



@server

iSeries

Enterprise Identity Mapping





@server

iSeries

Enterprise Identity Mapping

Kazalo

Preslikava identitete podjetja (EIM)	1
Natisni to temo	2
Pregled preslikave identitete podjetja	2
Zasnova EIM	4
Krmilnik domene EIM	5
Domena EIM	6
Identifikator EIM	7
Definicije registrov EIM	10
Definicije sistemskih in aplikacijskih registrov	12
Povezave EIM.	13
Operacije iskanja EIM	16
Pooblastila EIM	17
Koncepti LDAP za EIM	20
Razločevalno ime LDAP	20
Nadrejeno razločevalno ime LDAP	21
Omogočanje enotne prijave prek EIM	22
Načrtovanje za EIM.	23
Zahtevane možnosti Navigatorja iSeries za namestitvev	24
Konfiguriranje omrežne storitve overjanja	24
Konfiguriranje EIM	25
Izdelava in pridruževanje nove domene	26
Konfiguriranje zaščitene povezave s krmilnikom domene EIM	29
Pridruževanje obstoječe domene	29
Upravljanje EIM	31
Upravljanje domen EIM	32
Dodajanje domene v upravljanje domen	32
Povezovanje z domeno	32
Brisanje domene	32
Odstranjevanje domene iz upravljanja domene	33
Upravljanje povezav	33
Izdelava povezave	33
Brisanje povezave	34
Upravljanje identifikatorjev EIM	34
Izdelava identifikatorja EIM	34
Dodajanje vzdevka identifikatorju EIM	35
Brisanje identifikatorja EIM	35
Upravljanje pooblastil uporabnikov EIM	36
Upravljanje registrov uporabnikov.	36
Dodajanje registra uporabnikov	36
Dodajanje vzdevka registru uporabnikov	37
Definiranje zasebnega tipa registra uporabnikov v EIM	37
Odstranjevanje registra uporabnikov.	38
Odstranjevanje vzdevka iz registra uporabnikov	39
API-ji za EIM	39
Odpravljanje težav v EIM.	40
Povezava s krmilnikom domene ni mogoča	40
Dolgotrajen izpis identifikatorjev EIM	40
Čarovnik za konfiguracijo EIM se pri zaključni obdelavi obesil	41
Ročka EIM ni več veljavna	41
Sporočila Kerberos za overjanje in diagnosticiranje	41
Informacije, povezane z EIM	41

Preslikava identitete podjetja (EIM)

Večina omrežnih podjetij ima težave zaradi več uporabniških registrov, ki zahtevajo, da ima vsaka oseba ali enota znotraj podjetja v vsakem registru uporabniško identiteto. Potreba za več uporabniških registrov hitro preraste v veliko upravno težavo, ki vpliva na uporabnike, skrbnike in razvijalce aplikacij. Preslikava identitete podjetja (EIM) omogoča poceni rešitve za preprostejše upravljanje več uporabniških registrov in uporabniških identitet v podjetju.

EIM je mehanizem za preslikavo (povezavo) osebe ali identitete v ustrezne uporabniške identitete v različnih registrih podjetja. EIM nudi API-je za izdelavo in upravljanje teh povezav med preslikavami identitet, kot tudi API-je, ki jih uporabljajo aplikacije za poizvedovanje po teh informacijah. Poleg tega uporablja OS/400^(R) zmožnosti EIM in Kerberos, s katerimi nudi okolje enotne prijave.

V Navigator iSeries, grafični vmesnik iSeries, so vključeni čarovniki za konfiguriranje in upravljanje EIM. Skrbniki lahko prek Navigatorja iSeries tudi upravljajo razmerja EIM za profile uporabnikov.

Strežnik iSeries^(TM) s pomočjo EIM omogoči, da vmesniki overijo uporabnike s pomočjo omrežne storitve overjanja. Aplikacije, kot tudi OS/400, lahko sprejmejo dovolilnice Kerberos in s pomočjo EIM poiščejo profil uporabnika, ki predstavlja isto osebo kot dovolilnica Kerberos.

Naslednje teme vsebujejo specifične informacije o EIM:

Natisni to temo

Natisnite datoteko PDF te teme o EIM in druge z njo povezane teme.

Pregled preslikave identitete podjetja

Poučite se o težavah, ki jih lahko EIM reši, o trenutnih industrijskih pristopih k tem težavam in zakaj je pristop EIM boljša rešitev.

Koncepti EIM

Spoznajte koncepte EIM, ki jih morate razumeti za uspešno izvajanje EIM.

Koncepti LDAP za EIM

Spoznajte koncepte LDAP (Lightweight Directory Access Protocol), ki jih morate razumeti za uspešno izvajanje EIM.

Omogočanje enotne prijave

Spoznajte prednosti, ki jih nudi EIM pri poenostavitvi prijave uporabnika.

Načrtovanje za EIM

Preden konfigurirate EIM, preverite, ali ste konfigurirali vse zahtevane storitve in aplikacije.

Konfiguriranje EIM

Za začetek dela z EIM uporabite čarovnika za konfiguracijo preslikave identitete podjetja (ki ga bomo nadalje imenovali čarovnik za konfiguracijo EIM).

Upravljanje EIM

Upravljajte lastnosti EIM, domene EIM, uporabniške registre, pooblastila uporabnikov EIM in več.

API-ji za EIM

Uporabite API-je EIM v aplikacijah in v omrežju.

Odpravljanje težav v EIM

Poiščite rešitve za splošne težave in napake, ki se pojavljajo pri uporabi EIM v podjetju.

Informacije, povezane z EIM

Povezave na informacije, povezane z EIM.

Natisni to temo

Če si želite ogledati ali presneti različico PDF, izberite Preslikava identitete podjetja



(približno 390 kb ali 50 strani).

Druge informacije

Prikažete ali presnamete lahko naslednje povezane teme:

- Omrežne storitve overjanja (približno 199 kb ali 60 strani) vsebuje informacije o konfiguriranju omrežne storitve overjanja skupaj z EIM za izdelavo okolja enotne prijave.
- Imeniške storitve (LDAP) (približno 323 kb ali 66 strani) vsebuje informacije o konfiguriranju strežnika LDAP, ki ga lahko uporabite kot krmilnik domene EIM, in informacije o zahtevnejši konfiguraciji LDAP.

Shranitev datotek PDF files

Datoteke PDF takole shranite na delovno postajo, kjer si jih lahko ogledate ali natisnete:

1. Datoteko PDF odprite v pregledovalniku (kliknite zgornjo povezavo).
2. Na meniju pregledovalnika kliknite **Datoteka**.
3. Kliknite **Shrani kot...**
4. Pomaknite se v imenik, v katerega želite shraniti datoteko PDF.
5. Kliknite **Shrani**.

Snemanje programa Adobe Acrobat Reader

Če potrebujete za ogled ali natis teh datotek PDF program Adobe Acrobat Reader, lahko snamete kopijo na spletni strani podjetja Adobe (www.adobe.com/prodindex/acrobat/readstep.html)



.

Pregled preslikave identitete podjetja

Današnja omrežna okolja so sestavljena iz kompleksnih skupin sistemov in aplikacij, ki zahtevajo upravljanje več uporabniških registrov. Obravnava več uporabniških registrov lahko hitro preraste v veliko upravno težavo, ki vpliva na uporabnike, skrbnike in razvijalce aplikacij. Zaradi tega se veliko podjetij bori za varno overjanje in pooblašcanje sistemov in aplikacij. Preslikava identitete podjetja (EIM) je IBM-ova

@ server

infrastrukturalna tehnologija, ki omogoča skrbnikom in razvijalcem aplikacij preprostejšo in cenejšo obravnavo te težave kot v preteklosti.

Naslednje informacije opisujejo težave in trenutne industrijske pristope in razlagajo, zakaj je pristop EIM boljši.

Težava upravljanja več uporabniških registrov

Številni skrbniki upravljajo omrežja, sestavljena iz različnih sistemov in strežnikov, od katerih ima vsak unikaten način upravljanja uporabnikov prek različnih uporabniških registrov. V teh zapletenih omrežjih so

odgovorni skrbniki za upravljanje identite in gesel posameznih uporabnikov v več sistemih. Poleg tega morajo skrbniki pogosto uskladiti te identitete in gesla, uporabniki pa si morajo zapomniti več identitet in gesel in ohranjati njihovo skladnost. Obremenitev uporabnikov in skrbnikov v tem okolju je tako precejšnja. Zato skrbniki pogosto tratijo svoj dragocen čas pri odpravljanju neuspešnih poskusov prijavi in vnovičnem nastavljanju pozabljenih gesel, namesto da bi upravljali podjetje.

Težava upravljanja več uporabniških registrov vpliva tudi na razvijalce aplikacij, ki poskušajo razviti večplastne ali heterogene aplikacije. Ti razvijalci razumejo, da imajo stranke porazdeljene pomembne poslovne podatke v različnih vrstah sistemov, ki imajo lastne uporabniške registre. Posledično morajo izdelati razvijalci lastniške uporabniške registre in z njimi povezano semantiko zaščite za njihove aplikacije. To reši težavo za razvijalca aplikacije, poveča pa obremenitev uporabnikov in skrbnikov.

Trenutni pristopi

Trenutno je na voljo več industrijskih pristopov za reševanje težave upravljanja več uporabniških registrov, vendar vsi nudijo nepopolne rešitve. LDAP (Lightweight Directory Access Protocol) na primer nudi rešitev s porazdeljenim uporabniškim registrom. Vendar pa uporaba LDAP (ali drugih priljubljenih rešitev, kot je na primer Microsoft Passport) pomeni, da morajo skrbniki upravljati še dodaten uporabniški register in semantiko zaščite ali zamenjati obstoječe aplikacije, ki so izdelane za uporabo teh registrov.

Če uporabijo skrbniki to vrsto rešitve, morajo upravljati več mehanizmov zaščite za posamezna sredstva, s čimer povečajo upravno obremenitev in tudi možnost lukenj v zaščiti. Če več mehanizmov podpira eno sredstvo, je možnost spremembe pooblastila prek enega mehanizma in pozabe na spremembo pooblastila za enega ali več drugih mehanizmov, veliko večja. Do luknje v zaščiti lahko na primer pride, če je uporabniku ustrežno zavržen dostop prek enega vmesnika, vendar mu je dovoljen dostop prek enega ali več drugih vmesnikov.

Ko skrbniki opravijo ta del, ugotovijo, težava ni v celoti rešena. Na splošno so vložila podjetja preveč denarja v trenutne uporabniške registre in z njimi povezano semantiko zaščite, da bi postala uporaba te vrste rešitve praktična. Izdelava drugega uporabniškega registra in z njim povezane semantike zaščite reši težavo ponudnika aplikacij, ne pa tudi težav uporabnikov ali skrbnikov.

Druga možna rešitev je uporaba pristopa enotne prijave. Na voljo so številni izdelki, ki omogočajo skrbnikom upravljanje datotek, ki vsebujejo vse uporabnikove identitete in gesla. Vendar pa ima ta pristop več slabosti:

- Obravnava samo eno od težav, na katero naleti uporabnik. Čeprav uporabnikom omogoča prijavo v več sistemov z eno identiteto in geslom, mora imeti uporabnik gesla v drugih sistemih in jih tudi upravljati.
- Predstavlja tudi novo težavo, saj povzroči luknjo v zaščiti, ki je posledica shranitve gesel v teh datotekah v obliki čistega besedila ali besedila, ki ga je mogoče dešifrirati. Gesla ne smejo biti nikoli shranjena v datotekah s čistim besedilom ali preprosto dostopna komurkoli, vključno s skrbniki.
- Ne reši težav razvijalcev aplikacij drugih proizvajalcev, ki nudijo heterogene, večplastne aplikacije. Ti morajo za svoje aplikacije še vedno podati lastniške uporabniške registre.

Kljub tem slabostim so se nekatera podjetja odločila za uporabo teh pristopov, ker nekoliko olajšajo težave, povezane z več uporabniškimi registri.

Pristop EIM

EIM nudi nov pristop, ki nudi poceni rešitve za preprosto upravljanje več uporabniških registrov in uporabniških identitet v podjetju. EIM je arhitektura, ki opisuje razmerja med posamezniki ali enotami (kot so datotečni ali tiskalni strežniki) v podjetju in številnimi identitetami, ki jih predstavljajo znotraj podjetja. Poleg tega nudi EIM niz API-jev, ki omogočajo, da zastavljajo aplikacije vprašanja o teh razmerjih.

Tako lahko na primer s pomočjo uporabniške identitete osebe v enem uporabniškem registru določite, katera uporabniška identiteta v drugem uporabniškem registru predstavlja to isto osebo. Če je bil uporabnik overjen z eno uporabniško identiteto in lahko to identiteto preslikate v ustrezno identiteto v drugem uporabniškem

registru, uporabniku ni potrebno znova podati priporočil za namen overjanja. Na ta način veste, kdo je uporabnik - vedeti morate le, katera uporabniška identiteta predstavlja tega uporabnika v drugem uporabniškem registru. Zato nudi EIM splošno funkcijo preslikave identitet za podjetje.

Zmožnost preklopa med uporabniškimi identitetami v različnih uporabniških registrih nudi številne prednosti. Predvsem pa pomeni, da imajo aplikacije lahko prožnost za uporabo enega uporabniškega registra za overjanje in uporabo popolnoma drugega uporabniškega registra za pooblašcanje. Tako lahko na primer skrbnik preslika identiteto SAP (ali še bolje, da opravi SAP preslikavo sam) za dostop do sredstev SAP.

Uporaba preslikave identitet zahteva od skrbnikov naslednje:

1. Izdelajo identifikatorje EIM, ki predstavljajo osebe ali identitete v podjetju.
2. Izdelajo definicije registrov EIM, ki opisujejo obstoječe uporabniške registre v podjetju.
3. Definirajo razmerje med uporabniškimi identitetami v teh registrih in identifikatorji EIM, ki jih izdelajo.

Za obstoječe uporabniške registre ni potrebno opraviti nobene spremembe v kodi. Poleg tega ni nujno, da izdelata skrbnik preslikave za vse identitete v uporabniškem registru. EIM omogoča preslikavo tipa "eden v več" (ali z drugimi besedami - en uporabnik z več kot eno uporabniško identiteto v enem uporabniškem registru). EIM omogoča tudi preslikavo tipa "več v enega" (ali z drugimi besedami - več uporabnikov souporablja eno uporabniško identiteto v enem uporabniškem registru, katere uporaba je sicer podprta, vendar ni priporočena). Skrbnik lahko v EIM predstavi katerikoli uporabniški register kateregakoli tipa.

EIM je odprta arhitektura, ki jo lahko uporabijo skrbniki za predstavitev razmerij preslikave med identitetami v kateremkoli registru. Le-ta ne zahteva kopiranja obstoječih podatkov v novo odložišče in poskusa uskladitve obeh kopij. Edini novi podatki, ki jih uvaja EIM, so podatki o razmerjih. Skrbniki upravljajo te podatke v imeniku LDAP, ki nudi prožnost za upravljanje podatkov na enem mestu in ustvarjanje kopij tam, kjer so uporabljene informacije. Nenazadnje nudi EIM podjetjem in razvijalcem aplikacij prožnost za preprosto delo v različnih okoljih s precej manj stroškov kot brez uporabe te podpore.

Zasnova EIM

Če želite popolnoma razumeti, kako lahko uporabite EIM v vašem podjetju, morate dobro poznati zasnovo EIM (preslikava istovetnosti podjetja). Čeprav se lahko konfiguracija in izvedba API-jev EIM razlikuje na posameznih strežniških platformah, je zasnova EIM enaka na vseh IBM-ovih

@server

platformah.

