere host po potrebi)
- QFileSrv.400 ODBC (dozvoljava korištenje jedne prijave preko SQL-a)

- JDBC (dozvoljava korištenje EIM-a preko SQL-a)
- Arhitektura Distribuirane Relacijske Baze Podataka (DRDA) (dozvoljava korištenje EIM-a preko SQL-a)
- IBM WebSphere Host On-Demand Verzija 8, (Web Express Logon funkcija)
- i5/OS NetServer
- QFileSvr.400

Scenariji: Mapiranje identiteta u poduzeću

Koristite ove informacije da naučite kako upravljati korisničkim identitetima na različitim sistemima unutar okoline jednostruke prijave.

Mapiranje identiteta u poduzeću (EIM) je tehnologija IBM infrastrukture koja vam omogućuje praćenje i upravljanje korisničkim identitetima u cijelom poduzeću. Obično EIM koristite s tehnologijom provjere autentičnosti, kao što je usluga provjere autentičnosti mreže za primjenu okoline jednostruke prijave.

Srodne informacije

Scenariji jednostruke prijave

Planiranje Mapiranja identiteta u poduzeću

Prije nego postavite EIM trebate razviti plan primjene Mapiranja identiteta u poduzeću (EIM) da osigurate da ste uspješno konfigurirali EIM za System i okolinu, ili u okolini više platformi.

Plan implementacije je bitan za uspješno konfiguriranje i upotrebu Mapiranja identiteta u poduzeću (EIM) u vašem poduzeću. Da razvijete plan, morate skupiti podatke o sistemima, aplikacijama i korisnicima koji će koristiti EIM. Skupljene informacije ćete koristiti za odluke o tome kako najbolje konfigurirati EIM za vaše poduzeće.

S obzirom da je EIM tehnologija IBM eServer infrastrukture dostupna za sve IBM platforme, način planiranja vaše primjene ovisi o tome koje platforme se mogu naći u vašem poduzeću. Iako postoji mnoštvo aktivnosti planiranja koje su specifične za svaku platformu, mnoge aktivnosti planiranja EIM-a odnose se na sve IBM platforme. Trebate raditi pomoću uobičajenih aktivnosti planiranja EIM-a za kreiranje cijelog plana implementacije. Da naučite više o tome kako planirati implementaciju EIM-a, pogledajte sljedeće stranice:

Planiranje Mapiranja identiteta u poduzeću za eServer

Plan implementacije je bitan za uspješno konfiguriranje i upotrebu Mapiranja identiteta u poduzeću (EIM) u poduzeću s pomiješanim platformama. Za razvoj vašeg plana implementacije trebate skupiti podatke o sistemima, aplikacijama i korisnicima koji će koristiti EIM. Skupljene informacije ćete koristiti za odluke o tome kako najbolje konfigurirati EIM u okruženju s miješanim platformama.

Sljedeća lista dobavlja putokaz zadataka planiranja koje bi trebali dovršiti prije konfiguriranja i korištenja EIM-a u okruženju s miješanim platformama. Proučite informacije na tim stranicama da naučite kako uspješno planirati potrebe za vašu EIM konfiguraciju što uključuje osobine koje treba vaš tim za implementaciju, informacije koje trebate skupiti i odluke konfiguriranja koje trebate donijeti. Bit će vam od pomoći ako ispišete radne tablice EIM planiranja (broj 8 na donjem popisu) tako da ih možete dovršiti kako prolazite kroz proces planiranja.

Zahtjevi postava Mapiranja identiteta u poduzeću za eServer

Za uspješnu primjenu Mapiranja identiteta u poduzeću (EIM), morate ispuniti tri zahtjeva: razinu poduzeća ili mreže, sistem i aplikaciju.

Zahtjevi na razini poduzeća ili mreže

Morate konfigurirati jedan sistem u vašem poduzeću ili mreži tako da se ponaša kao EIM kontroler domene što je posebno konfigurirani Lightweight Directory Access Protocol (LDAP) poslužitelj koji pohranjuje i dobavlja EIM podatke domene. Postoje brojna razmatranja kod izbora proizvoda za usluge direktorija za korištenje kao kontrolera domene, uključujući činjenicu da ne osiguravaju svi proizvodi LDAP poslužitelja podršku za EIM kontrolera domene.

Drugo što se mora uzeti u obzir je dostupnost administracijskih alata. Jedna je opcija korištenje EIM API-ja u vašim vlastitim aplikacijama za obavljanje administrativnih funkcija. Ako planirate koristiti IBM Tivoli Directory Server za i5/OS kao EIM kontroler domene, za upravljanje EIM-om možete koristiti System i Navigator. Ako planirate koristiti proizvod IBM Direktorij, možete koristiti eimadmin pomoćni program koji je dio V1R4 LDAP SPE.

Sljedeće informacije osiguravaju osnovne informacije o IBM platformama koje osiguravaju proizvod poslužitelja direktorija koji podržava EIM. Detaljnije informacije o izboru poslužitelja direktorija za osiguravanje podrške EIM kontroleru domene možete pronaći pod Planiranje EIM kontrolera domene.

Zahtjevi za sisteme i aplikacije

Svaki sistem koji sudjeluje u EIM domeni mora zadovoljavati sljedeće uvjete:

- Da ima instaliran LDAP klijentski softver.
- Da ima implementirane EIM API-je.

Svaka aplikacija koja će sudjelovati u EIM domeni mora moći koristiti EIM API-je za izvođenje operacija pregledavanja mapiranja i ostalih operacija.

Bilješka: U slučaju distribuirane aplikacije, nije potrebno da i poslužiteljska strana i klijentska strana trebaju biti sposobni koristiti EIM API-je. Tipično, samo poslužiteljska strana aplikacije treba moći koristiti EIM API-je.

Sljedeća tablica omogućuje informacije o EIM podršci koju osiguravaju eServer platforme. Informacije su organizirane po platformi sa stupcima koji imaju sljedeće značenje:

- EIM klijent koji je potreban platformi za podršku EIM API-ja.
- Tipovi EIM konfiguracijskih i administracijskih alata dostupnih za platformu.
- Proizvod poslužitelja direktorija koji se može instalirati za platformu kako bi služio kao EIM kontroler domene.

Platforma ne treba biti sposobna služiti kao EIM kontroler domene da bi sudjelovala u EIM domeni.

Tablica 9. eServer EIM podrška

Platforma	EIM klijent (API podrška)	Kontroler domene	EIM administracijski alati
AIX na System p	AIX R5.2	IBM Directory V5.1	Nedostupan
Linux • SLES8 na PPC64 • Red Hat 7.3 na i386 • SLES7 na System z	Spustite jedno od sljedećeg: • IBM Direktorij V4.1 klijent • IBM Direktorij V5.1 klijent • Otvorite LDAP v2.0.23 klijenta	IBM Directory V5.1	Nedostupan
i5/OS na System i	i5/OS V5R3, ili novija verzija	IBM Tivoli Directory Server za i5/OS	System i Navigator
Windows 2000 na System x	Spustite jedno od sljedećeg: • IBM Direktorij V4.1 klijent • IBM Direktorij V5.1 klijent	IBM Direktorij V5.1 klijent	Nedostupan
z/OS na System z	z/OS V1R4 LDAP SPE OW57137	z/OS V1R4 LDAP	V1R4 LDAP SPE OW57137

Sve dok platforma osigurava EIM klijent (API) podršku da sistem može sudjelovati u EIM domeni. Nije potrebno da platforma osigurava podršku EIM kontrolera domene sve dok ne želite koristiti ovu posebnu platformu kao EIM kontroler domene za vaše poduzeće.

Srodne informacije

IBM Tivoli Directory Server

Identifikacija potrebnih sposobnosti i uloga

Mapiranje identiteta u poduzeću (EIM) je oblikovano tako da jedna osoba može jednostavno biti odgovorna za konfiguriranje i administriranje u maloj organizaciji. Ili u većim organizacijama, možda želite imati veći broj različitih pojedinaca koji rukuju tim odgovornostima.

Broj ljudi koji trebate u vašem timu ovisi o broju zahtijevanih sposobnosti koje posjeduje svaki član tima, o tipovima platformi koje su uključene u vašu EIM implementaciju i o tome kako vaša organizacija želi podijeliti svoje sigurnosne uloge i odgovornosti.

Uspješna EIM implementacija treba konfiguraciju i interakciju nekoliko softverskih proizvoda. Zato što svaki od tih proizvoda treba posebne sposobnosti i uloge, možete se odlučiti kreirati tim za EIM implementaciju koji se sastoji od ljudi iz nekoliko različitih područja, naročito ako radite u velikoj organizaciji.

Sljedeće informacije opisuju sposobnosti i ovlaštenje za kontrolu EIM pristupa potrebne za uspješnu implementaciju EIM-a. Te sposobnosti su predstavljene u obliku naziva zanimanja za ljude koji su specijalizirani za te sposobnosti. Na primjer, zadatak koji traži Lightweight Directory Access Protocol (LDAP) osobine se odnosi na zadatak za administratora Poslužitelja direktorija.

Članovi tima i njihove uloge

Sljedeće informacije opisuju odgovornosti i potrebno ovlaštenje uloga koje su potrebne za upravljanje EIM-om. Možete se koristiti ovom listom uloga kako bi odredili članove tima koji su potrebni za instaliranje i konfiguriranje preduvjetnih proizvoda i za konfiguriranje EIM-a i jedne ili više EIM domena.

Jedan od prvih skupova uloga koje trebate definirati je broj i tip administratora za vašu EIM domenu. Svo osoblje kojemu su dane EIM administrativne obaveze i ovlaštenje trebaju se uključiti u proces planiranja EIM-a kao članovi tima za EIM implementaciju.

Bilješka: EIM administratori imaju važnu ulogu u vašoj organizaciji i imaju takve ovlasti kao osobe da im je dozvoljeno kreiranje korisničkih identiteta na vašim sistemima. Kada kreirate EIM asocijacije za korisničke identitete, oni određuju tko može pristupiti vašim računalnim sistemima i s kakvim povlasticama. IBM preporuča da date ovo ovlaštenje onim osobama u koje imate visoku razinu povjerenja baziranu na sigurnosnoj politici vašeg poduzeća.

Sljedeća tablica ispisuje uloge potencijalnog člana tima i zadatke i potrebne sposobnosti za konfiguriranje i upravljanje EIM-om.

Bilješka: Ako će neka osoba u vašoj organizaciji biti odgovorna za sve zadatke EIM konfiguriranja i administracije, toj bi se osobi trebala dati uloga i ovlaštenje EIM administratora.

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

Uloga	Ovlašteni zadaci	Potrebne osobine
EIM administrator	• Koordinacija operacija na domeni • Dodavanje, uklanjanje i mijenjanje definicija registra, EIM identifikatora i asocijacija za korisničke identitete • Kontroler ovlaštenja za podatke unutar EIM domene	Znanje o alatima za EIM administraciju

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

Uloga	Ovlašteni zadaci	Potrebne osobine
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) • Ažuriranje definicija EIM registra	Znanje o: • Svim korisničkim registrima definiranih u EIM domeni (kao što su informacije o korisničkim identitetima) • Alatima EIM administracije
Administrator EIM registra X	Upravljanje određenom definicijom EIM registra: • Dodavanje i uklanjanje ciljnih asocijacija za određeni registar korisnika (na primjer, registar X) • Ažuriranje određene definicije EIM registra	Znanje o: • Posebnom korisničkom registru definiranom u EIM domeni (kao što su informacije o korisničkim identitetima) • Alatima EIM administracije
Administrator poslužitelja direktorija (LDAP)	• Instaliranje i konfiguriranje poslužitelja direktorija (ako je potrebno) • Prilagodba konfiguracije poslužitelja direktorija za EIM • Kreiranje EIM domene (pogledati opasku) • Definiranje korisnika koji imaju ovlaštenje pristupa EIM kontroleru domene • Opcijski: Definiranje prvog EIM administratora **Bilješka:** Administrator poslužitelja direktorija može činiti sve što može i EIM administrator.	Znanje o: • Instaliranje, konfiguriranje i prilagodba poslužitelja direktorija • EIM administracijski alati
Administrator registra korisnika	• Postavljanje korisničkog profila ili korisničkog identiteta za određeni registar korisnika • Opcijski: Služenje kao EIM administrator registra za određeni registar korisnika	Znanje o: • Alati za administraciju registra korisnika • EIM administracijski alati
Sistemski programer ili sistemski administrator	Instaliranje potrebnih softverskih proizvoda (uključuje i instaliranje EIM-a)	Znanje o: • Sistemsko programiranje i administracijske osobine • Instalacijske procedure za platformu
Programer aplikacije	Pisanje aplikacija koje koriste EIM API-je	Znanje o: • Platforma • Programerske osobine • Kompiliranje programa

Srodni koncepti

"EIM kontrola pristupa" na stranici 38
Korisnik Mapiranja identiteta u poduzeću (EIM) je korisnik koji posjeduje kontrolu pristupa EIM-u baziranu na njegovom članstvu u preddefiniranoj korisničkoj grupi Lightweight Directory Access Protocol (LDAP) za specifičnu domenu.

Planiranje domene Mapiranja identiteta u poduzeću

Dio početnog procesa planiranja implementacije Mapiranja identiteta u poduzeću (EIM) zahtijeva da definirate EIM domenu. Za postizanje maksimalne koristi od posjedovanja centraliziranog repozitorija informacija o mapiranju, trebate planirati domenu koja će biti dijeljena između nekih aplikacija i sistema.

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

Sljedeća tablica ispisuje informacije koje trebate skupiti prilikom planiranja vaše domene i predlaže 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 vaše organizacije. Na primjer, u manjoj organizaciji preferirate imenovati pojedinu osobu za EIM administratora koja će 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 već postoji domena za upotrebu koja zadovoljava vaše potrebe ili je pak trebate kreirati.	EIM administrator
2. Koji će se poslužitelj direktorija ponašati kao EIM kontroler domene. (Pregledajte "Planiranje kontrolera domene Mapiranja identiteta u poduzeću" za detaljne informacije o izboru kontrolera domene.)	Administrator poslužitelja direktorija (LDAP) ili EIM administrator
3. Ime za domenu. (Također možete dobaviti opcijski opis.)	EIM administrator
4. Gdje u direktoriju pohraniti EIM podatke o domeni. **Bilješka:** Ovisno o vašem izboru sistema koji će biti host poslužitelju direktorija i vašem izboru direktorija za pohranu podataka o EIM domeni, trebate izvesti neke zadatke konfiguriranja usluga direktorija prije no što kreirate domenu.	I administrator poslužitelja direktorija (LDAP) i EIM administrator
5. Aplikacije i operacijski sistemi koji će sudjelovati u domeni. Ako konfigurirate vašu prvu domenu, ovaj početni skup se može sastojati od samo jednog sistema. (Pregledajte "Razvijanje plana imenovanja za definiciju registra Mapiranja identiteta u poduzeću" na stranici 58 za više informacija.)	EIM tim
6. Ljudi i cjeline koji će sudjelovati u domeni. **Bilješka:** Kako bi olakšali početno testiranje, mogli biste ograničiti broj sudionika na jedan ili dva.	EIM tim

Planiranje kontrolera domene Mapiranja identiteta u poduzeću

Prilikom prikupljanja informacija koje definiraju domenu Mapiranja identiteta u poduzeću (EIM) morate odrediti koji proizvodi poslužitelja direktorija će se ponašati kao EIM kontroleri domene.

EIM zahtijeva da je kontroler domene smješten na poslužitelju direktorija koji podržava verziju 3 Lightweight Directory Access Protocola (LDAP). Dodatno, proizvod poslužitelja direktorija mora biti konfiguriran tako da prihvaća LDAP shemu i ostala razmatranja za EIM i razumije određene atribute i objektne klase.

Ako vaše poduzeće posjeduje više od jednog poslužitelja direktorija koji može biti host EIM kontroleru domene, trebali biste također razmotriti da li koristiti sekundarno replicirane kontrolere domene. Na primjer, ako očekujete da ćete imati veliki broj operacija EIM pregledavanja mapiranja, replike mogu poboljšati performansu operacija pregledavanja.

Također trebate razmotriti da li postaviti *lokalni* ili *udaljeni* kontroler domene u odnosu na sistem za koji se očekuje da će izvoditi najveći broj operacija pregledavanja mapiranja. S lokalno postavljenim kontrolerom domene u odnosu na visoko opterećeni sistem, možete poboljšati performansu operacija pregledavanja na lokalnom sistemu. Koristite radne tablice za zapis tih odluka planiranja kao i one tablice koje ste napravili za informacije o vašoj domeni i ostale informacije o direktoriju.

Nakon što ste odredili koji će poslužitelj direktorija u vašem poduzeću biti host vašem EIM kontroleru domene, trebate donijeti neke odluke o pristupu kontroleru domene.

Planiranje pristupa kontrolera domene

Trebate planirati kako ćete vi i EIM omogućene aplikacije i operacijski sistemi pristupati poslužitelju 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 član kontrolne grupe za EIM pristup ili LDAP administrator. Pogledajte Upravljanje kontrolom EIM pristupa za više informacija.

Izaberite tip povezivanja EIM

EIM API-ji podržavaju nekoliko različitih mehanizama za uspostavu povezivanja, također poznati pod nazivom vezivanje, s EIM kontrolerom domene. Svaki tip mehanizma vezivanja omogućava različite razine provjere autentičnosti i šifriranje za povezivanje. Mogući izbori su:

Jednostavne veze
Jednostavna veza je LDAP veza gdje LDAP klijenti osiguravaju razlikovno ime veze i lozinku veze LDAP poslužitelju radi provjere autentičnosti. Razlikovno ime vezivanja i lozinka su definirani od strane LDAP administratora u LDAP direktoriju. To je najslabiji oblik provjere autentičnosti i najmanje siguran, jer su razlikovno ime vezivanja i lozinka poslani poslužitelju bez šifriranja i ranjivi su na tajno praćenje protoka informacija. Koristite CRAM-MD5 (challenge-response authentication mechanism) da postavite dodatnu razinu zaštite za vezujuću lozinku. S CRAM-MD5 protokolom, klijent šalje raspršenu vrijednost umjesto čistog teksta lozinke poslužitelju za provjeru autentičnosti.

Provjera autentičnosti poslužitelja pomoću Sloja sigurnih utičnica (SSL) - provjera autentičnosti sa strane poslužitelja
LDAP poslužitelj može biti konfiguriran za SSL ili TLS (Sigurnost prijenosnog sloja) veze. LDAP poslužitelj koristi digitalni certifikat za provjeru autentičnosti poslužitelja na LDAP klijentu i uspostavlja sesiju šifrirane komunikacije između njih. Po značenju certifikata provjerava se autentičnost samo LDAP poslužitelja. Autentičnost krajnjeg korisnika se provjerava preko značenja razlikovnog imena vezivanja i lozinke. Snaga provjere autentičnosti je ista kao i kod jednostavnog vezivanja samo što se svi podaci (uključujući razlikovno ime vezivanja i lozinka) šifriraju zbog privatnosti.

Provjera autentičnosti klijenta pomoću SSL-a
LDAP poslužitelj može biti konfiguriran da zahtijeva provjeru autentičnosti krajnjeg korisnika pomoću digitalnih certifikata umjesto pomoću razlikovnog imena veze i lozinke za SSL ili TLS sigurne veze na LDAP poslužitelj. Provjerava se autentičnost i klijenta i poslužitelja, a sesija je šifrirana. Ova opcija osigurava jaču razinu provjere autentičnosti korisnika i štiti privatnost svih podataka koji se prenose.

Kerberos provjera autentičnosti
LDAP klijentu može biti provjerena autentičnost na poslužitelju pomoću Kerberos ulaznice kao opcijske zamjene za razlikovno ime i lozinku veze. (Kerberos), kao provjereni sistem provjere autentičnosti mreže preko treće strane, dozvoljava principalu (korisniku ili usluzi) da dokaže svoj identitet drugoj usluzi unutar nesigurne mreže. Provjera autentičnosti principala se izvodi preko centraliziranog poslužitelja pod nazivom centar distribucije ključa (KDC). KDC provjerava korisnika s Kerberos ulaznicom. Te ulaznice dokazuju

principalov identitet drugim uslugama na mreži. Nakon što se provjerila autentičnost principala preko tih ulaznica, principal i usluga mogu izmjenjivati šifrirane podatke s ciljnom uslugom. Ova opcija osigurava jaču razinu provjere autentičnosti korisnika i štiti privatnost informacija provjere autentičnosti.

Izbor mehanizama vezivanja ovisi o razini sigurnosti koju trebaju EIM-omogućena aplikacija i mehanizmi provjere autentičnosti koje podržava LDAP poslužitelj kao host EIM domeni.

Također, možda trebate izvesti dodatne zadatke konfiguracije LDAP poslužitelja kako bi omogućili mehanizam koji ste odlučili koristiti. Provjerite dokumentaciju LDAP poslužitelja koji je host vašem kontroleru domene kako bi odredili koje ostale konfiguracijske zadatke možda trebate izvesti.

Primjer planiranja radne tablice: informacije kontrolera domene

Nakon odluka koje ste donijeli o vašem EIM kontroleru domene, upotrijebite radne tablice za zapis informacija o EIM kontroleru domene koje trebaju vaši EIM-omogućeni operacijski sistemi i aplikacije. Informacije koje ste skupili kao dio ovog procesa može koristiti LDAP administrator za definiciju identiteta vezivanja aplikacije ili operacijskog sistema na LDAP poslužitelju direktorija koji je host EIM kontroleru domene.

Sljedeći dio uzorka radnih tablica planiranja pokazuje tip informacija koje trebate skupiti. Također su uključeni 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 poduzeća, odjela ili aplikacije koja koristi domenu.	MojaDomena
Opcijski: Ako konfigurirate EIM domenu u već postojećem LDAP direktoriju, specificirajte nadređeno razlikovno ime za domenu. To je razlikovno ime koje predstavlja unos odmah iznad unosa imena vaše domene u stablastoj hijerarhiji informacija o direktoriju, na primjer, o=ibm,c=us.	o=ibm,c=us
Rezultirajuće potpuno kvalificirano razlikovno ime EIM domene. To je potpuno definirano ime EIM domenu koje opisuje smještaj 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 nadređenog DN-a za domenu tada se potpuno kvalificirani DN domene sastoji od relativnog DN-a domene (ibm-eimDomainName=), imena domene (MyDomain) i nadređenog DN-a (o=ibm,c=us). **Bilješka:**	Bilo što od sljedećeg, ovisno da li ste izabrali nadređeni 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 sljedeće informacije:	ldap://
• Opcijski: Host ime ili IP adresa • Opcijski: Broj porta	• some.ldap.host • 389
Rezultirajuća potpuna adresa povezivanja za kontroler domene.	ldap://some.ldap.host:389
Mehanizam vezivanja potreban za aplikacije ili sisteme. Izbori uključuju: • Jednostavno vezivanje • CRAM MD5 • Provjera autentičnosti poslužitelja • Provjera autentičnosti klijenta • Kerberos	Kerberos

Ako se vaš tim za EIM konfiguraciju i administraciju sastoji od više članova tima, trebat ćete odrediti identitet vezivanja i mehanizam koji će koristiti svaki član tima za pristup EIM domeni baziran na njegovoj ulozi. Također, trebate odrediti identitet vezivanja i mehanizam za krajnje korisnike EIM aplikacije. Sljedeća bi vam radna tablica mogla pomoći kao primjer skupljanja ovih informacija.

Tablica 13. Primjer radne tablice planiranja identiteta vezivanja

EIM ovlaštenje 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 određenom definicijom registra
EIM pregledavanje mapiranja	cn=MyApp,c=US	jednostavno vezivanje	izvođenje operacija pregledavanja mapiranja aplikacije

Razvijanje plana imenovanja za definiciju registra Mapiranja identiteta u poduzeću

Da bi se korištenjem Mapiranja identiteta u poduzeću (EIM) mapirao korisnički identitet iz jednog registra korisnika u ekvivalentan korisnički identitet u drugom registru korisnika, oba registra korisnika moraju biti definirana u EIM-u.

Morate kreirati EIM definiciju registra za svaku aplikaciju ili registar korisnika operativnog sistema koji će sudjelovati u EIM domeni. Registri korisnika mogu predstavljati registre operacijskog sistema poput Resource Access Control Facility (RACF) ili i5/OS-a, razdijeljen registar poput Kerberosa ili podskup registra sistema korišten isključivo od strane aplikacije.

EIM domena može sadržavati definicije registra za korisničke registre koji postoje na platformi. Na primjer, domena upravljana od strane kontrolera domene na i5/OS može sadržavati definicije registra za ne-i5/OS platforme (poput registra AIX-a). Premda možete definirati bilo koji korisnički registar na EIM domeni, definiraju se korisnički registri za one aplikacije i operacijske sisteme koji su EIM-omogućeni.

Možete imenovati definiciju EIM registra kako god želite sve dok je ime jedinstveno u EIM domeni. Na primjer, možete imenovati definiciju EIM registra na osnovu imena sistema koji je host korisničkom registru. Ako to nije dovoljno za razlikovanje definicija registra od sličnih definicija, možete koristiti točku (.) ili podcrtavanje (_) za dodavanje tipa korisničkog registra koji definirate. Bez obzira na kriterije izabrane za korištenje, trebali bi razmotriti razvoj konvencije imenovanja za vaše definicije EIM registra. Čineći to osiguravate konzistentnost imena definicije po cijeloj domeni kao i prikladan opis tipa i instance definiranog korisničkog registra i njegovog korištenja. Na primjer, možete izabrati ime svake definicije registra upotrebom kombinacije imena aplikacije ili operacijskog sistema koji koristi registar i fizičke lokacije korisničkog registra u poduzeću.

Aplikacija koja je napisana za korištenje EIM-a može specificirati zamjensko ime izvornog registra ili zamjensko ime ciljnog registra ili zamjenska imena za oboje. Kada kreirate definicije EIM registra, trebate provjeriti dokumentaciju vaših aplikacija kako biste odredili da li trebate specificirati jedno ili više zamjenskih imena za definicije registra. Kada ova zamjenska imena dodijelite odgovarajućim definicijama registra, aplikacija može izvesti pregledavanje zamjenskog imena da bi pronašla EIM definiciju registra ili definicije koje odgovaraju zamjenskim imenima u aplikaciji.

Sljedeći vam dio primjera radne tablice planiranja može pomoći kao vodič za korištenje zapisivanja informacija o sudjelovanju korisničkih registara. Možete koristiti stvarnu radnu tablicu za specificiranje imena definicije registra za svaki korisnički registar, za specificiranje da li koristi zamjensko ime i za opis i korištenje lokacije korisničkog registra. Dokumentacija za instalaciju i konfiguraciju aplikacije će osigurati neke informacije koje trebate za radnu tablicu.

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

Ime definicije registra	Tip korisničkog registra	Pseudonim definicije registra	Opis registra
Sistem_C	i5/OS sistemski registar korisnika	Pregled dokumentacije uz aplikaciju	Registar korisnika glavnog sistema za i5/OS na Sistemu C
Sistem_A_WAS	WebSphere LTPA	app_23_alias_source	WebSphere LTPA registar korisnika na Sistemu A
Sistem_B	Linux	Pregled dokumentacije uz aplikaciju	Linux registar korisnika na Sistemu B
Sistem_A	i5/OS sistemski registar korisnika	app_23_alias_target app_xx_alias_target	Registar korisnika glavnog sistema za i5/OS na Sistemu A
Sistem_D	Kerberos korisnički registar	app_xx_alias_source	legal.mydomain.com Kerberos područje
Sistem_4	Windows 2000 registar korisnika	Pregled dokumentacije uz aplikaciju	Korisnički registar aplikacije ljudskih resursa na Sistemu 4

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

Nakon što dovršite ovu sekciju radne tablice planiranja, trebali biste razviti vaš plan mapiranja identiteta kako bi odredili da li koristiti asocijacije identifikatora, asocijacije politike ili oba tipa asocijacija za kreiranje mapiranja koja trebate za korisničke identitete u svakom definiranom korisničkom registru.

Razvoj plana mapiranja identiteta

Za kritični dio početnog procesa planiranja implementacije Mapiranja identiteta u poduzeću (EIM) je potrebno odrediti kako želite koristiti mapiranje identiteta u vašem poduzeću.

Postoje dvije metode koje možete koristiti za mapiranje identiteta u EIM-u:

- **Asocijacije identifikatora** opisuju odnose između nekog EIM identifikatora i korisničkih identiteta u korisničkim registrima koji predstavljaju tu osobu. Asocijacija identifikatora kreira izravno jedan-prema-jedan mapiranje između nekog EIM identifikatora i određenog korisničkog identiteta. Asocijacije identifikatora možete koristiti za indirektno definiranje odnosa između korisničkih identiteta upotrebom EIM identifikatora.

  Ako vaša sigurnosna politika treba visok stupanj detaljne pouzdanosti, trebat ćete koristiti gotovo isključivo asocijacije identifikatora za vašu implementaciju mapiranja identiteta. Zato što koristite asocijacije identiteta za kreiranje jedan-prema-jedan mapiranja za korisničke identitete koje korisnici posjeduju, moći ćete uvijek odrediti točno tko je obavio akciju na nekom objektu ili na sistemu.
- **Asocijacije politike** opisuju odnos između višestrukih korisničkih identiteta i pojedinačnog korisničkog identiteta u korisničkom registru. Asocijacije politike koriste podršku politike EIM mapiranja za kreiranje više-prema-jedan mapiranja između korisničkih identiteta bez uključivanja EIM identifikatora.

  Asocijacije politike mogu biti korisne kada imate jednu ili više velikih grupa korisnika koji trebaju pristup sistemima ili aplikacijama u vašem poduzeću, a pritom ne želite da imaju određene korisničke identitete za dobivanje tog pristupa. Na primjer, održavate Web aplikaciju koja pristupa određenoj internoj aplikaciji. Ne želite pritom postaviti stotine ili tisuće korisničkih identiteta kako biste ovlastili korisnike za te interne aplikacije. U tom slučaju želite konfigurirati mapiranje identiteta tako da su svi korisnici ove Web aplikacije mapirani u jedan korisnički identitet s najmanjom razinom ovlaštenja potrebnom za izvođenje aplikacije. Taj tip mapiranja identiteta možete napraviti korištenjem asocijacija politike.

Možda odlučite koristiti asocijacije identifikatora kako biste osigurali najbolju kontrolu korisničkih identiteta u vašem poduzeću dobivajući pritom visok stupanj upravljanja pojednostavljenom lozinkom. Ili, možda odlučite koristiti kombinaciju asocijacija politika i asocijacija identifikatora za oblikovanje jednostruke prijave tamo gdje je to prikladno, uz održavanje određene kontrole nad korisničkim identitetima za administratore. Bez obzira na tip mapiranja identiteta za koji ste odlučili da najbolje odgovara vašim poslovnim potrebama i da je prikladan za vašu sigurnosnu politiku, trebate kreirati plan mapiranja kako biste osigurali prikladno implementiranje mapiranja identiteta.

Za kreiranje plana mapiranja identiteta, trebate učiniti sljedeće:

Srodni koncepti

“Kreiranje EIM asocijacija” na stranici 98
Dva su različita tipa EIM asocijacija koja možete kreirati. Možete kreirati ili asocijaciju identifikatora ili asocijaciju politike.