Na Sliki 1 je prikazan zgled izvedbe EIM v podjetju. Trije strežniki delujejo kot odjemalci EIM in vsebujejo aplikacije EIM, ki zahtevajo podatke EIM z uporabo operacij iskanja

6

. Krmilnik domene

1

shrani informacije o domeni EIM

2

, ki vsebujejo identifikator EIM

3

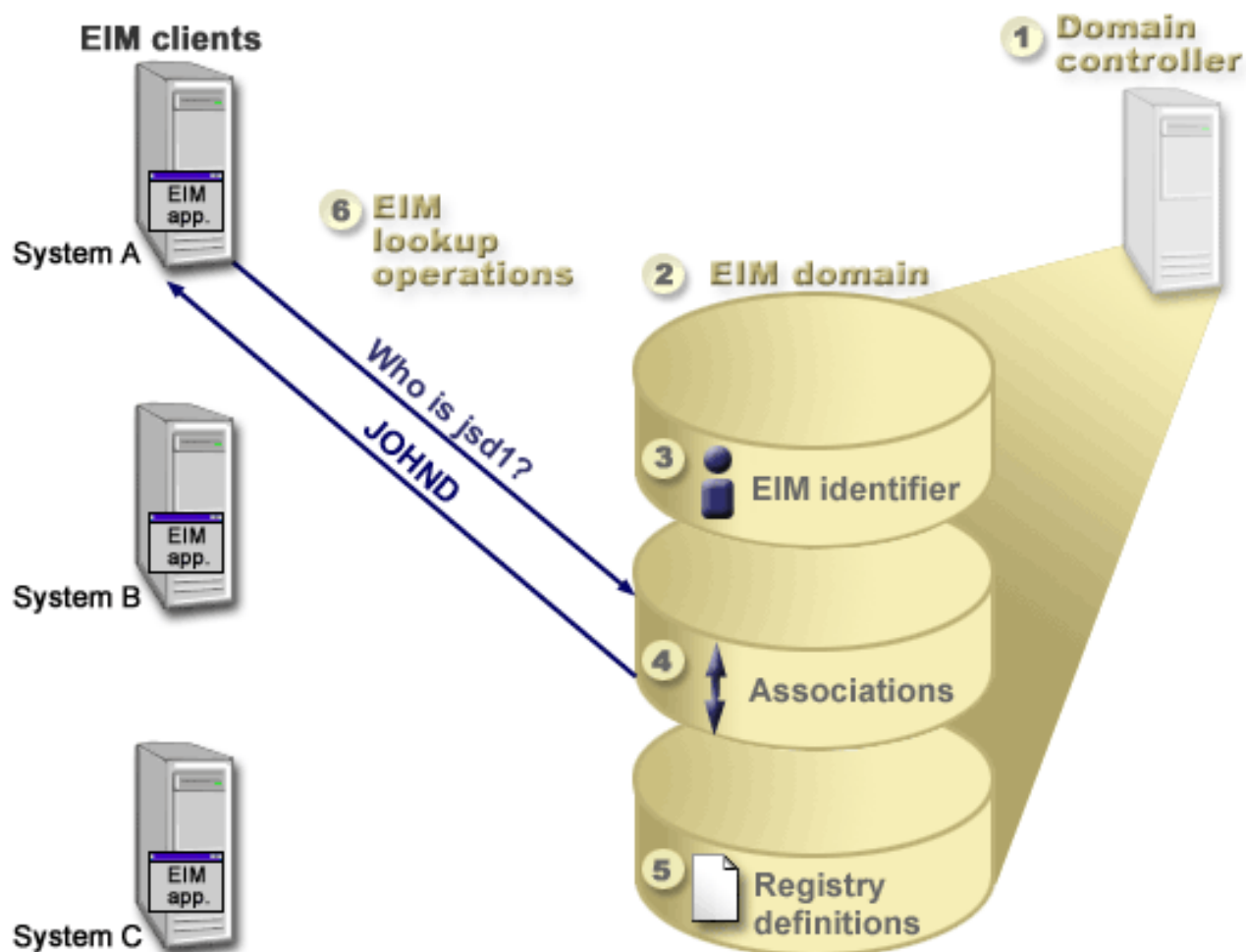
, povezave

4

med temi identifikatorji EIM in uporabniki in definicije registra EIM

5

Slika 1: Zgled izvedbe EIM



Če želite spoznati več o zasnovah EIM, preglejte naslednje informacije:

- Krmilnik domene EIM
- Domena EIM
- Identifikator EIM
- Definicije registra EIM
- Povezave EIM
- Operacije iskanja EIM
- Pooblastila EIM

Krmilnik domene EIM

Krmilnik domene EIM je strežnik LDAP (Lightweight Directory Access Protocol), ki je konfiguriran za upravljanje vsaj ene domene EIM. *Domena EIM* je imenik LDAP, ki je sestavljen iz vseh identifikatorjev EIM,

povezav EIM in uporabniških registrov, ki so definirani v tej domeni. Sistemi (odjemalci EIM) sodelujejo v domeni EIM z uporabo podatkov doemen za operacije iskanja EIM. V podjetju mora biti na voljo vsaj en krmilnik domene EIM.

Trenutno lahko konfigurirate nekatere IBM-ove

@ server

platforme, da delujejo kot krmilnik domene EIM. Vsi sistemi, ki podpirajo API-je EIM lahko sodelujejo kot odjemalec v domeni. Ti odjemalski sistemi API-je EIM za vzpostavitev povezave s krmilnikom domene EIM za izvajanje operacij iskanja EIM.

Mesto odjemalca EIM določa, ali je krmilnik domene EIM lokalni ali oddaljeni sistem. Krmilnik domene je *lokalni*, če se odjemalec EIM izvaja v istem sistemu, kot krmilnik domene. Krmilnik domene je *oddaljeni*, če se odjemalec EIM izvaja v ločenem sistemu od krmilnika domene.

Domena EIM

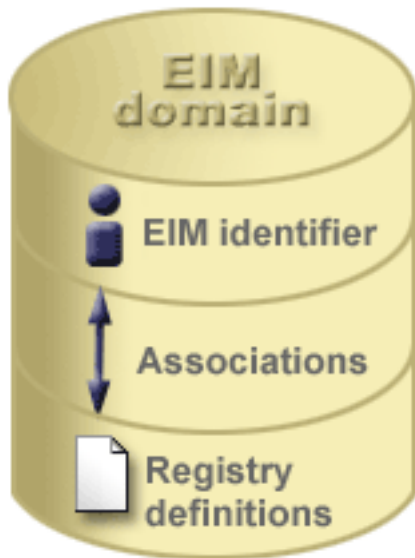
Domena EIM je imenik na strežniku LDAP (Lightweight Directory Access Protocol), ki vsebuje podatke EIM za podjetje. Domena EIM je zbirka vseh identifikatorjev EIM, povezav EIM in uporabniških registrov, ki so definirani v domeni. Sistemi (odjemalci EIM) sodelujejo v domeni z uporabo podatkov doemen za operacije iskanja EIM.

Domena EIM se razlikuje od uporabniškega registra. Uporabniški register določa niz identitet uporabnikov, ki jih pozna in jim zaupa določen primerek operacijskega sistema ali aplikacije. Register uporabnikov vsebuje tudi informacije, potrebne za overjanje uporabnika identitete. POleg tega register uporabnikov pogosto vsebuje ostale attribute, kot so uporabniške nastavitve, sistemska pooblastila ali osebne informacije za to identiteto.

V primerjavi s tem se domena EIM *nanaša* na identitete uporabnikov, ki so definirani v registrih uporabnikov. Domena EIM vsebuje informacije o *razmerju* med identitetami v različnih uporabniških registrih (uporabniško ime, tip registra in primerek registra) in dejanskimi ljudmi ali entitetami, ki jih te identitete predstavljajo. Ker EIM sledi samo informacijam o razmerjih, ni mogoče sinhronizirati uporabniških registrov in EIM.

Na sliki 2 so prikazani podatki, shranjeni znotraj domene EIM. Ti podatki zajemajo identifikatorje EIM, definicije registrov EIM in povezave EIM. Podatki EIM določajo razmerje med identitetami uporabnikov in ljudmi ali entitetami, ki jih te identitete predstavljajo v podjetju.

Slika 2: Domena EIM in podatki, ki so shranjeni znotraj domene



Podatki EIM vključuje naslednje:

- **Identifikatorje EIM.** Vsak identifikator EIM, ki ga izdelate, predstavlja osebo ali entiteto (na primer strežnik za tiskanje ali datotečni strežnik) znotraj podjetja. Za podrobnejše informacije preglejte temo Identifikator EIM.
- **Definicije registra EIM.** Vsaka definicija registra, ki jo izdelate, predstavlja dejanski register uporabnikov (in informacije o identiteti uporabnika, ki jih vsebuje), ki je v sistemu znotraj podjetja. Ko izdelate določen register uporabnikov v EIM, lahko ta register uporabnikov sodeluje v domeni EIM. Za podrobnejše informacije preglejte temo definicije registra EIM.
- **Povezave EIM.** Vsaka povezava EIM, ki jo izdelate, predstavlja razmerje med identifikatorjem EIM in povezano identiteto znotraj podjetja. Povezave izdelate za identitete v registrih uporabnikov, ki sodelujejo v domeni EIM. Povezave nudijo informacije, ki povezujejo identifikator EIM z določeno identiteto uporabnika v določenem registru uporabnikov. Zaradi tega morajo biti povezave definirane tako, da odjemalci EIM lahko uporabljajo API-je EIM za uspešno izvajanje operacij iskanja EIM. Te operacije iskanja EIM preiščejo domeno EIM za definirane povezave med identifikatorji EIM in identitetami uporabnikov v prepoznanih registrih uporabnikov. Za podrobnejše informacije preglejte Operacije iskanja EIM.

Ko izdelate identifikatorje EIM, definicije registrov in povezave, lahko EIM začnete uporabljati za preprostejše organiziranje in delanje z identitetami uporabnikov znotraj podjetja.

Identifikator EIM

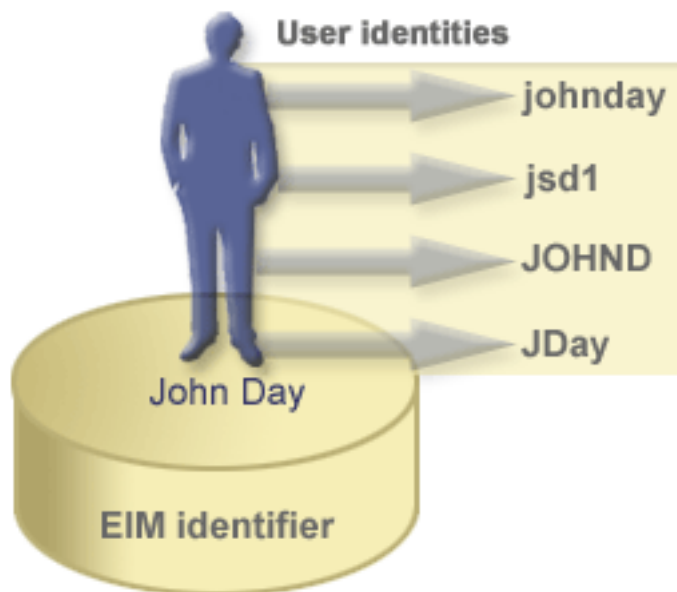
Identifikator EIM predstavlja osebo ali inteteto v podjetju. Običajno omrežje je sestavljeno iz različnih platform strojne opreme in aplikacij ter njihovih povezanih uporabniških registrov. Večina platform in veliko aplikacij uporablja uporabniške registre, ki so specifični za platformo ali aplikacijo. Ti uporabniški registri vsebujejo vse informacije o identifikaciji uporabnika za uporabnike, ki delajo s temi strežniki ali aplikacijami.

Če izdelate identifikator EIM in ga povežete z različnimi identiteami uporabnikov za osebo ali entiteto, je lažje izdelati različne večsledne aplikacije, na primer okolje za eno prijavo. Če izdelate identifikator EIM in povezave, je nato tudi lažje izdelati in uporabiti orodja, ki poenostavijo upravljanje, vključeno pri upravljanju posamezne identitete uporabnika, ki jo ima oseba ali entiteta znotraj podjetja.

Identifikator Elm, ki predstavlja osebo

Na sliki 3 je prikazan zgled identifikatorja EIM, ki predstavlja osebo z imenom *John Day* in njegovimi različnimi identitetami v podjetju. V tem primeru ima oseba *John Day* štiri uporabniške identitete v štirih različnih uporabniških registrih: johnday, jsd1, JOHND in JDay.

Slika 3: Razmerje med identifikatorjem EIM za *John Daya* in njegove različne uporabniške identitete

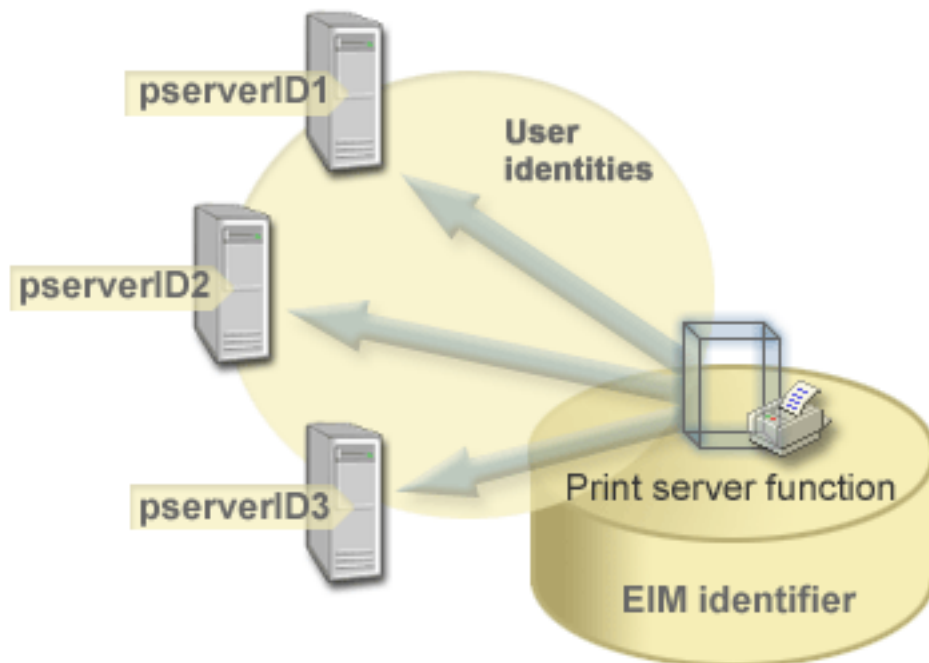


V EIM lahko izdelate povezave, ki definirajo razmerje med identifikatorjem osebe John Day in vsako od različnih uporabniških identitet za *John Daya*. Če izdelate te povezave in definirate ta razmerja, lahko vi in ostali napišete aplikacije, ki uporabljajo API-je EIM za iskanje potrebne, vendar neznane, identitete uporabnika na temelju znane identitete uporabnika.

Identifikator EIM, ki predstavlja entiteto

POleg uporabnikov, lahko identifikatorji EIM predstavljajo entitete znotraj podjetja, kot prikazuje slika 4. Na primer, pogosto se funkcija strežnika za tiskanje izvaja v več sistemih. Na sliki 4 se funkcija strežnika za tiskanje izvaja na treh različnih sistemih pod tremi različnimi identitetami uporabnikov, ki so pserverID1, pserverID2 in pserverID3.

Slika 4: Razmerje med identifikatorjem EIM, ki predstavlja funkcijo strežnika za tiskanje in različnimi identitetami uporabnikov za to funkcijo



Z EIM lahko izdelate en identifikator, ki predstavlja funkcijo strežnika za tiskanje znotraj celotnega podjetja. V tem zgledu identifikator EIM funkcija strežnika za tiskanje predstavlja dejansko funkcijo strežnika za tiskanje v podjetju. Z izdelanimi povezavami so definirana razmerja med identifikatorjem EIM (funkcija strežnika za tiskanje) in vsako od identitet uporabnika za to funkcijo (pserverID1, pserverID2 in pserverID3). Te povezave omogočajo razvijalcem aplikacij, da uporabijo operacije iskanja EIM za iskanje določene funkcije strežnika za tiskanje. Ponudniki aplikacij lahko nato napišejo porazdeljene aplikacije, s katerimi je možno lažje upravljanje funkcije strežnika za tiskanje v podjetju.

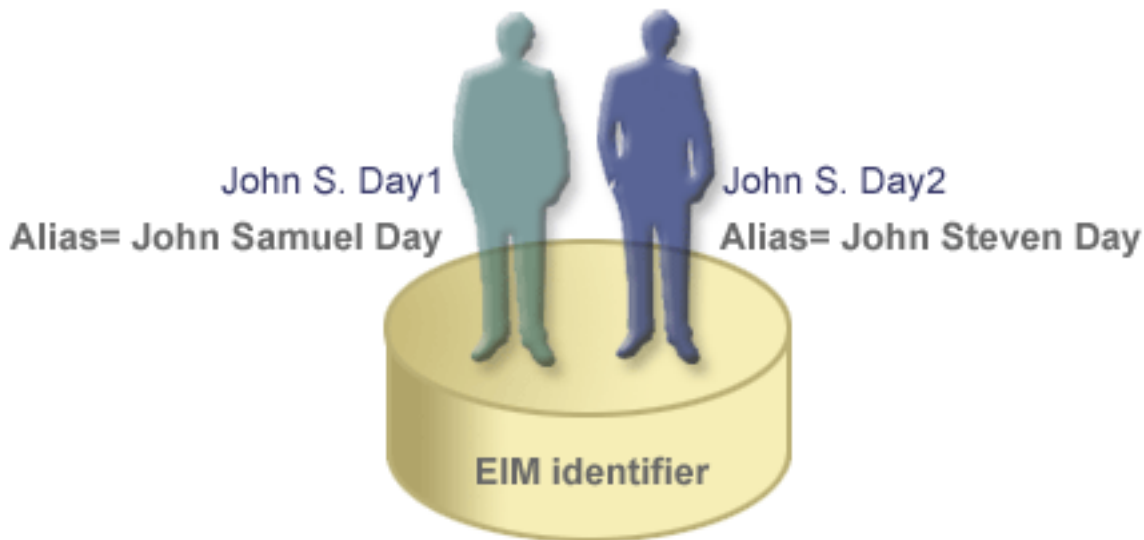
Identifikatorji EIM in dodeljevanje vzdevkov

Vzdevke lahko izdelate tudi za identifikatorje EIM. S pomočjo vzdevkov lahko lažje najdete določen identifikator EIM pri izvajanju operacij iskanja EIM. Tako so na primer vzdevki uporabni v primerih, ko se uradno ime nekoga razlikuje od imena, ki ga uporablja v zasebnem življenju.

Imena identifikatorjev EIM morajo biti unikatni znotraj domene EIM. Vzdevke lahko uporabite v primerih, ko je težko uporabiti unikatna imena identifikatorjev. Na primer, različni posamezniki v podjetju imajo lahko isto ime, kar lahko povzroči zmešnjavo, če uporabljate prava imena za identifikatorje EIM.

Na sliki 5 je prikazan zgled, v katerem ima podjetje dva uporabnika z imenom *John S. Day*. Skrbnik EIM izdelava dva različna identifikatorja EIM, da ju lahko loči: *John S. Day1* in *John S. Day2*. Iz tega poimenovanja ni očitno, kateri od *John S. Day*-ev ima katerega od identifikatorjev.

Slika 5: Vzdevka za dva identifikatorja EIM, ki temeljita na skupnem pravem imenu *John S. Day*



Z uporabo vzdevkov lahko skrbnik EIM poda dodatne informacije o posamezniku za posamezni identifikator EIM. Te informacije je mogoče uporabiti tudi v operaciji iskanja EIM za razločevanje med uporabniki, ki jih predstavlja identifikator. Tako je lahko na primer vzdevek za John S. Day1 John Samuel Day in za John S. Day2 je lahko vzdevek John Steven Day.

Vsak identifikator EIM ima lahko več vzdevkov za določanje, katerega *John S. Day*-a identifikator EIM predstavlja. Skrbnik EIM lahko doda še en vzdevek vsakemu identifikatorju EIM za oba posameznika, da ju lahko še dodatno razlikuje. Na primer, dodatni vzdevki lahko vsebujejo številko zaposlenega, številko oddelka, delovno mesto ali druge atribute.

Definicije registrov EIM

Definicija registra EIM predstavlja dejanski uporabniški register v sistemu znotraj podjetja. Uporabniški register deluje podobno kot imenik in vsebuje seznam veljavnih uporabniških identitet za določen sistem ali aplikacijo. Osnovni uporabniški imenik vsebuje uporabniške identitete in njihova gesla. Zgled uporabniškega registra je register z/OS Security Server Resource Access Control Facility (RACF^(R)). Uporabniški registri pa lahko vsebujejo tudi druge informacije. Imenik LDAP (Lightweight Directory Access Protocol) na primer vsebuje povezovalna razločevalna imena, gesla in krmiljenje dostopa do podatkov, ki so shranjeni v imeniku LDAP. Drug zgled za splošen uporabniški register je razdeljevalni center ključev (KDC) Kerberos in register uporabniških profilov OS/400.

Definicije registrov EIM nudijo informacije o teh uporabniških registrih v podjetju. Skrbnik definira te registre za EIM tako, da poda naslednje informacije:

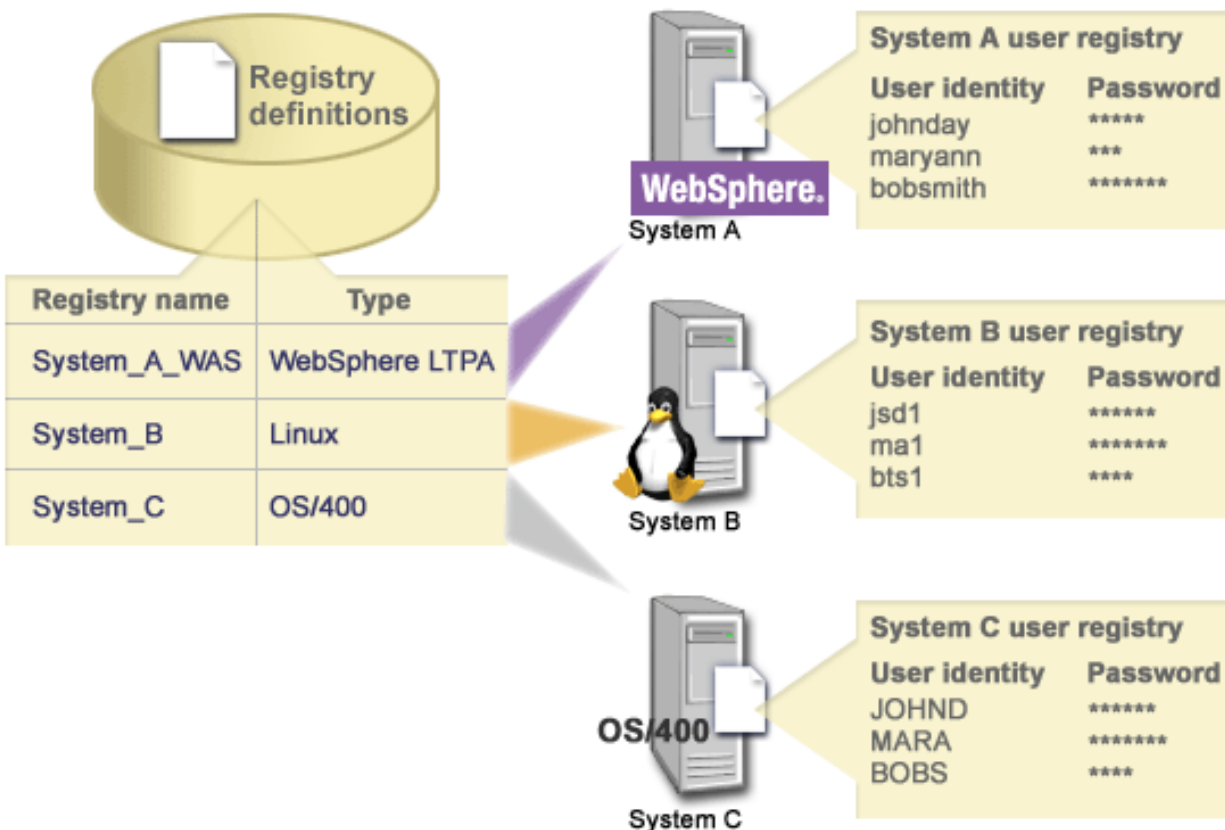
- Unikatno in poljubno ime registra EIM
- Tip uporabniškega registra

Vsaka definicija registra predstavlja specifičen primer uporabniškega registra. Zato izberite za definicijo registra EIM ime, ki vam bo pomagalo določiti posamezne primere uporabniških registrov. Za sistemski uporabniški register lahko na primer izberete ime gostitelja TCP/IP, za aplikacijski uporabniški register pa ime gostitelja, ki ga združite z imenom aplikacije. Za izdelavo unikatnih imen definicij registrov EIM lahko uporabite katerokoli kombinacijo alfanumeričnih znakov, mešanih črk in presledkov.

Na 6. sliki je izdelal skrbnik definicije registrov EIM za uporabniške registre, ki predstavljajo sistem A, sistem B in sistem C. Sistem A na primer vsebuje uporabniški register za LTPA (WebSphere Lightweight Third-Party Authentication). Ime definicije registra, ki ga uporabi skrbnik, pomaga določiti specifičen primer tipa uporabniškega registra. Za številne tipe uporabniških registrov na primer zadostuje naslov IP ali ime

gostitelja. V tem zgledu je skrbnik določil specifičen primer uporabniškega registra s pomočjo imena definicije registra System_A_WAS. Poleg imena poda skrbnik tudi tip registra kot WebSphere LTPA.

6. slika: Definicije registrov EIM za tri uporabniške registre v podjetju



Definirate lahko tudi uporabniške registre, ki obstajajo znotraj drugih uporabniških registrov. Register z/OS Security Server (RACF) lahko na primer vsebuje specifične uporabniške registre, ki so podniz uporabnikov znotraj celotnega uporabniškega registra RACF. Natančnejši zglede za to delovanje preberite v temi Definicije sistemskih in aplikacijskih registrov.

Definicije registrov EIM in dodeljevanje vzdevkov

Za definicije registrov EIM lahko izdelate tudi vzdevke. Uporabite lahko vnaprej definirane tipe vzdevkov ali definirate lastne tipe. Vnaprej definirani tipi vzdevkov vključujejo naslednje:

- Ime gostitelja imenskega sistema domen (DNS)
- Področje Kerberos
- Razločevalno ime (DN) izdajatelja
- Korensko razločevalno ime (DN)
- Naslov TCP/IP
- Ime gostitelja DNS LDAP

Ta podpora za vzdevke omogoča programerjem pisanje aplikacij brez vnaprejšnjega poznavanja poljubnega imena registra EIM, ki ga izbere skrbnik, ki razvije aplikacijo. Skrbnik za EIM lahko najde ime vzdevka, ki ga

uporablja aplikacija, v dokumentaciji aplikacije. S pomočjo teh informacij lahko dodeli skrbnik za EIM to ime vzdevka definiciji registra EIM, ki predstavlja dejanski uporabniški register, ki ga za aplikacijo predvidi skrbnik.

Ko doda skrbnik vzdevke za definicijo registra EIM, lahko izvede aplikacija iskanje vzdevkov in poišče ime registra EIM pri inicializaciji. Iskanje vzdevkov omogoča aplikaciji, da določi ime ali imena registrov EIM, ki bodo uporabljeni kot vhodni podatki za API-je, ki izvajajo iskalne operacije EIM.

Definicije sistemskih in aplikacijskih registrov

Nekatere aplikacije uporabljajo znotraj enega primerka uporabniškega registra podniz uporabniških identitet. EIM omogoča, da oblikujejo skrbniki ta model s pomočjo dveh vrst definicij registrov EIM: sistemskih in aplikacijskih.

Definicija sistema registra predstavlja ločen register znotraj delovne postaje ali strežnika. Definicijo sistema registra lahko izdelate, če ima register v podjetju eno izmed naslednjih značilnosti:

- Register je na voljo kot del operacijskega sistema kot je AIX^(R), OS/400^(R), ali izdelka za upravljanje zaščite z/OS Security Server Resource Access Control Facility (RACF^(R)).
- Register vsebuje uporabniške identitete, ki so unikatne za določeno aplikacijo kot je Lotus Notes^(R).
- Register vsebuje porazdeljene uporabniške identitete kot so principal Kerberos ali razločevalna imena LDAP (Lightweight Directory Access Protocol).

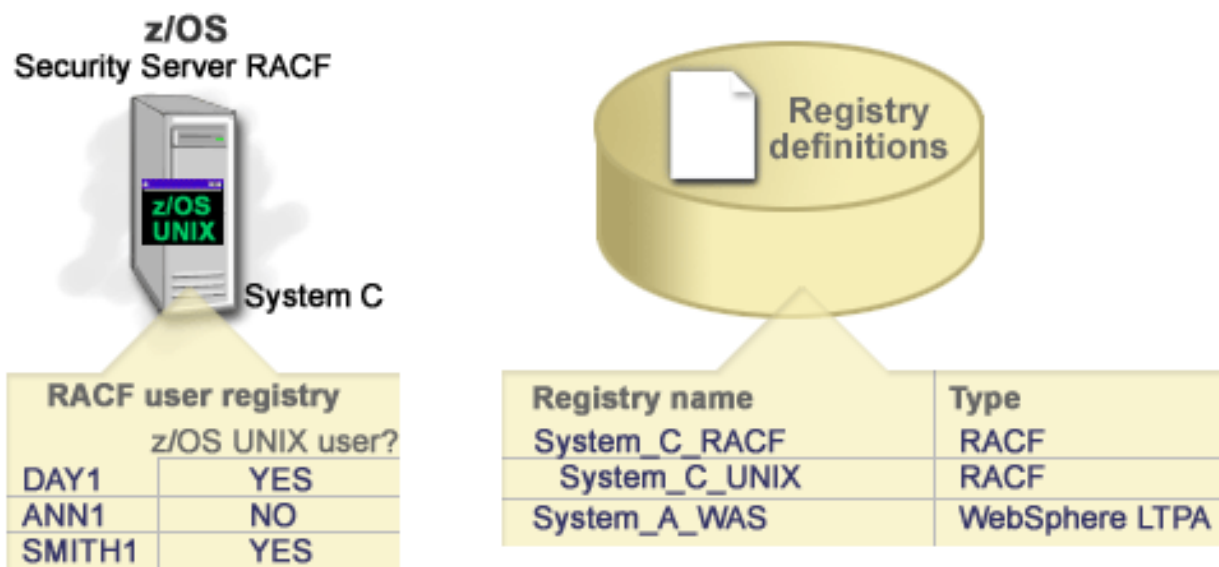
Definicija aplikacijskega registra predstavlja podniz uporabniških identitet, ki so definirane v sistemskem registru. Te uporabniške identitete souporabljajo skupen niz lastnosti ali značilnosti, ki jim omogočajo uporabo določene aplikacije ali niza aplikacij. Definicijo aplikacijskega registra lahko izdelate, če ima uporabniška identiteta naslednje značilnosti:

- Uporabniške identitete za aplikacijo ali niz aplikacij niso shranjene v uporabniškem registru, specifičnem za aplikacijo ali niz aplikacij.
- Uporabniške identitete za aplikacijo ali niz aplikacij so shranjene v sistemskem registru, ki vsebuje uporabniške identitete za druge aplikacije.