“Kreiranje asocijacije politike” na stranici 99
Asocijacija politike je sredstvo za direktno definiranje odnosa između višestrukih korisničkih identiteta u jednom ili više registara i individualnog ciljnog korisničkog identiteta u drugom registru.

Planiranje asocijacija Mapiranja identiteta u poduzeću:

Asocijacije su unosi koje kreirate o domeni Mapiranja identiteta u poduzeću (EIM) radi definiranja odnosa između korisničkih identiteta u različitim registrima korisnika.

U EIM-u možete kreirati jedan od dva tipa asocijacija: asocijacije identifikatora za definiranje jedan-prema-jedan mapiranja i asocijacije politika za definiranje više-prema-jedan mapiranja. Asocijacije politika možete koristiti umjesto ili u kombinaciji s asocijacijama identifikatora.

Određeni tipovi asocijacija koje ste odlučili kreirati ovise o tome kako korisnik koristi određeni korisnički identitet kao i o sveukupnom planu mapiranja identiteta.

Možete kreirati bilo koji od sljedećih tipova asocijacija identifikatora:

- **Ciljne asocijacije**

  Ciljne asocijacije se definiraju za korisnike koji u pravilu samo pristupaju ovom sistemu kao poslužitelju 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 korisnički identitet prvo što korisnik osigura za prijavu na sistemu ili mreži. Ovaj se tip asocijacije koristi kada neka aplikacija izvodi operacije pregledavanja mapiranja.
- **Administrativne asocijacije**

  Administrativne se asocijacije definiraju kada se želite osposobiti za traženje činjenice da korisnički identitet pripada određenom korisniku, a ne želite da korisnički identitet bude dostupan operacijama pregledavanja mapiranja. Možete koristiti ovaj tip asocijacije za traženje svih korisničkih identiteta koje osoba koristi u poduzeću.

Asocijacija politike uvijek definira ciljnu asocijaciju.

Moguće je da definicija jednostrukog registra ima više od jednog tipa asocijacije ovisno o tome kako se koristi korisnički registar na koji se definicija odnosi. Premda ne postoje ograničenja na broj ili kombinacije asocijacija koje možete definirati, držite broj na minimumu kako bi pojednostavili administraciju vaše EIM domene.

Obično će aplikacija osigurati upute o tome koje definicije registra očekuje 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 može biti jedan-prema-jedan mapiranje između njezinog jedinstvenog EIM identifikatora i korisničkog identiteta u potrebnom ciljnom registru ili više-prema-jedan mapiranje između izvornog registra čiji je korisnički identitet član 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 korisničke identitete u vašoj organizaciji s informacijama o EIM identifikatorima i potrebnim EIM definicijama registra. Sada trebate spojiti te informacije specificiranjem tipova asocijacija koje želite koristiti za mapiranje korisničkih identiteta u vašem poduzeću. Trebate odrediti da li definirati asocijaciju politike za određenu aplikaciju i njezin registar korisnika ili definirati određene asocijacije identifikatora (izvorne, ciljne ili administrativne) za svaki korisnički identitet u sistemu ili registru aplikacije. To možete učiniti zapisivanjem informacija o potrebnim tipovima asocijacije i u radnoj tablici planiranja definicije registra i u odgovarajućim recima svake radne tablice asocijacija.

Za dovršetak vašeg plana mapiranja identiteta, možete koristiti sljedeći primjer radnih tablica kao vodič za pomoć 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 korisničkog registra	Pseudonim definicije registra	Opis registra	Tipovi asocijacija
Sistem_C	i5/OS sistemski registar korisnika	Pregled dokumentacije uz aplikaciju	Registar korisnika glavnog sistema za i5/OS na Sistemu C	Ciljni
Sistem_A_WAS	WebSphere LTPA	app_23_alias_source	WebSphere LTPA registar korisnika na Sistemu A	Primarni izvor
Sistem_B	Linux	Pregled dokumentacije uz aplikaciju	Linux registar korisnika na Sistemu B	Izvorni i ciljni
Sistem_A	i5/OS sistemski registar korisnika	app_23_alias_target app_xx_alias_target	Registar korisnika glavnog sistema za i5/OS na Sistemu A	Ciljni
Sistem_D	Kerberos korisnički registar	app_xx_alias_source	legal.mydomain.com Kerberos područje	Izvorni
Sistem_4	Windows 2000 registar korisnika	Pregled dokumentacije uz aplikaciju	Korisnički registar aplikacije ljudskih resursa na Sistemu 4	Administrativni
order.mydomain.com	Windows 2000 registar korisnika		Glavni registar prijave za zaposlenike odjela nabave	Default politika registra (izvorni registar)
System_A_order_app	Aplikacija Odjela Nabave		Specifični registar aplikacije za ažuriranja u nabavi	Default politika registra (ciljni registar)
System_C_order_app	Aplikacija Odjela Nabave		Specifični registar aplikacije za ažuriranja 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_____		
Korisnički registar	**Korisnički identitet**	**Tipovi asocijacija**
Sistem A WAS na Sistemu A	johnday	Izvorni
Linux na Sistemu B	jsd1	Izvorni i ciljni
i5/OS 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 korisnički registar	Ciljni korisnički registar	Korisnički identitet	Opis
Default registar	order.mydomain.com	System_A_order_app	SYSUSERA	Mapira autentičnog Windows korisnika odjela nabave u prikladan korisnički identitet aplikacije
Default registar	order.mydomain.com	System_C_order_app	SYSUSERB	Mapira autentičnog Windows korisnika odjela nabave u prikladan korisnički identitet aplikacije

Razvijanje plana imenovanja EIM identifikatora:

Kod planiranja potreba za Mapiranjem identiteta u poduzeću (EIM), možete kreirati jedinstvene EIM identifikatore za korisnike EIM-omogućenih aplikacija i operativnih sistema u vašem poduzeću kada želite kreirate jedan-prema-jedan mapiranja između korisničkih identiteta korisnika. Upotrebom asocijacija identifikatora za kreiranje jedan-prema-jedan mapiranja možete maksimizirati koristi od upravljanja lozinkom koje omogućava EIM.

Plan imenovanja koji ste razvili ovisi o vašim poslovnim potrebama i preferencama; jedini zahtjev na imena EIM identifikatora je da budu jedinstveni. Neka poduzeća mogu preferirati korištenje potpunog i zakonitog imena za svaku osobu; druga poduzeća mogu preferirati korištenje drugog tipa podataka, kao npr. zaposleničkog broja za svaku osobu. Ako želite kreirati imena EIM identifikatora bazirana na potpunom imenu svake osobe, možete anticipirati moguće dupliciranje imena. Kako ćete rukovati s potencijalnim duplim imenima identifikatora stvar je osobne preference. Možda biste željeli rukovati svakim slučajem ručno s dodavanjem predodređenog niza znakova u svako ime identifikatora za osiguranje jedinstvenosti; na primjer mogli biste odlučiti dodati broj odjela svake osobe.

Kao dio razvoja plana imenovanja EIM identifikatora, trebate se odlučiti na ukupnom planu mapiranja identiteta. To vam može pomoći da odlučite kada trebate koristiti identifikatore i asocijacije identifikatora, a kada asocijacije politike za mapiranje identiteta unutar vašeg poduzeća. Za razvoj plana imenovanja EIM identifikatora, možete koristiti dolje navedenu radnu tablicu za pomoć prilikom skupljanja informacija o korisničkim identitetima u vašoj organizaciji i planiranju EIM identifikatora za korisničke 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 može navesti zamjensko ime koje koristi za pronalazak odgovarajućeg EIM identifikatora za aplikaciju kojeg ista može koristiti u zamjenu za određivanje određenog korisničkog identiteta koji će koristiti. Trebate provjeriti dokumentaciju vaših aplikacija da odredite da li trebate specificirati jedno ili više zamjenskih imena za identifikator. Opisna polja EIM identifikatora ili korisničkog identiteta nemaju formu i mogu se koristiti za dobavu opisnih informacija o korisniku.

Ne trebate odjednom kreirati EIM identifikatore za sve članove vašeg poduzeća. Nakon kreiranja početnog EIM identifikatora i njegovog korištenja za provjeru vaše EIM konfiguracije, možete kreirati dodatne EIM identifikatore bazirane na ciljevima korištenja EIM-a u vašoj organizaciji. Na primjer, možete dodati EIM identifikatore za područje odjela ili šire područje. Ili, možete dodati EIM identifikatore kako podižete dodatne EIM aplikacije.

Nakon što skupite potrebne informacije za razvoj plana imenovanja EIM identifikatora, možete planirati asocijacije za vaše korisničke identitete.

Radne tablice za planiranje implementacije Mapiranja identiteta u poduzeću

Dok ste radili s procesom planiranja Mapiranja identiteta u poduzeću (EIM), mogli ste primijetiti da je korisno korištenje tih radnih tablica za skupljanje informacija koje ćete trebati za konfiguraciju i korištenje EIM-a u vašem poduzeću. Dani su prikladni primjeri dovršenih odlomaka radnih tablica na stranicama za planiranje.

Te su radne tablice dane kao primjer tipova radnih tablica koje trebate za kreiranje vašeg plana EIM implementacije. Broj osiguranih unosa je manji od broja koji ćete vjerojatno trebati za vaše EIM informacije. Možete uređivati te radne tablice kako biste ih prilagodili vašoj situaciji.

Tablica 20. Radna tablica informacija o domeni i kontroleru domene

Informacije potrebne za konfiguriranje EIM domene i kontrolera domene	**Odgovori**
Smisleno ime za domenu. To bi moglo biti ime poduzeća, odjela ili aplikacije koja koristi domenu.	
Opcijski: Razlikovno ime po nadređenom za domenu. To je razlikovno ime koje predstavlja unos odmah iznad unosa imena vaše domene u stablastoj hijerarhiji informacija o direktoriju, na primjer, o=ibm,c=us.	
Rezultirajuće potpuno kvalificirano razlikovno ime EIM domene. To je potpuno definirano ime EIM domenu koje opisuje smještaj 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 nadređenog DN-a za domenu tada se potpuno kvalificirani DN domene sastoji od relativnog DN-a domene (ibm-eimDomainName=), imena domene (MyDomain) i nadređenog 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 sljedeće informacije:	
• Opcijski: Host ime ili IP adresa • Opcijski: Broj porta	
Rezultirajuća potpuna adresa povezivanja za kontroler domene.	
Mehanizam vezivanja potreban za aplikacije ili sisteme. Izbori uključuju: • Jednostavno vezivanje • CRAM MD5 • Provjera autentičnosti poslužitelja • Provjera autentičnosti klijenta • Kerberos	

Pregledajte Planiranje EIM kontrolera domene kao primjer kako koristiti ovu radnu tablicu.

Tablica 21. Radna tablica za planiranje identiteta vezivanja

EIM ovlaštenje ili uloga	**Vezujući identitet**	**Vezujući mehanizam**	**Potreban razlog**

Tablica 21. Radna tablica za planiranje identiteta vezivanja (nastavak)

Pregledajte Planiranje EIM kontrolera domene kao primjer kako koristiti ovu radnu tablicu.

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

Ime definicije registra	Tip registra korisnika	Zamjensko ime definicije registra	Opis registra	Tipovi asocijacija

Pregledajte Razvoj plana imenovanja definicije EIM registra kao primjer kako koristiti ovu radnu tablicu.

Tablica 23. Radna tablica za planiranje EIM identifikatora

Jedinstveno ime identifikatora	Opis identifikatora ili identiteta korisnika	Zamjensko ime identifikatora

Tablica 23. Radna tablica za planiranje EIM identifikatora (nastavak)

Pregledajte Razvoj plana imenovanja EIM identifikatora za primjer kako koristiti ovu radnu tablicu.

Tablica 24. Radna tablica za planiranje asocijacije identifikatora

Jedinstveno ime identifikatora: _____Ivan S Dan_____		
Korisnički registar	Korisnički identitet	Tipovi asocijacija

Pregledajte Plan EIM asocijacija za primjer kako koristiti ovu radnu tablicu.

Tablica 25. Radna tablica za planiranje asocijacije politike

Tip asocijacije politike	Izvorni korisnički registar	Ciljni korisnički registar	Korisnički identitet	Opis

Pregledajte Plan EIM asocijacija za primjer kako koristiti ovu radnu tablicu.

Planiranje razvoja aplikacija za Mapiranje identiteta u poduzeću

Da bi aplikacija mogla koristiti Mapiranje identiteta u poduzeću (EIM) i sudjelovati u domeni, ista mora biti sposobna koristiti EIM API-je.

Pregledajte EIM API dokumentaciju i EIM dokumentaciju specifičnu za platformu da odredite postoje li bilo kakva specijalna razmatranja kod planiranja koja trebate znati kod pisanja ili prilagodbe aplikacija za upotrebu EIM API-ja. Na primjer, mogu postojati razmatranja prevođenja i ostala razmatranja za C ili C++ aplikacije koje pozivaju EIM API-je. Ovisno o platformi aplikacije, mogu postojati razmatranja vezivanja i uređivanja kao i ostala razmatranja.

Srodni zadaci

"API-ji Mapiranja identiteta u poduzeću" na stranici 119
Mapiranje identiteta u poduzeću (EIM) dobavlja mehanizme upravljanja korisničkim identitetom preko različitih platformi. EIM ima višestruka sučelja aplikativnog programiranja (API-je) koje aplikacija može koristiti za vođenje EIM operacija u koristi aplikacije ili aplikacijskog korisnika.

Planiranje Mapiranja identiteta u poduzeću za i5/OS

Mapiranje identiteta u poduzeću (EIM) uključuje nekoliko tehnologija i usluga na System i platformi. Prije konfiguriranja EIM-a na vašem poslužitelju, odlučite koju funkcionalnost želite primijeniti koristeći mogućnosti EIM-a i jednostruke prijave.

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

Ako planirate koristiti Kerberos za provjeru autentičnosti korisnika kao dio implementacije jednostruke prijave, trebali biste također konfigurirati uslugu provjere autentičnosti mreže.

Da naučite više o tome kako planirati EIM konfiguraciju vaših sistema, pregledajte sljedeće informacije:

Srodne informacije

Planiranje usluga provjere autentičnosti mreže

Preduvjeti EIM instalacije za i5/OS

Radna tablica planiranja identificira usluge koje trebate instalirati prije konfiguriranja EIM-a.

Tablica 26. Radna tablica planiranja EIM instalacije

Radna tablica planiranja EIM preduvjeta	Odgovori
Da li vaš sistem radi s i5/OS V5R4, ili novijom verzijom?	
Da li su na vašem sistemu instalirane sljedeće opcije i licencni proizvodi? • i5/OS Host Servers (5761-SS1 Opcija 12) • System i Access za Windows (5761-XE1) • Qshell Interpreter (5761-SS1 Opcija 30) Potreban ako namjeravate konfigurirati uslugu provjere autentičnosti mreže i EIM. **Bilješka:** 5722 je kod proizvoda za i5/OS opcije i proizvode prije V6R1.	
Da li je System i Navigator instaliran na PC računalu administratora, uključujući sljedeće podkomponente? • Mreža • Sigurnost (potrebno ako namjeravate konfigurirati uslugu provjere autentičnosti mreže i EIM)	
Da li ste instalirati zadnji System i Access za Windows servisni paket? Za zadnji servisni paket pogledajte System i Access	
Ako je trenutno konfiguriran poslužitelj direktorija, na primjer IBM Tivoli Directory Server za i5/OS, i ako ga želite koristiti kao EIM kontroler domene, znate li razlikovno ime (DN) LDAP administratora i njegovu lozinku?	
Ako je trenutno konfiguriran poslužitelj direktorija može li se privremeno zaustaviti? (Ovo će biti potrebno za dovršavanje EIM konfiguracijske obrade.)	
Imate li *SECADM, *ALLOBJ i *IOSYSCFG specijalna ovlaštenja?	
Jeste li primijenili zadnje privremene popravke programa (PTF-ove)?	

Instalacija potrebnih System i Navigator opcija

Da omogućite okolinu jednostruke prijave pomoću Mapiranja identiteta u poduzeću (EIM) i usluge provjere autentičnosti mreže, morate instalirati opciju **Mreža** i opciju **Sigurnost** iz System i Navigator.

EIM je smješten unutar opcije **Mreža**, a usluga provjere autentičnosti mreže nalazi se u opciji **Sigurnost**. Ako ne planirate koristiti uslugu provjere autentičnosti mreže u vašoj mreži, ne trebate instalirati opciju **Sigurnost** iz System i Navigator.

Za instalaciju opcije Mreža iz System i Navigator, ili za provjeru da li je ova opcija trenutno instalirana, osigurajte da je System i Access za Windows instaliran na PC-u koji koristite za administraciju System i modela.

Za instaliranje opcije **Mreža**:

1. Kliknite **Pokreni > Programi > System i Access za Windows > Selektivni postav**.
2. Pratite upute u dijalogu. Na dijalogu **Izbor komponenti**, proširite **System i Navigator**, zatim izaberite opciju **Mreža**. Ako planirate koristiti usluge provjere autentičnosti mreže, također bi trebali izabrati opciju **Sigurnost**.
3. Nastavite s ostatkom **Selektivnog Postava**.

Srodne informacije

Usluge provjere autentičnosti mreže

Razmatranje sigurnosnog kopiranja i obnavljanja za EIM

Trebate razviti plan kopiranja i obnavljanja vaših podataka Mapiranja identiteta u poduzeću (EIM) kako biste osigurali zaštitu vaših EIM podataka i njihovu obnovu ako se ikada pojavi problem s poslužiteljem direktorija koji je host EIM kontroleru domene. Postoje također važne EIM informacije o konfiguraciji koje trebate za razumijevanje postupka obnove.

Srodne informacije

Replikacija poslužitelja direktorija

Zadaci replikacije

Razmatranja o spremanju i vraćanju poslužitelja direktorija

Kopiranje i obnavljanje podataka domene EIM:

Kako ćete spremati vaše EIM podatke ovisi o tome kako ćete odlučiti upravljati ovim aspektom poslužitelja koji se ponaša kao kontroler domene za vaše EIM podatke.

Jedan način za kopiranje podataka, posebno u svrhu obnavljanja iz katastrofa, je da spremite knjižnicu baze podataka. Po defaultu, to je QUSRDIRDB. Ako je changelog omogućen, tada trebate također spremiti knjižnicu QUSRDIRCL. Poslužitelj direktorija na sistemu na kojem želite vratiti knjižnicu mora imati istu LDAP shemu i konfiguraciju kao i originalni poslužitelj direktorija. Datoteke koje sadrže 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 vaš poslužitelj direktorija, trebate spremiti obje knjižnice, datoteke integriranog sistema datoteka i QUSRSYS objekte.

Na primjer, možete koristiti LDIF datoteku za spremanje cijelog ili dijelova sadržaja poslužitelja direktorija. Za sigurnosno kopiranje informacija o domeni za IBM Tivoli Directory Server za i5/OS kontroler domene, izvedite sljedeće korake:

1. U System i Navigator proširite **Mrežni > poslužitelji > TCP/IP**.
2. Desno kliknite **Directory Server**, izaberite **Alati**, zatim izaberite **Datoteka eksporta** za prikaz stranice koja vam omogućuje da specificirate dijelove sadržaja poslužitelja direktorija koje želite eksportirati u datoteku.
3. Prenesite datoteku eksporta na System i platformu koju želite koristiti kao vaš backup poslužitelj direktorija.
4. U System i Navigator na backup poslužitelju proširite **Mrežni > poslužitelji > TCP/IP**.
5. Desno kliknite **Directory Server**, izaberite **Alati**, zatim izaberite **Import** za punjenje sadržaja prenešene datoteke u novi poslužitelj direktorija.

Drugi način koji možete uzeti u obzir prilikom spremanja vaših EIM podataka o domeni, je da konfigurirate i koristite kopiju poslužitelja direktorija. Sve promjene EIM podataka o domeni se automatski prosljeđuju kopiji poslužitelja direktorija, tako da ako poslužitelj direktorija koji je host kontrolera domene ne uspije ili izgubi EIM podatke, možete još uvijek dohvatiti podatke s kopije poslužitelja.

Kako ćete konfigurirati i koristiti kopiju poslužitelja direktorija mijenja se ovisno o tipu replikacijskog modela koji ste izabrali za korištenje.

Kopiranje i obnavljanje informacija konfiguracije EIM:

Ako se vaš sistem sruši, trebat ćete vratiti informacije o EIM konfiguraciji za taj sistem. Te se informacije ne mogu spremiti i vratiti lako između 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 važnih informacija o konfiguraciji. Tada vratite QSYS objekt profila korisnika na svaki sistem.

Bilješka: Morate koristiti SAVSECDTA naredbu i vratiti QSYS objekt profila korisnika pojedinačno na svaki sistem s EIM konfiguracijom. Možete naići na probleme ako pokušate na nekom sistemu obnoviti QSYS objekt profila korisnika koji je bio spremljen na drugom sistemu.

- Ili ponovno izvedite EIM Čarobnjaka konfiguracije ili ručno ažurirajte svojstva foldera EIM Konfiguracije. Za olakšanje ovog procesa, trebali biste spremiti vaše radne tablice planiranja EIM implementacije ili zapisati informacije o EIM konfiguraciji za svaki sistem.

Dodatno, razmotrite i planirajte kako sigurnosno kopirati i obnoviti podatke vaše usluge provjere autentičnosti mreže ako ste uslugu provjere autentičnosti mreže konfigurirali kao dio primjene okoline s jednom prijavom.

Konfiguriranje Mapiranja identiteta u poduzeću

Čarobnjak EIM konfiguracije vam omogućuje dovršetak osnovne EIM konfiguracije za vaš sistem na brz i jednostavan način. Čarobnjak vam osigurava tri opcije EIM sistemske konfiguracije.

Kako ćete koristiti čarobnjaka za EIM konfiguraciju na određenom sistemu ovisi o ukupnom planu korištenja EIM-a u vašem poduzeću i vašim potrebama EIM konfiguracije. Na primjer, većina administratora želi koristiti EIM zajedno s uslugom provjere autentičnosti mreže za kreiranje okoline jednostruke prijave na više sistema i platformi, bez potrebe za promjenom temeljnih politika sigurnosti. Konzekventno, Čarobnjak EIM konfiguracije vam dozvoljava konfiguraciju usluge provjere autentičnosti mreže kao dio vaše EIM konfiguracije. Međutim, konfiguriranje i korištenje usluge provjere autentičnosti mreže nije preduvjet ili zahtjev za konfiguriranje i korišten je EIM-a.

Prije no što započnete proces konfiguriranja EIM-a za jedan ili više sistema, planirajte vašu EIM implementaciju za skupljanje potrebnih informacija. Na primjer, trebate odlučiti o sljedećem:

- Koju System i platformu želite konfigurirati kao EIM kontroler domene za EIM domenu? Koristite Čarobnjaka EIM konfiguracije za kreiranje nove domene najprije na ovom sistemu, zatim koristite čarobnjaka da konfigurirate spajanje svih dodatnih sistema na ovu domenu.
- Da li želite konfigurirati usluge provjere autentičnosti mreže na svakom sistemu koji konfigurirate za EIM? Ako da, možete koristiti Čarobnjaka EIM konfiguracije za kreiranje osnovne konfiguracije usluga provjere autentičnosti mreže na svakom System i modelu. Međutim, morate izvesti ostale zadatke za dovršenje vaše konfiguracije usluga provjere autentičnosti mreže.

Nakon upotrebe Čarobnjaka EIM konfiguracije za kreiranje osnovne konfiguracije za svaku System i platformu, još uvijek postoje brojni zadaci EIM konfiguracije koje morate izvesti prije nego ćete imati potpunu EIM konfiguraciju. Pregledajte Scenarij: Omogućavanje jednostruke prijave za primjer koji pokazuje kako je izmišljeno poduzeće konfiguriralo okolinu jednostruke prijave koristeći uslugu provjere autentičnosti mreže i EIM.

Za konfiguraciju EIM-a, morate imate sva od sljedećih posebnih ovlaštenja:

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

Prije no što koristite Čarobnjaka EIM konfiguracije, trebali biste izvesti sve “Planiranje Mapiranja identiteta u poduzeću” na stranici 51 korake za točno određivanje načina korištenja EIM-a. Ako EIM konfigurirate kao dio kreiranja okoline jednostruke prijave, tada trebate dovršiti i sve korake planiranja jednostruke prijave.

Za pristup EIM Konfiguracijskom čarobnjaku, pratite ove korake:

1. Pokrenite System i Navigator.
2. Prijavite se na sistem koji želite konfigurirati za EIM. Ako EIM konfigurirate za više od jednog sistema, započnite s onim na kojem želite konfigurirati kontroler domene za EIM.
3. Proširite **Mreža → Mapiranje identiteta u poduzeću**.
4. Desno kliknite **Konfiguracija** i izaberite **Konfiguriraj** da započnete Čarobnjaka EIM konfiguracije.
5. Izaberite opciju EIM konfiguracije i slijedite upute koje osigurava čarobnjak za dovršetak čarobnjaka.

6. Ako je potrebno kliknite **Pomoć** da odredite koje informacije specificirati kako prolazite kroz čarobnjaka.

Kada dovršite vaš plan, možete koristiti Čarobnjaka EIM konfiguracije za kreiranje jedne od tri osnovne EIM konfiguracije. Možete koristiti čarobnjaka za spajanje na postojeću domenu ili za kreiranje i spajanje na novu domenu. Kada za kreiranje i spajanje na novu domenu koristite čarobnjaka za EIM konfiguraciju, možete izabrati da li konfigurirati EIM kontroler domene na lokalnom ili na udaljenom sistemu. Sljedeće informacije dobavljaju upute za konfiguriranje EIM-a bazirane na potrebnom tipu osnovne EIM konfiguracije:

Srodne informacije

Usluge provjere autentičnosti mreže

Jednostruka prijava

Kreiranje i spajanje nove lokalne domene

Kada za kreiranje i spajanje na novu domenu koristite Čarobnjaka za EIM konfiguraciju, možete izabrati da li konfigurirati EIM kontroler domene na lokalnom sistemu kao dio kreiranja vaše EIM konfiguracije.

Ako je potrebno Čarobnjak EIM konfiguracije osigurava da vi dobavite osnovne konfiguracijske informacije za poslužitelja direktorija. Također, ako Kerberos trenutno nije konfiguriran na System i platformi, čarobnjak od vas traži da lansirate Čarobnjaka konfiguracije usluge provjere autentičnosti mreže.

Kada završite s Čarobnjakom EIM konfiguracije, možete obaviti sljedeće zadatke:

- Kreirati novu EIM domenu.
- Konfigurirati lokalnog poslužitelja direktorija da djeluje kao EIM kontroler domene.
- Konfigurirati uslugu provjere autentičnosti mreže za sistem.
- Kreirati definicije registra EIM-a za lokalni i5/OS registar i Kerberos registar.
- Konfigurirati sistem da sudjeluje u novoj EIM domeni.

Da konfigurirate vaš sistem za kreiranje i spajanje na novu EIM domenu, morate imati sva od sljedećih posebnih ovlaštenja:

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

Da koristite Čarobnjaka EIM konfiguracije za kreiranje i spajanje na novu lokalnu domenu, izvedite sljedeće korake:

1. U System i Navigator, izaberite sistem za koji elite konfigurirati EIM i proširite **Mreža > Mapiranje identiteta u poduzeću**.
2. Desno kliknite **Konfiguracija** i izaberite **Konfiguriraj** da započnete Čarobnjaka EIM konfiguracije.

   Bilješka: Ova je opcija je označena kao **Rekonfiguriraj** ako je EIM prethodno bio konfiguriran na sistemu.
3. Na stranici čarobnjaka **Dobro došli!**, izaberite **Kreiranje i spajanje nove domene** i kliknite **Sljedeće**.
4. Na stranici **Specificiranje lokacije EIM domene**, izaberite **Na lokalnom poslužitelju direktorija** i kliknite **Sljedeće**.

   Bilješka: Ova opcija konfigurira lokalnog poslužitelja direktorija da djeluje kao EIM kontroler domene. Zato što ovaj poslužitelj direktorija pohranjuje sve EIM podatke za domenu, on mora biti aktivan i ostati aktivan za podršku EIM pregledavanju mapiranja i ostale operacije.

   Ako usluga provjere autentičnosti mreže trenutno nije konfigurirana na System i platformi, ili ako su potrebne dodatne informacije o konfiguraciji provjere autentičnosti mreže za konfiguriranje okoline jednostruke prijave, prikazuje se stranica **Konfiguracija usluga provjere autentičnosti mreže**. Ova stranica vam dozvoljava da pokrenete Čarobnjaka konfiguracije usluge provjere autentičnosti mreže tako da možete konfigurirati uslugu provjere autentičnosti mreže. Ili, Uslugu provjere autentičnosti mreže možete konfigurirati kasnije koristeći

čarobnjaka konfiguracije za ovu uslugu preko System i Navigator. Kada dovršite konfiguraciju usluga provjere autentičnosti mreže, nastavlja se EIM Konfiguracijski čarobnjak.

5. Da konfigurirate usluge provjere autentičnosti mreže, izvedite sljedeće korake:
   a. Na stranici **Konfiguracija Usluga provjere autentičnosti mreže** izaberite **Da** da pokrenete čarobnjaka Konfiguracije Usluga provjere autentičnosti mreže. S ovim čarobnjakom, možete konfigurirati nekoliko i5/OS sučelja i servisa da sudjeluju u Kerberos području kao i konfigurirati jedno okruženje prijave koje koristi i EIM i servis provjere autentičnosti mreže.
   b. Na stranici **Specificiranje informacija područja** navedite ime default područja u polju **Default područje**. Ako koristite Microsoft Aktivni direktorij za Kerberos provjeru autentičnosti izaberite **Microsoft Aktivni direktorij se koristi za Kerberos provjeru autentičnosti** i kliknite **Sljedeće**.
   c. Na stranici **Specificiranje KDC informacija** navedite puno ispravno ime Kerberos poslužitelja za ovo područje u **KDC** polju, navedite 88 u polju **Port**, a zatim kliknite **Sljedeće**.
   d. Na stranici **Specificiranje informacija lozinke poslužitelja** izaberite ili **Da** ili **Ne** za postavljanje lozinke poslužitelja. Poslužitelj lozinki dozvoljava principalima mijenjanje lozinke na Kerberos poslužitelju. Ako izaberete **Da**, unesite ime poslužitelja lozinke u polje **Poslužitelj lozinke**. U polju **Port** prihvatite default vrijednost 464, a zatim kliknite Sljedeće.
   e. Na stranici **Izaberite unose tablice ključeva**, izaberite **i5/OS Kerberos provjera autentičnosti** i kliknite **Sljedeće**.