Iskalne operacije EIM se izvajajo pravilno ne glede na to, ali definira skrbnik za EIM register kot sistemski ali aplikacijski. Vendar pa ločene definicije registrov omogočajo upravljanje podatkov preslikav na osnovi aplikacij. Odgovornost za upravljanje preslikav, specifičnih za aplikacije, je mogoče poveriti skrbniku za določen register.

7. slika na primer kaže, kako je izdelal skrbnik za EIM definicijo sistema registra, ki predstavlja register z/OS Security Server RACF. Skrbnik je izdelal tudi definicijo aplikacijskega registra, ki predstavlja uporabniške identitete znotraj registra RACF, ki uporablja z/OS UNIX System Services (z/OS UNIX). Sistem C vsebuje uporabniški register RACF, ki vsebuje informacije za tri uporabniške identitete: DAY1, ANN1 in SMITH1. Dve od teh uporabniških identitet (DAY1 in SMITH1) dostopata do z/OS UNIX v sistemu C. Ti uporabniški identiteti sta dejansko uporabnika RACF z unikatnimi lastnostmi, ki ju določajo kot uporabnika z/OS UNIX. Znotraj definicij registrov EIM je definiral skrbnik za EIM System_C_RACF, ki predstavlja celoten uporabniški register RACF. Skrbnik je definiral tudi System_C_UNIX, ki predstavlja uporabniške identitete z lastnostmi z/OS UNIX.

7. slika: Definicije registrov EIM za uporabniški register RACF in za uporabnike z/OS UNIX.



Povezave EIM

Povezava EIM je povezava med identifikatorjem EIM, ki predstavlja določeno osebo in identiteto posameznega uporabnika v uporabniškem registru, ki prav tako predstavlja to osebo. Če izdelate povezave med identifikatorjem EIM in vsemi identitetami osebe ali entitete, podate eno popolno razumevanje, kako ta oseba ali entitea uporablja sredstva v podjetju. EIM nudi API-je, s katerimi lahko aplikacije najdejo identiteto neznanega uporabnika v določenem (ciljnem) uporabniškem registru, tako da podajo identiteto znanega uporabnika v drugem (izvornem) uporabniškem registru. Ta postopek se imenuje *preslikava identitete*.

Preden lahko izdelate povezavo, morate najprej izdelati ustrezeni identifikator EIM in ustrezno definicijo registra EIM za uporabniški register, ki vsebuje povezano identiteto uporabnika. Povezava določa razmerje med identifikatorjem EIM in identiteto uporabnika z uporabo naslednjih informacij:

- Ime identifikatorja EIM
- Ime identitete uporabnika
- Ime definicije registra EIM
- Tip povezave

Skrbnik lahko izdelata različne tipe povezav med identifikatorjem EIM in identiteto uporabnika na temelju uporabe identitete uporabnika. Uporabniške identitete lahko uporabite za overjanje, pooblašcanje ali oboje.

Overjanje je postopek, da ima entiteta ali oseba, ki podaja uporabniško identiteto, pooblastila za to identiteto. Preverjanje je pogosto izvedeno tako, da mora uporabniška identiteta podati skrivne ali zasebne informacije, povezane z uporabniško identiteto, kot je geslo.

Pooblašcanje je postopek zagotavljanja, da lahko ustrezno preverjeni uporabnik izvede samo funkcije ali dostopa do sredstev, za katera ima pooblastila. V preteklosti so bile skoraj vse aplikacije prisiljene k uporabi uporabniških identitet v enem uporabniškem registru za overjanje in za pooblašcanje. S pomočjo operacij iskanja EIM lahko aplikacije zdaj uporabljajo uporabniške identitete v enem uporabniškem registru za overjanje in povezane uporabniške identitete v drugem uporabniškem registru za pooblašcanje.

V EIM lahko skrbnik definira tri tipe povezav med identifikatorjem EIM in uporabniško identiteto. Ti tipi so izvorne, ciljne in upravne povezave.

Izvorna povezava

Če identiteto uporabnika uporabite za *overjanje*, mora imeti ta identiteta uporabnika izvorno povezavo z identifikatorjem EIM. Izvorna povezava omogoča, da je identiteta uporabnika lahko uporabljena kot izvor v operaciji iskanja EIM za iskanje druge identitete uporabnika, ki je povezana z istim identifikatorjem EIM. Če kot ciljno identiteto v operaciji iskanja EIM uporabite identiteto uporabnika s samo eno izvorno povezavo, ni vrnjena nobena povezana identiteta uporabnika.

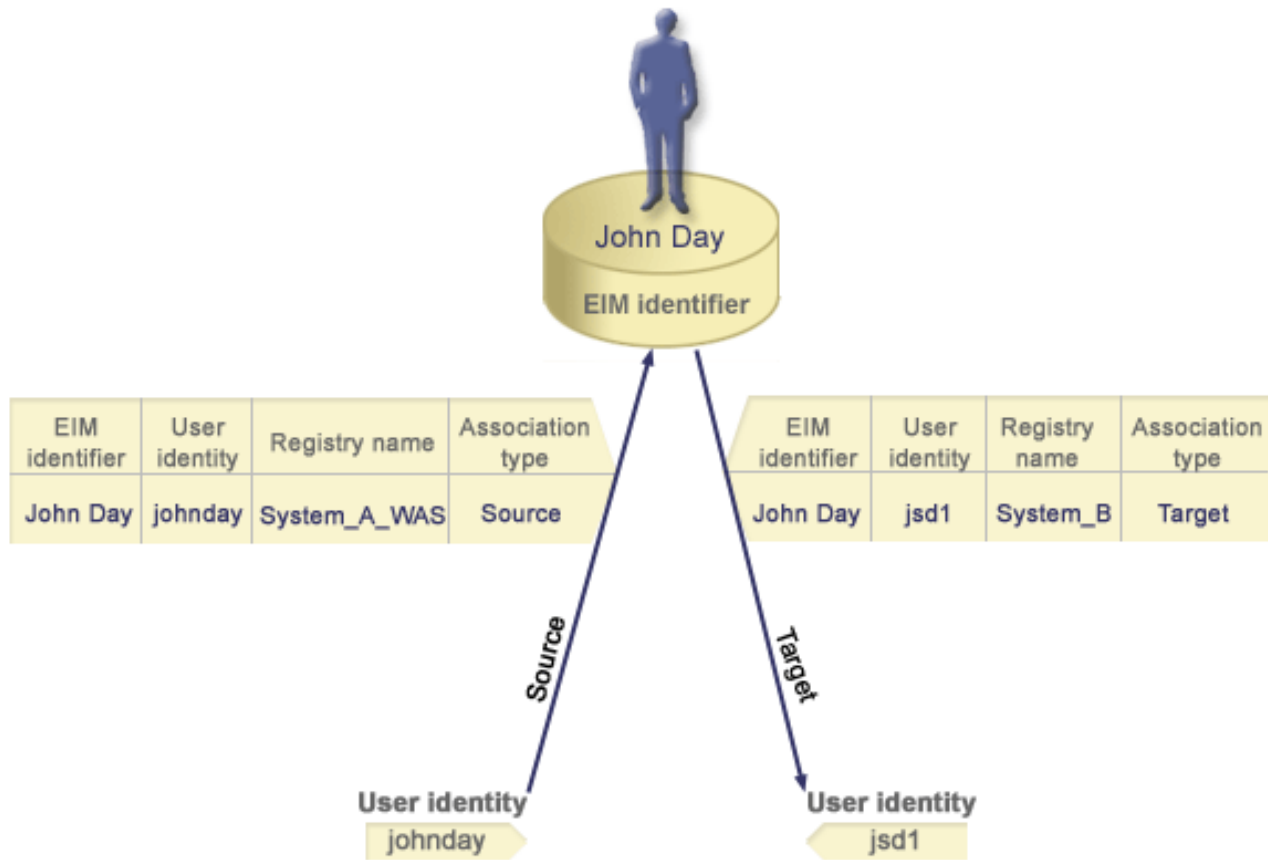
Ciljna povezava

Če identiteto uporabnika uporabite za *pooblašcanje* in ne za *overjanje*, mora imeti identiteta uporabnika ciljno povezavo z identifikatorjem EIM. Ciljna povezava omogoča identiteti uporabnika, da je vrnjena kot rezultat operacije iskanja EIM. Če kot izvorno identiteto v operaciji iskanja EIM uporabite identiteto uporabnika s samo eno ciljno povezavo, ni vrnjena nobena povezana identiteta uporabnika.

Za identiteto enega uporabnika boste morda morali izdelati ciljno in izvorno povezavo. To je zahtevano, če posameznik uporablja en sistem kot odjemalca in strežnik ali za posameznike, ki delujejo kot skrbniki. Na primer, uporabnik se ponavadi prijavi na platformo Windows in zaganja aplikacije, ki dostopajo do strežnika AIX. Zaradi službenih odgovornosti uporabnika, se mora občasno prijaviti neposredno na strežnik AIX. V tem primeru morate izdelati izvorne in ciljne povezave med identiteto uporabnika AIX in identifikatorjem EIM osebe. Identitete uporabnikov, ki predstavljajo končne uporabnike, ponavadi potrebujejo samo ciljno povezavo.

Na sliki 6 je prikazan zgled izvorne in ciljne povezave. V tem zgledu je skrbnik izdelal dve povezavi za identifikator EIM John Day in definiral razmerje med tem identifikatorjem in dvema povezanima uporabniškima identitetama. Skrbnik je izdelal izvorno povezavo za johnday, identiteto uporabnika LTPA (Lightweight Third-Party Authentication) WebSphere v uporabniškem registru System_A_WAS. Skrbnik je izdelal tudi ciljno povezavo za jsd1, uporabniški profil OS/400 v uporabniškem registru sistema B. S pomočjo teh povezav lahko aplikacije pridobijo neznano identiteto uporabnika (cilj jsd1) na temelju znane identitete uporabnika (johnday) kot del operacije iskanja EIM.

Slika 6: Ciljna in izvorna povezava EIM za identifikator EIM John Day



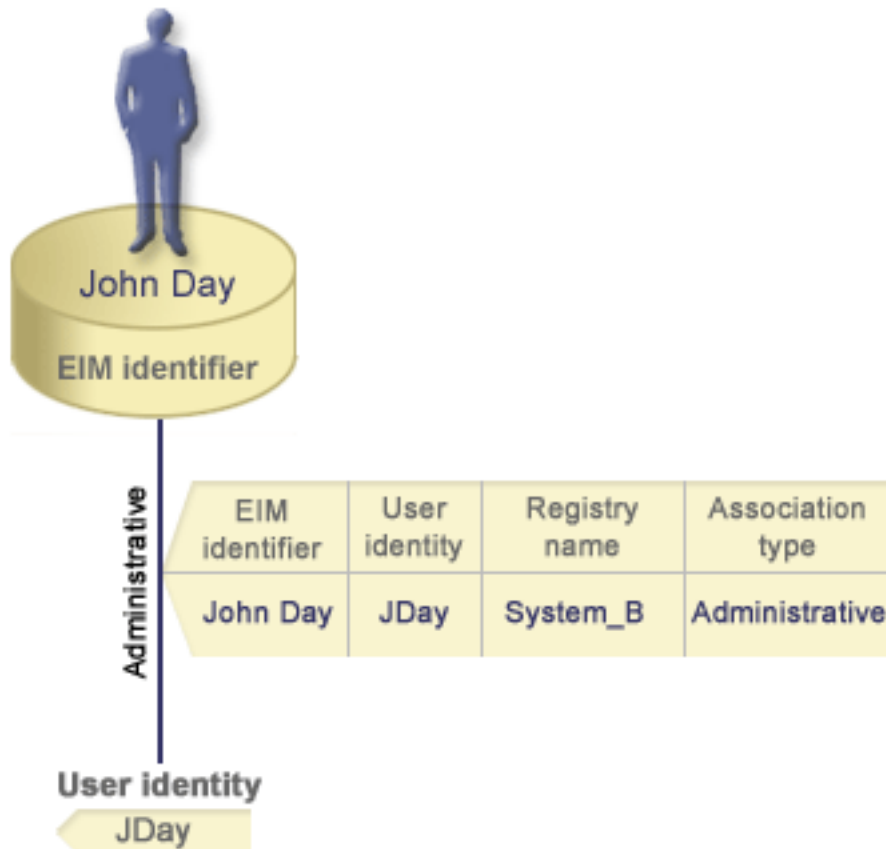
Upravna povezava

Upravna povezava za identifikator EIM se ponavadi uporablja za prikaz, da je oseba ali entiteta, predstavljena z identifikatorjem EIM, lastnik identitete uporabnika, ki zahteva posebno obravnavanje za podani sistem. Ta tip povezave lahko uporabite za zelo občutljive uporabniške registre.

Zaradi tega, kaj upravna povezava predstavlja, operacija iskanja EIM, ki podaja izvorno identiteto uporabnika z upravno povezavo, ne vrne nobenega rezultata. Podobno identiteta uporabnika z upravno povezavo nikoli ni vrnjena kot rezultat operacije iskanja EIM.

Na sliki 7 je prikazan zgled upravne povezave. V tem zgledu ima John Day eno identiteto uporabnika v sistemu A in drugo identiteto uporabnika v sistemu B, ki je zelo zaščiten sistem. Skrbnik sistema želi zagotoviti, da se uporabniki prijavijo v sistem B z uporabo samo lokalnega uporabniškega registra tega sistema. Skrbnik ne želi, da bi aplikacija omogočila prijavo za John Day v sistem z uporabo nekega tujega načina za overjanje. Z uporabo upravne povezave za identiteto uporabnika JDay v sistemu B, lahko skrbnik EIM vidi, da je John Day lastnik šifre v sistemu B, vendar EIM ne vrne informacije o identiteti JDay v operacijah iskanja EIM. Tudi če so v sistemu aplikacije, ki uporabljajo operacije iskanja EIM, ne morejo najti identitet uporabnika, ki imajo upravne povezave.

Slika 7: Upravna povezava EIM za identifikator EIM John Day



Operacije iskanja EIM

Operacija iskanja EIM je postopek, s katerim aplikacija ali operacijski sistem poišče neznano povezano identiteto uporabnika v določenem ciljnim registru, tako da poda nekatere znane ali overjene informacije. Aplikacije, ki uporabljajo API-je EIM izvedejo te operacije iskanja EIM za informacije samo, če so te informacije shranjene v domeni EIM. Aplikacija lahko izvede eno od dveh tipov operacij iskanja EIM na temelju tipa informacij, ki jih aplikacija podaja kot izvor operacije iskanja EIM: identiteta uporabnika ali identifikator EIM.