      Bilješka: Dodatno, možete također kreirati unose tablice ključeva za IBM Tivoli Directory Server za i5/OS, i5/OS NetServer, i IBM HTTP poslužitelj za i5/OS ako želite da ove usluge koriste Kerberos provjeru autentičnosti. Možda ćete trebati dodatno konfigurirati ove usluge da bi mogle koristiti Kerberos provjeru autentičnosti.
   f. Na stranici **Kreiraj unos tablice ključeva i5/OS-a**, unesite i potvrdite lozinku i kliknite **Sljedeće**. To je ista lozinka koju ćete koristiti kada dodajete i5/OS principale na Kerberos poslužitelj.
   g. Opcijsko: Na stranici **Kreiranje Paketne Datoteke** izaberite **Da**, navedite sljedeće informacije i kliknite **Sljedeće**:
      - U polju **Paketna datoteka** ažurirajte stazu direktorija. Kliknite **Pregled** da biste pronašli odgovarajuću stazu direktorija ili u polju **Paketna datoteka** uredili stazu.
      - U polju **Uključi lozinku** izaberite **Da**. To osigurava da su sve lozinke pridružene s principalom uslugei5/OS-a uključene u paketnu datoteku. Važno je primijetiti da su lozinke prikazane u čistom tekstu i da ih može pročitati bilo tko tko ima dozvolu za čitanje paketne datoteke. Prema tome, bitno je da paketnu datoteku izbrišete s Kerberos poslužitelja i s PC-a odmah nakon njene upotrebe. Ako lozinku ne uključite, ona će se od vas zatražiti prilikom pokretanja paketne datoteke.

        Bilješka: Također možete ručno dodati principale usluge koje generira čarobnjak u Microsoft Aktivnom direktoriju. Da naučite kako to učiniti, pregledajte Dodavanje i5/OS principala Kerberos poslužitelju
      - Na stranici **Sažetak** pregledajte pojedinosti konfiguracije usluge provjere autentičnosti mreže, a zatim kliknite **Završi** da biste se vratili u čarobnjak EIM konfiguracije.
6. Ako lokalni poslužitelj direktorija nije trenutno konfiguriran, prikazuje se stranica **Konfiguriraj Poslužitelja direktorija** kada Čarobnjak EIM konfiguracije ponovo započne. Osigurajte sljedeće informacije za konfiguraciju lokalnog poslužitelja direktorija:

   Bilješka: Ako konfigurirate lokalnog poslužitelja direktorija prije korištenja Čarobnjaka EIM konfiguracije, prikazuje se stranica **Specificiranje korisnika za Povezivanje** umjesto čarobnjaka. Koristite ovu stranicu za specifikaciju razlikovnog imena i lozinke za LDAP administratora kako bi osigurali da čarobnjak ima dovoljno ovlaštenje za administraciju EIM domene i objekata u njoj i nastavite sa sljedećim korakom u ovoj proceduri. Ako je potrebno kliknite **Pomoć** da odredite koje informacije osigurati za ovu stranicu.
   a. U polju **Port** prihvatite default broj porta 389 ili specificirajte drugi broj porta koji se koristi za nesigurne EIM komunikacije s poslužiteljem direktorija.

b. U polju **Razlikovno ime** navedite LDAP razlikovno ime (DN) koje identificira LDAP administratora za poslužitelja direktorija. Čarobnjak EIM konfiguracije kreira taj DN LDAP administratora i koristi ga za konfiguraciju poslužitelja direktorija kao kontrolera domene za novu domenu koju kreirate.

c. U polju **Lozinka**, specificirajte lozinku za LDAP administratora.

d. U polju **Potvrda lozinke** drugi put navedite lozinku za svrhu provjere valjanosti.

e. Kliknite **Sljedeće**.

7. Na stranici **Specificiranje domene** , osigurajte sljedeće informacije:

   a. U polju **Domena** specificirajte ime EIM domene koju želite kreirati. Prihvatite defaultno ime EIM ili upotrijebite bilo koji niz znakova koji vam imaju smisla. Ipak, ne možete koristiti specijalne znakove kao što su **= + < > ,** # **;** \ i *.

   b. U polju **Opis** unesite tekst za opis domene.

   c. Kliknite **Sljedeće**.

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

   Bilješka: Kada kreirate domenu na lokalnom poslužitelju direktorija, nadređeni DN je opcija. Specificiranjem nadređenog DN-a, možete specificirati gdje se trebaju nalaziti EIM podaci u lokalnom LDAP imenskom prostoru. Kada ne trebate specificirati nadređeni DN, EIM podaci se nalaze u svom vlastitom sufiksu u imenskom prostoru. Ako izaberete **Da**, koristite kućicu s popisom u izboru lokalnog LDAP sufiksa za upotrebu kao nadređenog DN-a ili unesite tekst za kreiranje i imenovanje novog nadređenog DN-a. Nije potrebno specificirati nadređeni DN nove domene. Kliknite **Pomoć** za dodatne informacije o korištenju nadređenog DN-a.

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

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

   a. Izaberite **Lokalni i5/OS** 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 specifičnu instancu tog registra.

   b. 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 područja. Prihvaćanjem default imena i upotrebom istog imena Kerberos registra kao imena područja, možete povećati performansu pri dohvaćanju informacija iz registra. Ako je potrebno, izaberite **Kerberos korisnički identiteti osjetljivi su na velika i mala slova**.

   c. Kliknite **Sljedeće**.

10. Na stranici **Specificiranje EIM sistemskog korisnika** izaberite **Tip korisnika** kojeg želite da sistem koristi kada izvodi EIM operacije za funkcije operativnog sistema. Ove operacije uključuju operacije pregledavanja mapiranja i brisanje asocijacija kada se briše lokalni profil i5/OS korisnika. Možete izabrati jedan od sljedećih korisničkih tipova: **Razlikovno ime i lozinka**, **Kerberos datoteka tablice ključeva i principal** ili **Kerberos principal i lozinka**. Tip korisnika koji možete izabrati varira ovisno o trenutnoj konfiguraciji sistema. Na primjer, ako Usluga Mrežne Provjere Autentičnosti nije konfigurirana za sistem, tada Kerberos korisnički tipovi možda neće biti dostupni za izbor. Tip korisnika koji izaberete određuje ostale informacije koje morate osigurati da bi se stranica ispunila kako slijedi:

    Bilješka: Morate navesti korisnika koji je trenutno definiran u poslužitelju direktorija koji je host EIM kontrolera domene. Korisnik kojeg specificirate mora imati minimalne povlastice za izvođenje pregledavanja mapiranja i administraciju registra za lokalni korisnički registar. Ako korisnik kojeg ste specificirali nema te povlastice, neke određene funkcije operativnog sistema koje se odnose na upotrebu jednostruke prijave i na brisanje korisničkih profila mogu biti neuspješne.

Ako niste konfigurirali poslužitelj direktorija prije izvođenja ovog čarobnjaka, jedini tip korisnika kojeg možete izabrati je **Razlikovno ime i lozinka**, a jedino razlikovno ime koje možete specificirati je DN LDAP administratora.

- Ako izaberete **Razlikovno ime i lozinka**, osigurajte sljedeće informacije:
  - U polju **Razlikovno ime** navedite LDAP razlikovno ime koje identificira korisnika, a koje će sistem koristiti prilikom izvođenja 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 sljedeće informacije:
  - U polju **Principal** navedite ime Kerberos principala kojeg će sistem koristiti prilikom izvođenja EIM operacija.
  - U polju **Područje** navedite puno ispravno ime Kerberos područja čiji je principal član. Ime principala i područja jedinstveno identificira Kerberos korisnike u datoteci tablice ključeva. Na primjer, principal jsmith u području ordept.myco.com u datoteci tablice ključeva 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 ključeva i principal**, osigurajte sljedeće informacije:
  - U polju **Datoteka tablice ključeva** navedite punu ispravnu stazu i ime datoteke tablice ključeva koja sadrži Kerberos principala kojeg će sistem koristiti prilikom izvođenja EIM operacija. Ili, kliknite **Pregledaj** za pretraživanje kroz direktorije u System i integriranom sistemu datoteka za brisanje datoteke tablice ključeva.
  - U polju **Principal** navedite ime Kerberos principala kojeg će sistem koristiti prilikom izvođenja EIM operacija.
  - U polju **Područje** navedite puno ispravno ime Kerberos područja čiji je principal član. Ime principala i područja jedinstveno identificira Kerberos korisnike u datoteci tablice ključeva. Na primjer, principal jsmith u području ordept.myco.com u datoteci tablice ključeva predstavljen je kao jsmith@ordept.myco.com.
- Kliknite **Provjeri Vezu** da osigurate da čarobnjak može koristiti navedene korisničke informacije za uspješnu uspostavu veze s EIM kontrolerom domene.
- Kliknite **Sljedeće**.

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

Finaliziranje vaše konfiguracije EIM-a za domenu

Kada čarobnjak završi on dodaje novu domenu u folder **Upravljanje domenom** i na taj ste način kreirali osnovnu EIM konfiguraciju za ovaj sistem. Međutim, ove zadatke trebate dovršiti da biste završili vašu EIM konfiguraciju za domenu:

1. Koristite Čarobnjaka EIM konfiguracije na svakom dodatnom poslužitelju kojeg želite spojiti na domenu.
2. Ako je potrebno dodajte EIM definicije registra EIM domeni, ili drugim ne-System i platformama i aplikacijama za koje želite da sudjeluju u EIM domeni. Ove definicije registra odnose se na stvarne korisničke registre koji moraju sudjelovati u domeni. Možete dodati sistemske definicije registra ili dodati definicije registra aplikacije ovisno o potrebama vaše EIM implementacije.
3. Ovisno o potrebama vaše 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 korisnički identitet.
   - Kreirati kombinaciju istih.
4. Koristite EIM funkciju testiranje mapiranja da testirate mapiranje identiteta vaše EIM konfiguracije.
5. Ako je jedini EIM korisnik kojeg ste definirali DN za LDAP administratora, tada vaš EIM korisnik ima visoku razinu ovlaštenja nad svim podacima na poslužitelju direktorija. Prema tome, možete razmotriti kreiranje jednog ili više DN-ova kao dodatne korisnike koji imaju prikladniju i ograničenu kontrolu pristupa za podatke EIM-a. Da naučite više o kreiranju DN-ova za poslužitelj direktorija, pregledajte Razlikovna imena u i5/OS Informacijski

centar. Broj dodatnih EIM korisnika koje definirate ovisi o vašoj sigurnosnoj politici s naglaskom na razdvajanju sigurnosnih zadataka i odgovornosti. Tipično, možete kreirati barem dva sljedeća tipa DN-ova:

- **Korisnik koji ima kontrolu pristupa EIM administratora**

  Ovaj EIM administratorski DN omogućuje prikladnu razinu ovlaštenja za administratora koji je odgovoran za upravljanje EIM domenom. Ovaj EIM administratorski DN se ne može koristiti za povezivanje na kontroler domene kod upravljanja svim aspektima EIM domene pomoću System i Navigator.
- **Barem jedan korisnik koji ima sve od sljedećih kontrola pristupa**:
  - Administrator identifikatora
  - Administrator registra
  - EIM operacije mapiranja

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

Bilješka: Za upotrebu ovog novog DN-a za sistemskog korisnika umjesto LDAP administratorskog DN-a, morate promijeniti svojstva EIM konfiguracije za System i platformu. Pregledajte Upravljanje svojstvima EIM konfiguracije da naučite kako promijeniti DN sistemskog korisnika.

Dodatno, možda ćete željeti koristiti Sloj Sigurnih Utičnica (SSL) ili Sigurnost Transportnog Sloja (TLS) za konfiguraciju sigurnog povezivanja na EIM kontroler domene za zaštitu prijenosa EIM podataka. Ako omogućite SSL za poslužitelja direktorija, morate ažurirati svojstva EIM konfiguracije da specificirate da System i platforma koristi sigurnu SSL vezu. Također, morate ažurirati svojstva za domenu da specificirate da EIM koristi SSL veze za upravljanje domenom preko System i Navigator.

Bilješka: Možda ćete morati izvesti dodatne zadatke ako ste kreirali osnovnu konfiguraciju usluge provjere autentičnosti mreže, posebno ako primjenjujete okolinu jednostruke prijave. Informacije o dodatnim koracima možete pronaći pregledavanjem svih koraka konfiguracije prikazanih u scenariju, Omogućavanje jednostruke prijave za i5/OS.

Kreiranje i spajanje nove udaljene domene

Kada za kreiranje i spajanje na novu domenu koristite Čarobnjaka za EIM konfiguraciju, možete izabrati da li konfigurirati poslužitelja direktorija na udaljenom sistemu koji djeluje kao EIM kontroler domene, kao dio kreiranja vaše EIM konfiguracije.

Morate specificirati odgovarajuće informacije za povezivanje na udaljeni poslužitelj direktorija kako bi konfigurirali EIM. Ako Kerberos trenutno nije konfiguriran na System i platformi, čarobnjak od vas traži da pokrenete Čarobnjaka konfiguracije usluge provjere autentičnosti mreže.

Bilješka: Poslužitelj direktorija na udaljenom sistemu mora osiguravati EIM podršku. EIM zahtjeva da je kontroler domene smješten na poslužitelju direktorija koji podržava verziju 3 Lightweight Directory Access Protocola (LDAP). Dodatno, proizvod poslužitelja direktorija mora imati konfiguriranu EIM shemu. Na primjer, IBM Poslužitelj direktorija V5.1 osigurava tu podršku. Za detaljnije informacije o zahtjevima EIM kontrolera domene, pregledajte “Planiranje kontrolera domene Mapiranja identiteta u poduzeću” na stranici 55.

Kada završite s Čarobnjakom EIM konfiguracije, možete obaviti sljedeće zadatke:

- Kreirati novu EIM domenu.
- Konfigurirati udaljenog poslužitelja direktorija da djeluje kao EIM kontroler domene.
- Konfigurirati uslugu provjere autentičnosti mreže za sistem.
- Kreirati definicije registra EIM-a za lokalni i5/OS registar i Kerberos registar.
- Konfigurirati sistem da sudjeluje u novoj EIM domeni.

Da konfigurirate vaš sistem za kreiranje i spajanje na novu EIM domenu, morate imati sva od sljedećih posebnih ovlaštenja:

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

Da koristite Čarobnjaka EIM konfiguracije za kreiranje i spajanje na novu udaljenu domenu, izvedite sljedeće korake:

1. Provjerite da je poslužitelj direktorija na udaljenom sistemu aktivan.
2. U System i Navigator, izaberite sistem za koji elite konfigurirati EIM i proširite **Mreža > Mapiranje identiteta u poduzeću**.
3. Desno kliknite **Konfiguracija** i izaberite **Konfiguriraj** da započnete Čarobnjaka EIM konfiguracije.

   Bilješka: Ova je opcija je označena kao **Rekonfiguriraj** ako je EIM prethodno bio konfiguriran na sistemu.
4. Na stranici čarobnjaka **Dobro došli!**, izaberite **Kreiranje i spajanje nove domene** i kliknite **Sljedeće**.
5. Na stranici **Specificiranje lokacije EIM domene**, izaberite **Na lokalnom poslužitelju direktorija** i kliknite **Sljedeće**.

   Bilješka: Ova opcija konfigurira lokalnog poslužitelja direktorija da djeluje kao EIM kontroler domene. Zato što ovaj poslužitelj direktorija pohranjuje sve EIM podatke za domenu, on mora biti aktivan i ostati aktivan za podršku EIM pregledavanju mapiranja i ostale operacije.

   Ako usluga provjere autentičnosti mreže trenutno nije konfigurirana na System i platformi, ili ako su potrebne dodatne informacije o konfiguraciji provjere autentičnosti mreže za konfiguriranje okoline jednostruke prijave, prikazuje se stranica **Konfiguracija usluga provjere autentičnosti mreže**. Ova stranica vam dozvoljava da pokrenete Čarobnjaka konfiguracije usluge provjere autentičnosti mreže tako da možete konfigurirati uslugu provjere autentičnosti mreže. Ili, Uslugu provjere autentičnosti mreže možete konfigurirati kasnije koristeći čarobnjaka konfiguracije za ovu uslugu preko System i Navigator. Kada dovršite konfiguraciju usluga provjere autentičnosti mreže, nastavlja se EIM Konfiguracijski čarobnjak.
6. Da konfigurirate usluge provjere autentičnosti mreže, izvedite sljedeće korake:
   a. Na stranici **Konfiguracija Usluga provjere autentičnosti mreže** izaberite **Da** da pokrenete čarobnjaka Konfiguracije Usluga provjere autentičnosti mreže. S ovim čarobnjakom, možete konfigurirati nekoliko i5/OS sučelja i servisa da sudjeluju u Kerberos području kao i konfigurirati jedno okruženje prijave koje koristi i EIM i servis provjere autentičnosti mreže.
   b. Na stranici **Specificiranje informacija područja** navedite ime default područja u polju **Default područje**. Ako koristite Microsoft Aktivni direktorij za Kerberos provjeru autentičnosti izaberite **Microsoft Aktivni direktorij se koristi za Kerberos provjeru autentičnosti** i kliknite **Sljedeće**.
   c. Na stranici **Specificiranje KDC informacija** navedite puno ispravno ime Kerberos poslužitelja za ovo područje u **KDC** polju, navedite 88 u polju **Port**, a zatim kliknite **Sljedeće**.
   d. Na stranici **Specificiranje informacija Lozinke poslužitelja** izaberite ili **Da** ili **Ne** za postavljanje lozinke poslužitelja. Poslužitelj lozinki dozvoljava principalima mijenjanje lozinke na Kerberos poslužitelju. Ako izaberete **Da**, unesite ime poslužitelja lozinke u polje **Poslužitelj lozinke**. U polju **Port** prihvatite default vrijednost 464, a zatim kliknite Sljedeće.
   e. Na stranici **Izaberite unose tablice ključeva**, izaberite **i5/OS Kerberos provjera autentičnosti** i kliknite **Sljedeće**.

      Bilješka: Dodatno, možete također kreirati unose tablice ključeva za IBM Tivoli Directory Server za i5/OS, i5/OS NetServer, i IBM HTTP poslužitelj za i5/OS poslužitelj ako želite da ove usluge koriste Kerberos provjeru autentičnosti. Možda ćete trebati dodatno konfigurirati ove usluge da bi mogle koristiti Kerberos provjeru autentičnosti.
   f. Na stranici **Kreiraj unos tablice ključeva i5/OS-a**, unesite i potvrdite lozinku i kliknite **Sljedeće**. To je ista lozinka koju ćete koristiti kada dodajete i5/OS principale na Kerberos poslužitelj.
   g. Opcijsko: Na stranici **Kreiranje Paketne Datoteke** izaberite **Da**, navedite sljedeće informacije i kliknite **Sljedeće**:
      - U polju **Paketna datoteka** ažurirajte stazu direktorija. Kliknite **Pregled** da biste pronašli odgovarajuću stazu direktorija ili u polju **Paketna datoteka** uredili stazu.

- U polju **Uključi lozinku** izaberite **Da**. To osigurava da su sve lozinke pridružene s principalom uslugei5/OS-a uključene u paketnu datoteku. Važno je primijetiti da su lozinke prikazane u čistom tekstu i da ih može pročitati bilo tko tko ima dozvolu za čitanje paketne datoteke. Prema tome, bitno je da paketnu datoteku izbrišete s Kerberos poslužitelja i s PC-a odmah nakon njene upotrebe. Ako lozinku ne uključite, ona će se od vas zatražiti prilikom pokretanja paketne datoteke.

  Bilješka: Također možete ručno dodati principale usluge koje generira čarobnjak u Microsoft Aktivnom direktoriju. Da naučite kako to učiniti, pregledajte Dodavanje i5/OS principala Kerberos poslužitelju.
- Na stranici **Sažetak** pregledajte pojedinosti konfiguracije usluge provjere autentičnosti mreže, a zatim kliknite **Završi** da biste se vratili u čarobnjak EIM konfiguracije.

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

        Bilješka: Morate provjeriti je li EIM kontroler domene konfiguriran za korištenje sigurne veze. U suprotnom, veza s kontrolerom domene može ne uspjeti.
      - U polju **Port** navedite TCP/IP port na kojem sluša poslužitelj direktorija. Ako je izabrano **Koristi sigurnu vezu**, default port je 636; u suprotnom je port 389.
   c. Kliknite **Provjera veze** da provjerite može li čarobnjak koristiti navedene informacije za uspješnu uspostavu veze s EIM kontrolerom domene.
   d. Kliknite **Sljedeće**.
8. Na stranici **Specificiranje korisnika za vezu** izaberite **Tip korisnika** za povezivanje. Možete izabrati jednog od sljedećih tipova korisnika: **Razlikovno ime i lozinka**, **Kerberos datoteka tablice ključeva i principal**, **Kerberos principal i lozinka** ili **Korisnički profil i lozinka**. Dva Kerberos tipa korisnika su dostupna samo ako je usluga provjere autentičnosti mreže konfigurirana za lokalnu System i platformu. Tip korisnika koji izaberete određuje druge informacije koje morate dobaviti za dovršavanje dijaloga kako slijedi:

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

   Možete navesti različitog korisnika za vezu, međutim, korisnik kojeg navedete mora imati ekvivalent LDAP administratorskom ovlaštenju za udaljenog poslužitelja direktorija.
   a. Ako izaberete **Razlikovno ime i lozinka**, pružite sljedeće informacije:
      - U polje **Razlikovno ime** upišite LDAP administratorsko razlikovno ime (DN) i lozinku da osigurate da čarobnjak ima dovoljno ovlaštenja 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.
   b. Ako ste izabrali **Kerberos datoteka tablice ključeva i principal**, osigurajte sljedeće informacije:
      - U polju **Datoteka tablice ključeva** navedite punu ispravnu stazu i ime datoteke tablice ključeva koja sadrži Kerberos principala kojeg će čarobnjak koristiti prilikom povezivanja na EIM domenu. Ili, kliknite **Pregledaj** za pretraživanje kroz direktorije u i5/OS integriranom sistemu datoteka za brisanje datoteke tablice ključeva.
      - U polju **Principal** navedite ime Kerberos principala koji će se koristiti za identificiranje korisnika.

- U polju **Područje** navedite puno ispravno ime Kerberos područja čiji je principal član. Ime principala i područja jedinstveno identificiraju Kerberos korisnike u datoteci tablice ključeva. Na primjer, principal jsmith u području ordept.myco.com, predstavljeno je u datoteci tablice ključeva kao jsmith@ordept.myco.com.

c. Ako izaberete **Kerberos principal i lozinka**, osigurajte sljedeće informacije:
   - U polju **Principal** navedite ime Kerberos principala koje će čarobnjak koristiti prilikom spajanja na EIM domenu.
   - U polju **Područje** navedite puno ispravno ime Kerberos područja čiji je principal član. Ime principala i područja jedinstveno identificiraju Kerberos korisnike u datoteci tablice ključeva. Na primjer, principal jsmith u području ordept.myco.com u datoteci tablice ključeva 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.

d. Ako izaberete **Korisnički profil i lozinka**, navedite sljedeće informacije:
   - U polju **Korisnički profil** navedite ime korisničkog profila koje će čarobnjak koristiti prilikom spajanja na EIM domenu.
   - U polju **Lozinka** navedite lozinku korisničkog profila.
   - U polju **Potvrda lozinke** drugi put navedite lozinku za svrhu provjere valjanosti.

e. Kliknite **Provjera veze** da provjerite može li čarobnjak koristiti navedene korisničke informacije za uspješnu uspostavu veze s EIM kontrolerom domene.

f. Kliknite **Sljedeće**.

9. Na stranici **Specificiranje domene** , osigurajte sljedeće informacije:
   a. U polju **Domena** specificirajte ime EIM domene koju želite kreirati. Prihvatite defaultno ime EIM ili upotrijebite bilo koji niz znakova koji vam imaju smisla. Ipak, ne možete koristiti specijalne znakove kao što su **= + < > ,** # **;** \ i *.
   b. U polju **Opis** unesite tekst za opis domene.
   c. Kliknite **Sljedeće**.
10. U dijalogu **Specificiranje nadređenog DN-a za domenu**, izaberite **Da** za specifikaciju nadređenog DN-a koje će čarobnjak koristiti za lokaciju EIM domene koju kreirate. To je DN koji predstavlja unos odmah iznad unosa imena vaše domene u stablastoj hijerarhiji informacija o direktoriju. Ili specificirajte **Ne** da imate EIM podatke pohranjene na lokaciji direktorija sa sufiksom čije je ime izvedeno iz imena EIM domene.

    Bilješka: Kada koristite čarobnjaka za konfiguraciju domene na udaljenom kontroleru domene, trebate specificirati odgovarajući nadređeni DN za domenu. Zato što svi potrebni konfiguracijski objekti za nadređeni DN moraju već postojati, jer u suprotnom EIM konfiguracija neće uspjeti, trebate pregledati kako bi našli prikladan nadređeni DN umjesto da ručno unesete DN informacije. Kliknite **Pomoć** za dodatne informacije o korištenju nadređenog DN-a.
11. Na stranici **Informacije registra** navedite treba li dodati lokalne korisničke registre u EIM domenu kao definicije registra. Izaberite jedan od sljedećih ili oba korisnička tipa registra:

    Bilješka: U ovom trenutku ne morate kreirati definicije registra. Ako izaberete kreiranje definicija registra malo kasnije, pogledajte dodavanje definicije sistemskog registra i svojstva EIM konfiguracije.
    a. Izaberite **Lokalni i5/OS** 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 specifičnu instancu tog registra.
    b. 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 područja. Prihvaćanjem default imena i upotrebom istog imena Kerberos registra kao imena područja, možete povećati performansu pri dohvaćanju informacija iz registra. Ako je potrebno, izaberite **Kerberos korisnički identiteti osjetljivi su na velika i mala slova**.
    c. Kliknite **Sljedeće**.

12. Na stranici **Specificiranje EIM sistemskog korisnika** izaberite **Tip korisnika** kojeg želite da sistem koristi kada izvodi EIM operacije za funkcije operativnog sistema. Ove operacije uključuju operacije pregledavanja mapiranja i brisanje asocijacija kada se briše lokalni profil i5/OS korisnika. Možete izabrati jedan od sljedećih korisničkih tipova: **Razlikovno ime i lozinka**, **Kerberos datoteka tablice ključeva i principal** ili **Kerberos principal i lozinka**. Tip korisnika koji možete izabrati varira ovisno o trenutnoj konfiguraciji sistema. Na primjer, ako Usluga Mrežne Provjere Autentičnosti nije konfigurirana za sistem, tada Kerberos korisnički tipovi možda neće biti dostupni za izbor. Tip korisnika koji izaberete određuje ostale informacije koje morate osigurati da bi se stranica ispunila kako slijedi:

    Bilješka: Morate navesti korisnika koji je trenutno definiran u poslužitelju direktorija koji je host EIM kontrolera domene. Korisnik kojeg specificirate mora imati minimalne povlastice za izvođenje pregledavanja mapiranja i administraciju registra za lokalni korisnički registar. Ako korisnik kojeg ste specificirali nema te povlastice, neke određene funkcije operativnog sistema koje se odnose na upotrebu jednostruke prijave i na brisanje korisničkih profila mogu biti neuspješne.

    Ako niste konfigurirali poslužitelj direktorija prije izvođenja ovog čarobnjaka, jedini tip korisnika koji možete izabrati je **Razlikovno ime i lozinka**, a jedino razlikovno ime koje možete specificirati je DN LDAP administratora.

    a. Ako izaberete **Razlikovno ime i lozinka**, pružite sljedeće informacije:
        - U polju **Razlikovno ime** navedite LDAP razlikovno ime koje identificira korisnika, a koje će sistem koristiti prilikom izvođenja EIM operacija.
        - U polju **Lozinka** navedite lozinku razlikovnog imena.
        - U polju **Potvrda lozinke** drugi put navedite lozinku za svrhu provjere valjanosti.

    b. Ako izaberete **Kerberos principal i lozinka**, osigurajte sljedeće informacije:
        - U polju **Principal** navedite ime Kerberos principala kojeg će sistem koristiti prilikom izvođenja EIM operacija.
        - U polju **Područje** navedite puno ispravno ime Kerberos područja čiji je principal član. Ime principala i područja jedinstveno identificiraju Kerberos korisnike u datoteci tablice ključeva. Na primjer, principal jsmith u području ordept.myco.com u datoteci tablice ključeva 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.

    c. Ako ste izabrali **Kerberos datoteka tablice ključeva i principal**, osigurajte sljedeće informacije:
        - U polju **Datoteka tablice ključeva** navedite punu ispravnu stazu i ime datoteke tablice ključeva koja sadrži Kerberos principala kojeg će sistem koristiti prilikom izvođenja EIM operacija. Ili, kliknite **Pregledaj** za pretraživanje kroz direktorije u System i integriranom sistemu datoteka za brisanje datoteke tablice ključeva.
        - U polju **Principal** navedite ime Kerberos principala kojeg će sistem koristiti prilikom izvođenja EIM operacija.
        - U polju **Područje** navedite puno ispravno ime Kerberos područja čiji je principal član. Ime principala i područja jedinstveno identificiraju Kerberos korisnike u datoteci tablice ključeva. Na primjer, principal jsmith u području ordept.myco.com u datoteci tablice ključeva predstavljen je kao jsmith@ordept.myco.com.

    d. Kliknite **Provjera veze** da osigurate da čarobnjak može koristiti navedene korisničke informacije za uspješnu uspostavu veze s EIM kontrolerom domene.

    e. Kliknite **Sljedeće**.

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

Finaliziranje vaše konfiguracije EIM-a za domenu

Kada čarobnjak završi on dodaje novu domenu u folder **Upravljanje domenom** i na taj ste način kreirali osnovnu EIM konfiguraciju za ovaj sistem. Međutim, ove zadatke trebate dovršiti da biste završili vašu EIM konfiguraciju za domenu:

1. Koristite Čarobnjaka EIM konfiguracije na svakom dodatnom poslužitelju za kojeg želite da se spoji na postojeću domenu. Pregledajte poglavlje "Spajanje na postojeću domenu" za više informacija.
2. Ako je potrebno dodajte EIM definicije registra EIM domeni, ili drugim ne-System i platformama i aplikacijama za koje želite da sudjeluju u EIM domeni. Ove definicije registra odnose se na stvarne korisničke registre koji moraju sudjelovati u domeni. Ovisno o vašim potrebama EIM implementacije, pogledajte "Dodavanje definicije sistemskog registra" na stranici 89 ili "Dodavanje definicije registra aplikacija" na stranici 89.
3. Ovisno o potrebama vaše EIM implementacije odredite da li:
   a. "Kreiranje EIM identifikatora" na stranici 95 za svakog jedinstvenog korisnika u domeni i "Kreiranje asocijacije EIM identifikatora" na stranici 98 za njih.
   b. "Kreiranje asocijacije politike" na stranici 99 za mapiranje grupe korisnika u jednostruki ciljni korisnički identitet.
   c. Kreirajte kombinaciju istih.
4. Koristite EIM funkciju "Testiranje EIM mapiranja" na stranici 85 za testiranje mapiranja identiteta za vašu EIM konfiguraciju.
5. Ako je jedini EIM korisnik kojeg ste definirali DN za LDAP administratora, tada vaš EIM korisnik ima visoku razinu ovlaštenja nad svim podacima na poslužitelju direktorija. Prema tome, možete razmotriti kreiranje jednog ili više DN-ova kao dodatne korisnike koji imaju prikladniju i ograničenu kontrolu pristupa za podatke EIM-a. Da naučite više o kreiranju DN-ova za poslužitelj direktorija, pregledajte Razlikovna imena u i5/OS Informacijski centar. Broj dodatnih EIM korisnika koje definirate ovisi o vašoj sigurnosnoj politici s naglaskom na razdvajanju sigurnosnih zadataka i odgovornosti. Tipično, možete kreirati barem dva sljedeća tipa DN-ova:
   - **Korisnik koji ima kontrolu pristupa EIM administratora**

     Ovaj EIM administratorski DN omogućuje prikladnu razinu ovlaštenja za administratora koji je odgovoran za upravljanje EIM domenom. Ovaj EIM administratorski DN se ne može koristiti za povezivanje na kontroler domene kod upravljanja svim aspektima EIM domene pomoću System i Navigator.
   - **Barem jedan korisnik koji ima sve od sljedećih kontrola pristupa**:
     – Administrator identifikatora
     – Administrator registra
     – EIM operacije mapiranja

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

   Bilješka: Za upotrebu ovog novog DN-a za sistemskog korisnika umjesto LDAP administratorskog DN-a, morate promijeniti svojstva EIM konfiguracije za System i platformu. Pregledajte "Upravljanje svojstvima EIM konfiguracije" na stranici 112 da naučite kako promijeniti DN sistemskog korisnika.

Možda ćete morati izvesti dodatne zadatke ako ste kreirali osnovnu konfiguraciju usluge provjere autentičnosti mreže, posebno ako primjenjujete okolinu jednostruke prijave. Informacije o dodatnim koracima možete pronaći pregledavanjem svih koraka konfiguracije prikazanih u scenariju, Omogućavanje jednostruke prijave za i5/OS.

Spajanje na postojeću domenu

Koristite Čarobnjaka konfiguracije Mapiranja identiteta u poduzeću (EIM) na jednoj System i platformi za konfiguraciju kontrolera domene i kreiranje EIM domene, a zatim možete koristiti čarobnjaka za konfiguriranje ostalih sistema za sudjelovanje u domeni.

Nakon što kreirate EIM domenu i konfigurirate kontroler domene na jednom sistemu, možete konfigurirati sve dodatne System i platforme za spajanje na postojeću EIM domenu. Kako radite kroz čarobnjaka, morate dobaviti informacije o domeni, uključujući informacije povezivanja na EIM kontroler domene. Kada koristite EIM Čarobnjak konfiguracije za

spajanje na postojeću domenu, čarobnjak vam i dalje omogućuje mogućnost pokretanja čarobnjaka Konfiguracije usluge provjere autentičnosti mreže za konfiguraciju Kerberosa kao dijela konfiguriranja EIM-a na sistemu.

Kada završite s čarobnjakom EIM konfiguracije tako da se spoji na postojeću domenu, možete izvesti sljedeće zadatke:

- Konfigurirati uslugu provjere autentičnosti mreže za sistem.
- Kreirati definicije registra EIM-a za lokalni i5/OS registar i Kerberos registar.
- Konfigurirati sistem da sudjeluje u postojećoj EIM domeni.

Da konfigurirate sistem da se spoji na postojeću EIM domenu, morate imati sva od sljedećih posebnih ovlaštenja:

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

Da započnete i koristite čarobnjaka EIM konfiguracije za spajanje na postojeću EIM domenu, izvedite sljedeće korake:

1. Provjerite da je poslužitelj direktorija na udaljenom sistemu aktivan.
2. U System i Navigator, izaberite sistem za koji elite konfigurirati EIM i proširite **Mreža > Mapiranje identiteta u poduzeću**.
3. Desno kliknite **Konfiguracija** i izaberite **Konfiguriraj...** da započnete čarobnjaka EIM konfiguracije.

   Bilješka: Ova je opcija je označena kao **Rekonfiguriraj...** ako je EIM prethodno konfiguriran na sistemu.
4. Na stranici čarobnjaka **Dobro došli** izaberite **Spajanje na postojeću domenu**, a zatim kliknite **Sljedeće**.

   Bilješka: Ako usluga provjere autentičnosti mreže trenutno nije konfigurirana na System i modelu, ili ako su potrebne dodatne informacije o konfiguraciji provjere autentičnosti mreže za konfiguriranje okoline jednostruke prijave, prikazuje se stranica **Konfiguracija usluga provjere autentičnosti mreže**. Ova stranica vam dozvoljava da pokrenete Čarobnjaka konfiguracije usluge provjere autentičnosti mreže tako da možete konfigurirati uslugu provjere autentičnosti mreže. Ili, Uslugu provjere autentičnosti mreže možete konfigurirati kasnije koristeći čarobnjaka konfiguracije za ovu uslugu preko System i Navigator. Kada dovršite konfiguraciju usluga provjere autentičnosti mreže, nastavlja se EIM Konfiguracijski čarobnjak.
5. Da konfigurirate usluge provjere autentičnosti mreže, izvedite sljedeće korake:
   a. Na stranici **Konfiguracija Usluga provjere autentičnosti mreže** izaberite **Da** da pokrenete čarobnjaka Konfiguracije Usluga provjere autentičnosti mreže. S ovim čarobnjakom, možete konfigurirati nekoliko i5/OS sučelja i servisa da sudjeluju u Kerberos području kao i konfigurirati jedno okruženje prijave koje koristi i EIM i servis provjere autentičnosti mreže.
   b. Na stranici **Specificiranje informacija područja** navedite ime default područja u polju **Default područje**. Ako koristite Microsoft Aktivni direktorij za Kerberos provjeru autentičnosti izaberite **Microsoft Aktivni direktorij se koristi za Kerberos provjeru autentičnosti** i kliknite **Sljedeće**.
   c. Na stranici **Specificiranje KDC informacija** navedite puno ispravno ime Kerberos poslužitelja za ovo područje u **KDC** polju, navedite 88 u polju **Port**, a zatim kliknite **Sljedeće**.
   d. Na stranici **Specificiranje informacija Lozinke poslužitelja** izaberite ili **Da** ili **Ne** za postavljanje lozinke poslužitelja. Poslužitelj lozinki dozvoljava principalima mijenjanje lozinke na Kerberos poslužitelju. Ako izaberete **Da**, unesite ime poslužitelja lozinke u polje **Poslužitelj lozinke**. U polju **Port** prihvatite default vrijednost 464, a zatim kliknite Sljedeće.
   e. Na stranici **Izaberite unose tablice ključeva**, izaberite **i5/OS Kerberos provjera autentičnosti** i kliknite **Sljedeće**.

      Bilješka: Dodatno, možete također kreirati unose tablice ključeva za IBM Tivoli Directory Server za i5/OS, i5/OS NetServer, i IBM HTTP poslužitelj za i5/OS ako želite da ove usluge koriste Kerberos provjeru autentičnosti. Možda ćete trebati dodatno konfigurirati ove usluge da bi mogle koristiti Kerberos provjeru autentičnosti.
   f. Na stranici **Kreiraj unos tablice ključeva i5/OS-a**, unesite i potvrdite lozinku i kliknite **Sljedeće**. To je ista lozinka koju ćete koristiti kada dodajete i5/OS principale na Kerberos poslužitelj.

g. Opcijsko: Na stranici **Kreiranje paketne datoteke** izaberite **Da**, navedite sljedeće informacije i kliknite **Sljedeće**:
   - U polju **Paketna datoteka** ažurirajte stazu direktorija. Kliknite **Pregled** da biste pronašli odgovarajuću stazu direktorija ili u polju **Paketna datoteka** uredili stazu.
   - U polju **Uključi lozinku** izaberite **Da**. To osigurava da su sve lozinke pridružene s principalom uslugei5/OS-a uključene u paketnu datoteku. Važno je primijetiti da su lozinke prikazane u jasnom tekstu i da ih može pročitati bilo tko tko ima dozvolu za čitanje paketne datoteke. Prema tome, bitno je da paketnu datoteku izbrišete s Kerberos poslužitelja i s PC-a odmah nakon njene upotrebe. Ako lozinku ne uključite, ona će se od vas zatražiti prilikom pokretanja paketne datoteke.

     Bilješka: Također možete ručno dodati principale usluge koje generira čarobnjak u Microsoft Aktivnom direktoriju. Da naučite kako to učiniti, pregledajte Dodavanje i5/OS principala Kerberos poslužitelju
   - Na stranici **Sažetak** pregledajte pojedinosti konfiguracije usluge provjere autentičnosti mreže, a zatim kliknite **Završi** da biste se vratili u čarobnjak EIM konfiguracije.

6. Na stranici **Specificiranje kontrolera domene** osigurajte sljedeće informacije:

   Bilješka: Poslužitelj direktorija koji djeluje kao kontroler domene mora biti aktivan da bi uspješno dovršio EIM konfiguraciju.

   a. U polju **Ime kontrolera domene**, specificirajte ime sistema koji služi kao kontroler domene za EIM domenu kojoj želite da se s njom spoji System i platforma.
   b. Kliknite **Koristi sigurnu vezu (SSL ili TLS)** ako želite koristiti sigurnu vezu s EIM kontrolorom domene. Kada je ovo izabrano, veza koristi ili Sloj Sigurnih Utičnica (SSL) ili Sigurnost Transportnog Sloja (TLS) za uspostavu sigurne veze za zaštitu EIM prijenosa podataka preko nepouzdane mreže kakav je Internet.

      Bilješka: Morate provjeriti je li EIM kontroler domene konfiguriran za korištenje sigurne veze. U suprotnom, veza s kontrolerom domene može ne uspjeti.
   c. U polju **Port** navedite TCP/IP port na kojem sluša poslužitelj direktorija. Ako je izabrano **Koristi sigurnu vezu**, default port je 636; u suprotnom je port 389.
   d. Kliknite **Provjeri vezu** da provjerite može li čarobnjak koristiti navedene informacije za uspješnu uspostavu veze s EIM kontrolerom domene.
   e. Kliknite **Sljedeće**.

7. Na stranici **Specificiranje korisnika za vezu** za vezu izaberite **Tip korisnika**. Možete izabrati jedan od sljedećih tipova korisnika: **Razlikovno ime i lozinka**, **Kerberos datoteka tablice ključeva i principal**, **Kerberos principal i lozinka**, ili **Korisnički profil i lozinka**. Dva Kerberos tipa korisnika su dostupna samo ako je usluga provjere autentičnosti mreže konfigurirana za lokalnu System i platformu. Tip korisnika koji izaberete određuje druge informacije koje morate dobaviti za dovršavanje dijaloga kako slijedi:

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

   Možete navesti različitog korisnika za vezu, međutim, korisnik kojeg navedete mora imati ekvivalent LDAP administratorskom ovlaštenju za udaljenog poslužitelja direktorija.

   - Ako izaberete **Razlikovno ime i lozinka**, omogućite sljedeće informacije:
     – U polju **Razlikovno ime** navedite LDAP razlikovno ime (DN) koje identificira korisnika koji ima ovlaštenja za kreiranje objekata u lokalnom prostoru LDAP poslužitelja. Ako ste ovog čarobnjaka koristili za konfiguriranje LDAP poslužitelja 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 ključeva i principal**, omogućite sljedeće informacije:

– U polju **Datoteka tablice ključeva** navedite punu ispravnu stazu i ime datoteke tablice ključeva koja sadrži Kerberos principala kojeg će čarobnjak koristiti prilikom povezivanja na EIM domenu. Ili, kliknite **Pregledaj...** za pretraživanje kroz direktorije u System i integriranom sistemu datoteka za brisanje datoteke tablice ključeva.
– U polju **Principal** navedite ime Kerberos principala koji će se koristiti za identificiranje korisnika.
– U polju **Područje** navedite puno ispravno ime Kerberos područja čiji je principal član. Ime principala i područja jedinstveno identificiraju Kerberos korisnike u datoteci tablice ključeva. Na primjer, principal jsmith u području ordept.myco.com, predstavljeno je u datoteci tablice ključeva kao jsmith@ordept.myco.com.

• Ako izaberete **Kerberos principal i lozinka**, osigurajte sljedeće informacije:
– U polju **Principal** navedite ime Kerberos principala koje će čarobnjak koristiti prilikom spajanja na EIM domenu.
– U polju **Područje** navedite puno ispravno ime Kerberos područja čiji je principal član. Ime principala i područja jedinstveno identificiraju Kerberos korisnike u datoteci tablice ključeva. Na primjer, principal jsmith u području ordept.myco.com u datoteci tablice ključeva 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 **Korisnički profil i lozinka**, navedite sljedeće informacije:
– U polju **Korisnički profil** navedite ime korisničkog profila koje će čarobnjak koristiti prilikom spajanja na EIM domenu.
– U polju **Lozinka** navedite lozinku korisničkog profila.
– U polju **Potvrda lozinke** drugi put navedite lozinku za svrhu provjere valjanosti.

• Kliknite **Provjera veze** da provjerite može li čarobnjak koristiti navedene korisničke informacije za uspješnu uspostavu veze s EIM kontrolerom domene.
• Kliknite **Sljedeće**.

8. Na stranici **Specificiranje domene** izaberite ime domene kojoj želite pristupiti i kliknite **Sljedeće**.
9. Na stranici **Informacije registra** navedite treba li dodati korisničke registre u EIM domenu kao definicije registra. Izaberite jedan ili oba korisnička tipa registra:
• Izaberite **Lokalni i5/OS** 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 specifičnu instancu tog registra.

Bilješka: Trenutno ne morate kreirati lokalnu definiciju registra i5/OS-a. Ako odlučite kasnije kreirati i5/OS definiciju registra, morate dodati definiciju registra sistema i ažurirati svojstva konfiguracije EIM-a.

• 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 područja. Prihvaćanjem default imena upotrebom istog imena Kerberos registra možete povećati performanse pri dohvaćanju informacija iz registra. Ako je potrebno, izaberite **Kerberos korisnički identiteti osjetljivi su na velika i mala slova**.

Bilješka: Ako ste Čarobnjaka EIM konfiguracije koristili na drugom sistemu za dodavanje definicije registra za Kerberos registar za koji ovaj System i model ima principal servisa, ne trebate dodavati definiciju Kerberos registra kao dio ove konfiguracije. Međutim, ime Kerberos registra trebat ćete navesti u konfiguracijskim svojstvima za ovaj sistem nakon što završite s čarobnjakom.

• Kliknite **Sljedeće**.

10. Na stranici **Specificiranje EIM sistemskog korisnika** izaberite **Tip korisnika** kojeg želite da korisnik koristi kada izvodi EIM operacije za funkcije operativnog sistema. Ove operacije uključuju operacije pregledavanja mapiranja i brisanje asocijacija kada se briše lokalni profil i5/OS korisnika. Možete izabrati jedan od sljedećih korisničkih tipova: **Razlikovno ime i lozinka**, **Kerberos datoteka tablice ključeva i principal** ili **Kerberos principal i lozinka**. Tip korisnika koji možete izabrati varira ovisno o trenutnoj konfiguraciji sistema. Na primjer,

ako Usluga Mrežne Provjere Autentičnosti nije konfigurirana za sistem, tada Kerberos tip korisnika možda neće biti dostupan za izbor. Tip korisnika koji izaberete određuje ostale informacije koje morate omogućiti da bi se stranica ispunila na sljedeći način:

Bilješka: Morate navesti korisnika koji je trenutno definiran u poslužitelju direktorija na kojem je smješten EIM kontroler domene. Korisnik kojeg specificirate mora imati minimalne povlastice za izvođenje pregledavanja mapiranja i administracije registra za lokalni korisnički registar. Ako korisnik kojeg ste specificirali nema te povlastice, neke određene funkcije operativnog sistema koje se odnose na upotrebu jednostruke prijave i na brisanje korisničkih profila mogu biti neuspješne.

- Ako izaberete **Razlikovno ime i lozinka**, omogućite sljedeće informacije:
  - U polju **Razlikovno ime** navedite LDAP razlikovno ime koje identificira korisnika, a koje će sistem koristiti prilikom izvođenja 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 sljedeće informacije:
  - U polju **Principal** navedite ime Kerberos principala kojeg će sistem koristiti prilikom izvođenja EIM operacija.
  - U polju **Područje** navedite puno ispravno ime Kerberos područja čiji je principal član. Ime principala i područja jedinstveno identificiraju Kerberos korisnike u datoteci tablice ključeva. Na primjer, principal jsmith u području ordept.myco.com u datoteci tablice ključeva 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 ključeva i principal**, omogućite sljedeće informacije:
  - U polju **Datoteka tablice ključeva** navedite punu ispravnu stazu i ime datoteke tablice ključeva koja sadrži Kerberos principala kojeg će sistem koristiti prilikom izvođenja EIM operacija. Ili, kliknite **Pregledaj...** za pretraživanje kroz direktorije u System i integriranom sistemu datoteka za brisanje datoteke tablice ključeva.
  - U polju **Principal** navedite ime Kerberos principala kojeg će sistem koristiti prilikom izvođenja EIM operacija.
  - U polju **Područje** navedite puno ispravno ime Kerberos područja čiji je principal član. Ime principala i područja jedinstveno identificiraju Kerberos korisnike u datoteci tablice ključeva. Na primjer, principal jsmith u području ordept.myco.com u datoteci tablice ključeva predstavljen je kao jsmith@ordept.myco.com.
- Kliknite **Provjera veze** da osigurate da čarobnjak može koristiti navedene korisničke informacije za uspješnu uspostavu veze s EIM kontrolerom domene.
- Kliknite **Sljedeće**.

11. Na stranici **Sažetak** pregledajte informacije konfiguracije koje ste osigurali. Ako su sve informacije točne, kliknite **Završetak**.

Finaliziranje vaše konfiguracije EIM-a za domenu

Kada se čarobnjak završi on dodaje domenu u folder **Upravljanje domenom** i na taj ste način kreirali osnovnu EIM konfiguraciju za ovaj sistem. Međutim, možda ćete ove zadatke trebati dovršiti da biste vašu EIM konfiguraciju za domenu završili:

1. Ako je potrebno, dodajte definicije EIM registra u EIM domenu za sisteme koji ne izvode i5/OS sisteme i aplikacije za koje želite da sudjeluju u EIM domeni. Ove definicije registra odnose se na stvarne korisničke registre koji moraju sudjelovati u domeni. Možete Dodati sistemske definicije registra ili Dodati definicije registra aplikacije ovisno o potrebama vaše EIM implementacije.
2. Ovisno o potrebama vaše 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 korisnički identitet.

- Kreirati kombinaciju istih.

3. Koristite EIM funkciju testiranje mapiranja da testirate mapiranje identiteta vaše EIM konfiguracije.
4. Ako je jedini EIM korisnik kojeg ste definirali, DN za LDAP administratora, tada vaš EIM korisnik ima visoku razinu ovlaštenja nad svim podacima na poslužitelju direktorija. Prema tome, možete razmotriti kreiranje jednog ili više DN-ova kao dodatne korisnike koji imaju prikladniju i ograničenu kontrolu pristupa za podatke EIM-a. Da naučite više o kreiranju DN-ova za poslužitelj direktorija, pregledajte Razlikovna imena u i5/OS Informacijski centar. Broj dodatnih EIM korisnika koje definirate ovisi o vašoj sigurnosnoj politici s naglaskom na razdvajanju sigurnosnih zadataka i odgovornosti. Tipično, možete kreirati barem dva sljedeća tipa DN-ova:
   - **Korisnik koji ima kontrolu pristupa EIM administratora**

     Ovaj EIM administratorski DN omogućuje prikladnu razinu ovlaštenja za administratore koji su odgovorni za upravljanje EIM domenom. Ovaj EIM administratorski DN se ne može koristiti za povezivanje na kontroler domene kod upravljanja svim aspektima EIM domene pomoću System i Navigator.
   - **Barem jedan korisnik koji ima sljedeće kontrole pristupa**:
     - Administrator identifikatora
     - Administrator registra
     - EIM operacije mapiranja

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

   Bilješka: Za upotrebu ovog novog DN-a za sistemskog korisnika umjesto LDAP administratorskog DN-a, morate promijeniti svojstva EIM konfiguracije za System i platformu. Pregledajte Upravljanje svojstvima EIM konfiguracije da naučite kako promijeniti DN sistemskog korisnika.

Možda ćete morati izvesti dodatne zadatke ako ste kreirali osnovnu konfiguraciju usluge provjere autentičnosti mreže, posebno ako primjenjujete okolinu jednostruke prijave. Informacije o dodatnim koracima možete pronaći pregledavanjem svih koraka konfiguracije prikazanih u scenariju, Omogućavanje jednostruke prijave za i5/OS.

Konfiguriranje sigurne veze na EIM kontroler domene

Možda ćete htjeti koristiti Sloj sigurnih utičnica (SSL) ili Sigurnosni protokol transportnog sloja (TLS) za uspostavu sigurne veze na kontroler domene Mapiranja identiteta u poduzeću (EIM) da zaštitite podatke EIM-a.

Da konfigurirate SSL ili TLS za EIM, morate dovršiti sljedeće zadatke:

1. Ako je potrebno, koristite Upravitelj digitalnih certifikata (DCM) da kreirate certifikat za poslužitelj direktorija za upotrebu u SSL.
2. Omogućite SSL za lokalne poslužitelje direktorija na kojem je smješten EIM kontroler domene.
3. Ažurirajte svojstva EIM Konfiguracije da specificirate da System i model koristi sigurnu SSL vezu. Za ažuriranje EIM svojstava konfiguracije, izvedite sljedeće korake:
   a. U System i Navigator, izaberite sistem na kojem želite konfigurirati EIM i proširite **Mreža → Mapiranje identiteta u poduzeću**.
   b. Desno kliknite **Konfiguracija** i izaberite **Svojstva**.
   c. Na stranici **Domena** izaberite **Koristi sigurnu vezu (SSL ili TLS)**, navedite sigurni port na kojem poslužitelj direktorija sluša ili prihvaća default vrijednost 636 u polju **Port**, a zatim kliknite **OK**.
4. Ažurirajte svojstva EIM Domene za svaku EIM domenu da specificirate da EIM koristi SSL vezu kod upravljanja domenom preko System i Navigator. Za ažuriranje svojstava EIM domene, izvedite sljedeće korake:
   a. U System i Navigator, izaberite sistem na kojem ste konfigurirali EIM i proširite **Mreža → Mapiranje identiteta u poduzeću → Upravljanje domenom**.
   b. Izaberite EIM domenu u kojoj želite raditi.
      - Ako EIM domena s kojom želite raditi nije popisana pod **Upravljanje domenom**, pregledajte Dodaj EIM domenu u Upravljanje domenom.

- Ako trenutno niste povezani na EIM domenu u kojoj želite raditi, pregledajte Povezivanje na EIM kontroler 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 poslužitelj direktorija sluša ili prihvaća default vrijednost 636 u polju **Port**, a zatim kliknite **OK**.

Upravljanje Mapiranjem identiteta u poduzeću

Nakon konfiguracije Mapiranja identiteta u poduzeću (EIM) na vašoj System i platformi, postoji mnogo administrativnih zadataka koje trebate izvesti tijekom vremena za upravljanje EIM domenom i podacima za domenu.

Za naučiti više o EIM upravljanju u vašem poduzeću, pregledajte ove stranice.

Upravljanje domenama Mapiranja identiteta u poduzeću

Koristite System i Navigator za upravljanje svim vašim EIM domenama.

Za upravljanje bilo kojom EIM domenom, domena mora biti popisana, ili ju morate dodati u folder **Upravljanje domenom** pod folder **Mreža** u System i Navigator. Kada koristite čarobnjaka EIM konfiguracije za kreiranje i konfiguriranje nove EIM domene, domena se automatski dodaje u folder **Upravljanje domenom** tako da možete upravljati domenom i informacijama u domeni.

Za upravljanje bilo kojom EIM domenom koja se nalazi bilo gdje na istoj mreži možete koristiti bilo koju System i vezu, čak i ako sistem koji koristite ne sudjeluje u domeni.

Možete izvesti sljedeće zadatke upravljanja za domenu:

Dodavanje EIM domene u folder Upravljanje domenom

Za dodavanje EIM domene u folder Upravljanje domenom morate imati *SECADM posebno ovlaštenje i domena koju dodajete mora postojati prije njenog dodavanja u folder Upravljanje domenom.

Za dodavanje postojeće domene Mapiranja identiteta u poduzeću (EIM) u folder **Upravljanje domenom**, izvedite ove korake:

1. Proširite **Mreža >Mapiranje identiteta u poduzeću**.
2. Desno kliknite **Upravljanje domenom** i izaberite **Dodaj domenu**.
3. U dijalogu **Dodavanje domene**, specificirajte potrebnu domenu i informacije povezivanja. Ili, kliknite **Pregledaj** za pogled na popis domena kojima upravlja specificirani kontroler domene.

   Bilješka: Ako kliknete **Pregledaj**, prikazuje se dijalog **Povezivanje na EIM kontroler domene**. Za pogled na popis domena, morate se povezati na kontroler domene pomoću LDAP administratorske kontrole pristupa, ili pomoću EIM administratorske kontrole pristupa. Sadržaji liste domena variraju ovisno o tipu EIM kontrole pristupa koju imate. Ako imate LDAP administratorsku kontrolu pristupa, možete 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 **Pomoć** da odredite koje informacije navesti u određenom polju.
5. Kliknite **OK** za dodavanje domene.

Povezivanje na EIM domenu

Prije nego možete raditi s domenom Mapiranja identiteta u poduzeću (EIM), morate se prvo povezati na EIM kontroler domene za domenu. Na EIM domenu se možete povezati čak i ako System i model trenutno nije konfiguriran za sudjelovanje u ovoj domeni.

Za povezivanje na EIM kontroler domene, korisnik s kojim se povezujete mora biti član grupe za EIM kontrolu pristupa. Vaše članstvo grupe za EIM kontrolu pristupa određuje koje zadatke možete izvoditi u domeni i koje EIM podatke možete pregledavati ili mijenjati.

Da se povežete na EIM domenu, dovršite sljedeće korake:

1. Proširite **Mreža > Mapiranje identiteta u poduzeću > Upravljanje domenom**.
2. Desno kliknite na domenu na koju se želite povezati.

   Bilješka: Ako domena s kojom želite raditi nije popisana pod **Upravljanje domenom**, EIM domenu morate dodati u folder za upravljanje domenom.
3. Desno kliknite na EIM domenu na koju se želite 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 **Pomoć** da odredite koje informacije navesti u svakom polju u dijalogu.
6. Kliknite **OK** za povezivanje na kontroler domene.

Omogućavanje asocijacija politike za domenu

Asocijacija politike pruža načine kreiranja više-na-jedan mapiranja u situacijama gdje asocijacije između identiteta korisnika i identifikatora Mapiranja identiteta u poduzeću (EIM) ne postoje.

Asocijaciju politike možete koristiti za mapiranje izvornog skupa višestrukih korisničkih identiteta (umjesto jednostrukog korisničkog identiteta) na jednostruki ciljni korisnički identitet u određenom ciljnom korisničkom registru. Da biste mogli koristiti asocijacije politike morate biti sigurni da ste domenu omogućili za korištenje asocijacija politika za operacije pregledavanja mapiranja.

Da omogućite podršku politike mapiranja za upotrebu asocijacija politike, morate biti povezani na EIM domenu na kojoj želite raditi i morate imati EIM administratorsku kontrolu pristupa.

Za omogućavanje podrške pregledavanja mapiranja da koristi asocijacije politike za domenu, izvedite sljedeće korake:

1. Proširite **Mreža > Mapiranje identiteta u poduzeću > Upravljanje domenom**.
2. Desno kliknite na EIM domenu na kojoj želite raditi i izaberite **Politika mapiranja**.
   - Ako EIM domena s kojom želite raditi nije popisana pod **Upravljanje domenom**, EIM domenu morate dodati u folder za upravljanje domenom.
   - Ako trenutno niste povezani na EIM domenu u kojoj želite raditi, morate se povezati na EIM kontroler domene. (Opcija **Politika mapiranja** nije dostupna sve dok se ne povežete na domenu.)
3. Na stranici **Općenito** izaberite **Omogući pregledavanje mapiranja korištenjem asocijacija politika za domenu**.
4. Kliknite **OK**.

Bilješka: Također, morate omogućiti pregledavanje mapiranja i upotrebu asocijacija politike za svaku definiciju ciljnog registra za koju je definirana asocijacija politika. Ako ne omogućite pregledavanja mapiranja za definiciju ciljnog registra, taj registar ne može sudjelovati u EIM operacijama pregledavanja mapiranja. Ako ne navedete da ciljni registar može koristiti asocijacije politike, tada EIM operacije pregledavanja mapiranja ignoriraju bilo koju definiranu asocijaciju politike za taj registar.

Srodni koncepti

"Podrška politici mapiranja EIM i omogućivanje" na stranici 37
Podrška politike Mapiranja identiteta u poduzeću (EIM) dozvoljava vam korištenje asocijacija politike kao i određenih asocijacija identifikatora u nekoj EIM domeni. Asocijacije politika možete koristiti umjesto ili u kombinaciji s asocijacijama identifikatora.

Testiranje EIM mapiranja

Testiranje Mapiranja identiteta u poduzeću (EIM) vam omogućuje izdavanje operacija pregledavanja EIM mapiranja nad vašom EIM konfiguracijom. Testiranje možete koristiti za provjeravanje da se specifični izvorni korisnički identitet ispravno mapira na odgovarajući ciljni korisnički identitet. Testiranje osigurava da operacije pregledavanja EIM mapiranja mogu vratiti ispravne ciljne korisničke identitete bazirane na specificiranim informacijama.

Za upotrebu funkcije testiranja mapiranja za testiranje vaše EIM konfiguracije morate biti povezani na EIM domenu u kojoj želite raditi i morate imati EIM kontrolu pristupa na jednu od sljedećih razina:

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

Za korištenje podrške testiranja mapiranja za testiranje vaše EIM konfiguracije, izvedite sljedeće korake:

1. Proširite **Mreža > Mapiranje identiteta u poduzeću > Upravljanje domenom**.
2. Izaberite EIM domenu u kojoj želite raditi.
   - Ako EIM domena s kojom želite raditi nije popisana pod **Upravljanje domenom**, pregledajte Dodaj EIM domenu u Upravljanje domenom.
   - Ako trenutno niste povezani na EIM domenu u kojoj želite raditi, pregledajte Povezivanje na EIM kontroler domene.
3. Desno kliknite EIM domenu na koju ste spojeni i izaberite **Testiranje mapiranja**
4. U dijalogu **Testiranje mapiranja** navedite sljedeće informacije:
   a. U polju **Izvorni registar** osigurajte ime definicije registra koje se odnosi na korisnički registar koji želite koristiti kao izvor testiranja operacije pregledavanja mapiranja.
   b. U polju **Izvorni korisnik** osigurajte ime korisničkog identiteta koji želite koristiti kao izvor testiranja operacije pregledavanja mapiranja.
   c. U polju **Ciljni registar** osigurajte ime definicije registra koje se odnosi na korisnički registar koji želite koristiti kao cilj testiranja operacije pregledavanja mapiranja.
   d. Opcijski: U polju **Informacije pregledavanja**, pružite sve informacije pregledavanja definirane za ciljnog korisnika.
5. Ako je potrebno, za više pojedinosti o tome koje informacije su potrebne za svako polje dijaloga kliknite **Pomoć**.
6. Kliknite **Testiraj** i pogledajte rezultate operacije pregledavanja mapiranja kada se oni pojave.