Če aplikacija poda *identiteto uporabnika kot izvor*, mora aplikacija podati tudi ime definicije registra EIM za izvorno identiteto uporabnika in ime definicije registra EIM, ki je cilj operacije iskanja EIM. Če želite identiteto uporabnika uporabiti kot izvor v operaciji iskanja EIM, mora imeti definirano povezavo.

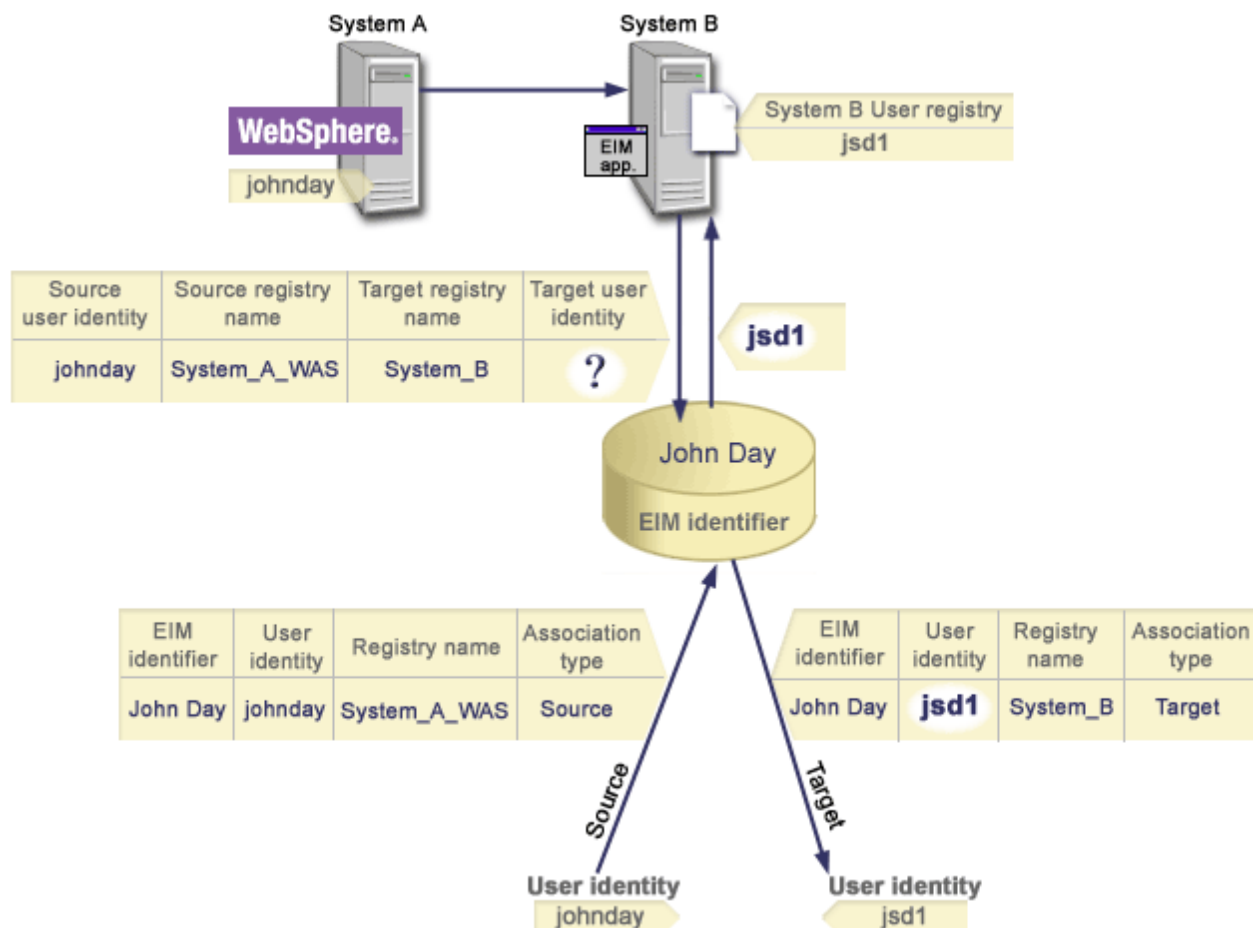
Če aplikacija poda *identifikator EIM kot izvor* operacije iskanja EIM, mora aplikacija podati tudi ime definicije registra EIM, ki je cilj operacije iskanja EIM. Če želite, da bo identiteta uporabnika vrnjena kot cilj kateregakoli tipa operacije iskanja EIM, mora imeti identiteta uporabnika definirano ciljno povezavo.

Podane informacije so posredovane krmilniku domene EIM, kjer so vse informacije o EIM shranjene in operacija iskanja EIM poišče izvorno povezavo, ki se ujema s podanimi informacijami. Na temelju identifikatorja EIM (podano API-ju ali določeno iz informacij izvorne povezave) operacija iskanja EIM nato poišče ciljno povezavo za identifikator, ki se ujema s ciljnim imenom definicije registra EIM.

Na sliki 10 se identiteta uporabnika johnday prijavi na strežnik aplikacij Websphere z uporabo LPTA (Lightweight Third-Party Authentication) v sistemu A. Strežnik aplikacij Websphere v sistemu A nato pokliče izvorni program v sistemu B za dostop do podatkov v sistemu B. Izvirni program uporabi API EIM, da izvede operacijo iskanja EIM za identiteto uporabnika v sistemu A kot izvor operacije. Aplikacija poda naslednje informacije za izvedbo operacije: johnday kot izvorno identiteto uporabnika, System_A_WAS kot ime

definicije izvornega registra EIM in System_B kot ime definicije ciljnega registra EIM. Te izvorne informacije so posredovane krmilniku domene EIM in operacija iskanja EIM poišče izvorno povezavo, ki se ujema z informacijami. Z uporabo imena identifikatorja EIM operacija iskanja EIM poišče ciljno povezavo za identifikator John Day, ki se ujema z imenom definicije ciljnega registra EIM za System_B. Ko je najdena ujemajoča ciljna povezava, operacija iskanja EIM vrne identiteto uporabnika jsd1 aplikaciji.

Slika 10: Operacija iskanja EIM na temelju znane identitete uporabnika johnday



Pooblastila EIM

Pooblastila EIM omogočajo uporabniku, da izvaja določene upravne naloge ali operacije iskanja EIM. Pooblastila lahko drugim uporabnikom dodeljujejo in preklicujejo samo uporabniki s pooblastili skrbnika EIM. Pooblastila EIM so dodeljena samo identitetam uporabnikov, ki so poznane krmilniku domen EIM.

Spodaj so kratki opisi funkcij, ki jih lahko izvedejo posamezne pooblastitvene skupine:

- **Skrbnik LDAP (Lightweight Directory Access Protocol).** To pooblastilo uporabniku omogoča konfiguriranje nove domene EIM. Uporabnik s tem pooblastilom lahko izvede naslednje funkcije:
 - Izdelava domene
 - Brisanje domene
 - Izdelava in odstranjevanje identifikatorjev EIM
 - Izdelava in odstranjevanje definicije registra EIM
 - Izdelava in odstranjevanje izvorne, ciljne in upravne povezave

- Izvajanje operacij iskanja EIM
- Iskanje povezav, identifikatorjev EIM in definicij registra EIM
- Dodajanje, odstranjevanje in prikaz seznama informacij o pooblastilih EIM
- **Skrbnik EIM.** S tem pooblastilom lahko uporabnik upravlja vse podatke EIM znotraj te domene EIM. Uporabnik s tem pooblastilom lahko izvede naslednje funkcije:
 - Brisanje domene
 - Izdelava in odstranjevanje identifikatorjev EIM
 - Izdelava in odstranjevanje definicije registra EIM
 - Izdelava in odstranjevanje izvorne, ciljne in upravne povezave
 - Izvajanje operacij iskanja EIM
 - Iskanje povezav, identifikatorjev EIM in definicij registra EIM
 - Dodajanje, odstranjevanje in prikaz seznama informacij o pooblastilih EIM
- **Skrbnik identifikatorjev EIM.** S tem pooblastilom lahko uporabnik doda in spremeni identifikatorje EIM in upravlja izvorne in upravne povezave. Uporabnik s tem pooblastilom lahko izvede naslednje funkcije:
 - Izdelava identifikatorja EIM
 - Dodajanje in odstranjevanje izvornih povezav
 - Dodajanje in odstranjevanje upravnih povezav
 - Izvajanje operacij iskanja EIM
 - Iskanje povezav, identifikatorjev EIM in definicij registra EIM
- **Iskanje preslikav EIM.** S tem pooblastilom lahko uporabnik izvede operacije iskanja EIM. Uporabnik s tem pooblastilom lahko izvede naslednje funkcije:
 - Izvajanje operacij iskanja EIM
 - Iskanje povezav, identifikatorjev EIM in definicij registra EIM
- **Skrbnik registrov EIM.** S tem pooblastilom lahko uporabnik upravlja vse definicije registra EIM. Uporabnik s tem pooblastilom lahko izvede naslednje funkcije:
 - Dodajanje in odstranjevanje ciljnih povezav
 - Izvajanje operacij iskanja EIM
 - Iskanje povezav, identifikatorjev EIM in definicij registra EIM
- **Skrbnik X registra EIM** S tem pooblastilom lahko uporabnik upravlja določeno definicijo registra EIM. S tem pooblastilom lahko uporabnik izvede naslednje funkcije:
 - Dodajanje in odstranjevanje ciljnih povezav za definicijo registra EIM
 - Izvajanje operacij iskanja EIM
 - Iskanje povezav, identifikatorjev EIM in definicij registra EIM

Vse naslednje tabele so urejene po opravilu EIM, ki ga izvede API. Vsaka tabela prikaže vsak API EIM, različna pooblastila EIM in dostop, ki ga ima vsaka od teh funkcij do določenih funkcij EIM.

Tabela 1: Delo z domenami

API EIM	Skrbnik LDAP	Skrbnik EIM	Skrbnik identifikatorjev EIM	Iskanje preslikav EIM	Skrbnik registrov EIM	Skrbnik X registrov EIM
eimChangeDomain	X	X	-	-	-	-
eimCreateDomain	X	-	-	-	-	-
eimDeleteDomain	X	X	-	-	-	-
eimListDomains	X	X	-	-	-	-

Tabela 2: Delo z identifikatorji

API EIM	Skrbnik LDAP	Skrbnik EIM	Skrbnik identifikatorjev EIM	Iskanje preslikav EIM	Skrbnik registrov EIM	Skrbnik X registrov EIM
eimAddIdentifier	X	X	X	-	-	-
eimChangeIdentifier	X	X	X	-	-	-
eimListIdentifiers	X	X	X	X	X	X
eimRemoveIdentifier	X	X	-	-	-	-

Tabela 3: Delo z registri

API EIM	Skrbnik LDAP	Skrbnik EIM	Skrbnik identifikatorjev EIM	Iskanje preslikav EIM	Skrbnik registrov EIM	Skrbnik X registrov EIM
eimAddApplicationRegistry	X	X	-	-	-	-
eimAddSystemRegistry	X	X	-	-	-	-
eimChangeRegistry	X	X	-	-	X	X
eimChangeRegistryUser	X	X	-	-	X	X
eimChgRegistryAlias	X	X	-	-	X	X
eimGetRegistryFromAlias	X	X	X	X	X	X
eimListRegistries	X	X	X	X	X	X
eimListRegistryAliases	X	X	X	X	X	X
eimListRegistryUsers	X	X	X	X	X	X
eimRemoveRegistry	X	X	-	-	-	-

Tabela 4: Delo s povezavami

Za API-ja `eimAddAssociation()` in `eimRemoveAssociation()` so na voljo štirje parametri, ki določajo tip povezave, ki se dodaja ali briše. Pooblastila za te API-je so odvisna od tipa povezave, podanega v teh parametrih. V naslednji tabeli je tip povezave vključen za vsakega od teh API-jev.

API EIM	Skrbnik LDAP	Skrbnik EIM	Skrbnik identifikatorjev EIM	Iskanje preslikav EIM	Skrbnik registrov EIM	Skrbnik X registrov EIM
eimAddAssociation (upravno)	X	X	X	-	-	-
eimAddAssociation (izvor)	X	X	X	-	-	-
eimAddAssociation (izvor in cilj)	X	X	X	-	X	X
eimAddAssociation (cilj)	X	X	-	-	X	X

API EIM	Skrbnik LDAP	Skrbnik EIM	Skrbnik identifikatorjev EIM	Iskanje preslikav EIM	Skrbnik registrov EIM	Skrbnik X registrov EIM
eimListAssociations	X	X	X	X	X	X
eimRemoveAssociation (upravno)	X	X	X	-	-	-
eimRemoveAssociation (izvor)	X	X	X	-	-	-
eimRemoveAssociation (izvor in cilj)	X	X	X	-	X	X
eimRemoveAssociation (cilj)	X	X	-	-	X	X

Tabela 5: Delo s preslikavami

API EIM	Skrbnik LDAP	Skrbnik EIM	Skrbnik identifikatorjev EIM	Iskanje preslikav EIM	Skrbnik registrov EIM	Skrbnik X registrov EIM
eimGetAssociatedIdentifier	X	X	X	X	X	X
eimGetTargetFromIdentifier	X	X	X	X	X	X
eimGetTargetFromSource	X	X	X	X	X	X

Tabela 6: Delo z dostopom

API EIM	Skrbnik LDAP	Skrbnik EIM	Skrbnik identifikatorjev EIM	Iskanje preslikav EIM	Skrbnik registrov EIM	Skrbnik X registrov EIM
eimAddAccess	X	X	-	-	-	-
eimListAccess	X	X	-	-	-	-
eimListUserAccess	X	X	-	-	-	-
eimQueryAccess	X	X	-	-	-	-
eimRemoveAccess	X	X	-	-	-	-

Koncepti LDAP za EIM

Preslikava identitete podjetja (EIM) uporablja strežnik LDAP (Lightweight Directory Access Protocol) kot krmilnik domene EIM za shranitev podatkov EIM. Razločevalna imena LDAP lahko uporabite pri konfiguriranju EIM za strežnik iSeries in kot način overjanja za krmilnik domene EIM.

Če želite uporabiti razločevalna imena LDAP pri konfiguriranju in upravljanju EIM, morate razumeti naslednje koncepte LDAP:

- Razločevalno ime LDAP
- Nadrejeno razločevalno ime LDAP

Razločevalno ime LDAP

Razločevalno ime (DN) LDAP je postavka LDAP (Lightweight Directory Access Protocol), ki določa in opisuje pooblaščenega uporabnika za strežnik LDAP. Strežnik LDAP lahko konfigurirate za shranjevanje

informacij o domeni EIM s pomočjo čarovnika za konfiguracijo EIM. Razločevalna imena LDAP lahko uporabite za dostopanje do teh podatkov EIM in njihovo pridobivanje, tako da lahko sodeluje strežnik iSeries v okolju enotne prijave.

Razločevalna imena so sestavljena iz imena same postavke in iz imen objektov (v vrstnem redu od dna proti vrhu), ki so v imeniku LDAP navedena nad njim. Zgled celotnega razločevalnega imena LDAP je lahko na primer `cn=Tine Rožanc, o=IBM, c=SL`. Vsaka postavka ima vsaj eno lastnost, ki se uporablja za poimenovanje postavke. Ta lastnost poimenovanja se imenuje relativno razločevalno ime (RDN) postavke. Postavka nad podanim RDN se imenuje njegovo nadrejeno razločevalno ime LDAP. V tem zgledu poimenuje `cn=Tine Rožanc` postavko in je torej RDN. `o=IBM, c=SL` je nadrejeni DN za `cn=Tineta Rožanca`. Če se želite poučiti o podrobnejši uporabi teh elementov v EIM, preberite temo Nadrejeno razločevalno ime LDAP.

Ker uporablja EIM za shranitev podatkov EIM strežnik LDAP, lahko uporabite razločevalna imena LDAP za overjanje za krmilnik domene EIM. Razločevalna imena LDAP lahko uporabite tudi pri konfiguriranju EIM za strežnik iSeries. Razločevalna imena LDAP lahko na primer uporabite v naslednjih primerih:

- Če konfigurirate strežnik LDAP tako, da deluje kot krmilnik domene EIM. To naredite z izdelavo in uporabo razločevalnega imena LDAP, ki določa skrbnika LDAP za strežnik LDAP. Če strežnika LDAP niste predhodno konfigurirali, lahko to naredite pri uporabi čarovnika za konfiguracijo EIM, s katerim izdelate in povežete novo domeno.
- Če uporabite čarovnika za konfiguracijo EIM za izbiro tipa uporabniške identitete, za katero želite, da jo uporabi čarovnik pri povezavi s krmilnikom domene EIM. Razločevalno ime je eden izmed uporabniških tipov, med katerimi lahko izberete. Razločevalno ime LDAP mora predstavljati uporabnika, ki je pooblaščen za izdelavo objektov v lokalnem imenskem prostoru strežnika LDAP.
- Če uporabite čarovnika za konfiguracijo EIM za izbiro tipa uporabnika, ki bo izvajal operacije EIM v imenu funkcij operacijskega sistema. Te operacije vključujejo preslikavo iskanj in brisanje povezav pri brisanju lokalnega profila uporabnika OS/400. Razločevalno ime je eden izmed uporabniških tipov, med katerimi lahko izberete.
- Če se za izvajanje upravljanja EIM, kot je na primer upravljanje registrov in identifikatorjev in za izvajanje operacij iskanja preslikav, povežete s krmilnikom domene.

Če se želite podrobneje poučiti o razločevalnih imenih in o njihovi uporabi v LDAP, preberite temo Osnove LDAP.

Nadrejeno razločevalno ime LDAP

Nadrejeno razločevalno ime (DN) LDAP je postavka v imenskem prostoru strežnika LDAP (Lightweight Directory Access Protocol). Postavke strežnika LDAP so urejene v hierarhični strukturi, ki lahko odraža politične, geografske, organizacijske ali domenske meje. Razločevalno ime je nadrejeni DN, če je DN na najvišji ravni imenskega prostora strežnika LDAP.

Zgled celotnega razločevalnega imena LDAP je lahko na primer `cn=Tine Rožanc, o=IBM, c=SL`. Vsaka postavka ima vsaj eno lastnost, ki se uporablja za poimenovanje postavke. Ta lastnost poimenovanja se imenuje relativno razločevalno ime (RDN) postavke. Postavka nad podanim RDN se imenuje njegovo nadrejeno razločevalno ime. V tem zgledu poimenuje `cn=Tine Rožanc` postavko in je torej RDN. `o=IBM, c=SL` je nadrejeni DN za `cn=Tineta Rožanca`.

Ker uporablja EIM za shranitev podatkov EIM strežnik LDAP, lahko uporabite razločevalna imena LDAP za overjanje za krmilnik domene EIM. Razločevalna imena LDAP in nadrejena razločevalna imena LDAP lahko uporabite tudi pri konfiguriranju EIM za strežnik iSeries. Če na primer s pomočjo čarovnika za konfiguracijo EIM izdelate in povežete novo domeno, lahko podate nadrejeni DN za domeno, ki jo izdelujete. Z uporabo nadrejenega DN lahko podate, kje v lokalnem imenskem prostoru LDAP naj bodo shranjeni podatki EIM za domeno. Če nadrejenega DN ne podate, so shranjeni podatki EIM v lastni priponi imenskega prostora.

Če se želite podrobneje poučiti o razločevalnih imenih in njihovi uporabi, preberite temo Osnove LDAP.

Omogočanje enotne prijave prek EIM

EIM nudi poceni mehanizem za omogočanje enotne prijave znotraj podjetja. Izvedba EIM in Kerberos na OS/400 nudi resnično večplastno in heterogeno okolje enotne prijave. Okolje enotne prijave nudi uporabnikom, skrbnikom in razvijalcem aplikacij v podjetju naslednje prednosti:

Prednosti za uporabnike

V okolju enotne prijave se izvaja overjanje vsakič, ko poskusi uporabnik dostopiti do novega sistema, vendar uporabniku ni potrebno vnesti gesla. Uporaba EIM zmanjša potrebo za sledenje in upravljanje več uporabniških imen in gesel za dostop do drugih sistemov v omrežju. Ko je uporabnik overjen v omrežju, lahko dostopa do storitev in aplikacij v podjetju, ne da bi za te druge sisteme potreboval več gesel.

Prednosti za skrbnike

Za skrbnike poenostavi enotna prijava celotno upravljanje zaščite v podjetju. Če enotna prijava ni omogočena, lahko shranijo uporabniki in aplikacije gesla v predpomnilnik drugih sistemov, kar lahko oslabi zaščito celotnega omrežja. Skrbniki porabijo veliko časa in denarja za rešitve, ki bi zmanjšale tveganja v zaščiti. Enotna prijava zmanjša upravno obremenitev pri vodenju overjanja, vendar ohrani zaščito celotnega omrežja. Poleg tega zmanjša enotna prijava tudi upravne stroške, povezane z vnovnično nastavitvijo pozabljenih gesel.

Prednosti za razvijalce aplikacij

Za razvijalce aplikacij, ki se morajo izvajati v heterogenih omrežjih, nudi EIM infrastrukturo za razvijanje aplikacij, ki delujejo na več platformah. S pomočjo API-jev, vključenih v EIM, lahko razvijejo programerji aplikacije, ki uporabljajo najustreznejši obstoječi uporabniški register za overjanje in drug uporabniški register za pooblašcanje. Razvijalcem aplikacij ni potrebno razviti znotraj aplikacij, ki jih oblikujejo, uporabniških registrov, specifičnih za platforme, ker nudi EIM infrastrukturo za izdelavo aplikacij, ki preslikajo uporabniške identitete znotraj teh uporabniških registrov v enoten identifikator EIM. Poleg tega omogoča EIM programerjem vzdrževanje teh aplikacij brez spreminjanja povezane semantike zaščite, zaščita na ravni aplikacij pa tudi zmanjša stroške izvajanja večplastnih aplikacij za več platform.

Omogočanje enotne prijave na iSeries

Za omogočanje okolja enotne prijave uporablja IBM dve tehnologiji, ki delujeta ena z drugo: EIM in omrežna storitev overjanja, ki je IBM-ova izvedba storitve Kerberos in API-jev GSS. S konfiguracijo teh dveh tehnologij lahko omogoči skrbnik okolje enotne prijave. Operacijski sistemi Windows 2000, XP, AIX in zSeries overjajo uporabnike v omrežju s pomočjo protokola Kerberos. Kerberos vključuje uporabo na omrežju temelječega in varnega centra za razdeljevanje ključev, ki overja principale (uporabnike Kerberos) v omrežju. Uporabnik prejme iz osrednjega centra za razdeljevanje ključev dovolilnico Kerberos. Ta dovolilnica overi uporabnika za drugo storitev v omrežju. Dovolilnico je mogoče posredovati od uporabnika storitvi, ki sprejema dovolilnice. Storitve, ki sprejema dovolilnice, z njihovo pomočjo določi, kdo je uporabnik (znotraj uporabniškega registra in področja Kerberos) in ali je v resnici ta uporabnik.

Omrežna storitev overjanja omogoča sodelovanje strežnika iSeries v področju Kerberos, EIM pa nudi mehanizem za povezavo teh principalov Kerberos z enotnim identifikatorjem EIM, ki predstavlja tega uporabnika znotraj celotnega podjetja. Z identifikatorjem EIM je mogoče povezati tudi druge uporabniške identitete, kot je na primer ime uporabnika OS/400. Na osnovi teh povezav nudi EIM mehanizem, s pomočjo katerega OS/400 in aplikacije določijo, kateri profil uporabnika OS/400 predstavlja osebo ali enoto, predstavljeno s principalom Kerberos. Informacije v EIM si lahko zamislimo kot drevo: identifikator EIM predstavlja korenino, seznam uporabniških identitet, povezanih z identifikatorjem EIM, pa veje.

Vzememo za zgled spodnjo sliko si zamislimo, da se uporabnik Tine Bence prijavi v omrežje prek svojega PC-ja Windows in dostopi do primerka OS/400, da dostopi do aplikacij, omogočenih za Kerberos. Tinetu ni potrebno podati imena uporabnika OS/400. Te aplikacije lahko poiščejo ime uporabnika OS/400 tako, da poiščejo povezavo s Tinetovim identifikatorjem EIM. Tine Bence v svojem profilu uporabnika OS/400 ne potrebuje več gesla, ker se profil uporabnika ne uporablja za overjanje, pač pa samo za pooblašcanje.

1. slika: Okolje enotne prijave



Tema Scenarij: omogočanje enotne prijave vsebuje zgled, ki kaže, kako konfigurira skrbnik omrežno storitev overjanja in EIM, da omogoči okolje enotne prijave.

Prek enotne prijave je mogoče dostopiti do naslednjih aplikacij:

- Navigator iSeries
- Emulator PC5250
- Distributed Relational Database Architecture ^(TM)(DRDA)^(R)
- NetServer
- QFileSvr.400

Načrtovanje za EIM

EIM na strežniku iSeries obsega več tehnologij in storitev. Preden na strežniku konfigurirate EIM, se odločite, katero funkcionalnost želite izvajati s pomočjo EIM in katere zmožnosti za enotno prijavo.

Preden začnete delati z EIM, morate določiti osnovne zaščitne zahteve za omrežje in jih tudi izvesti. EIM nudi skrbnikom in uporabnikom preprostejše upravljanje identitet v celotnem podjetju. Če uporabite EIM z omrežno storitvijo overjanja, nudi podjetjem tudi zmožnosti enotne prijave.

Naslednja načrtovalna preglednica določa storitve, ki jih namestite, preden konfigurirate EIM.

Načrtovalna preglednica	Odgovori
Ali uporabljate OS/400 izdaje V5R2 (5722-SS1) ali novejše?	
Ali imate na strežnikih iSeries nameščen ponudnik šifriranega dostopa (5722-AC3)?	
Ali imate na ustreznih PC-jih v omrežju (PC-ji, ki jih uporabljate za delo s strežniki iSeries) in na strežnikih iSeries nameščen iSeries Access za Windows (5722-XE1)?	
Ali imate na vseh PC-jih v omrežju in v sistemih iSeries nameščeno omrežno podkomponento Navigatorja iSeries?	
Ali poznate razločevalno ime (DN) in geslo skrbnika LDAP, če imate trenutno konfiguriran strežnik LDAP in ga želite uporabiti kot krmilnik domene EIM?	
Ali je mogoče začasno zaustaviti trenutno konfiguriran strežnik LDAP? (To je zahtevano za dokončanje konfiguracijskega postopka EIM.)	
Ali imate posebna pooblastila *SECADM, *ALLOBJ in *IOSYSCFG?	
Ali ste uveljavili najnovejše začasne popravke programov (PTF-je)?	

Če nameravate uporabiti za overjanje uporabnikov Kerberos, konfigurirajte tudi omrežno storitev overjanja. Celotno preglednico za načrtovanje omrežne storitve overjanja lahko najdete v temi Načrtovanje omrežne storitve overjanja.

Če konfigurirate omrežno storitev overjanja in EIM, da bi omogočili enotno prijavo, preberite temo Scenarij: omogočanje enotne prijave, ki kaže, sta ta izdelka konfigurirana v podjetju.

Zahtevane možnosti Navigatorja iSeries za namestitev

Če želite omogočiti z EIM in omrežno storitvijo overjanja okolje enotne prijave, morate namestiti možnosti Navigatorja iSeries Omrežje in Zaščita. EIM se nahaja znotraj možnosti Omrežje, omrežna storitev overjanja pa znotraj možnosti Zaščita. Če v omrežju ne nameravate uporabljati omrežne storitve overjanja, ni potrebno namestiti možnosti Navigatorja iSeries Zaščita.

Če želite namestiti možnost Navigatorja iSeries Omrežje ali preveriti, ali je ta možnost trenutno nameščena, preverite, ali je na PC-ju, ki ga uporabljate za delo s strežnikom iSeries, nameščen iSeries Access za Windows.

Možnost Omrežje namestite takole:

1. Kliknite **Start** → **Programi** → **IBM iSeries Access za Windows** → **Izbirna namestitev**.
2. Sledite navodilom v pogovornem oknu. V pogovornem oknu **Izbira komponent** razširite ikono **Navigatorja Series**, nato pa izberite možnost **Omrežje**.
Če nameravate uporabljati omrežno storitev overjanja, izberite tudi možnost **Zaščita**.
3. Nadaljujte z izbirno namestitvijo.

Konfiguriranje omrežne storitve overjanja

Omrežna storitev overjanja omogoča uporabo overjanja Kerberos na strežniku iSeries. Ta storitev ni predpogoj za uporabo EIM na strežniku, vendar pa nudi uporaba overjanja Kerberos za zaščito omrežja veliko prednosti.

Če uporabite omrežno storitev overjanja skupaj z EIM, omogoča okolje enotne prijave. Okolje enotne prijave je koristno za uporabnike in skrbnike. Uporabniki imajo manj uporabniških imen in gesel za upravljanje, skrbnikom pa ni potrebno slediti toliko informacijam za vsakega uporabnika. Ker pripomore omogočanje enotne prijave tudi k premostitvi vrzeli med več platformami in različnimi sistemi znotraj omrežja, je mogoče zmanjšati stroške za razvijanje aplikacij in splošne upravne stroške.

Če trenutno na strežniku iSeries ali na vseh strežnikih v omrežju nimate konfigurirane omrežne storitve overjanja, preberite temo Načrtovanje omrežne storitve overjanja, ki vsebuje načrtovalne informacije, ki vam bodo pomagale pri prvih korakih. Če omrežno storitev overjanja že poznate, preberite temo Konfiguriranje omrežne storitve overjanja, ki vam bo pomagala začeti postopek konfiguracije.

Konfiguriranje EIM

Če želite omogočiti eno okolje za prijavo na več platformah, ne da bi spremenili pripadajoča načela, morate konfigurirati EIM in tudi storitve za overjanje omrežja. Konfiguriranje in uporaba storitev overjanja omrežja ni zahtevano za konfiguriranje in uporabo EIM.

Če želite začeti s postopkom konfiguriranja EIM za strežnik iSeries za okolje z eno prijavo, lahko uporabite čarovnika za konfiguriranje EIM. Odvisno od potreb po konfiguriranju lahko čarovnika uporabite za pridruževanje obstoječih domen ali izdelavo in pridruževanje novih domen.

S čarovnikom za konfiguriranje EIM lahko preprosto dokončate osnovno konfiguriranje EIM. Na primer, če še nimate konfiguriranega strežnika LDAP ali če niste konfigurirali storitev za overjanje omrežja, lahko te naloge izvedete s pomočjo čarovnika za konfiguriranje EIM.

Ko uporabite čarovnika za izvajanje osnovnega konfiguriranja EIM, morate izvesti še dodatno konfiguriranje, preden lahko uporabite okolje za eno prijavo. V Scenarij: Omogočitev ene prijave je prikazan zgled, kako je izmišljeno podjetje konfiguriralo okolje z eno prijavo z uporabo storitev za overjanje omrežja in EIM.