   Bilješka: Ako operacija pregledavanja mapiranja vraća dvosmislene rezultate, prikazuje se dijalog Test mapiranja - Rezultati koji pokazuje poruku greške i listu ciljnih korisnika koje operacija pregledavanja pronalazi.
   a. Da preispitate dvosmislene rezultate, izaberite ciljnog korisnika i kliknite **Detalji**.
   b. Prikazuje se dijalog Test mapiranja - Detalji koji pokazuje informacije o rezultatima operacije pregledavanja mapiranja za navedenog ciljnog korisnika. Kliknite Pomoć za detaljnije informacije o rezultatima operacije pregledavanja mapiranja.
   c. Kliknite **Zatvori** za izlaz iz dijaloga **Test mapiranja - Rezultati**.
7. Nastavite testirati vašu konfiguraciju ili za izlaz kliknite **Zatvori**.

Srodni koncepti

“Rješavanje problema EIM mapiranja” na stranici 116
Postoje brojni uobičajeni problemi koji mogu prouzročiti potpuni neuspjeh mapiranja u Mapiranju identiteta u poduzeću (EIM) ili neočekivani rad. Pregledajte sljedeću tablicu da pronađete informacije o tome koji problemi mogu uzrokovati neuspjeh EIM mapiranja i moguća rješenja tog problema. Ako ne uspije EIM mapiranje, trebati ćete proučiti svako rješenje u tablici kako bi osigurali pronalazak i rješenje jednog ili više problema koji su uzrok neuspjeha mapiranja.

Rad s rezultatima testiranja i rješavanje problema:

Kada se test izvodi, vraća se ciljni korisnički identitet ako obrada testa pronađe asocijaciju između izvornog korisničkog identiteta i ciljnog korisničkog identiteta koji je osigurao administrator. Test također pokazuje tip asocijacije koji je pronađen između dva korisnička identiteta. Kada postupak testa ne pronađe asocijaciju koja je zasnovana na osiguranim informacijama, test vraća za ciljni korisnički identitet ništa.

Test, poput svake EIM operacije pregledavanja mapiranja, traži i vraća prvi odgovarajući ciljni identitet registra pretražujući sljedećim redoslijedom:

1. Specifična asocijacija identifikatora

2. Asocijacija politike filtera certifikata
3. Asocijacije politike default registra
4. Asocijacija politike default domene

U nekim slučajevima, test ne vraća rezultat ciljnog korisničkog identiteta iako su asocijacije za domenu konfigurirane. Provjerite da ste za test osigurali ispravne informacije. Ako su informacije ispravne i test ne vraća rezultate, tada problem može biti uzrokovan jednim od sljedećeg:

- Podrška asocijacije politike nije omogućena na razini domene. Trebat ćete omogućiti asocijacije politike za domenu.
- Podrška pregledavanja mapiranja ili podrška asocijacije politike nije omogućena na individualnoj razini registra. Možda ćete morati omogućiti podršku pregledavanja mapiranja i korištenje 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 netočni korisnički identitet. Prikažite sve asocijacije identifikatora za EIM identifikator da provjerite asocijacije za specifični identifikator.
- Asocijacija politike nije ispravno konfigurirana. Prikažite sve asocijacije politika za domenu da provjerite izvorne i ciljne informacije za sve asocijacije politike definirane u domeni.
- Definicija registra i korisnički identitet ne podudaraju se zbog osjetljivosti na velika i mala slova. Možete obrisati i ponovo kreirati registar, ili obrisati i ponovo kreirati asocijaciju s ispravnim slovnikom.

U drugim slučajevima, test može imati dvosmislene rezultate. U takvim slučajevima, prikazuje se poruka pogreške koja na to ukazuje. Test vraća dvosmislene rezultate kada više od jednog ciljnog korisničkog rezultata odgovara navedenim kriterijima testa. Operacija pregledavanja mapiranja može vratiti višestruke korisničke registre kada postoji jedna ili više od sljedećih situacija:

- EIM identifikator ima višestruke individualne ciljne asocijacije na istom ciljnom registru.
- Više od jednog EIM identifikatora ima isti korisnički identitet naveden u izvornoj asocijaciji i svaki ih tih EIM identifikatora ima ciljnu asocijaciju na istom ciljnom registru, iako korisnički identitet naveden za svaku ciljnu asocijaciju može biti različit.
- Više od jedne asocijacije politike default domene specificira isti ciljni registar.
- Više od jedne default asocijacije politike registra specificira isti izvorni registar i isti ciljni registar.
- Više od jedne asocijacije politike filtera certifikata specificira isti izvorni X.509 registar, filter certifikata i ciljni registar.

Operacija pregledavanja mapiranja koja vraća više od jednog identiteta ciljnog korisnika može stvoriti probleme EIM-omogućenim aplikacijama, uključujući i5/OS aplikacije i proizvode. Prema tome potrebno je odrediti uzrok dvosmislenih rezultata i koje akcije treba poduzeti da bi se riješila situacija. Ovisno o uzroku možete učiniti jedno ili više od sljedećeg:

- Test vraća neželjene višestruke ciljne identitete. To ukazuje da konfiguracije asocijacije za domenu nije ispravna zbog jednog od sljedećeg:
  - 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 netočni korisnički identitet. Prikažite sve asocijacije identifikatora za EIM identifikator da provjerite asocijacije za specifični identifikator.
  - Asocijacija politike nije ispravno konfigurirana. Prikažite sve asocijacije politika za domenu da provjerite izvorne i ciljne informacije za sve asocijacije politike definirane u domeni.
- Ako test vraća višestruke ciljne korisničke identitete i ti su rezultati odgovarajući za način na koji ste konfigurirali asocijacije, tada morate navesti informacije pregledavanja za svaki ciljni korisnički identitet. Morate definirati jedinstvene informacije pregledavanja za sve ciljne korisničke identitete koji imaju isti cilj (bilo EIM identifikator za asocijacije identifikatora ili ciljni korisnički registar za asocijacije politika). Definiranjem informacija pregledavanja za svaki ciljni korisnički identitet osiguravate da operacija pregledavanja vraća jednostruki ciljni korisnički identitet umjesto svih mogućih ciljnih korisničkih identiteta. Pregledajte Dodavanje informacija pregledavanja ciljnom korisničkom identitetu. Morate navesti ove informacije pregledavanja o operaciji pregledavanja mapiranja.

Bilješka: Ovaj pristup radi samo ako je aplikacija omogućena za korištenje informacija pregledavanja. Ipak, osnovne i5/OS aplikacije kao na primjer System i Access za Windows ne mogu koristiti informacije pregledavanja za razlikovanje između više ciljnih korisničkih identiteta vraćenih od strane operacije pregledavanja. Prema tome, možete razmotriti redefiniciju asocijacija za domenu da osigurate da operacija pregledavanja mapiranja može vratiti jednostruki ciljni identitet korisnika, da osigurate da osnovne i5/OS aplikacije mogu uspješno izvoditi operacije pregledavanja i mapirati identitete.

Uklanjanje EIM domene iz foldera Upravljanje domenom

EIM domenu kojom više ne želite upravljati možete ukloniti iz foldera **Upravljanje domenom**. Međutim, uklanjanje domene iz foldera **Upravljanje domenom nije** isto što i brisanje domene, jer se pritom ne brišu podaci domene iz kontrolera domene.

Za uklanjanje domene nije vam potrebna EIM kontrola pristupa.

Za uklanjanje domene Mapiranja identiteta u poduzeću (EIM) kojom više ne želite upravljati iz foldera **Upravljanje domenom**, poduzmite ove korake:

1. Proširite **Mreža >Mapiranje identiteta u poduzeću**.
2. Desno kliknite na **Upravljanje domenom** i izaberite **Ukloni domenu**.
3. Izaberite EIM domenu koju želite ukloniti iz **Upravljanja domenom**.
4. Kliknite **OK** za uklanjanje domene.

Srodni zadaci

"Brisanje EIM domene i svih konfiguracijskih objekata"
Prije nego možete obrisati EIM domenu, morate obrisati sve definicije registra i sve identifikatore Mapiranja identiteta u poduzeću (EIM) u domeni. Ako ne želite obrisati domenu i sve podatke u domeni, ali i ne želite više upravljati domenom, imate mogućnost uklanjanja domene.

Brisanje EIM domene i svih konfiguracijskih objekata

Prije nego možete obrisati EIM domenu, morate obrisati sve definicije registra i sve identifikatore Mapiranja identiteta u poduzeću (EIM) u domeni. Ako ne želite obrisati domenu i sve podatke u domeni, ali i ne želite više upravljati domenom, imate mogućnost uklanjanja domene.

Za brisanje EIM domene morate imati EIM kontrolu pristupa na jednu od sljedećih razina:

- LDAP administrator.
- EIM administrator.

1. Proširite **Mreža > Mapiranje identiteta u poduzeću > Upravljanje domenom**.
2. Ako je potrebno obrišite sve definicije registra iz EIM domene.
3. Ako je potrebno obrišite sve EIM identifikatore iz EIM domene.
4. Desno kliknite domenu kojom želite obrisati i izaberite **Brisanje**.
5. Kliknite **Da** u dijalogu **Potvrda brisanja**.

Bilješka: Prikazuje se dijalog Brisanje u tijeku da pokazuje status brisanja domene dok se proces ne dovrši.

Srodni zadaci

"Uklanjanje EIM domene iz foldera Upravljanje domenom"
EIM domenu kojom više ne želite upravljati možete ukloniti iz foldera **Upravljanje domenom**. Međutim, uklanjanje domene iz foldera **Upravljanje domenom nije** isto što i brisanje domene, jer se pritom ne brišu podaci domene iz kontrolera domene.

Upravljanje definicijama registra Mapiranja identiteta u poduzeću

Da bi korisnički registri i korisnički identiteti koje sadrže sudjelovali u EIM domeni, morate za njih kreirati definicije registra. Tada možete upravljati kako korisnički registri i njihovi korisnički identiteti sudjeluju u EIM-u s upravljanjem tim EIM definicijama registra.

Možete izvesti sljedeće zadatke upravljanja za definicije registra:

Srodni koncepti

"Kreiranje asocijacije politike" na stranici 99
Asocijacija politike je sredstvo za direktno definiranje odnosa između višestrukih korisničkih identiteta u jednom ili više registara i individualnog ciljnog korisničkog identiteta u drugom registru.

Srodni zadaci

"Brisanje asocijacije politike" na stranici 111
Za brisanje asocijacije politike morate biti povezani na domenu Mapiranja identiteta u poduzeću (EIM) na kojoj želite raditi i morate imati EIM kontrolu pristupa za Administratora registra, ili za EIM administratora.

Dodavanje definicije sistemskog registra

Za kreiranje definicije sistemskog registra, morate biti povezani na domenu Mapiranja identiteta u poduzeću (EIM) na kojoj želite raditi i morate imati kontrolu pristupa EIM administratora.

Za dodavanje definicije sistemskog registra u EIM domenu, izvedite sljedeće korake.

1. Proširite **Mreža > Mapiranje identiteta u poduzeću > Upravljanje domenom**.
2. Izaberite EIM domenu u kojoj želite raditi.
   - Ako EIM domena s kojom želite raditi nije popisana pod Upravljanje domenom, pregledajte "Dodavanje EIM domene u folder Upravljanje domenom" na stranici 84.
   - Ako trenutno niste povezani na EIM domenu na kojoj želite raditi, pregledajte "Povezivanje na EIM domenu" na stranici 84.
3. Proširite EIM domenu na koju ste sada povezani.
4. Desno kliknite **Korisnički registri**, izaberite **Dodaj registar**, zatim izaberite **Sistemski**.
5. U dijalogu **Dodavanje sistemskog registra** osigurajte informacije o definiciji sistemskog registra kako slijedi:
   a. Ime za definiciju sistemskog registra.
   b. Tip definicije registra.
   c. Opis definicije sistemskog registra.
   d. (Opcijski.) Korisnički registar URL.
   e. Ako je potrebno, jedno ili više zamjenskih imena za definiciju sistemskog registra.
6. Kliknite **OK** za spremanje informacija i dodavanje definicije registra u EIM domenu.

Dodavanje definicije registra aplikacija

Za kreiranje definicije registra aplikacije, morate biti povezani na domenu Mapiranja identiteta u poduzeću (EIM) na kojoj želite raditi i morate imati kontrolu pristupa EIM administratora.

Za dodavanje definicije registra aplikacije u EIM domenu, izvedite sljedeće korake:

1. Proširite **Mreža > Mapiranje identiteta u poduzeću > Upravljanje domenom**.
2. Izaberite EIM domenu u kojoj želite raditi.
   - Ako EIM domena s kojom želite raditi nije popisana pod Upravljanje domenom, pregledajte "Dodavanje EIM domene u folder Upravljanje domenom" na stranici 84.
   - Ako trenutno niste povezani na EIM domenu na kojoj želite raditi, pregledajte "Povezivanje na EIM domenu" na stranici 84.
3. Proširite EIM domenu na koju ste sada povezani.
4. Desno kliknite **Korisnički registri**, izaberite **Dodaj registar**, zatim izaberite **Aplikacija**.
5. U dijalogu **Dodavanje registra aplikacija** osigurajte informacije o definiciji registra aplikacije kako slijedi:
   a. Ime za definiciju registra aplikacije.
   b. Ime definicije sistemskog registra čiji je podskup registar korisnika aplikacije koji definirate. Definicija sistemskog registra koji specificirate mora već postojati u EIM-u inače kreiranje definicije registra aplikacije neće uspjeti.

c. Tip definicije registra.
d. Opis definicije registra aplikacije.
e. Ako je potrebno, jedno ili više zamjenskih imena za definiciju registra aplikacije.

6. Ako je potrebno kliknite **Pomoć** da odredite koje informacije osigurati za svako polje.
7. Kliknite **OK** za spremanje informacija i dodavanje definicije registra u EIM domenu.

Srodni koncepti

"Definicije registra sistema" na stranici 13
Definicija registra sistema je unos koji kreirate u Mapiranju identiteta u poduzeću (EIM) da predstavlja i opisuje zasebni registar korisnika unutar radne stanice ili poslužitelja.

Dodavanje definicije registra grupe

Za kreiranje definicije registra grupe, morate biti povezani na EIM domenu na kojoj želite raditi i morate imati kontrolu pristupa EIM administratora.

Za dodavanje definicije registra grupe u EIM domenu, dovršite ove korake:

1. Proširite **Mreža → Mapiranje identiteta u poduzeću → Upravljanje domenom.**
2. Izaberite EIM domenu u kojoj želite raditi.
   a. Ako EIM domena s kojom želite raditi nije popisana pod Upravljanje domenom, pregledajte Dodavanje EIM domene Upravljanju domenom.
   b. Ako trenutno niste povezani na EIM domenu na kojoj želite raditi, pregledajte Povezivanje na EIM kontroler domene.
3. Proširite EIM domenu na koju ste povezani.
4. Desno kliknite **Korisnički registri**, izaberite **Dodaj registar**, zatim izaberite **Grupa.**
5. U dijalogu Dodaj registar grupe, unesite informacije o definiciji registra grupe, kako slijedi:
   a. Ime za definiciju registra grupe.
   b. Izaberite **Članovi registra grupe su osjetljivi na velika i mala slova** ako su svi članovi definicije registra grupe osjetljivi na velika i mala slova.
   c. Opis definicije registra grupe.
   d. Jedno ili više zamjenskih imena za definiciju registra grupe, ako je potrebno.
6. Ako je potrebno kliknite **Pomoć** da odredite koje informacije osigurati za svako polje.
7. Kliknite **OK** za spremanje informacija i dodavanje definicije registra u EIM domenu.

Dodavanje zamjenskog imena definiciji registra

Vi ili vaš razvijač aplikacija ćete možda htjeti specificirati dodatne razlikovne informacije za definiciju registra. To možete napraviti s kreiranjem zamjenskog imena za definiciju registra. Vi možete ili netko drugi može onda koristiti zamjensko ime za definiciju registra za lakše razlikovanje jednog korisničkog registra od ostalih.

Ta podrška zamjenskom imenu dozvoljava programerima da pišu aplikacije bez da unaprijed znaju proizvoljno ime definicije registra Mapiranja identiteta u poduzeću (EIM) izabrano od strane administratora koji postavlja aplikaciju. Dokumentaciju aplikacije može dobaviti EIM administrator sa zamjenskim imenom koje aplikacija koristi. Korištenjem ovih informacija, EIM administrator može dodijeliti ovo zamjensko ime definiciji EIM registra koja predstavlja stvarni korisnički registar za koji administrator želi da ga aplikacija koristi.

Za dodavanje zamjenskog imena definiciji registra, morate biti povezani na EIM domenu u kojoj želite raditi i morate imati EIM kontrolu pristupa na jednu od sljedećih razina:

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

Za dodavanje zamjenskog imena definiciji EIM registra, izvedite sljedeće korake:

1. Proširite **Mreža > Mapiranje identiteta u poduzeću > Upravljanje domenom**.
2. Izaberite EIM domenu u kojoj želite raditi.
   - Ako EIM domena s kojom želite raditi nije popisana pod Upravljanje domenom, pregledajte “Dodavanje EIM domene u folder Upravljanje domenom” na stranici 84.
   - Ako trenutno niste povezani na EIM domenu na kojoj želite raditi, pregledajte “Povezivanje na EIM domenu” na stranici 84.
3. Proširite EIM domenu na koju ste sada povezani.
4. Za prikaz popisa definicija registra za domenu kliknite **Korisnički registri**.

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

   Bilješka: Možete specificirati tip zamjenskog imena koji nije uključen u popis tipova.
7. Ako je potrebno kliknite **Pomoć** da odredite koje informacije navesti u određenom polju.
8. Kliknite **Dodaj**.
9. Kliknite **OK** za spremanje promjena u definiciju registra.

Definiranje privatnog tipa korisničkog registra u EIM-u

Kada kreirate definiciju registra Mapiranja identiteta u poduzeću (EIM), možete specificirati jedan od niza preddefiniranih tipova registara korisnika radi prikaza stvarnog registra korisnika koji postoji na sistemu unutar poduzeća.

Iako preddefinirani tipovi definicije registra pokrivaju većinu operativnih korisničkih registara, možda ćete trebati kreirati definiciju registra za koju EIM ne uključuje unaprijed definirane tipove registra. U ovoj situaciji imate dvije mogućnosti. Možete ili koristiti postojeću definiciju registra koja se podudara s karakteristikama vašeg korisničkog registra ili možete definirati privatni tip korisničkog registra.

Za definiranje tipa korisničkog registra za koji EIM nije preddefiniran da prepoznaje, morate koristiti objektni identitet (OID) za specificiranje tipa registra u obliku **ObjectIdentifier-normalizacija**, gdje je **ObjectIdentifier** objektni identifikator s decimalnom točkom kao 1.2.3.4.5.6.7, a **normalizacija** ili vrijednost **caseExact** ili vrijednost **caseIgnore**. Na primjer, identifikator objekta (OID) za System i je 1.3.18.0.2.33.2-caseIgnore.

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

Postoje dva načina dobavljanja OID-a:

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

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

- American National Standards Institute (ANSI) je ovlaštenje registracije Sjedinjenih država za imena organizacija pod globalnom registracijskom obradom uspostavljenom od International Standards Organization (ISO) i International Telecommunication Union (ITU). Stranicu činjenica u Microsoft Word formatu o primjeni za Identifikator registriranog dobavljača aplikacija (RID), lociran je na Web stranici ANSI Javna knjižnica dokumenata

http://public.ansi.org/ansionline/Documents/ . Popis činjenica možete pronaći izborom **Ostale usluge > Programi za registraciju**. ANSI OID luk za organizacije je 2.16.840.1. ANSI naplaćuje pristojbu za dodjele OID luka. Potrebno je otprilike dva tjedna za primanje dodijeljenog OID luka iz ANSI-a. ANSI će dodijeliti broj (NEWNUM) za kreiranje novog OID luka; na primjer: 2.16.840.1.NEWNUM.

- U većini zemalja ili regija, udruženje nacionalnih standarda održava OID registar. Kao kod ANSI luka, ovi su općeniti lukovi dodijeljeni pod OID-om 2.16. Može biti potrebno malo istraživanje da se pronađe OID ovlaštenje za određenu zemlju ili regiju. Adrese tijela ISO nacionalnih članova možete pronaći na

  http://www.wssn.net/WSSN/listings/links_national.html . Informacije uključuju poštansku adresu i elektroničku poštu. U mnogim slučajevima specificirana je i Web stranica.
- Ovlaštenje Dodijele Brojeva Internetom (IANA) dodjeljuje privatne brojeve za poduzeća, što su OID-ovi u luku 1.3.6.1.4.1. IANA je dodijelila lukove više od 7500 tvrtki do danas. Aplikacijska stranica smještena je na

  http://www.iana.org/cgi-bin/enterprise.pl , pod Brojevima privatnih poduzeća. IANA obično traje oko jedan tjedan. OID od IANA-e je besplatan. IANA će dodijeliti broj (NEWNUM) za kreiranje novog OID luka; na primjer: 1.3.6.1.4.1.NEWNUM.
- Savezna vlada Sjedinjenih Država održava Computer Security Objects Registry (CSOR). CSOR je ovlaštenje imenovanja za luk 2.16.840.1.101.3 i za trenutne objekte registriranja za sigurnosne labele, kriptografske 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 država. Za više informacija o CSOR-u, pregledajte

  http://www.csrc.nist.gov/pki/CSOR/csor.html .

  Srodni koncepti

  “Definicije EIM registra” na stranici 11
  Definicija registra Mapiranja identiteta u poduzeću (EIM) je unos unutar EIM-a koji kreirate radi prikaza stvarnog korisničkog registra koji postoji na sistemu unutar poduzeća. Korisnički registar djeluje kao direktorij i sadrži listu važećih korisničkih identiteta za pojedinačni sistem ili aplikaciju.

Omogućavanje podrške pregledavanja mapiranja i upotrebe asocijacije politika za ciljni registar

Podrška politike Mapiranja identiteta u poduzeću (EIM) vam dozvoljava upotrebu asocijacija politike kao načina za kreiranje više-na-jedan mapiranja u situacijama gdje ne postoje asocijacije između korisničkih identiteta i EIM identifikatora. Asocijaciju politike možete koristiti za mapiranje izvornog skupa višestrukih korisničkih identiteta (umjesto jednostrukog korisničkog identiteta) na jednostruki ciljni korisnički identitet u određenom ciljnom korisničkom registru.

Da biste mogli koristiti asocijacije politika morate prvo biti sigurni da ste omogućili pregledavanje mapiranja upotrebom asocijacija za domenu. Također morate omogućiti jednu ili dvije postavke za svaki registar:

- **Omogućavanje pregledavanja mapiranja za registar** Izaberite ovu opciju da osigurate da registar može sudjelovati u EIM operacijama pregledavanja mapiranja bez obzira je li za registar definirana bilo kakva asocijacija politika.
- **Upotreba asocijacija politika** Izaberite ovu opciju da omogućite da ovaj registar bude ciljni registar asocijacije politike i da osigurate da može sudjelovati u EIM operacijama pregledavanja mapiranja.

Ako ne omogućite pregledavanja mapiranja za registar, taj registar ne može 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 omogućavanje da pregledavanje mapiranja koristi asocijacije politika za ciljni registar morate biti spojeni na EIM domenu u kojoj želite raditi i morate imati “EIM kontrola pristupa” na stranici 38 na jednoj od sljedećih razina:

- EIM administrator
- Administrator registra
- Administrator za izabrane registre (za registar koji želite omogućiti)

Za općenito omogućavanje podrške pregledavanja mapiranja i dozvole specifičnog korištenja asocijacija politike, izvedite sljedeće korake:

1. Proširite **Mreža > Mapiranje identiteta u poduzeću > Upravljanje domenom**.
2. Izaberite EIM domenu u kojoj želite raditi.
   - Ako EIM domena s kojom želite raditi nije popisana pod **Upravljanje domenom**, pregledajte “Dodavanje EIM domene u folder Upravljanje domenom” na stranici 84.
   - Ako trenutno niste povezani na EIM domenu u kojoj želite raditi, pregledajte Povezivanje na EIM kontroler domene.
3. Za prikaz popisa definicija registra za domenu izaberite **Korisnički registri**.

   Bilješka: Ako za kontrolu pristupa izabranih registara imate Administrator, popis sadrži samo one definicije registara nad kojima imate specifično ovlaštenje.
4. Desno kliknite na definiciju registra za koju želite omogućiti podršku politike mapiranja za asocijacije politike i izaberite **Politika mapiranja**
5. Na stranici **Općenito** izaberite **Omogući pregledavanja mapiranja za registar**. Izbor ove opcije omogućuje da registar sudjeluje u EIM operacijama pregledavanja mapiranja. Ako ova opcija nije izabrana, operacija pregledavanja ne može 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 omogućuje se da operacije pregledavanja koriste asocijacije politika kao osnovu za vraćanje podataka kada je registar cilj operacije pregledavanja.
7. Kliknite **OK** da spremite promjene.

Bilješka: Da bi registar mogao koristiti asocijacije politika, morate također osigurati da ste omogućili asocijacije politika za domenu.

Srodni koncepti

“Podrška politici mapiranja EIM i omogućivanje” na stranici 37
Podrška politike Mapiranja identiteta u poduzeću (EIM) dozvoljava vam korištenje asocijacija politike kao i određenih asocijacija identifikatora u nekoj EIM domeni. Asocijacije politika možete koristiti umjesto ili u kombinaciji s asocijacijama identifikatora.

Brisanje definicije registra

Kada brišete definiciju registra iz domene Mapiranja identiteta u poduzeću (EIM), ne utječete na korisnički registar na koji se definicija registra odnosi, ali taj korisnički registar više ne može sudjelovati u EIM domeni.

Trebate razmotriti sljedeće stvari kada brišete definiciju registra:

- Kada brišete definiciju registra, gubite sve asocijacije za taj korisnički registar. Ako ponovo definirate registar u domeni, morate kreirati ponovo sve potrebne asocijacije.
- Kada brišete definiciju X.509 registra, također gubite sve filtere certifikata definirane za taj registar. Ako ponovo definirate registar u domeni, morate kreirati ponovo sve potrebne filtere certifikata.
- Ne možete brisati definiciju sistemskog registra ako postoje definicije registra aplikacije koje specificiraju definiciju sistemskog registra kao nadređenog registra.

Za brisanje definicije registra, morate biti povezani na EIM domenu na kojoj želite raditi i morate imati kontrolu pristupa EIM administratora.

Za brisanje EIM definicije registra, izvedite sljedeće korake:

1. Proširite **Mreža > Mapiranje identiteta u poduzeću > Upravljanje domenom**.
2. Izaberite EIM domenu u kojoj želite raditi.
   - Ako EIM domena s kojom želite raditi nije popisana pod **Upravljanje domenom**, pregledajte “Dodavanje EIM domene u folder Upravljanje domenom” na stranici 84.
   - Ako trenutno niste povezani na EIM domenu u kojoj želite raditi, pregledajte Povezivanje na EIM kontroler domene.

3. Proširite EIM domenu na koju ste povezani.
4. Za prikaz popisa definicija registra za domenu kliknite na **Korisnički registri**.

   Bilješka: Ako za kontrolu pristupa izabranih registara imate Administrator, popis sadrži samo one definicije registara nad kojima imate specifična ovlaštenja.
5. Desno kliknite korisnički registar koji želite obrisati i izaberite **Brisanje**.
6. Kliknite **Da** na dijalogu **Potvrda** za brisanje definicije registra.

Uklanjanje zamjenskog imena iz definicije registra

Za uklanjanje zamjenskog imena iz definicije registra Mapiranja identiteta u poduzeću (EIM), morate biti povezani na EIM domenu u kojoj želite raditi i morate imati EIM kontrolu pristupa kao Administrator registra, Administrator za izabrane registre, ili kao EIM administrator.

Za uklanjanje zamjenskog imena definiciji EIM registra, izvedite sljedeće korake:

1. Proširite **Mreža > Mapiranje identiteta u poduzeću > Upravljanje domenom**.
2. Izaberite EIM domenu u kojoj želite raditi.
   - Ako EIM domena s kojom želite raditi nije popisana pod **Upravljanje domenom**, pregledajte “Dodavanje EIM domene u folder Upravljanje domenom” na stranici 84.
   - Ako trenutno niste povezani na EIM domenu u kojoj želite raditi, pregledajte Povezivanje na EIM kontroler domene.
3. Proširite EIM domenu na koju ste povezani.
4. Za prikaz popisa definicija registra za domenu kliknite na **Korisnički registri**.

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

Dodavanje člana definicije registra grupe

Za dodavanje člana definiciji registra grupe morate biti povezani na EIM domenu na kojoj želite raditi i morate imati EIM kontrolu pristupa kao EIM administrator, Administrator registra, Administrator za izabrane registre (za definiciju registra grupe kojoj želite dodati član i za pojedinačnog člana kojeg želite dodati).

Za dodavanje člana definiciji registra grupe, dovršite ove korake:

1. **Proširite Mreža → Mapiranje identiteta u poduzeću → Upravljanje domenom.**
2. Izaberite EIM domenu u kojoj želite raditi.
   a. Ako EIM domena s kojom želite raditi nije popisana pod Upravljanje domenom, pregledajte Dodavanje EIM domene Upravljanju domenom.
   b. Ako trenutno niste povezani na EIM domenu na kojoj želite raditi, pregledajte Povezivanje na EIM kontroler domene.
3. Proširite EIM domenu na koju ste povezani.
4. 4. Kliknite **Registri korisnika** za prikaz liste definicija registra u domeni.
5. 5. Desno kliknite na definiciju registra grupe kojoj želite dodati član i izaberite **Svojstva.**
6. 6. Izaberite stranicu **Članovi** i kliknite **Dodaj**.
7. 7. U **dijalogu Dodaj člana registra grupe EIM-a**, izaberite jednu ili više definicija registra i kliknite **OK**. Sadržaj liste se mijenja ovisno o tipu kontrole pristupa EIM-u koji imate i ograničen je na definicije registara s istom osjetljivošću na velika i mala slova kao ostali članovi grupe.
8. 8. Kliknite **OK** za izlaz.

Upravljanje identifikatorima Mapiranja identiteta u poduzeću

Koristite ove informacije da saznate kako kreirati i upravljati identifikatorima Mapiranja identiteta u poduzeću (EIM) za domenu.

Kreiranje i upotreba EIM identifikatora koja predstavlja korisnike u vašoj mreži može biti vrlo korisna kao pomoć u praćenju koja osoba posjeduje određeni korisnički identitet. Korisnici unutar poduzeća se skoro stalno mijenjaju, neki dolaze, neki odlaze, a neki se premještaju među područjima. Ove se promjene dodaju stalnom administrativnom problemu zadržavanja traga korisničkih identiteta i lozinki za sisteme i aplikacije u mreži. Dodatno, upravljanje lozinkom oduzima veliku količinu vremena u nekom poduzeću. Kreiranjem identifikatora Mapiranja identiteta u poduzeću (EIM) i njihovim pridruživanjem korisničkim identitetima za svakog korisnika, možete napraviti proces praćenja tko je vlasnik određenog korisničkog identiteta. Time možete također pojednostaviti upravljanje lozinkom.

Primjena okoline jednostruke prijave čini obradu upravljanja korisničkim identitetima jednostavnijom i za korisnike, posebno kada se premještaju u drugi odjel ili područje unutar poduzeća. Mogućnost jednostruke prijave može eliminirati potrebu da ovi korisnici pamte nova korisnička imena i lozinke na novim sistemima.

Bilješka: Kako ćete kreirati i koristiti EIM identifikatore ovisi o potrebama vaše organizacije. Da naučite više pregledajte “Razvijanje plana imenovanja EIM identifikatora” na stranici 62.