Preden uporabite čarovnika za konfiguriranje EIM, morate dokončati vse korake načrtovanja in ugotoviti, kako boste z EIM in storitvami overjanja omrežja omogočili okolje z eno prijavo. Ko dokončate načrtovanje, lahko s čarovnikom konfigurirate EIM za strežnik iSeries: tako da izdelate nove domene ali združite obstoječe domene. V naslednjih temah so na voljo navodila za konfiguriranje EIM:

Izdelava in pridruževanje nove domene

S pomočjo tega opravila lahko izdelate domeno EIM za omrežje in konfigurirate strežnik iSeries za sodelovanje. Čarovnik izdelava novo domeno in konfigurira lokalni strežnik LDAP za krmilnik domene EIM za novo domeno. Če Kerberos trenutno ni konfiguriran na strežniku iSeries, čarovnik predlaga zagon čarovnika za konfiguriranje storitev overjanja omrežja. Ko dokončate to nalogo, lahko konfigurirate ostale strežnike iSeries za sodelovanje v domeni. Če želite konfigurirati ostale strežnike za sodelovanje v domeni, se povežite z vsako od njih in s čarovnikom za konfiguriranje EIM konfigurirajte strežnik, da se bo pridružil obstoječi domeni EIM.

Pridruževanje obstoječe domene

Ko s čarovnikom za konfiguriranje EIM konfigurirate krmilnik domene in domeno EIM, lahko s tem opravilom konfigurirate ostale strežnike iSeries za sodelovanje v domeni. To opravilo morate dokončati za vse strežnike iSeries v omrežju, ki bodo uporabljali EIM. Ko dokončate čarovnika, morate podati informacije o domeni, ki jo pridružujete, vključno z informacijami o povezavi (številka vrat in ali naj bosta za krmilnik odmene uporabljeni zaščita transportne plasti (TLS)/plast zaščitenih vtičnic (SSL). Če Kerberos trenutno ni konfiguriran na strežniku iSeries, čarovnik predlaga zagon čarovnika za konfiguriranje storitev overjanja omrežja.

Kako dostopiti do čarovnika za konfiguriranje EIM

Če želite dostopiti do čarovnika za konfiguriranje EIM, naredite naslednje:

1. Zaženite Navigator iSeries.
2. Prijavite se na strežnik iSeries, za katerega želite konfigurirati EIM.
Če konfigurirate EIM za več strežnikov iSeries, začnite s tistim, na katerem želite konfigurirati krmilnik domene za EIM.
3. Razširite **Omrežje** —> **Preslikava istovetnosti podjetja**.
4. Z desnim gumbom kliknite **Konfiguracija** in izberite **Konfiguriraj...**, da zaženete čarovnika za EIM.

5. Izberite **Pridruži obstoječo domeno** ali **Izdelaj in pridruži novo domeno**.

Ko s čarovnikom za konfiguriranje EIM izdelate krmilnik domen in konfigurirate strežnike iSeries za sodelovanje v domeni, morate z naslednjimi nalogami dokončati konfiguracijo EIM:

1. Dodajte registre EIM v domeno EIM za strežnike ne-iSeries in aplikacije, ki naj sodelujejo v domeni EIM.
2. Izdelajte identifikatorje EIM v domeni za vsakega unikatnega uporabnika ali identiteto za sisteme, ki sodelujejo v domeni EIM.
3. Izdelajte povezave med različnimi uporabniškimi identitetami osebe ali entitete s temi identifikatorji EIM.

Izdelava in pridruževanje nove domene

S čarovnikom za konfiguriranje EIM lahko konfigurirate strežnik LDAP na strežniku iSeries, da bo krmilnik domene EIM za novo domeno. Če je potrebno, čarovnik za konfiguriranje EIM zagotovi, da podate osnovne informacije o konfiguraciji za strežnik LDAP.

Če Kerberos trenutno ni konfiguriran na strežniku iSeries, čarovnik predlaga zagon čarovnika za konfiguriranje storitev overjanja omrežja. Ko dokončate čarovnika, je nova domena EIM konfigurirana, sistem iSeries je konfiguriran za pridružitve novi domeni in podani uporabniški registri so dodani domeni.

Če želite s čarovnikom dokončati to nalogo, morate imeti posebna pooblastila skrbnika sistema (*SECADM), za vse objekte (*ALLOBJ) in posebna pooblastila za konfiguriranje sistema (*IOSYSCFG).

Če želite zagnati in uporabiti čarovnika za konfiguriranje EIM za izdelavo in pridruževanje nove domene EIM, dokončajte naslednje korake znotraj Navigatorja iSeries.

Opomba: Ta čarovnik konfigurira tudi lokalni strežnik LDAP kot nov krmilnik domene EIM.

1. Razširite **Omrežje** → **Preslikava istovetnosti podjetja**.
2. Z desnim gumbom kliknite **Konfiguracija** in izberite **Konfiguriraj...**, da zaženete čarovnika za EIM.
3. Na strani **Dobrodošli** čarovnika izberite **Izdelaj in pridruži novo domeno** in kliknite **Naprej**.
4. Če storitve za overjanje omrežja trenutno niso konfigurirane na strežniku iSeries, se prikaže pogovorno okno **Konfiguriranje storitev za overjanje omrežja**. V tem pogovornem oknu morate izbrati, ali želite konfigurirati storitve za overjanje omrežja. Če izberete **Da**, bo zagnan čarovnik za konfiguriranje storitev za overjanje omrežja. Ko dokončate konfiguriranje storitve overjanja omrežja, se nadaljuje čarovnika za konfiguriranje EIM.
5. Če strežnik LDAP trenutno ni konfiguriran, se prikaže pogovorno okno **Konfiguriranje imeniškega strežnika**. V pogovornem oknu podajte naslednje informacije, da konfigurirate strežnik LDAP:
 - V polju **Vrata** sprejmite privzeto številko vrat **389** ali vnesite drugo številko vrat, ki bo uporabljena za nezaščitene komunikacije EIM z imeniškim strežnikom.
 - V polje **Razločevalno ime** vnesite razločevalno ime LDAP, ki določa skrbnika LDAP za strežnik LDAP. Čarovnik za konfiguriranje EIM izdelava ta skrbniški DN LDAP in ga uporabi za konfiguriranje strežnika LDAP kot krmilnika domene za domeno, ki jo izdelujete.
 - V polje **Geslo** vnesite geslo za skrbnika LDAP.
 - V polje **Potrditev gesla** znova vnesite geslo.
 - Kliknite **Naprej**.
6. V pogovornem oknu **Podajanje krmilnika domene** podajte naslednje informacije:
 - V polju **Domena** podajte ime domene EIM, ki jo želite izdelati. Sprejmite privzeto ime **EIM** ali uporabite poljubni niz znakov, ki vam kaj pomeni. Uporabiti ne smete posebnih znakov, kot so = + < > , # ; \ in *.
 - V polje **Opis** vnesite besedilo, ki opisuje domeno.
 - Kliknite **Naprej**.

7. V pogovornem oknu **Podajanje nadrejenega DN domene** izberite, ali želite podati nadrejeni DN za domeno, ki jo izdelujete. Če podate nadrejeni DN, lahko podate kje v imenskem prostoru lokalnega LDAP naj bo za domeno. Če ne podate nadrejenega DN, so podatki EIM v svoji priponi v imenskem prostoru. Če izberete **Da**, s pomočjo seznama izberite lokalno pripono LDAP za uporabo kot nadrejeni DN ali vnesite besedilo, da izdelate in poimenujete novi nadrejeni DN. Za novo domeni ni potrebno podati nadrejenega DN.
8. V pogovornem oknu **Podajanje uporabnika za povezavo** izberite **tip uporabnika** za povezavo. Izberete lahko enega od naslednjih tipov uporabnikov: razločevalno ime in geslo, datoteka s tabulatorskim ključem Kerberos in nadrejenim ali nadrejeni Kerberos in geslo. Tipa uporabnikov Kerberos sta na voljo samo, če so storitve za overjanje omrežja konfigurirane za lokalni sistem iSeries. Tip uporabnika, ki ga izberete, določa ostale informacije, ki jih morate podati za dokončanje pogovornega okna:
 - Če izberete **Razločevalno ime geslo**, podajte naslednje informacije:
 - V polje **Razločevalno ime** vnesite razločevalno ime (DN) LDAP, ki določa uporabnika, pooblaščenega za izdelavo objektov v lokalnem imenskem prostoru strežnika LDAP. Če ste uporabili tega čarovnika za konfiguriranje strežnika LDAP v prejšnjem koraku, morate vnesti razločevalno ime skrbnika LDAP, ki ste izdelali v tem koraku.
 - V polje **Geslo** vnesite geslo za uporabnika.
 - V polje **Potrditev gesla** znova vnesite geslo.
 - Če izberete **Datoteka s tabulatorskim ključem Kerberos in nadrejeni**, podajte naslednje informacije:
 - V polje **Datoteka s tabulatorskim ključem** vnesite ime datoteke s tabulatorskim ključem na strežniku iSeries, ki določa uporabnika, pooblaščenega za izdelavo objektov v lokalnem imenskem prostoru strežnika LDAP. Lahko kliknete tudi **Preglej** in izberete datoteko s tabulatorskim ključem.
 - V polje **Nadrejeni** vnesite ime nadrejenega Kerberos, ki naj bo uporabljen za določanje uporabnika.
 - V polje **Področje** vnesite ime področja Kerberos za nadrejenega. Ime nadrejenega in področja unikatno določata uporabnike Kerberos v datoteki tabulatorskega ključa. Tako je na primer nadrejeni jsmith v področju ordept.myco.com predstavljen v datoteki tabulatorksega ključa kot jsmith@ordept.myco.com.
 - Če izberete **Nadrejeni Kerberos in geslo**, podajte naslednje informacije:
 - V polje **Nadrejeni** vnesite ime nadrejenega Kerberos, ki določa uporabnika, pooblaščenega za izdelavo objektov v lokalnem imenskem prostoru strežnika LDAP.
 - V polje **Področje** vnesite ime področja Kerberos za nadrejenega.
 - V polje **Geslo** vnesite geslo za uporabnika.
 - V polje **Potrditev gesla** znova vnesite geslo. Ime nadrejenega in področja unikatno določata uporabnike Kerberos v datoteki tabulatorskega ključa. Tako je na primer nadrejeni jsmith v področju ordept.myco.com predstavljen v datoteki tabulatorksega ključa kot jsmith@ordept.myco.com.
 - Kliknite **Preveri povezavo**, da preverite informacije o konfiguraciji uporabnika za povezovanje s krmilnikom domene.
 - Kliknite **Naprej**.
9. V pogovornem oknu **Informacij o registru** izberite tip uporabniških registrov, ki jih želite dodati v domeno EIM. Izberite enega ali oba tipa uporabniških registrov:
 - Izberite **OS400**, da dodate uporabniški register, ki predstavlja lokalni register domeni EIM. V podano polje vnesite ime registra, ki naj bo izdelan v domeni. Ime registra Elm je poljuben niz, ki predstavlja tip registra in določen primerek tega registra.
 - Izberite **Kerberos**, da dodate uporabniški register Kerberos v domeno EIM. V podano polje vnesite ime registra, ki naj bo izdelan v domeni in po potrebi izberite **Imena uporabnikov Kerberos so občutljiva na velike in male črke**.

- Kliknite **Naprej**.
10. V pogovornem oknu **Podajanje systemskega uporabnika EIM** izberite tip uporabnika, ki naj ga sistem uporabi pri izvajanju operacij EIM v imenu funkcij operacijskega sistema. te operacije zajemajo iskanja preslikav in brisanje povezav pri brisanju lokalnega uporabniškega profila OS/400. Izberete lahko enega od naslednjih tipov uporabnikov: razločevalno ime in geslo, datoteka s tabulatorskim ključem Kerberos in nadrejenim ali nadrejeni Kerberos in geslo. Tip uporabnika, ki ga izberete, določa ostale informacije, ki jih morate podati za dokončanje pogovornega okna:

Opomba: Podani uporabnik mora imeti vsaj pooblastila za izvajanje iskanja preslikav in upravljanje registra za lokalni uporabniški register. Če podani uporabnik nima teh pooblastil, določene funkcije operacijskega sistema, povezane z eno prijavo in brisanjem uporabniških profilov, morda ne bodo uspele.
 11. Če izberete **Razločevalno ime geslo**, podajte naslednje informacije:
 - V polje **Razločevalno ime** vnesite razločevalno ime LDAP, ki določa uporabnika za OS/400 za uporabniku pri komuniciranju s krmilnikom domene EIM.
 - V polje **Geslo** vnesite geslo za uporabnika.
 - V polje **Potrditev gesla** znova vnesite geslo.
 12. Če izberete **Nadrejeni Kerberos in geslo**, podajte naslednje informacije:
 - V polje **Nadrejeni** vnesite ime nadrejenega Kerberos, ki določa uporabnika, ki naj ga sistem OS/400 uporabi pri komuniciranju s krmilnikom domene EIM.
 - V polje **Področje** vnesite ime področja Kerberos za nadrejenega.
 - V polje **Geslo** vnesite geslo za uporabnika.
 - V polje **Potrditev gesla** znova vnesite geslo. Ime nadrejenega in področja unikatno določata uporabnike Kerberos v datoteki tabulatorskega ključa. Tako je na primer nadrejeni jsmith v področju ordept.myco.com predstavljen v datoteki tabulatorskega ključa kot jsmith@ordept.myco.com.
 13. Če izberete **Datoteka s tabulatorskim ključem Kerberos in nadrejeni**, podajte naslednje informacije:
 - V polje **Datoteka tabulatorskega ključa** vnesite ime datoteke tabulatorskega ključa na strežniku iSeries, ki določa uporabnika, ki naj ga OS/400 uporabi pri komuniciranju s krmilnikom domene EIM. Lahko kliknete tudi **Preglej** in izberete datoteko s tabulatorskim ključem.
 - V polje **Nadrejeni** vnesite ime nadrejenega Kerberos, ki naj bo uporabljen za določanje uporabnika.
 - V polje **Področje** vnesite ime področja Kerberos za nadrejenega. Ime nadrejenega in področja unikatno določata uporabnike Kerberos v datoteki tabulatorskega ključa. Tako je na primer nadrejeni jsmith v področju ordept.myco.com predstavljen v datoteki tabulatorskega ključa kot jsmith@ordept.myco.com.
 14. Kliknite **Preveri povezavo**, da preizkusite povezavo s krmilnikom domene za systemskega uporabnika, ki ste ga pravkar izdelali.
 15. Kliknite **Naprej**.
 16. V oknu **Povzetek** preglejte informacije o konfiguraciji, ki ste jih podali. Če so vse informacije pravilne, kliknite **Dokončaj**.

Ko se čarovnik zaključi, ste zaključili osnovno konfiguriranje EIM. Če želite dokončati konfiguriranje EIM za ta strežnik, morate dokončati naslednje naloge:

1. Dodajte domeno, ki ste jo izdelali, v mapo Upravljanje domen EIM.
2. Dodajte registre EIM v domeno EIM za ostale strežnike in aplikacije, ki naj sodelujejo v domeni EIM.
3. Izdelajte identifikatorje EIM v domeni za vsakega unikatnega uporabnika ali identiteto za sisteme, ki sodelujejo v domeni EIM.
4. Izdelajte povezave med različnimi uporabniškimi identitetami osebe ali entitete s temi identifikatorji EIM.

S pomočjo plasti zaščitene vtičnice (SSL) ali zaščite transportne plasti (TLS) lahko konfigurirate zaščiteni povezavo s krmilnikom domen.