Možete upravljati EIM identifikatorima za neku EIM domenu koja je dostupna pod folderom **Upravljanje domenom**. Možete izvesti bilo koji od sljedećih zadataka za upravljanje EIM identifikatorima u EIM domeni:

Srodne informacije

Jednostruka prijava

Kreiranje EIM identifikatora

Za kreiranje EIM identifikatora, morate biti povezani na domenu Mapiranja identiteta u poduzeću (EIM) na kojoj želite raditi i morate imati EIM kontrolu pristupa kao Administrator identifikatora, ili kao EIM administrator.

Za kreiranje EIM identifikatora za osobu ili cjelinu u vašem poduzeću, izvedite ove korake:

1. Proširite **Mreža > Mapiranje identiteta u poduzeću > Upravljanje domenom**.
2. Izaberite EIM domenu u kojoj želite raditi.
   - Ako EIM domena s kojom želite raditi nije popisana pod **Upravljanje domenom**, pregledajte “Dodavanje EIM domene u folder Upravljanje domenom” na stranici 84.
   - Ako trenutno niste povezani na EIM domenu na kojoj želite raditi, pregledajte “Povezivanje na EIM domenu” na stranici 84.
3. Proširite EIM domenu na koju ste povezani.
4. Desno kliknite **Identifikatori** i izaberite **Novi identifikator**.
5. U dijalogu **Novi EIM identifikator**, osigurajte informacije o EIM identifikatoru kako slijedi:
   a. Ime za identifikator.
   b. Ako je potrebno da li želite da sistem generira jedinstveno ime.
   c. Opis identifikatora.
   d. Ako je potrebno, jedno ili više zamjenskih imena za identifikator.
6. Ako je potrebno kliknite **Pomoć** da odredite koje informacije navesti u određenom polju.
7. Nakon što osigurate potrebne informacije, za kreiranje EIM identifikatora kliknite **OK**.

Bilješka: Ako kreirate veliki broj EIM identifikatora, ponekad prođe puno vremena prije no što se pokaže popis identifikatora kada proširite folder **Identifikatori**. Za poboljšanje izvedbe kada imate velik broj EIM identifikatora, pregledajte “Prilagodba pogleda EIM identifikatora” na stranici 97.

Dodavanje zamjenskog imena EIM identifikatoru

Možda ćete htjeti kreirati zamjensko ime da omogućite dodatne informacije za razlikovanje EIM identifikatora. Zamjenska imena mogu pomoći u lociranju određenog identifikatora Mapiranja identiteta u poduzeću (EIM) prilikom

izvođenja operacije EIM pregledavanja. Na primjer, zamjenska imena mogu biti korisna u situacijama gdje je nečije zakonsko ime različito od imena po kojoj je ta osoba poznata.

Imena EIM identifikatora moraju biti jedinstvena u EIM domeni. Zamjenska imena mogu pomoći u adresiranju situacija gdje korištenje jedinstvenih imena identifikatora može biti teško. Na primjer, različite individue unutar poduzeća mogu dijeliti isto ime, što može biti zbunjujuće ako koristite prava imena kao EIM identifikatore. Na primjer, ako imate dva korisnika s imenom Ivan I. Ivanić, mogli biste kreirati zamjensko ime Ivan Ivo Ivanić za jednog i Ivan Ivica Ivanić za drugog kako bi lakše razlikovali identitet svakog korisnika. Dodatna zamjenska imena mogu sadržavati zaposlenički 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 želite raditi i morate imati “EIM kontrola pristupa” na stranici 38 na jednoj od sljedećih razina:

- EIM administrator.
- Administrator identifikatora.

Da dodate zamjensko ime EIM identifikatoru, dovršite ove korake.

1. Proširite **Mreža > Mapiranje identiteta u poduzeću > Upravljanje domenom**.
2. Izaberite EIM domenu u kojoj želite raditi.
   - Ako EIM domena s kojom želite raditi nije popisana pod **Upravljanje domenom**, pregledajte “Dodavanje EIM domene u folder Upravljanje domenom” na stranici 84.
   - Ako trenutno niste povezani na EIM domenu na kojoj želite raditi, pregledajte “Povezivanje na EIM domenu” na stranici 84.
3. Proširite EIM domenu na koju ste povezani.
4. Kliknite **Identifikatori** da prikažete, u desnom oknu, listu EIM identifikatora dostupnih u domeni.

   Bilješka: Ponekad kada pokušate proširiti folder **Identifikatori** može proći puno vremena prije nego se popis identifikatora prikaže. Za poboljšanje izvedbe kada imate velik broj EIM identifikatora u domeni, pregledajte “Prilagodba pogleda EIM identifikatora” na stranici 97.
5. Desno kliknite na EIM identifikator za koji želite dodati zamjensko ime i izaberite **Svojstva...**
6. U polju **Zamjensko ime**, specificirajte zamjensko ime koje želite dodati u ovaj EIM identifikator i kliknite **Dodaj**.
7. Kliknite **OK** za spremanje promjena EIM identifikatora.

Uklanjanje zamjenskog imena iz EIM identifikatora

Za uklanjanje zamjenskog imena iz identifikatora Mapiranja identiteta u poduzeću (EIM), morate biti povezani na EIM domenu u kojoj želite raditi i morate imati EIM kontrolu pristupa kao Administrator identifikatora, ili kao EIM administrator.

Za uklanjanje zamjenskog imena iz EIM identifikatora, izvedite sljedeće korake:

1. Proširite **Mreža > Mapiranje identiteta u poduzeću > Upravljanje domenom**.
2. Izaberite EIM domenu u kojoj želite raditi.
   - Ako EIM domena s kojom želite raditi nije popisana pod **Upravljanje domenom**, pregledajte “Dodavanje EIM domene u folder Upravljanje domenom” na stranici 84.
   - Ako trenutno niste povezani na EIM domenu na kojoj želite raditi, pregledajte “Povezivanje na EIM domenu” na stranici 84.
3. Proširite EIM domenu na koju ste povezani.
4. Kliknite **Identifikatori** da prikažete, u desnom oknu, listu EIM identifikatora dostupnih u domeni.

   Bilješka: Ponekad kada pokušate proširiti folder **Identifikatori** može proći puno vremena prije nego se popis identifikatora prikaže. Za poboljšanje izvedbe kada imate velik broj EIM identifikatora u domeni, pregledajte “Prilagodba pogleda EIM identifikatora” na stranici 97.
5. Desno kliknite na EIM identifikator za koji želite dodati zamjensko ime i izaberite **Svojstva...**

6. Izaberite zamjensko ime koje želite ukloniti i kliknite **Ukloni**.
7. Za spremanje promjena kliknite **OK**.

Brisanje EIM identifikatora

Za brisanje EIM identifikatora, morate biti povezani na domenu Mapiranja identiteta u poduzeću (EIM) na kojoj želite raditi i morate imati kontrolu pristupa EIM administratora.

Za brisanje EIM identifikatora, izvedite sljedeće korake:

1. Proširite **Mreža > Mapiranje identiteta u poduzeću > Upravljanje domenom**.
2. Izaberite EIM domenu u kojoj želite raditi.
   - Ako EIM domena s kojom želite raditi nije popisana pod **Upravljanje domenom**, pregledajte “Dodavanje EIM domene u folder Upravljanje domenom” na stranici 84.
   - Ako trenutno niste povezani na EIM domenu u kojoj želite raditi, pregledajte Povezivanje na EIM kontroler domene.
3. Proširite EIM domenu na koju ste sada povezani.
4. Kliknite **Identifikatori**.

   Bilješka: Ponekad kada pokušate proširiti folder **Identifikatori** može proći puno vremena prije nego se popis identifikatora prikaže. Da poboljšate performanse kada imate velik broj EIM identifikatora u domeni, možete “Prilagodba pogleda EIM identifikatora”.
5. Izaberite EIM identifikator koji želite obrisati. Za brisanje višestrukih 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 EIM identifikatora

Ponekad kada pokušate proširiti folder Identifikatori može proći puno vremena prije nego se prikaže popis identifikatora. Za poboljšanje performansi kada imate velik broj identifikatora Mapiranja identiteta u poduzeću (EIM) u domeni možete prilagoditi pogled za folder Identifikatori.

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

1. Proširite **;Mreža —> Mapiranje identiteta u poduzeću —> Upravljanje domenom**.
2. Izaberite EIM domenu u kojoj želite raditi.
   - Ako EIM domena s kojom želite raditi nije popisana pod **Upravljanje domenom**, pregledajte “Dodavanje EIM domene u folder Upravljanje domenom” na stranici 84.
   - Ako trenutno niste povezani na EIM domenu na kojoj želite raditi, pregledajte “Povezivanje na EIM domenu” na stranici 84.
3. Desno kliknite folder **Identifikatori** pa izaberite **Prilagodi Ovaj Pogled**.
4. Specificirajte kriterije koje želite koristiti za prikaz EIM identifikatora u domeni. Za smanjenje broja prikazanih EIM identifikatora, specificirajte znakove koje želite koristiti za sortiranje identifikatora. Možete specificirati jedan ili više generičkih znakova (*) u imenu identifikatora. Na primjer, možete upisati *JOHNSON* za vaš kriterij sortiranja u polje **Identifikatori**. Rezultati će vratiti sve EIM identifikatore u kojima je niz znakova JOHNSON definiran kao dio imena EIM identifikatora, a također će 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 EIM asocijacijama

EIM vam omogućuje kreiranje i upravljanje s dva tipa asocijacija koje definiraju izravne ili neizravne odnose između korisničkih identiteta: asocijacije identifikatora i asocijacije politike. EIM vam dozvoljava kreiranje i upravljanje asocijacijama identifikatora između EIM identifikatora i njihovih korisničkih identiteta što vam omogućuje definiranje neizravnih ali specifičnih pojedinačnih odnosa između korisničkih identiteta.

EIM vam također dozvoljava kreiranje asocijacija politike za opis odnosa između višestrukih korisničkih identiteta iz jednog ili više registara i pojedinačnog ciljnog korisničkog identiteta u drugom registru. Asocijacije politike koriste podršku politike EIM mapiranja za kreiranje više-prema-jedan mapiranja između korisničkih identiteta bez uključivanja EIM identifikatora. Zbog toga što oba tipa asocijacija definiraju odnose između korisničkih identiteta u nekom poduzeću, upravljanje asocijacijama je važan element upravljanja EIM-om.

Održavanje asocijacija unutar domene je ključ pojednostavljivanja administrativnih zadataka potrebnih za praćenje korisnika koji imaju račune na različitim sistemima na mreži. Asocijacije identifikatora i asocijacije politike uvijek moraju biti ažurne kada primjenjujete sigurnu mrežu s jednostrukom prijavom.

Možete izvesti sljedeće zadatke upravljanja za asocijacije:

Kreiranje EIM asocijacija

Dva su različita tipa EIM asocijacija koja možete kreirati. Možete kreirati ili asocijaciju identifikatora ili asocijaciju politike.

Asocijaciju identifikatora možete kreirati da neizravno definirate odnos između dva korisnička identiteta koje koristi jedan pojedinac. Asocijacija identifikatora opisuje odnos između nekog EIM identifikatora i korisničkog identiteta u korisničkom registru. Asocijacije identifikatora dozvoljavaju vam kreiranje jedan-prema-jedan mapiranja između EIM identifikatora i svakog od raznolikih korisničkih identiteta koji se odnose na korisnika kojeg predstavlja EIM identifikator.

Asocijaciju politike možete kreirati za izravno definiranje odnosa između višestrukih korisničkih identiteta u jednom ili više registara i individualnog ciljnog korisničkog identiteta u drugom registru. Asocijacije politike koriste podršku politike EIM mapiranja za kreiranje više-prema-jedan mapiranja između korisničkih identiteta bez uključivanja EIM identifikatora. Asocijacije politike omogućuju brzo kreiranje velikog broja mapiranja između povezanih korisničkih identiteta u različitim korisničkim registrima.

Da li ćete izabrati kreirati asocijacije identifikatora, kreirati asocijacije politike ili koristiti mješavinu obje metode ovisi o vašim potrebama EIM implementacije.

Srodni koncepti

“Razvoj plana mapiranja identiteta” na stranici 59
Za kritični dio početnog procesa planiranja implementacije Mapiranja identiteta u poduzeću (EIM) je potrebno odrediti kako želite koristiti mapiranje identiteta u vašem poduzeću.

“Kreiranje asocijacije politike” na stranici 99
Asocijacija politike je sredstvo za direktno definiranje odnosa između višestrukih korisničkih identiteta u jednom ili više registara i individualnog ciljnog korisničkog identiteta u drugom registru.

Srodni zadaci

“Kreiranje asocijacije EIM identifikatora”
Asocijacije identifikatora definiraju odnos između identifikatora Mapiranja identiteta u poduzeću (EIM) i korisničkog identiteta u vašem poduzeću za osobu ili entitet na koji se EIM identifikator odnosi.

Kreiranje asocijacije EIM identifikatora:

Asocijacije identifikatora definiraju odnos između identifikatora Mapiranja identiteta u poduzeću (EIM) i korisničkog identiteta u vašem poduzeću za osobu ili entitet na koji se EIM identifikator odnosi.

Možete kreirati tri tipa asocijacije identifikatora: ciljni, izvorni i administrativni. Da spriječite moguće probleme s asocijacijama i s načinom na koji mapiraju identitete, pregledajte “Razvoj plana mapiranja identiteta” na stranici 59.

Za kreiranje asocijacije identifikatora morate biti povezani na EIM domenu u kojoj želite raditi i morate imati EIM kontrolu pristupa zahtijevanu od strane tipa asocijacije koji želite obrisati.

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

- Administrator identifikatora.

- EIM administrator.

Za kreiranje ciljne asocijacije morate imati EIM kontrolu pristupa na jednoj od sljedećih razina:
- Administrator registra.
- Administrator za izabrane registre (za definiciju registra koja se odnosi na korisnički registar koji sadrži ciljni korisnički identitet)
- EIM administrator.

Za kreiranje asocijacije identifikatora, izvedite sljedeće korake:
1. Proširite **Mreža > Mapiranje identiteta u poduzeću > Upravljanje domenom**.
2. Izaberite EIM domenu u kojoj želite raditi.
   - Ako EIM domena s kojom želite raditi nije popisana pod **Upravljanje domenom**, pregledajte “Dodavanje EIM domene u folder Upravljanje domenom” na stranici 84.
   - Ako trenutno niste povezani na EIM domenu na kojoj želite raditi, pregledajte “Povezivanje na EIM domenu” na stranici 84.
3. Proširite EIM domenu na koju ste sada povezani.
4. Kliknite **Identifikatori** za prikaz liste EIM identifikatora za domenu.

   Bilješka: Ponekad kada pokušate proširiti folder **Identifikatori** može proći puno vremena prije nego se popis identifikatora prikaže. Za poboljšanje izvedbe kada imate velik broj EIM identifikatora u domeni, pregledajte “Prilagodba pogleda EIM identifikatora” na stranici 97.
5. Desno kliknite EIM identifikator za koji želite kreirati asocijaciju i izaberite **Svojstva...**
6. Izaberite stranicu **Asocijacije** pa kliknite **Dodaj...**.
7. Za definiranje asocijacije u dijalogu **Dodavanje asocijacije** osigurajte informacije kao što slijedi:
   - Ime registra koji sadrži korisnički identitet koji želite pridružiti s EIM identifikatorom. Navedite točno ime postojeće definicije registra ili ga potražite i izaberite.
   - Ime korisničkog identiteta koje želite pridružiti EIM identifikatoru.
   - Tip asocijacije. Možete kreirati jedan od tri različita tipa asocijacija:
     – Administrativni
     – Izvorni
     – Ciljni
8. Ako je potrebno kliknite **Pomoć** da odredite koje informacije navesti u određenom polju.
9. Opcijski. Za ciljnu asocijaciju kliknite **Napredno...** za prikaz dijaloga **Dodavanje asocijacije - Napredno**. Za ciljni korisnički identitet navedite informacije pregledavanja i kliknite **OK** za povratak u dijalog **Dodavanje asocijacije**.
10. Nakon što osigurate potrebne informacije za kreiranje asocijacije kliknite **OK**.

Srodni koncepti

“Kreiranje EIM asocijacija” na stranici 98
Dva su različita tipa EIM asocijacija koja možete kreirati. Možete kreirati ili asocijaciju identifikatora ili asocijaciju politike.

Kreiranje asocijacije politike:

Asocijacija politike je sredstvo za direktno definiranje odnosa između višestrukih korisničkih identiteta u jednom ili više registara i individualnog ciljnog korisničkog identiteta u drugom registru.

Asocijacije politike koriste podršku politike Mapiranja identiteta u poduzeću (EIM) za kreiranje više-na-jedan mapiranja između identiteta korisnika bez uključivanja EIM identifikatora. Budući da možete koristiti asocijacije politika na mnoštvo preklapajućih načina, morate dobro razumjeti EIM podršku politike mapiranja da biste mogli

kreirati i koristiti asocijacije politika. Također, da biste spriječili moguće probleme s asocijacijama i s načinom mapiranja identiteta, za vaš posao morate razviti cjelokupni plan mapiranja identiteta prije nego počnete definirati asocijacije.

Da li ćete izabrati kreirati asocijacije identifikatora, kreirati asocijacije politike ili koristiti kombinaciju obaju metoda ovisi o vašim potrebama EIM implementacije.

Kako ćete kreirati asocijacije politike varira ovisno o tipu asocijacije politike. Da naučite više o tome kako kreirati asocijaciju politike pogledajte:

Srodni koncepti

"Upravljanje definicijama registra Mapiranja identiteta u poduzeću" na stranici 88
Da bi korisnički registri i korisnički identiteti koje sadrže sudjelovali u EIM domeni, morate za njih kreirati definicije registra. Tada možete upravljati kako korisnički registri i njihovi korisnički identiteti sudjeluju u EIM-u s upravljanjem tim EIM definicijama registra.

"Kreiranje EIM asocijacija" na stranici 98
Dva su različita tipa EIM asocijacija koja možete kreirati. Možete kreirati ili asocijaciju identifikatora ili asocijaciju politike.

"Podrška politici mapiranja EIM i omogućivanje" na stranici 37
Podrška politike Mapiranja identiteta u poduzeću (EIM) dozvoljava vam korištenje asocijacija politike kao i određenih asocijacija identifikatora u nekoj EIM domeni. Asocijacije politika možete koristiti umjesto ili u kombinaciji s asocijacijama identifikatora.

"Razvoj plana mapiranja identiteta" na stranici 59
Za kritični dio početnog procesa planiranja implementacije Mapiranja identiteta u poduzeću (EIM) je potrebno odrediti kako želite koristiti mapiranje identiteta u vašem poduzeću.

Kreiranje default asocijacije politike domene:

Za kreiranje default asocijacije politike domene morate biti povezani na domenu Mapiranja identiteta u poduzeću (EIM) na kojoj želite raditi i morate imati EIM kontrolu pristupa kao EIM administrator, ili kao Administrator registra.

Asocijacija politike opisuje odnos između višestrukih korisničkih identiteta i jednostrukog korisničkog identiteta u ciljnom korisničkog registru. Asocijaciju politike možete koristiti za opis odnosa između izvornog skupa višestrukih korisničkih identiteta i jednostrukog ciljnog korisničkog identiteta u određenom ciljnom korisničkom registru. Asocijacije politike koriste EIM podršku politike mapiranja za kreiranje mapiranja među korisničkim identitetima s više na jednog bez uključivanja EIM identifikatora.

Bilješka: Budući da možete koristiti asocijacije politika na mnoštvo preklapajućih načina, morate dobro razumjeti EIM podršku politike mapiranja da biste mogli kreirati i koristiti asocijacije politika. Također, da biste spriječili moguće probleme s asocijacijama i s načinom mapiranja identiteta, za vaš posao morate razviti cjelokupni plan mapiranja identiteta prije nego počnete 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. Možete definirati default asocijaciju politike domene za svaki registar u domeni. Ako se dvije ili više asocijacija politike domene odnose na isti ciljni registar, možete definirati jedinstvene informacije pregledavanja za svaku od tih asocijacija politike da osigurate da ih operacije pregledavanja mapiranja mogu razlikovati. Inače, operacije pregledavanja mapiranja mogu vratiti višestruke ciljne korisničke identitete. Rezultat ovih dvosmislenih rezultata je da aplikacija koja ovisi o EIM-u neće moći odrediti koji točno ciljni identitet treba koristiti.

Za kreiranje default asocijacije politike domene izvedite sljedeće korake:

1. Proširite **Mreža > Mapiranje identiteta u poduzeću > Upravljanje domenom**.
2. Desno kliknite na EIM domenu na kojoj želite raditi i izaberite **Politika mapiranja**
   - Ako EIM domena s kojom želite raditi nije ispisana u **Upravljanje domenom**, pogledajte "Dodavanje EIM domene u folder Upravljanje domenom" na stranici 84.

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

3. Na stranici Općenito izaberite **Omogući preglede mapiranja korištenjem asocijacija politika za domenu** .
4. Izaberite stranicu **Domena** i kliknite **Dodaj**.
5. U dijalogu **Dodavanje default asocijacije politike domene** navedite sljedeće potrebne informacije:
   - Ime definicije registra **Ciljnog registra** za asocijaciju politike.
   - Ime korisničkog identiteta **Ciljnog korisnika** za asocijaciju politike.
6. Ako je potrebno, za više pojedinosti o tome kako ovo napraviti i o daljnjim dijalozima, kliknite **Pomoć**.
7. Opcijski. Kliknite **Napredno** za prikaz dijaloga **Dodaj asocijaciju - Napredno**. Specificirajte **Informacije pregledavanja** za asocijaciju politike i kliknite **OK** za povratak u dijalog **Dodavanje default asocijacije politike domene**.

   Bilješka: Ako se dvije ili više default asocijacija politike domene odnose na isti ciljni registar, za svakog od ciljnih korisničkih identiteta u ovim asocijacijama politike morate definirati jedinstvene informacije pregledavanja. U ovoj situaciji definiranjem informacija pregledavanja za svaki ciljni korisnički identitet osiguravate da ih operacije pregledavanja mapiranja mogu razlikovati. Inače, operacije pregledavanja mapiranja mogu vratiti višestruke ciljne korisničke identitete. Rezultat ovih dvosmislenih rezultata je da aplikacija koja ovisi o EIM-u neće moći odrediti koji točno 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 omogućena za ciljni registar.
10. Da spremite svoje promjene i izađete iz dijaloga **Politika mapiranja** kliknite **OK**.

Bilješka: Provjerite da je politika mapiranja podržana i da je korištenje asocijacija politika za ciljni korisnički registar ispravno omogućeno. Ako nije omogućeno, asocijacija politike neće imati nikakav učinak.

Kreiranje default asocijacije politike registra:

Za kreiranje default asocijacije politike registra morate biti povezani na domenu Mapiranja identiteta u poduzeću (EIM) na kojoj želite raditi i morate imati EIM kontrolu pristupa kao Administrator registra, ili kao EIM administrator.

Asocijacija politike opisuje odnos između višestrukih korisničkih identiteta i jednostrukog korisničkog identiteta u ciljnom korisničkog registru. Asocijaciju politike možete koristiti za opis odnosa između izvornog skupa višestrukih korisničkih identiteta i jednostrukog ciljnog korisničkog identiteta u određenom ciljnom korisničkom registru. Asocijacije politike koriste EIM podršku politike mapiranja za kreiranje mapiranja među korisničkim identitetima s više na jednog bez uključivanja EIM identifikatora.

Bilješka: Budući da možete koristiti asocijacije politika na mnoštvo preklapajućih načina, morate dobro razumjeti EIM podršku politike mapiranja da biste mogli kreirati i koristiti asocijacije politika. Također, da biste spriječili moguće probleme s asocijacijama i s načinom mapiranja identiteta, za vaš posao morate razviti cjelokupni plan mapiranja identiteta prije nego počnete 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 omogućite default asocijaciju politike registra za ciljni registar, asocijacija politike osigurava da se ti izvorni korisnički identiteti mogu mapirati u jednostruki određeni ciljni registar i ciljnog korisnika.

Za kreiranje default asocijacije politike registra, izvedite sljedeće korake:

1. Proširite **Mreža > Mapiranje identiteta u poduzeću > Upravljanje domenom**.
2. Izaberite EIM domenu u kojoj želite raditi.
   - Ako EIM domena s kojom želite raditi nije popisana pod **Upravljanje domenom**, pregledajte “Dodavanje EIM domene u folder Upravljanje domenom” na stranici 84.

- Ako trenutno niste povezani na EIM domenu u kojoj želite raditi, pregledajte Povezivanje na EIM kontroler domene.

3. Na stranici Općenito izaberite **Omogući preglede mapiranja korištenjem asocijacija politika za domenu** .
4. Na stranici Općenito izaberite **Omogući preglede mapiranja korištenjem asocijacija politika za domenu** .
5. U dijalogu **Dodavanje default asocijacije politike registra** navedite sljedeće potrebne informacije:
   - Ime definicije registra **Izvornog registra** za asocijaciju politike.
   - Ime definicije registra **Ciljnog registra** za asocijaciju politike.
   - Ime korisničkog identiteta **Ciljnog korisnika** za asocijaciju politike.
6. Ako je potrebno, za više pojedinosti o tome kako ovo napraviti i o daljnjim dijalozima, kliknite **Pomoć**.
7. Opcijski. Kliknite **Napredno** za prikaz dijaloga **Dodaj asocijaciju - Napredno**. Specificirajte **informacije pregledavanja** za asocijaciju politike i kliknite **OK** za povratak u dijalog **Dodavanje default asocijacije politike registra**. Ako se dvije ili više asocijacija politike s istim izvornim registrom odnose na isti ciljni registar, za svaki od ciljnih korisničkih identiteta u ovim asocijacijama politika morate definirati jedinstvene informacije pregledavanja. U ovoj situaciji definiranjem informacija pregledavanja za svaki ciljni korisnički identitet osiguravate da ih operacije pregledavanja mapiranja mogu razlikovati. Inače, operacije pregledavanja mapiranja mogu vratiti višestruke ciljne korisničke identitete. Rezultat ovih dvosmislenih rezultata je da aplikacija koja ovisi o EIM-u neće moći odrediti koji točno 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 omogućena za ciljni registar.
10. Da spremite svoje promjene i izađete iz dijaloga **Politika mapiranja** kliknite **OK**.

Bilješka: Provjerite da je politika mapiranja podržana i da je korištenje asocijacija politika za ciljni korisnički registar ispravno omogućeno. Ako nije omogućeno, asocijacija politike neće imati nikakav učinak.

Kreiranje asocijacije politike filtera certifikata:

Za kreiranje asocijacije politike filtera certifikata, morate biti povezani na domenu Mapiranja identiteta u poduzeću (EIM) na kojoj želite raditi i morate imati EIM kontrolu pristupa kao Administrator registra, ili kao EIM administrator.

Asocijacija politike opisuje odnos između izvornog skupa višestrukih korisničkih identiteta i jednostrukog ciljnog korisničkog identiteta u određenom ciljnom korisničkom registru. Asocijacije politike koriste EIM podršku politike mapiranja za kreiranje mapiranja među korisničkim identitetima s više na jednog bez uključivanja EIM identifikatora.

Bilješka: Budući da možete koristiti asocijacije politika na mnoštvo preklapajućih načina, morate dobro razumjeti EIM podršku politike mapiranja da biste mogli kreirati i koristiti asocijacije politika. Također, da biste spriječili moguće probleme s asocijacijama i s načinom mapiranja identiteta, za vaš posao morate razviti cjelokupni plan mapiranja identiteta prije nego počnete definirati asocijacije.

U asocijaciji politike filtera certifikata u jednostrukom X.509 registru kao izvor asocijacija politike određujete 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 možete u registru navesti podskup certifikata. Filter certifikata koji ste naveli za asocijaciju politike određuje svoj opseg.

Bilješka: Kreirajte i koristite default asocijaciju politike registra kada želite sve certifikate iz X.509 korisničkog registra mapirati u jednostruki ciljni korisnički identitet.

Filter certifikata kontrolira kako asocijacija politike filtera certifikata mapira jedan izvorni skup korisničkih identiteta, u ovom slučaju digitalne certifikate, u određeni ciljni korisnički identitet. Prema tome, da bi mogli kreirati asocijaciju politike filtera certifikata mora postojati filter certifikata koji želite koristiti.

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

Za kreiranje asocijacije politike filtera certifikata, izvedite sljedeće korake:

1. Proširite **Mreža > Mapiranje identiteta u poduzeću > Upravljanje domenom**.
2. Desno kliknite na EIM domenu na kojoj želite raditi i izaberite **Politika mapiranja**
   - Ako EIM domena s kojom želite raditi nije popisana pod **Upravljanje domenom**, pregledajte “Dodavanje EIM domene u folder Upravljanje domenom” na stranici 84.
   - Ako trenutno niste povezani na EIM domenu u kojoj želite raditi, pregledajte Povezivanje na EIM kontroler domene.
3. Na stranici Općenito izaberite **Omogući preglede mapiranja korištenjem asocijacija politika za domenu** .
4. Izaberite stranicu **Filter certifikata** i kliknite **Dodaj** za prikaz dijaloga **Dodaj asocijaciju politike filtera certifikata**.
5. Ako je potrebno, za više pojedinosti o tome kako ovo napraviti i o daljnjim dijalozima, kliknite **Pomoć**.
6. Navedite sljedeće potrebne informacije za definiranje asocijacije politike:
   a. Unesite ime definicije registra X.509 korisničkog registra koji će se koristiti kao **Izvorni X.509 registar** za asocijaciju politike. Ili, kliknite **Pregledaj** za izbor registra s popisa definicija registara za domenu
   b. Za prikaz dijaloga **Izbor filtera certifikata** kliknite **Izbor** i izaberite postojeći filter certifikata koji će se koristiti kao osnova za novu asocijaciju politike filtera certifikata.

      Bilješka: **Morate** koristiti postojeći filter certifikata. Ako filter certifikata koji želite koristiti nije popisan, kliknite **Dodaj** za kreiranje novog filtera certifikata.
   c. Specificirajte ime definicije registra **Ciljnog registra**, ili kliknite **Pregledaj** za izbor jednog registra s popisa postojećih definicija registara za domenu.
   d. Navedite ime **Ciljnog korisnika** na kojeg želite mapirati sve certifikate iz **Izvornog X.509 registra** koji odgovaraju filteru certifikata. Ili, kliknite **Pregledaj** za izbor jednog s popisa korisnika koji su poznati domeni.
   e. Opcijski. Kliknite **Napredno** za prikaz dijaloga **Dodaj asocijaciju - Napredno**. Za ciljni korisnički identitet navedite **Informacije pregledavanja**, a za povratak u dijalog **Dodavanje asocijacije politike filtera certifikata** kliknite **OK**.

      Bilješka: Ako se dvije ili više asocijacija politike s istim izvornim X.509 registrom i istim kriterijem filtera certifikata odnose na isti ciljni registar, za ciljni korisnički identitet u svakoj od tih asocijacija politike morate definirati jedinstvene informacije pregledavanja. U ovoj situaciji definiranjem informacija pregledavanja za svaki ciljni korisnički identitet osiguravate da ih operacija pregledavanja mapiranja može razlikovati. Inače, operacije pregledavanja mapiranja mogu vratiti višestruke ciljne korisničke identitete. Rezultat ovih dvosmislenih rezultata je da aplikacija koja ovisi o EIM-u neće moći odrediti koji točno ciljni identitet treba koristiti.
7. Kliknite **OK** za kreiranje asocijacije politike filtera certifikata i za vraćanje na stranicu **Filteri certifikata**. Nova asocijacija politike prikazana je na popisu.
8. Provjerite da je nova asocijacija politike omogućena za ciljni registar.
9. Da spremite svoje promjene i izađete iz dijaloga **Politika mapiranja** kliknite **OK**.

Bilješka: Provjerite da je politika mapiranja podržana i da je korištenje asocijacija politika za ciljni korisnički registar ispravno omogućeno. Ako nije omogućeno, asocijacija politike neće imati nikakav učinak.

Kreiranje filtera certifikata:

Filter certifikata definira skup sličnih atributa certifikata razlikovnog imena za grupu korisničkih certifikata u X.509 izvornom registru korisnika. Filter certifikata možete koristiti kao osnovu asocijacija politika filtera certifikata.

Filter certifikata u asocijaciji politike određuje koji će se certifikati u navedenom X.509 izvornom registru mapirati u određene ciljne korisnike. Oni certifikati koji imaju informacije DN naslova i DN izdavača koje zadovoljavaju kriterij filtera se mapiraju na navedenog ciljnog korisnika tijekom operacija pregledavanja Mapiranja identiteta u poduzeću (EIM).

Da kreirate filter certifikata morate biti spojeni na EIM domenu u kojoj želite raditi i morate imati "EIM kontrola pristupa" na stranici 38 barem jednu od sljedećih razina:

- EIM administrator
- Administrator registra
- Administrator za izabrane registre (za definiciju registra koja se odnosi na X.509 korisnički registar za koji želite kreirati filter certifikata)

Filter certifikata kreirate ovisno o određenim informacijama razlikovnog imena (DN) iz digitalnog certifikata. DN informacija koju navedete može biti razlikovno ime subjekta, koje označava vlasnika certifikata ili razlikovno ime izdavača, koje označava izdavača certifikata. Možete označiti potpune ili djelomične DN informacije za filter certifikata.

Kada filter certifikata dodate u asocijaciju politike filtera certifikata, certifikat filtera određuje koji su certifikati u X.509 registru mapirani u ciljni korisnički identitet koji je navela asocijacija politike. Kada je digitalni certifikat izvorni korisnički identitet u EIM operaciji pregledavanja mapiranja (nakon što zahtijevana aplikacija koristi eimFormatUserIdentity() EIM API za formatiranje imena korisničkog identiteta) i kada se primjenjuje asocijacija politike filtera certifikata, EIM uspoređuje DN informacije iz certifikata s DN-om ili djelomičnim DN informacijama koje su navedene u filteru. Ako se DN informacije iz certifikata podudaraju s filterom, EIM vraća ciljni korisnički identitet koji je navela asocijacija politike filtera certifikata.

Prilikom kreiranja filtera certifikata potrebne informacije razlikovnog imena možete osigurati na jedan od tri načina:

- Možete unijeti određene pune ili djelomične DN-ove certifikata za **DN Subjekta**, **DN Izdavača** ili oboje.
- Informacije iz određenog certifikata možete kopirati u memoriju za isječke i koristiti ih za generiranje popisa kandidata filtera certifikata zasnovanih na informacijama razlikovnog imena u certifikatu. Zatim možete izabrati koje DN-ove koristiti za filter certifikata.

  Bilješka: Želite li potrebne informacije razlikovnog imena generirati za kreiranje filtera certifikata, informacije certifikata morate kopirati u memoriju za isječke prije izvođenja ovog zadatka. Također, certifikat mora biti kodiran formatom za kodiranje base64. Za više informacija o metodama za pribavljanje certifikata u određenom formatu, pogledajte Filter certifikata.
- Popis kandidata filtera certifikata zasnovanih na informaciji razlikovnog imena možete generirati iz digitalnog certifikata za koji postoji izvorna asocijacija s EIM identifikatorom. Zatim možete izabrati koje DN-ove koristiti za filter certifikata.

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

1. Proširite **Mreža > Mapiranje identiteta u poduzeću > Upravljanje domenom**.
2. Desno kliknite na EIM domenu na kojoj želite raditi i izaberite **Politika mapiranja**
   - Ako EIM domena s kojom želite raditi nije ispisana u **Upravljanje domenom**, pogledajte "Dodavanje EIM domene u folder Upravljanje domenom" na stranici 84.
   - Ako trenutno niste povezani s EIM domenom u kojoj želite raditi, pogledajte Povezivanje s EIM kontrolerom domene.
3. Izaberite stranicu **Filter certifikata** i kliknite **Filteri certifikata** za prikaz dijaloga **Filteri certifikata**.

   Bilješka: Ako kliknete **Filteri certifikata** bez izbora asocijacije politike, prikazuje se dijalog **Pregledaj EIM registre**. Ovaj vam dijalog omogućuje izbor X.509 registra s popisa X.509 definicija registra u domeni za koju želite pogledati filtere certifikata. Sadržaj popisa varira ovisno o tipu EIM kontrole pristupa koju imate.

4. Kliknite **Dodaj** za prikaz dijaloga **Dodaj filter certifikata**.
5. U dijalogu **Dodavanje filtera certifikata** morate izabrati da li dodati jednostruki filter certifikata ili generirati certifikat zasnovan na specifičnom digitalnom certifikatu. Ako je potrebno, za više pojedinosti o tome kako ovo napraviti i o daljnjim dijalozima, kliknite **Pomoć**.
   a. Ako izaberete **Dodavanje jednostrukog filtera certifikata**, možete unijeti određene potpune ili djelomične informacije **DN-a subjekta**, potpune ili djelomične informacije **DN-a izdavača** ili oboje. Kliknite **OK** za kreiranje filtera certifikata i za vraćanje 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 isječke.
      2) Kliknite **OK** za generiranje popisa potencijalnih filtera certifikata zasnovanih na certifikatovom **DN-u subjekta** i **DN-u izdavača**.
      3) Iz dijaloga **Pregled filtera certifikata** izaberite jedan ili više od ovih filtera certifikata. Kliknite **OK** za vraćanje dijaloga **Izbor filtera certifikata** u kojem se sada prikazuju filteri certifikata.
   c. Ako izaberete **Generiranje filtera certifikata iz asocijacije izvora za X.509 korisnika**, kliknite **OK** za prikaz dijaloga **Generiranje filtera certifikata**. Ovaj dijalog prikazuje popis X.509 korisničkih identiteta koji su u domeni izvorno asocirani s EIM identifikatorom.
      1) Izaberite X.509 korisnički identitet čiji digitalni certifikat želite koristiti za generiranje jednog ili više kandidata filtera certifikata pa kliknite **OK**.
      2) Kliknite **OK** za generiranje popisa potencijalnih filtera certifikata zasnovanih na certifikatovom **DN-u subjekta** i **DN-u izdavača**.
      3) Iz dijaloga **Pregled filtera certifikata** izaberite jedan ili više od ovih potencijalnih filtera certifikata. Kliknite **OK** za vraćanje dijaloga **Izbor filtera certifikata** u kojem se sada prikazuju filteri certifikata.

Novi filter certifikata sada možete koristiti kao osnovu za kreiranje asocijacije politike filtera certifikata.

Dodavanje informacija pregledavanja ciljnom korisničkom identitetu

Informacije pregledavanja su opcijski jedinstveni identifikacijski podaci za ciljni korisnički identitet definiran u asocijaciji. Ta asocijacija može biti ili ciljna asocijacija identifikatora ili asocijacija politike.

Informacije pregledavanja su potrebne samo kada operacija pregledavanja mapiranja može vratiti više od jedan ciljni korisnički identitet. Ova situacija može stvoriti probleme za aplikacije omogućene za Mapiranje identiteta u poduzeću (EIM), uključujući i5/OS aplikacije i proizvode, koji nisu oblikovani za rukovanje ovim dvosmislenim rezultatima.

Po potrebi, možete dodati jedinstvene informacije pregledavanja za svaki ciljni korisnički identitet kako bi se osigurale detaljnije identifikacijske informacije za dodatni opis svakog korisničkog identiteta. Ako definirate informacije pregledavanja za ciljni korisnički identitet, te se informacije pregledavanja moraju dobaviti operaciji pregledavanja mapiranja kako bi se osiguralo da operacija može vratiti jedinstveni ciljni korisnički identitet. U suprotnom, aplikacije koje ovise o EIM-u možda neće moći odrediti koji točno ciljni identitet upotrijebiti.

Bilješka: Ako ne želite da operacije EIM pregledavanja vraćaju više od jedan ciljni korisnički identitet, tada trebate ispraviti vašu konfiguraciju EIM asocijacija umjesto korištenja informacija pregledavanja za rješenje problema. Pregledajte “Rješavanje problema EIM mapiranja” na stranici 116 za detaljnije informacije.

Kako ćete dodati informacije pregledavanja za daljnju definiciju ciljnog korisničkog identiteta ovisi o tome da li je definiran korisnički identitet u asocijaciji identifikatora ili ciljnoj asocijaciji. Bez obzira na metodu korištenu za dodavanje informacija pregledavanja, specificirane informacije su povezane s ciljnim korisničkim identitetom, a ne s asocijacijama identifikatora ili asocijacijama politike u kojima je pronađen taj korisnički identitet.

Dodavanje informacija pregledavanja ciljnom korisničkom identitetu u asocijaciji identifikatora:

Za dodavanje informacija pregledavanja ciljnom korisničkom identitetu u asocijaciji identifikatora, morate biti povezani na EIM domenu u kojoj želite raditi i trebate imati "EIM kontrola pristupa" na stranici 38 na jednoj od ovih razina:

- Administrator registra.
- Administrator za izabrane registre (za definicije registara koje se odnose na korisnički registar koji sadrži ciljni korisnički identitet).
- EIM administrator.

Za dodavanje informacija pregledavanja ciljnom korisničkom identitetu u asocijaciji identifikatora izvedite sljedeće korake:

1. Proširite **Mreža > Mapiranje identiteta u poduzeću > Upravljanje domenom**.
2. Izaberite EIM domenu u kojoj želite raditi.
   - Ako EIM domena s kojom želite raditi nije popisana pod **Upravljanje domenom**, pregledajte "Dodavanje EIM domene u folder Upravljanje domenom" na stranici 84.
   - Ako trenutno niste povezani na EIM domenu u kojoj želite raditi, pregledajte Povezivanje na EIM kontroler domene.
3. Proširite EIM domenu na koju ste povezani.
4. Kliknite **Identifikatori** za prikaz liste EIM identifikatora za domenu.

   Bilješka: Ponekad kada pokušate proširiti folder **Identifikatori** može proći puno vremena prije nego se popis identifikatora prikaže. Da poboljšate performanse kada imate velik broj EIM identifikatora u domeni, možete prilagoditi pogled foldera **Identifikatori** ograničavajući vrijednost traženja korištenu za prikaz identifikatora. Desno kliknite **Identifikatori**, izaberite **Prilagodi ovaj pogled > Uključi** i specificirajte kriterije prikaza za upotrebu kod generiranja popisa EIM identifikatora koje treba uključiti u ovaj pogled.
5. Desno kliknite EIM identifikator i izaberite **Svojstva**.
6. Izaberite stranicu **Asocijacije**, izaberite ciljnu asocijaciju u koju želite dodati informacije pregledavanja i kliknite **Detalji**. Ako je potrebno kliknite **Pomoć** da odredite koje informacije navesti u određenom polju.
7. U dijalogu **Asocijacije - Detalji** specificirajte **Informacije pregledavanja** koje želite koristiti za daljnju identifikaciju ciljnog korisničkog identiteta u ovoj asocijaciji i kliknite **Dodaj**.
8. Ponovite ovaj korak za svaki unos informacija pregledavanja koje želite dodati asocijaciji.
9. Kliknite **OK** za spremanje promjena i vraćanje u dijalog **Asocijacija - Detalji**.
10. Za izlaz kliknite **OK**.

Dodavanje informacija pregledavanja ciljnom korisničkom identitetu u asocijaciji politike:

Za dodavanje informacija pregledavanja ciljnom korisničkom identitetu u asocijaciji politike, morate biti povezani na EIM domenu u kojoj želite raditi i trebate imati "EIM kontrola pristupa" na stranici 38 na jednoj od ovih razina:

- Administrator registra.
- Administrator za izabrane registre (za definiciju registara koja se odnosi na korisnički registar koji sadrži ciljni korisnički identitet (ID)).
- EIM administrator.

Za dodavanje informacija pregledavanja ciljnom korisničkom identitetu u asocijaciji politike izvedite sljedeće korake:

1. Proširite **Mreža > Mapiranje identiteta u poduzeću > Upravljanje domenom**.
2. Izaberite EIM domenu u kojoj želite raditi.
   - Ako EIM domena s kojom želite raditi nije popisana pod **Upravljanje domenom**, pregledajte "Dodavanje EIM domene u folder Upravljanje domenom" na stranici 84.
   - Ako trenutno niste povezani na EIM domenu u kojoj želite raditi, pregledajte Povezivanje na EIM kontroler domene.

3. U dijalogu **Politika mapiranja** koristite stranice za gledanje asocijacija politike za domenu.
4. Pronađite i izaberite asocijaciju politike za ciljni registar koji koristi ciljni korisnički identitet kojemu želite dodati informacije pregledavanja.
5. Kliknite **Detalji** za prikaz odgovarajućeg dijaloga **Asocijacija politika - Detalji** za tip asocijacije politika koji ste izabrali. Ako je potrebno kliknite **Pomoć** da odredite koje informacije navesti u određenom polju.
6. Navedite **Informacije pregledavanja** koje želite koristiti za daljnje identificiranje ciljnog identiteta korisnika u ovoj asocijaciji politike i kliknite **Dodati**. Ponovite ovaj korak za svaki unos informacija pregledavanja koje želite dodati asocijaciji.
7. Kliknite **OK** za spremanje promjena i vraćanje u originalni dijalog **Asocijacija - Detalji**.
8. Za izlaz kliknite **OK**.

Uklanjanje informacija pregledavanja s ciljnog korisničkog identiteta

Informacije pregledavanja su opcijski jedinstveni identifikacijski podaci za ciljni korisnički identitet definiran u asocijaciji. Ta asocijacija može biti ili ciljna asocijacija identifikatora ili asocijacija politike.

Informacije pregledavanja su potrebne samo kada operacija pregledavanja mapiranja može vratiti jedan ili više ciljni korisnički identitet. Ova situacija može stvoriti probleme za aplikacije omogućene za Mapiranje identiteta u poduzeću (EIM), uključujući i5/OS aplikacije i proizvode, koji nisu oblikovani za rukovanje ovim dvosmislenim rezultatima.

Te se informacije pregledavanja moraju dati operaciji pregledavanja mapiranja da bi se osiguralo da operacija može vratiti jedinstveni ciljni korisnički identitet. Međutim, ako prethodno definirane informacije pregledavanja nisu više potrebne, možda ćete ih htjeti ukloniti tako da više ne moraju biti osigurane za operacije pregledavanja.

Kako ćete ukloniti informacije pregledavanja s ciljnog korisničkog identiteta ovisi o tome je li ciljni korisnički identitet definiran u asocijaciji identifikatora ili ciljnoj asocijaciji. Informacije pregledavanja su vezane na ciljni korisnički identitet, a ne za asocijacije identifikatora ili asocijacije politika u kojima se taj identitet nalazi. Prema tome, kada brišete zadnju asocijaciju identifikatora ili asocijaciju politike koja se odnosi na taj ciljni korisnički identitet, iz EIM domene se brišu korisnički identitet i informacije pregledavanja.

Uklanjanje informacija pregledavanja ciljnog korisničkog identiteta u asocijaciji identifikatora:

Za uklanjanje informacija pregledavanja ciljnog korisničkog identiteta u asocijaciji identifikatora, morate biti povezani na EIM domenu u kojoj želite raditi i morate imati “EIM kontrola pristupa” na stranici 38 na jednoj od ovih razina:

- Administrator registra.
- Administrator za izabrane registre (za definicije registara koje se odnose na korisnički registar koji sadrži ciljni korisnički identitet).
- EIM administrator.

Za uklanjanje informacija pregledavanja ciljnog korisničkog identiteta u asocijaciji identifikatora izvedite sljedeće korake:

1. Proširite **Mreža > Mapiranje identiteta u poduzeću > Upravljanje domenom**.
2. Izaberite EIM domenu u kojoj želite raditi.
   - Ako EIM domena s kojom želite raditi nije popisana pod **Upravljanje domenom**, pregledajte “Dodavanje EIM domene u folder Upravljanje domenom” na stranici 84.
   - Ako trenutno niste povezani na EIM domenu u kojoj želite raditi, pregledajte Povezivanje na EIM kontroler domene.
3. Proširite EIM domenu na koju ste povezani.
4. Kliknite **Identifikatori** za prikaz liste EIM identifikatora za domenu.

   Bilješka: Ponekad kada pokušate proširiti folder **Identifikatori** može proći puno vremena prije nego se popis identifikatora prikaže. Da poboljšate performanse kada imate velik broj EIM identifikatora u domeni, možete prilagoditi pogled foldera **Identifikatori** ograničavajući vrijednost traženja korištenu za prikaz

identifikatora. Desno kliknite **Identifikatori**, izaberite **Prilagodi ovaj pogled > Uključi** i specificirajte kriterije prikaza za upotrebu kod generiranja popisa EIM identifikatora koje treba uključiti u ovaj pogled.

5. Desno kliknite EIM identifikator i izaberite **Svojstva**.
6. Izaberite stranicu **Asocijacije**, izaberite ciljnu asocijaciju za korisnički identitet za koji želite ukloniti informacije pregledavanja i kliknite **Detalji**.
7. U dijalogu **Asocijacije - Detalji** izaberite informacije pregledavanja koje želite ukloniti s ciljnog korisničkog identiteta i kliknite **Ukloni**.

   Bilješka: Nakon što kliknete **Ukloni** od vas se ne traži da akciju potvrdite.
8. Kliknite **OK** za spremanje promjena i vraćanje u dijalog **Asocijacija - Detalji**.
9. Za izlaz kliknite **OK**.

Uklanjanje informacija pregledavanja ciljnog korisničkog identiteta u asocijaciji politike:

Za uklanjanje informacija pregledavanja ciljnog korisničkog identiteta u asocijaciji politike, morate biti povezani na EIM domenu u kojoj želite raditi i morate imati “EIM kontrola pristupa” na stranici 38 na jednoj od ovih razina:

- Administrator registra.
- Administrator za izabrane registre (za definiciju registara koja se odnosi na korisnički registar koji sadrži ciljni korisnički identitet (ID)).
- EIM administrator.

Za uklanjanje informacija pregledavanja ciljnog korisničkog identiteta u asocijaciji politike izvedite sljedeće korake:

1. Proširite **Mreža > Mapiranje identiteta u poduzeću > Upravljanje domenom**.
2. Izaberite EIM domenu u kojoj želite raditi.
   - Ako EIM domena s kojom želite raditi nije popisana pod **Upravljanje domenom**, pregledajte “Dodavanje EIM domene u folder Upravljanje domenom” na stranici 84.
   - Ako trenutno niste povezani na EIM domenu u kojoj želite raditi, pregledajte Povezivanje na EIM kontroler domene.
3. U dijalogu **Politika mapiranja** koristite stranice za gledanje asocijacija politike za domenu.
4. Pronađite i izaberite asocijaciju politike za ciljni registar koji koristi ciljni korisnički identitet kojemu želite ukloniti informacije pregledavanja.
5. Kliknite **Detalji** za prikaz odgovarajućeg dijaloga **Asocijacija politika - Detalji** za tip asocijacije politika koji ste izabrali.
6. Izaberite informacije pregledavanja koje želite ukloniti s ciljnog korisničkog registra, a zatim kliknite **Ukloni**.

   Bilješka: Nakon što kliknete **Ukloni** od vas se ne traži da akciju potvrdite.
7. Kliknite **OK** za spremanje promjena i vraćanje u originalni dijalog **Asocijacija - Detalji**.
8. Za izlaz kliknite **OK**.

Prikazivanje svih asocijacija identifikatora za EIM identifikatore

Za prikaz svi asocijacija za identifikator Mapiranja identiteta u poduzeću (EIM) morate biti povezani na EIM domenu na kojoj želite raditi i morate imati neku razinu EIM kontrole pristupa za izvođenje ovog zadatka.

Možete pogledati sve asocijacije s bilo kojom razinom kontrole pristupa osim kontrole pristupa Administrator za izabrane registre. Ova razina kontrole pristupa omogućuje vam ispis i pogled svih onih asocijacija na registre za koje imate eksplicitno ovlaštenje, osim ako nemate kontrolu pristupa EIM operacija pregledavanja mapiranja.

Za prikaz svih asocijacija između EIM identifikatora i korisničkih identiteta (ID-ova) za koje su asocijacije definirane za EIM identifikator, izvedite sljedeće korake:

Za prikaz asocijacija za identifikator, izvedite sljedeće korake:

1. Proširite **Mreža > Mapiranje identiteta u poduzeću > Upravljanje domenom**.
2. Izaberite EIM domenu u kojoj želite raditi.
   - Ako EIM domena s kojom želite raditi nije popisana pod **Upravljanje domenom**, pregledajte “Dodavanje EIM domene u folder Upravljanje domenom” na stranici 84.
   - Ako trenutno niste povezani na EIM domenu u kojoj želite raditi, pregledajte Povezivanje na EIM kontroler domene.
3. Proširite EIM domenu na koju ste povezani.
4. Kliknite **Identifikatori** za prikaz liste EIM identifikatora za domenu.

   Bilješka: Ponekad kada pokušate proširiti folder **Identifikatori** može proći puno vremena prije nego se popis identifikatora prikaže. Da poboljšate performanse kada imate velik broj EIM identifikatora u domeni, možete prilagoditi pogled foldera **Identifikatori** ograničavajući vrijednost traženja korištenu za prikaz identifikatora. Desno kliknite **Identifikatori**, izaberite **Prilagodi ovaj pogled > Uključi** i specificirajte kriterije prikaza za upotrebu kod generiranja popisa EIM identifikatora koje treba uključiti u ovaj pogled.
5. Izaberite EIM identifikator, desno kliknite taj EIM identifikator i izaberite **Svojstva**.
6. Za prikaz popisa korisničkih identiteta za izabrani EIM identifikator izaberite stranicu **Asocijacije**.
7. Za kraj kliknite **OK**.

Prikazivanje svih asocijacija politika za domenu

Za prikaz svih asocijacija politika za domenu morate biti povezani na domenu Mapiranja identiteta u poduzeću (EIM) u kojoj želite raditi i morate imati neku razinu EIM kontrole pristupa za izvođenje ovog zadatka.

Možete pogledati sve asocijacije politike s bilo kojom razinom kontrole pristupa osim kontrole pristupa Administrator za izabrane registre. Ova razina kontrole pristupa omogućuje vam ispis i pogled samo onih asocijacija za registre za koje imate eksplicitno ovlaštenje. Prema tome s ovom kontrolom pristupa ne možete 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 sljedeće korake:

1. Proširite **Mreža > Mapiranje identiteta u poduzeću > Upravljanje domenom**.
2. Desno kliknite na EIM domenu na kojoj želite raditi i izaberite **Politika mapiranja**
   - Ako EIM domena s kojom želite raditi nije popisana pod **Upravljanje domenom**, pregledajte “Dodavanje EIM domene u folder Upravljanje domenom” na stranici 84.
   - Ako trenutno niste povezani na EIM domenu u kojoj želite raditi, pregledajte Povezivanje na EIM kontroler domene.
3. Izaberite stranicu za prikaz asocijacija politika definiranih za domenu, kao što slijedi:
   a. Izaberite stranicu **Domena** za pogled asocijacija politike default domene definiranih za domenu i za provjeru je li asocijacija politike omogućena na razini registra.
   b. Izaberite stranicu **Registar** za pogled default asocijacija politike definiranih za domenu. Također možete pogledati na koje izvorne registre i ciljne registre utječu asocijacije politike.
   c. Izaberite stranicu **Filter certifikata** za pogled asocijacija politike filtera certifikata definiranih i omogućenih na razini registra.
4. Za kraj kliknite **OK**.

Prikazivanje svih asocijacija politika za definiciju registra

Za prikaz svih asocijacija politika za specifični registar morate biti povezani na domenu Mapiranja identiteta u poduzeću (EIM) u kojoj želite raditi i morate imati neku razinu EIM kontrole pristupa za izvođenje ovog zadatka.

Možete pogledati sve asocijacije politike s bilo kojom razinom kontrole pristupa osim kontrole pristupa Administrator za izabrane registre. Ova razina kontrole pristupa omogućuje vam ispis i pogled samo onih asocijacija za registre za koje imate eksplicitno ovlaštenje. Prema tome s ovom kontrolom pristupa ne možete 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 sljedeće korake:

1. Proširite **Mreža > Mapiranje identiteta u poduzeću > Upravljanje domenom**.
2. Izaberite EIM domenu u kojoj želite raditi.
   - Ako EIM domena s kojom želite raditi nije popisana pod **Upravljanje domenom**, pregledajte “Dodavanje EIM domene u folder Upravljanje domenom” na stranici 84.
   - Ako trenutno niste povezani na EIM domenu u kojoj želite raditi, pregledajte Povezivanje na EIM kontroler domene.
3. Desno kliknite na definiciju registra s kojom želite raditi i izaberite **Politika mapiranja**.
4. Izaberite stranicu za prikaz asocijacija politika definiranih za navedenu definiciju registra, kao što slijedi:
   - Izaberite stranicu **Domena** za pogled asocijacija politike default domene definiranih za registar.
   - Izaberite stranicu **Registar** za pogled default asocijacija politike registra definiranih i omogućenih za registar.
   - Izaberite stranicu **Filter certifikata** za pogled asocijacija politika filtera certifikata definiranih i omogućenih za registar.
5. Za kraj kliknite **OK**.

Brisanje asocijacije identifikatora

Za brisanje asocijacije identifikatora morate biti povezani na domenu Mapiranja identiteta u poduzeću (EIM) u kojoj želite raditi i morate imati EIM kontrolu pristupa zahtijevanu od strane tipa asocijacije koji želite obrisati.

Za brisanje izvorne ili administrativne asocijacije morate imati EIM kontrolu pristupa na jednoj od sljedećih razina:

- Administrator identifikatora.
- EIM administrator.

Za brisanje ciljne asocijacije morate imati EIM kontrolu pristupa na jednoj od sljedećih razina:

- Administrator registra.
- Administrator za izabrane registre (za definiciju registara koja se odnosi na korisnički registar koji sadrži ciljni korisnički identitet).
- EIM administrator.

Za brisanje asocijacije identifikatora, izvedite sljedeće korake.

1. Proširite **Mreža > Mapiranje identiteta u poduzeću > Upravljanje domenom**.
2. Izaberite EIM domenu u kojoj želite raditi.
   - Ako EIM domena s kojom želite raditi nije popisana pod **Upravljanje domenom**, pregledajte “Dodavanje EIM domene u folder Upravljanje domenom” na stranici 84.
   - Ako trenutno niste povezani na EIM domenu u kojoj želite raditi, pregledajte Povezivanje na EIM kontroler domene.
3. Proširite EIM domenu na koju ste povezani.
4. Kliknite **Identifikatori** za prikaz liste EIM identifikatora za domenu.

   Bilješka: Ponekad kada pokušate proširiti folder **Identifikatori** može proći puno vremena prije nego se popis identifikatora prikaže. Da poboljšate performanse kada imate velik broj EIM identifikatora u domeni, možete prilagoditi pogled foldera **Identifikatori** ograničavajući kriterij traženja korišten za prikaz identifikatora. Desno kliknite **Identifikatori**, izaberite **Prilagodi ovaj pogled > Uključi** i specificirajte kriterije prikaza za upotrebu kod generiranja popisa EIM identifikatora koje treba uključiti u ovaj pogled.
5. Izaberite EIM identifikator, desno kliknite taj EIM identifikator i izaberite **Svojstva**.
6. Za prikaz popisa korisničkih identiteta za izabrani EIM identifikator izaberite stranicu **Asocijacije**.
7. Izaberite asocijaciju koju želite brisati i kliknite **Ukloni** za brisanje asocijacije.

   Bilješka: Nema potvrdnog prompta nakon što kliknete **Ukloni**.
8. Za spremanje promjena kliknite **OK**.

Bilješka: Kada uklonite ciljnu asocijaciju bilo kakva operacija pregledavanja mapiranja u ciljni registar koji ovisi o korištenju obrisane asocijacije možda neće uspjeti ako druge asocijacije (bilo asocijacije politike ili asocijacije identifikatora) ne postoje za taj zahvaćeni ciljni registar.

Jedini način da se za EIM definira korisnički identitet je kada navedete korisnički identitet kao dio kreiranja asocijacije bilo asocijacije identifikatora ili asocijacije politike. Prema tome kada izbrišete zadnju ciljnu asocijaciju za korisnički identitet (bilo uklanjanjem individualne ciljne asocijacije ili uklanjanjem asocijacije politike) taj korisnički identitet nije više definiran u EIM-u. Prema tome gubi se ime korisničkog identiteta i bilo koje informacije pregledavanja za taj korisnički identitet.

Brisanje asocijacije politike

Za brisanje asocijacije politike morate biti povezani na domenu Mapiranja identiteta u poduzeću (EIM) na kojoj želite raditi i morate imati EIM kontrolu pristupa za Administratora registra, ili za EIM administratora.

Za brisanje asocijacije politike izvedite sljedeće korake:

1. Proširite **Mreža > Mapiranje identiteta u poduzeću > Upravljanje domenom**.
2. Izaberite EIM domenu u kojoj želite raditi.
   - Ako EIM domena s kojom želite raditi nije popisana pod **Upravljanje domenom**, pregledajte “Dodavanje EIM domene u folder Upravljanje domenom” na stranici 84.
   - Ako trenutno niste povezani na EIM domenu u kojoj želite raditi, pregledajte Povezivanje na EIM kontroler domene.
3. Izaberite prikladnu stranicu za tip asocijacije politike koji želite obrisati.
4. Na toj stranici izaberite odgovarajuću asocijaciju politike i kliknite **Ukloni**.

   Bilješka: Nakon što kliknete **Ukloni** od vas se ne traži da akciju potvrdite.
5. Kliknite **OK** da izađete iz dijaloga **Politika mapiranja** i spremite vaše promjene.

Bilješka: Kada uklonite ciljnu asocijaciju politike, bilo kakve operacije pregledavanja mapiranja u ciljnom registru koje ovise o korištenju obrisane asocijacije politike možda neće uspjeti ako druge asocijacije (bilo asocijacije politike ili asocijacije identifikatora) ne postoje za taj ciljni registar.

Jedini način da se za EIM definira korisnički identitet je kada navedete korisnički identitet kao dio kreiranja asocijacije bilo asocijacije identifikatora ili asocijacije politike. Prema tome kada izbrišete zadnju ciljnu asocijaciju za korisnički identitet (bilo uklanjanjem individualne ciljne asocijacije ili uklanjanjem asocijacije politike) taj korisnički identitet nije više definiran u EIM-u. Prema tome gubi se ime korisničkog identiteta i bilo koje informacije pregledavanja za taj korisnički identitet.

Srodni koncepti

“Upravljanje definicijama registra Mapiranja identiteta u poduzeću” na stranici 88
Da bi korisnički registri i korisnički identiteti koje sadrže sudjelovali u EIM domeni, morate za njih kreirati definicije registra. Tada možete upravljati kako korisnički registri i njihovi korisnički identiteti sudjeluju u EIM-u s upravljanjem tim EIM definicijama registra.

Upravljanje EIM kontrole pristupa korisnika

Korisnik Mapiranja identiteta u poduzeću (EIM) je korisnik koji posjeduje kontrolu pristupa EIM-u baziranu na njegovom članstvu u preddefiniranim korisničkim grupama Lightweight Directory Access Protocol (LDAP). Specificiranjem EIM kontrole pristupa za korisnika dodaje se taj korisnik u određenu LDAP korisničku grupu.

Svaka LDAP grupa ima ovlaštenje za izvođenje raznolikih EIM administrativnih zadataka za tu domenu. Koje i kakve tipove administrativnih zadataka EIM korisnik može izvesti, uključujući i operacije pregledavanja, određeno 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 što korisnik može postati član grupe za EIM kontrolu pristupa, taj se korisnik mora unijeti u poslužitelja direktorija koji djeluje kao EIM kontroler domene. Također, samo određeni tipovi korisnika mogu biti učinjeni članovima grupe kontrole pristupa EIM-u: Kerberos principali, razlikovna imena i profili korisnika i5/OS-a.

Bilješka: Da biste imali tip korisnika Kerberos principala dostupan u EIM-u, na sistemu mora biti konfigurirana usluga provjere autentičnosti mreže. Da tip profila korisnika i5/OS-a bude dostupno u EIM-u, morate konfigurirati sufiks objekta sistema na poslužitelju direktorija. To dozvoljava poslužitelju direktorija da referencira objekte i5/OS sistema, poput profila korisnika i5/OS-a.

Za upravljanje kontrolom pristupa za postojećeg korisnika poslužitelja direktorija ili dodavanje postojećeg korisnika direktorija u grupu EIM kontrole pristupa, izvedite sljedeće korake:

1. Proširite **Mreža > Mapiranje identiteta u poduzeću > Upravljanje domenom**.
2. Izaberite EIM domenu u kojoj želite raditi.
   - Ako EIM domena s kojom želite raditi nije popisana pod **Upravljanje domenom**, pregledajte “Dodavanje EIM domene u folder Upravljanje domenom” na stranici 84.
   - Ako trenutno niste povezani na EIM domenu u kojoj želite raditi, pregledajte Povezivanje na EIM kontroler domene.
3. Desno kliknite EIM domenu na koju ste spojeni i izaberite **Kontrola pristupa**
4. U dijalogu **Uređivanje EIM kontrole Pristupa**, izaberite **Tip korisnika** za prikaz polja potrebnih za dobavu identifikacijskih informacija za korisnika.
5. Unesite potrebne korisničke informacije za identifikaciju korisnika za kojeg želite da upravlja EIM kontrolom pristupa i kliknite **OK** za prikaz panela **Uređivanje EIM kontrole Pristupa**. Ako je potrebno kliknite **Pomoć** da odredite koje informacije navesti u određenom polju.
6. Izaberite jednu ili više grupa **Kontrole pristupa** za korisnika i kliknite **OK** da dodate korisnika u izabrane grupe. Kliknite **Pomoć** za detaljnije informacije o tome koje ovlaštenje ima svaka grupa i za naučiti o posebnim zahtjevima.
7. Nakon što osigurate potrebne informacije, za spremanje vaših promjena kliknite **OK**.

Srodni koncepti

“EIM kontrola pristupa” na stranici 38
Korisnik Mapiranja identiteta u poduzeću (EIM) je korisnik koji posjeduje kontrolu pristupa EIM-u baziranu na njegovom članstvu u preddefiniranoj korisničkoj grupi Lightweight Directory Access Protocol (LDAP) za specifičnu domenu.

Srodne informacije

Usluge provjere autentičnosti mreže

Upravljanje svojstvima EIM konfiguracije

Za vaš poslužitelj možete upravljati nekoliko različitim svojstvima EIM konfiguracije. Tipično, to ne trebate često činiti.

Međutim, postoje situacije koje zahtijevaju promjene na svojstvima konfiguracije. Na primjer, ako vam se sruši sistem i morate ponovno kreirati vaša konfiguracijska svojstva EIM-a, možete ili ponovno pokrenuti Čarobnjaka konfiguracije EIM-a ili promijeniti svojstva ovdje. Drugi primjer je kada izaberete ne kreirati definicije registra za lokalne registre kada pokrećete čarobnjaka EIM konfiguracije tada ovdje možete ažurirati informacije definicije registra.

Svojstva koja možete mijenjati uključuju:

- EIM domenu u kojoj poslužitelj sudjeluje.
- Informacije povezivanja za EIM kontroler domene.
- Korisnički identitet koji sistem koristi za izvođenje EIM operacija na račun funkcija operativnog sistema.
- Imena definicije registra koja se odnose na stvarne korisničke registre koje sistem može koristiti prilikom izvođenja EIM operacije u ime funkcija operativnog sistema. Ta imena definicije registara odnose se na lokalne korisničke registre koje kreirate kada pokrenete čarobnjaka EIM konfiguracije.

Bilješka: Ako izaberete ne kreirati imena lokalne definicije registra kada pokrenete čarobnjaka EIM konfiguracije zato, jer su registri već definirani na EIM domeni ili, jer ste ih izabrali kasnije definirati na domeni, morate ovdje ažurirati svojstva konfiguracije sistema s tim imenima definicije registra. Sistem te informacije definicije registra treba za izvođenje EIM operacija za funkcije operativnog sistema.

Za promjenu EIM svojstava konfiguracije morate imati ova posebna ovlaštenja:

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

Za promjenu svojstava EIM konfiguracije za vašu System i platformu, dovršite sljedeće korake:

1. Proširite **Mreža >Mapiranje identiteta u poduzeću**.
2. Desno kliknite **Konfiguracija** i izaberite **Svojstva**.
3. Napravite promjene na EIM informacijama konfiguracije.
4. Za određivanje koje informacije navesti u svakom polju dijaloga kliknite **Pomoć**.
5. Kliknite **Provjeri konfiguraciju** da osigurate da sve navedene informacije omogućuju sistemu da uspješno uspostavi vezu s EIM kontrolerom domene.
6. Za spremanje promjena kliknite **OK**.

Bilješka: Ako niste koristili čarobnjaka EIM konfiguracije za kreiranje domene ili spajanje na domenu, ne pokušavajte kreirati EIM konfiguraciju ručnim specificiranjem svojstava konfiguracije. Upotrebom čarobnjaka za kreiranje osnovne EIM konfiguracije možete spriječiti moguće konfiguracijske probleme, jer čarobnjak čini više od samog konfiguriranja tih svojstava.

Rješavanje problema Mapiranja identiteta u poduzeću

Koristite sljedeće metode rješavanja problema da riješite neke od osnovnih problema na koje možete naići kod konfiguriranja i upotrebe Mapiranja identiteta u poduzeću (EIM).

EIM čini nekoliko tehnologija i mnoštvo aplikacija i funkcija. Prema tome, problemi se mogu dogoditi u mnogim područjima. Sljedeće informacije opisuju neke uobičajene probleme i pogreške na koje možete naići kada upotrebljavate EIM i neke sugestije kako ispraviti te pogreške i probleme.

Srodne informacije

Rješavanje problema konfiguracije jednostruke prijave

Rješavanje problema povezivanja na kontroler domene

Velik broj faktora može pridonijeti problemima povezivanja kod pokušaja povezivanja na kontroler domene. Pregledajte sljedeću tablicu da odredite kako riješiti moguće probleme s povezivanjem na kontroler domene

Tablica 27. Uobičajeni problemi i rješenja povezivanja EIM kontrolera domene

Mogući problem	Moguća rješenja
Ne možete se povezati na kontroler domene kada koristite System i Navigator za upravljanje EIM-om.	Informacije veze kontrolera domene mogu biti neispravno navedene za domenu kojom želite upravljati. Izvedite sljedeće korake za provjeru informacija veze domene: • Proširite **Mreža-->Mapiranje identiteta u poduzeću-->Mreža->Upravljanje domenom**. Desno kliknite domenu kojom želite upravljati i izaberite **Svojstva**. • Provjerite da je ime **Kontrolera domene** ispravno i da je **Nadređeni 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)** poslužitelj direktorija mora biti konfiguriran za korištenje SSL-a. Kliknite **Provjeri vezu** da provjerite da možete koristiti navedene informacije za uspješnu uspostavu veze s kontrolerom domene. • Provjerite da su korisničke informacije u panelu **Povezivanje na kontroler domene** ispravne.
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 može dešavati, jer je EIM konfiguracija na sistemu ili sistemima neispravna.	Provjerite vašu EIM konfiguraciju. Proširite **Mreža-->Mapiranje identiteta u poduzeću-->Konfiguracija** na sistemu na kojem pokušavate izvesti provjeru autentičnosti. Desno kliknite folder **Konfiguracija** i izaberite **Svojstva** i provjerite sljedeće: • 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 **Omogući EIM operacije za ovaj sistem**. • Stranica **Korisnik sistema**: – Da li navedeni korisnik ima dostatnu EIM kontrolu pristupa za izvođenje pregledavanja mapiranja i lozinka je važeća za korisnika. Pogledajte on-line pomoć da naučite više o različitim tipovima korisničkih vjerodajnica. **Bilješka:** Ako ste lozinku promijenili za specifičnog sistemskog korisnika u poslužitelju direktorija, lozinku morate također i ovdje promijeniti. Ako te lozinke ne odgovaraju, tada korisnik sistema ne može izvesti EIM funkcije za operativni sistem i operacija pregledavanja mapiranja neće uspjeti. – Kliknite **Provjeri vezu** da potvrdite da su navedene korisničke informacije ispravne.

Tablica 27. Uobičajeni problemi i rješenja povezivanja EIM kontrolera domene (nastavak)

Mogući problem	Moguća rješenja
Izgleda da su informacije konfiguracije ispravne, ali ne možete se spojiti na kontroler domene.	• Provjerite da li je aktivan poslužitelj direktorija koji djeluje kao EIM kontroler domene. Ako je kontroler domene System i platforma, možete koristiti System i Navigator i slijediti sljedeće korake: 1. Proširite **Mreža > Poslužitelji > TCP/IP**. 2. Provjerite da poslužitelj direktorija ima stanje **Pokrenut**. Ako je poslužitelj zaustavljen, desno kliknite **Directory Server** i izaberite **Pokreni**

Nakon što se provjerili informacije veze i da je poslužitelj direktorija aktivan, pokušajte se povezati na kontroler domene tako da slijedite ove korake:

1. Proširite **Mreža > Mapiranje identiteta u poduzeću > Upravljanje domenom**.
2. Desno kliknite na EIM domenu na koju se želite povezati i izaberite **Povezivanje**.
3. Specificirajte tip korisnika i potrebne korisničke informacije koje bi se trebale koristiti za povezivanje na kontroler EIM domene.
4. Kliknite **OK**.

Rješavanje općenitih problema EIM konfiguracije i domene

Postoji veliki broj općenitih problema na koje možete naići kada konfigurirate EIM za vaš sistem, kao i problemi na koje možete naići kada pristupate EIM domeni. Pregledajte sljedeću tablicu da naučite više o nekim uobičajenim problemima i mogućim rješenjima koja možete koristiti za rješavanje ovih problema.

Tablica 28. Uobičajeni problemi i rješenja EIM konfiguracije i domene

Mogući problem	Moguća rješenja
Izgleda da Čarobnjak EIM konfiguracije visi za vrijeme obrade **Završetka**.	Čarobnjak možda čeka da se kontroler domene pokrene. Provjerite da se u toku pokretanja poslužitelja direktorija nisu pojavile pogreške. Za System i platforme provjerite dnevnik posla za QDIRSRV posao u QSYSWRK podsistemu. Da provjerite dnevnik posla, pratite ove korake: 1. U System i Navigator proširite **Upravljanje poslom > Podsistemi > Qsyswrk**. 2. Desno kliknite na **Qdirsrv** i izaberite **Dnevnik posla**.
Za vrijeme upotrebe čarobnjaka EIM konfiguracije za kreiranje domene na udaljenom sistemu, primili ste sljedeću poruku o grešci: ″Nadređeno razlikovno ime (DN) koje ste unijeli, nije važeće″. DN mora postojati na udaljenom poslužitelju direktorija. Navedite ili izaberite novi ili postojeći nadređeni DN.	Nadređeni DN naveden za udaljenu domenu ne postoji. Pogledajte “Kreiranje i spajanje nove udaljene domene” na stranici 73 za naučiti više o tome kako koristiti čarobnjaka EIM konfiguracije. Također, pogledajte on-line pomoć za detaljne informacije o specificiranju nadređenog DN-a kada kreirate domenu.
Primili ste poruku koja ukazuje da EIM domena ne postoji.	Ako niste kreirali EIM domenu, koristite čarobnjaka za EIM konfiguraciju. Ovaj čarobnjak za vas kreira EIM domenu ili vam omogućuje konfiguriranje postojeće EIM domene. Ako ste kreirali EIM domenu, osigurajte da je navedeni korisnik član neke “EIM kontrola pristupa” na stranici 38 grupe s dostatnim ovlaštenjima da joj pristupi.
Primili ste poruku koja ukazuje da EIM objekt (identifikator, registar, asocijacija, asocijacija politike ili filter certifikata) nije pronađen ili da nemate ovlaštenja na EIM podacima.	Provjerite da EIM objekt postoji i je li naveden korisnik član neke “EIM kontrola pristupa” na stranici 38 grupe s dostatnim ovlaštenjima za taj objekt.

Tablica 28. Uobičajeni problemi i rješenja EIM konfiguracije i domene (nastavak)

Mogući problem	Moguća rješenja
Kada proširite folder **Identifikatori** prođe puno vremena prije nego se pokaže popis identifikatora.	Ovo se može desiti ako u domeni postoji veliki broj EIM identifikatora. Da biste to riješili, možete prilagoditi pogled foldera **Identifikatori** tako da ograničite kriterije pretraživanja za prikaz identifikatora. Da prilagodite pogled EIM identifikatora, pratite ove korake: 1. U System i Navigator, proširite **Mreža > Mapiranje identiteta u poduzeću > Upravljanje domenom**. 2. Proširite EIM domenu u kojoj želite prikazati EIM identifikatore. 3. Desno kliknite **Identifikatori** i izaberite **Prilagodi ovaj pogled > Uključi**. 4. Navedite kriterij prikaza koji će se koristiti za generiranje popisa EIM identifikatora koji će se uključiti u pogled. **Bilješka:** Kao generički znak možete koristiti zvjezdicu (*****). 5. Kliknite **OK**. Kada sljedeći put kliknete **Identifikatori**, prikazuju se samo oni EIM identifikatori koji odgovaraju kriteriju koji ste naveli.
Za vrijeme upravljanja EIM-om preko System i Navigator, primate grešku koja označava da EIM nadimak više nije važeći.	Veza s kontrolerom domene je izgubljena. Da se ponovno povežete na kontroler domene, pratite ove korake: 1. U System i Navigator, proširite **Mreža > Mapiranje identiteta u poduzeću > Upravljanje domenom**. 2. Desno kliknite domenu s kojom želite raditi i izaberite **Ponovno spoji**. 3. Specificirajte informacije povezivanja. 4. Kliknite **OK**.
Kada koristite Kerberos protokol za provjeru autentičnosti s EIM-om, dijagnostička se poruka CPD3E3F piše u dnevnik posla.	Ova je poruka generirana kad god ne uspije provjera autentičnosti ili operacija pregledavanja mapiranja. Dijagnostičke poruke sadrže glavne i manje važne kodove stanja za označavanje gdje se desio problem. Najčešće greške su dokumentirane u poruci zajedno s obnavljanjem. Pogledajte informacije pomoći pridružene dijagnostičkoj poruci za pokretanje ispravljanja grešaka u problemu. Od pomoći vam može biti i da pregledate Rješavanje problema konfiguracije s jednostrukom prijavom.

Rješavanje problema EIM mapiranja

Postoje brojni uobičajeni problemi koji mogu prouzročiti potpuni neuspjeh mapiranja u Mapiranju identiteta u poduzeću (EIM) ili neočekivani rad. Pregledajte sljedeću tablicu da pronađete informacije o tome koji problemi mogu uzrokovati neuspjeh EIM mapiranja i moguća rješenja tog problema. Ako ne uspije EIM mapiranje, trebati ćete proučiti svako rješenje u tablici kako bi osigurali pronalazak i rješenje jednog ili više problema koji su uzrok neuspjeha mapiranja.

Tablica 29. Uobičajeni problemi i rješenja EIM mapiranja

Mogući problem	Moguća rješenja
Informacije povezivanja za kontroler domene možda nisu ispravne ili kontroler domene možda nije aktivan.	Pregledajte Problemi povezivanja za kontroler domene da naučite kako provjeriti informacije o vezi za kontroler domene i kako provjeriti da li je kontroler domene aktivan.

Tablica 29. Uobičajeni problemi i rješenja EIM mapiranja (nastavak)

Mogući problem	Moguća rješenja
Operacije pregledavanja EIM mapiranja koje su se izvodile za sistem ne uspijevaju. To se dešava zbog pogrešne EIM konfiguracije na sistemu ili sistemima.	Provjerite vašu EIM konfiguraciju. Proširite **Mreža-->Mapiranje identiteta u poduzeću-->Konfiguracija** na sistemu na kojem pokušavate izvesti provjeru autentičnosti. Desno kliknite folder **Konfiguracija** i izaberite **Svojstva** i provjerite sljedeće: • **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 omogući EIM operacije**. • **Korisnik sistema** stranica: – Navedeni korisnik ima dostatnu EIM kontrolu pristupa za izvođenje pregledavanja mapiranja, a lozinka je važeća za korisnika. Pregledajte online pomoć da naučite više o različitim tipovima korisničkih vjerodajnica. **Bilješka:** Ako ste lozinku promijenili za specifičnog sistemskog korisnika u poslužitelju direktorija, lozinku morate također i ovdje promijeniti. Ako te lozinke ne odgovaraju, tada korisnik sistema ne može izvesti EIM funkcije za operativni sistem i operacije pregledavanja mapiranja neće uspjeti. – Kliknite **Provjeri vezu** da potvrdite da su navedene korisničke informacije ispravne.

Tablica 29. Uobičajeni problemi i rješenja EIM mapiranja (nastavak)

Mogući problem	Moguća rješenja
Operacija pregledavanja mapiranja može vraćati višestruke ciljne korisničke identitete. Ovo se može desiti kada postoji jedna ili više sljedećih situacija: • EIM identifikatora ima višestruke individualne ciljne asocijacije na istom ciljnom registru. • Više od jednog EIM identifikatora ima isti korisnički identitet naveden u izvornoj asocijaciji i svaki od tih EIM identifikatora ima ciljnu asocijaciju na istom ciljnom registru, iako korisnički identitet naveden za svaku ciljnu asocijaciju može biti različit. • Više od jedne default asocijacije politike domene specificira isti ciljni registar. • Više od jedne default asocijacije politike registra specificira isti izvorni registar i isti ciljni registar. • Više od jedne asocijacije politike filtera certifikata specificira isti izvorni X.509 registar, filter certifikata i ciljni registar.	Koristite funkciju Provjera EIM Mapiranja za provjeru da li se određeni izvorišni identitet korisnika ispravno mapira na odgovarajući ciljni identitet korisnika. Kako ćete ispraviti problem ovisi o rezultatima koje dobijete iz testiranja, kako slijede: • Provjera vraća neželjene višestruke ciljne identifikatore zbog jednog od sljedećih razloga: – To može označavati da konfiguracija asocijacije za domenu nije ispravna, zbog jednog od sljedećeg: - 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 netočni korisnički identitet. Prikažite sve asocijacije identifikatora za EIM identifikator da provjerite asocijacije za specifični identifikator. - Asocijacija politike nije ispravno konfigurirana. Prikažite sve asocijacije politika za domenu da provjerite izvorne i ciljne informacije za sve asocijacije politike definirane u domeni. – To može označavati da su definicije registra grupe koje sadrže zajedničke članove izvorišni ili ciljni registri za asocijacije identifikatora EIM-a ili asocijacije politike. Koristite detalje dobivene testnom operacijom pregledavanja mapiranja da odredite da li su izvorišni ili ciljni registri definicije registra grupe. Ako jesu, provjerite svojstva definicije registra grupe da odredite da li definicije registra grupe sadrže zajedničke članove. – Test vraća višestruke ciljne korisničke identitete i ti su rezultati prikladni za način na koji ste konfigurirali asocijacije. Ako je ovo slučaj, tada trebate specificirati informacije pregledavanja za svaki ciljni korisnički identitet kako bi osigurali da operacija pregledavanja vraća jednostruki ciljni korisnički identitet umjesto svih mogućih korisničkih identiteta. Pregledajte Dodavanje informacija pregledavanja ciljnom korisničkom identitetu. **Bilješka:** Ovaj pristup radi samo ako je aplikacija omogućena za korištenje informacije pregledavanja. Ipak, osnovne i5/OS aplikacije kao na primjer System i Access za Windows ne mogu koristiti informacije pregledavanja za razlikovanje između više ciljnih korisničkih identiteta vraćenih od strane operacije pregledavanja. Prema tome, možete razmotriti redefiniciju asocijacija za domenu da osigurate da operacija pregledavanja mapiranja može vratiti jednostruki ciljni identitet korisnika, da osigurate da osnovne i5/OS aplikacije mogu uspješno izvoditi operacije pregledavanja i mapirati identitete.

Tablica 29. Uobičajeni problemi i rješenja EIM mapiranja (nastavak)

Mogući problem	Moguća rješenja
Operacije EIM pregledavanja ne vraćaju rezultate, a asocijacije su konfigurirane za domenu.	Koristite funkciju Provjera EIM Mapiranja za provjeru da li se određeni izvorišni identitet korisnika ispravno mapira na odgovarajući ciljni identitet korisnika. Provjerite da ste za test osigurali ispravne informacije. Ako su informacije ispravne i test ne vraća rezultate, tada problem može biti uzrokovan jednim od sljedećeg: • Konfiguracija asocijacije je pogrešna. Provjerite vašu konfiguraciju asocijacije korištenjem informacija o rješavanju problema iz prethodnog ulaza. • Podrška asocijacije politike nije omogućena na razini domene. Trebat ćete omogućiti asocijacije politike za domenu. • Podrška pregledavanja mapiranja ili podrška asocijacije politike nije omogućena na individualnoj razini registra. Možda ćete morati omogućiti podršku pregledavanja mapiranja i korištenje asocijacija politike za ciljni registar. • Definicija registra i korisnički identitet ne podudaraju se zbog osjetljivosti na velika i mala slova. Registar možete obrisati i ponovno kreirati ili izbrisati i ponovno kreirati asocijaciju s ispravnom veličinom slova.

Srodni zadaci

"Testiranje EIM mapiranja" na stranici 85
Testiranje Mapiranja identiteta u poduzeću (EIM) vam omogućuje izdavanje operacija pregledavanja EIM mapiranja nad vašom EIM konfiguracijom. Testiranje možete koristiti za provjeravanje da se specifični izvorni korisnički identitet ispravno mapira na odgovarajući ciljni korisnički identitet. Testiranje osigurava da operacije pregledavanja EIM mapiranja mogu vratiti ispravne ciljne korisničke identitete bazirane na specificiranim informacijama.

API-ji Mapiranja identiteta u poduzeću

Mapiranje identiteta u poduzeću (EIM) dobavlja mehanizme upravljanja korisničkim identitetom preko različitih platformi. EIM ima višestruka sučelja aplikativnog programiranja (API-je) koje aplikacija može koristiti za vođenje EIM operacija u koristi aplikacije ili aplikacijskog korisnika.

Možete koristiti ove API-je za vođenje operacija pregledavanja mapiranja identiteta, vođenje različitih EIM funkcija upravljanja i konfiguracije, kao i promjene informacija i sposobnosti upita. Svaki od tih API-ja su podržani preko IBM platformi.

EIM API-ji spadaju u više 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 ovlaštenjem

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

1. Dohvat EIM hvatišta

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 završetka, uništi EIM hvatište

Srodni koncepti

“Planiranje razvoja aplikacija za Mapiranje identiteta u poduzeću” na stranici 65
Da bi aplikacija mogla koristiti Mapiranje identiteta u poduzeću (EIM) i sudjelovati u domeni, ista mora biti sposobna koristiti EIM API-je.

Srodne informacije

API-ji Mapiranja identiteta u poduzeću (EIM)

Slične informacije za Mapiranje identiteta u poduzeću

IBM Redbooks publikacije i ostale zbirke poglavlja u Informacijskom centru sadrže informacije koje se odnose na zbirku poglavlja Mapiranje identiteta u poduzeću (EIM). Možete pogledati ili ispisati bilo koju od PDF datoteka.

IBM Redbooks

- Windows-bazirana jednostruka prijava i EIM okvir na IBM eServer iSeries poslužitelju
- iSeries Access za Windows V5R2 Vruća poglavlja: Prilagođene slike, Administracija aplikacija, SSL i Kerberos

Ostale informacije

- Jednostruka prijava
- Usluge provjere autentičnosti mreže
- IBM Tivoli Directory Server za i5/OS (LDAP)

Termini i uvjeti

Dozvole za upotrebu ovih publikacija se dodjeljuju prema sljedećim terminima i uvjetima.

Osobna upotreba: Možete reproducirati ove publikacije za vašu osobnu, nekomercijalnu upotrebu, uz uvjet da su sve napomene o vlasništvu sačuvane. Ne smijete distribuirati, prikazivati ili raditi izvedena djela iz ovih publikacija ili bilo kojeg njihovog dijela, bez izričite suglasnosti IBM-a.

Komercijalna upotreba: Možete reproducirati, distribuirati i prikazivati ove publikacije samo unutar vašeg poduzeća uz uvjet da su sve napomene o vlasništvu sačuvane. Ne smijete raditi izvedena dijela iz ovih publikacija ili kopirati, distribuirati ili prikazivati te publikacije ili bilo koji njihov dio izvan vašeg poduzeća, bez izričite suglasnosti IBM-a.

Osim kako je izričito dodijeljeno u ovoj dozvoli, nisu dane nikakve dozvole, licence ili prava, niti izričita niti posredna, na publikacije ili bilo koje podatke, softver ili bilo koje drugo intelektualno vlasništvo sadržano unutar.

IBM rezervira pravo da bilo kad, po vlastitom nahođenju, povuče ovdje dodijeljene dozvole, ako je upotreba publikacija štetna za njegove interese ili je ustanovljeno od strane IBM-a da gornje upute nisu bile ispravno slijeđene.

Ne smijete spustiti, eksportirati ili reeksportirati ove informacije, osim kod potpune usklađenosti sa svim primjenjivim zakonima i propisima, uključujući sve zakone i propise o izvozu Sjedinjenih Država.

IBM NE DAJE NIKAKVA JAMSTVA NA SADRŽAJ OVIH PUBLIKACIJA. PUBLIKACIJE SE DAJU ″KAKVE JESU″ I BEZ JAMSTAVA BILO KOJE VRSTE, IZRAVNIH ILI POSREDNIH, UKLJUČUJUĆI, ALI NE OGRANIČAVAJUĆI SE NA, POSREDNA JAMSTVA PROĐE NA TRŽIŠTU, NEKRŠENJA I PRIKLADNOSTI ZA

ODREĐENU SVRHU.

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 dvobajtne (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, POSREDNA 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 opisan u ovom dokumentu i sav licencni materijal koji je za njega dostupan IBM isporučuje prema uvjetima IBM Korisničkog ugovora, IBM Međunarodnog ugovora za programske licence, IBM Licencnog ugovora za strojni kod i bilo kojeg ekvivalentnog ugovora između nas.

Podaci o performansama sadržani u ovom dokumentu su utvrđeni u kontroliranom okruženju. 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.

Svaka kopija ili dio tih primjera programa ili bilo kakav izvedeni rad, mora uključivati napomenu o autorskom pravu kako slijedi:

© (ime vašeg poduzeća) (godina). Dijelovi ovog koda su izvedeni iz IBM Corp. primjera programa. ©Autorsko pravo IBM Corp. _unesite godinu ili godine_. Sva prava pridržana.

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
eServer
i5/OS
IBM
iSeries
Lotus Notes
NetServer
OS/400
pSeries
RACF
RDN
System i
Tivoli
WebSphere
xSeries
z/OS

| Adobe, Adobe logo, PostScript i PostScript logo su registrirani zaštitni znaci ili zaštitni znaci Adobe Systems
| Incorporated u Sjedinjenim Državama i/ili drugim zemljama.

| Linux je registrirani zaštitni znak Linus Torvaldsa 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.

Ostala imena poduzeća, proizvoda ili usluga mogu biti zaštitni znaci ili oznake usluga drugih.

Termini i uvjeti

Dozvole za upotrebu ovih publikacija se dodjeljuju prema sljedećim terminima i uvjetima.

Osobna upotreba: Možete reproducirati ove publikacije za vašu osobnu, nekomercijalnu upotrebu, uz uvjet da su sve napomene o vlasništvu sačuvane. Ne smijete distribuirati, prikazivati ili raditi izvedena djela iz ovih publikacija ili bilo kojeg njihovog dijela, bez izričite suglasnosti IBM-a.

Komercijalna upotreba: Možete reproducirati, distribuirati i prikazivati ove publikacije samo unutar vašeg poduzeća uz uvjet da su sve napomene o vlasništvu sačuvane. Ne smijete raditi izvedena dijela iz ovih publikacija ili kopirati, distribuirati ili prikazivati te publikacije ili bilo koji njihov dio izvan vašeg poduzeća, bez izričite suglasnosti IBM-a.

Osim kako je izričito dodijeljeno u ovoj dozvoli, nisu dane nikakve dozvole, licence ili prava, niti izričita niti posredna, na publikacije ili bilo koje podatke, softver ili bilo koje drugo intelektualno vlasništvo sadržano unutar.

IBM rezervira pravo da bilo kad, po vlastitom nahođenju, povuče ovdje dodijeljene dozvole, ako je upotreba publikacija štetna za njegove interese ili je ustanovljeno od strane IBM-a da gornje upute nisu bile ispravno slijeđene.

Ne smijete spustiti, eksportirati ili reeksportirati ove informacije, osim kod potpune usklađenosti sa svim primjenjivim zakonima i propisima, uključujući sve zakone i propise o izvozu Sjedinjenih Država.

IBM NE DAJE NIKAKVA JAMSTVA NA SADRŽAJ OVIH PUBLIKACIJA. PUBLIKACIJE SE DAJU ″KAKVE JESU″ I BEZ JAMSTAVA BILO KOJE VRSTE, IZRAVNIH ILI POSREDNIH, UKLJUČUJUĆI, ALI NE OGRANIČAVAJUĆI SE NA, POSREDNA JAMSTVA PROĐE NA TRŽIŠTU, NEKRŠENJA I PRIKLADNOSTI ZA

ODREĐENU SVRHU.

Tiskano u Hrvatskoj