Konfiguriranje zaščitene povezave s krmilnikom domene EIM

Ko s pomočjo čarovnika izdelate in povežete novo domeno, lahko s pomočjo protokola SSL (Secure Sockets Layer) ali TLS (Transport Layer Security) vzpostavite zaščiteno povezavo s krmilnikom domene EIM. Za konfiguriranje SSL ali TLS za EIM morate opraviti naslednje naloge:

1. Omogočiti SSL za krmilnik domene strežnika LDAP.
2. S pomočjo Upravljalnika digitalnih potrdil (DCM) izdelati potrdilo, ki ga potrebuje strežnik LDAP za uporabo SSL.
3. S pomočjo DCM dodeliti potrdilo strežniku LDAP.
4. Ažurirati lastnosti konfiguracije EIM, tako da podajajo, da uporablja strežnik iSeries zaščiteno povezavo SSL.
5. Ažurirati lastnosti domene EIM za vsako domeno EIM, tako da podajajo, da uporablja EIM pri upravljanju domene prek Navigatorja iSeries povezavo SSL.

Pridruževanje obstoječe domene

S čarovnikom za konfiguriranje EIM lahko pridružite obstoječo domeno EIM. To možnost v čarovniku za konfiguriranje EIM uporabite, če sta domena Elm ali krmilnik domene že konfigurirana v omrežju. Med delom s čarovnikom morate podati informacije o domeni, vključno z informacijami o povezavi za krmilnik domene EIM. Čarovnik shrani te informacije na strežniku iSeries in jih nato uporabi za povezovanje s krmilnikom domene EIM. Čarovnik izdelava tudi uporabniški register EIM, ki predstavlja register uporabniškega profila OS/400 na tem strežniku iSeries.

Če želite s čarovnikom dokončati to nalogo, morate imeti posebna pooblastila skrbnika sistema (*SECADM) in za vse objekte (*ALLOBJ).

Če želite zagnati in uporabiti čarovnika za konfiguriranje EIM za pridruževanje obstoječe domene EIM, z Navigatorjem iSeries dokončajte naslednje korake:

1. Razširite **Omrežje** → **Preslikava istovetnosti podjetja**.
2. Z desnim gumbom kliknite **Konfiguracija** in izberite **Konfiguriraj...**, da zaženete čarovnika za EIM. Ko se čarovnik zažene, med izpolnjevanjem pogovornih oken podajte naslednje informacije.
3. V pogovornem oknu **Dobrodošli** čarovnika izberite **Pridruži obstoječo domeno** in kliknite **Naprej**.
4. Če storitve za overjanje omrežja trenutno niso konfigurirane na strežniku iSeries, se prikaže pogovorno okno **Konfiguriranje storitev za overjanje omrežja**. V tem pogovornem oknu morate izbrati, ali želite konfigurirati storitve za overjanje omrežja. Če izberete **Da**, bo zagnan čarovnik za konfiguriranje storitev za overjanje omrežja. Ko dokončate konfiguriranje storitve overjanja omrežja, se nadaljuje čarovnika za konfiguriranje EIM.
5. V pogovornem oknu **Podajanje krmilnika domene** podajte naslednje informacije:
 - V polje **Ime krmilnika domene** vnesite ime sistema, ki služi kot krmilnik domene za domeno EIM, ki naj jo strežnik iSeries pridruži.
 - Kliknite **Uporabi plast zaščitene vtičnic (SSL)**, če želite prebrati informacije o EIM prebrati s krmilnika domene in uporabiti SSL za zaščito prenosa podatkov EIM.
 - Kliknite **Preveri povezavo**, da preverite informacije o konfiguraciji krmilnika domene.

Opomba: Če ste izbrali SSL in se prikaže sporočilo o napaki, sporočilo morda nakazuje, da strežnik LDAP ni konfiguriran za uporabo SSL.

- Kliknite **Naprej**.
6. V pogovornem oknu **Podajanje uporabnika za povezavo** izberite **tip uporabnika** za povezavo. Izberete lahko enega od naslednjih tipov uporabnikov: razločevalno ime in geslo, datoteka s tabulatorskim ključem Kerberos in nadrejenim ali nadrejeni Kerberos in geslo. Tipa uporabnikov Kerberos sta na voljo samo, če so storitve za overjanje omrežja konfigurirane za lokalni sistem iSeries. Tip uporabnika, ki ga izberete, določa ostale informacije, ki jih morate podati za dokončanje pogovornega okna:

- Če izberete **Razločevalno ime geslo**, podajte naslednje informacije:
 - V polje **Razločevalno ime** vnesite razločevalno ime (DN) LDAP, ki določa uporabnika, pooblaščenega za izdelavo objektov v lokalnem imenskem prostoru strežnika LDAP.
 - V polje **Geslo** vnesite geslo za uporabnika.
 - V polje **Potrditev gesla** znova vnesite geslo.
 - Če izberete **Datoteka s tabulatorskim ključem Kerberos in nadrejeni**, podajte naslednje informacije:
 - V polje **Datoteka s tabulatorskim ključem** vnesite ime datoteke s tabulatorskim ključem na strežniku iSeries, ki določa uporabnika, pooblaščenega za izdelavo objektov v lokalnem imenskem prostoru strežnika LDAP. Lahko kliknete tudi **Preglej** in izberete datoteko s tabulatorskim ključem.
 - V polje **Nadrejeni** vnesite ime nadrejenega Kerberos, ki naj bo uporabljen za določanje uporabnika.
 - V polje **Področje** vnesite ime področja Kerberos za nadrejenega. Ime nadrejenega in področja unikatno določata uporabnike Kerberos v datoteki tabulatorskega ključa. Tako je na primer nadrejeni jsmith v področju ordept.myco.com predstavljen v datoteki tabulatorskega ključa kot jsmith@ordept.myco.com.
 - Če izberete **Nadrejeni Kerberos in geslo**, podajte naslednje informacije:
 - V polje **Nadrejeni** vnesite ime nadrejenega Kerberos, ki določa uporabnika, pooblaščenega za izdelavo objektov v lokalnem imenskem prostoru strežnika LDAP.
 - V polje **Področje** vnesite ime področja Kerberos za nadrejenega.
 - V polje **Geslo** vnesite geslo za uporabnika.
 - V polje **Potrditev gesla** znova vnesite geslo. Ime nadrejenega in področja unikatno določata uporabnike Kerberos v datoteki tabulatorskega ključa. Tako je na primer nadrejeni jsmith v področju ordept.myco.com predstavljen v datoteki tabulatorskega ključa kot jsmith@ordept.myco.com.
 - Kliknite **Preveri povezavo**, da preverite informacije o konfiguraciji uporabnika za povezovanje s krmilnikom domene.
 - Kliknite **Naprej**.
7. Na strani **Podajanje domene** izberite ime domene, ki jo želite pridružiti in kliknite **Naprej**.
 8. V pogovornem oknu **Informacij o registru** izberite tip uporabniških registrov, ki jih želite dodati v domeno EIM. Izberite enega ali oba tipa uporabniških registrov:
 - Izberite **OS400**, da dodate uporabniški register, ki predstavlja lokalni register domeni EIM. V podano polje vnesite ime registra, ki naj bo izdelan v domeni. Ime registra Elm je poljuben niz, ki predstavlja tip registra in določen primerek tega registra.
 - Izberite **Kerberos**, da dodate uporabniški register Kerberos v domeno EIM. V podano polje vnesite ime registra, ki naj bo izdelan v domeni in po potrebi izberite **Imena uporabnikov Kerberos so občutljiva na velike in male črke**. Sprejmete lahko privzeto vrednost; ime registra Kerberos je enako imenu področja. Če za ime registra Kerberos in ime področja uporabite isto ime, lahko povečate zmogljivost pri pridobivanju informacij iz registra. Za podrobnejše informacije o definiranju uporabniških registrov znotraj EIM preglejte Definicije registra EIM.
 - Kliknite **Naprej**.
 9. V pogovornem oknu **Podajanje systemskega uporabnika EIM** izberite tip uporabnika, ki naj ga sistem uporabi pri izvajanju operacij EIM v imenu funkcij operacijskega sistema. te operacije zajemajo iskanja preslikav in brisanje povezav pri brisanju lokalnega uporabniškega profila OS/400. Izberete lahko enega od naslednjih tipov uporabnikov: razločevalno ime in geslo, datoteka s tabulatorskim ključem Kerberos in nadrejenim ali nadrejeni Kerberos in geslo. Tip uporabnika, ki ga izberete, določa ostale informacije, ki jih morate podati za dokončanje pogovornega okna:
 - Če izberete **Razločevalno ime geslo**, podajte naslednje informacije:

- V polje **Razločevalno ime** vnesite razločevalno ime LDAP, ki določa uporabnika za OS/400 za uporabniku pri komuniciranju s krmilnikom domene EIM.
 - V polje **Geslo** vnesite geslo za uporabnika.
 - V polje **Potrditev gesla** znova vnesite geslo.
 - Če izberete **Nadrejeni Kerberos in geslo**, podajte naslednje informacije:
 - V polje **Nadrejeni** vnesite ime nadrejenega Kerberos, ki določa uporabnika, ki naj ga sistem OS/400 uporabi pri komuniciranju s krmilnikom domene EIM.
 - V polje **Področje** vnesite ime področja Kerberos za nadrejenega.
 - V polje **Geslo** vnesite geslo za uporabnika.
 - V polje **Potrditev gesla** znova vnesite geslo. Ime nadrejenega in področja unikatno določata uporabnike Kerberos v datoteki tabulatorskega ključa. Tako je na primer nadrejeni jsmith v področju ordept.myco.com predstavljen v datoteki tabulatorskega ključa kot jsmith@ordept.myco.com.
 - Če izberete **Datoteka s tabulatorskim ključem Kerberos in nadrejeni**, podajte naslednje informacije:
 - V polje **Datoteka tabulatorskega ključa** vnesite ime datoteke tabulatorskega ključa na strežniku iSeries, ki določa uporabnika, ki naj ga OS/400 uporabi pri komuniciranju s krmilnikom domene EIM. Lahko kliknete tudi **Preglej** in izberete datoteko s tabulatorskim ključem.
 - V polje **Nadrejeni** vnesite ime nadrejenega Kerberos, ki naj bo uporabljen za določanje uporabnika.
 - V polje **Področje** vnesite ime področja Kerberos za nadrejenega.
 - Kliknite **Preveri povezavo**, da preizkusite povezavo za sistemskega uporabnika, ki ste ga pravkar izdelali.
 - Kliknite **Naprej**.
10. V oknu **Povzetek** preglejte informacije o konfiguraciji, ki ste jih podali. Če so vse informacije pravilne, kliknite **Dokončaj**.

Ko se čarovnik zaključí, ste zaključili osnovno konfiguriranje EIM. Če želite dokončati konfiguriranje EIM za ta strežnik, morate dokončati naslednje naloge:

1. Dodajte domeno, ki ste jo pridružili, v mapo Upravljanje domen EIM.
2. Dodajte registre EIM v domeno EIM za strežnike ne-iSeries in aplikacije, ki naj sodelujejo v domeni EIM.
3. Izdelajte identifikatorje EIM v domeni za vsakega unikatnega uporabnika ali identiteto za sisteme, ki sodelujejo v domeni EIM.
4. Izdelajte povezave med različnimi uporabniškimi identitetami osebe ali entitete s temi identifikatorji EIM.

Če želite omogočiti okolje z eno prijavo, morate konfigurirati storitve za overjanje omrežja za strežnik iSeries.

Upravljanje EIM

Po konfiguriranju EIM na vašem strežniku iSeries lahko izvedete mnogo nalog, s katerimi upravljate vašo domeno in informacije EIM. Naslednje teme opisujejo specifične naloge, ki jih lahko uporabite za upravljanje EIM na vašem strežniku iSeries ter v omrežju podjetja.

Upravljanje domen EIM

Delo z informacijami EIM, ki so vsebovane v domeni EIM ter v lastnostih domene EIM.

Upravljanje povezav

Vzdrževanje povezav identitet uporabnikov z identifikatorji EIM za vse uporabnike v podjetju.

Upravljanje identifikatorjev EIM

Vzdrževanje identifikatorjev EIM, ki so povezani z uporabniki v podjetju.

Upravljanje pooblastil uporabnikov EIM

Vzdrževanje zaščite informacij EIM s pomočjo dela s pooblastili EIM za krmiljenje funkcij EIM ter operacij, ki jih lahko izvajajo uporabniki.

Upravljanje registrov uporabnikov

Delo z registri uporabnikov, ki ste jih dodali domeni EIM.

Upravljanje domen EIM

Za upravljanje vseh domen lahko uporabljate Navigator iSeries. Če želite upravljati katerokoli domeno EIM, mora biti domena navedena ali pa jo morate dodati v mapo Upravljanje domene pod mapo Omrežje v Navigatorju iSeries. Po izdelavi in konfiguriranju nove domene EIM jo morate dodati v mapo Upravljanje domen, kjer lahko upravljate informacije v domeni.

Za upravljanje domene EIM, ki se nahaja kjerkoli v istem omrežju, lahko uporabite katerokoli povezavo iSeries. iSeriesu, ki je povezan z Navigatorjem iSeries, ni treba sodelovati v domeni za upravljanje te domene.

Za upravljanje domen EIM lahko izvedete naslednje naloge:

- Dodajanje domene v upravljanje domene
- Povezovanje z domeno
- Brisanje domene
- Odstranjevanje domene iz Upravljanja domen

Dodajanje domene v upravljanje domen

Če želite dodati domeno, morate imeti posebno pooblastilo *SECADM. Če želite obstoječo domeno dodati v upravljanje domene, naredite naslednje:

1. Razširite **Omrežje** → **Preslikava identitete podjetja**.
2. Z desno tipko miške kliknite **Upravljanje domen** in izberite **Dodaj domeno....**
3. Podajte zahtevane informacije o domeni in povezavi.
4. Kliknite **Potrdi**, da dodate domeno.

Povezovanje z domeno

Če trenutno niste povezani z domeno EIM, v kateri želite delati, se morate z njo najprej povezati. Z domeno EIM se lahko povežete tudi v primeru, da strežnik iSeries trenutno ni konfiguriran za sodelovanje v tej domeni.

Če se želite povezati z domeno EIM, naredite naslednje:

1. Razširite **Omrežje** → **Preslikava identitete podjetja** → **Upravljanje domene**.
2. Izberite domeno, s katero se želite povezati. Če domena, s katero se želite povezati, ni navedena, morate Dodati domeno EIM v upravljanje domen.
3. Z desno tipko miške kliknite domeno EIM, s katero se želite povezati, in izberite **Vzpostavi povezavo....**
4. Podajte tip uporabnika in zahtevane informacije o uporabniku, ki jih želite uporabiti pri povezovanju s krmilnikom domene EIM.
5. Kliknite **Potrdi**.

Brisanje domene

Če želite izvesti to nalogo, morate imeti pooblastilo skrbnika LDAP ali pooblastilo za upravljanje EIM. Preden zbrisate domeno EIM, morate najpred odstraniti vse registre in informacije o identifikatorju EIM iz domene.

Če se želite zbrisati domeno EIM, naredite naslednje:

1. Razširite **Omrežje** → **Preslikava identitete podjetja** → **Upravljanje domene**.
2. Odstranite vse registre uporabnikov iz domene EIM.
3. Zbrišite vse identifikatorje EIM iz domene EIM.
4. Z desno tipko miške kliknite domeno, ki jo želite zbrisati, in izberite **Zbriši....**
5. V pogovornem oknu **Potrditev brisanja** kliknite **Da**.

Odstranjevanje domene iz upravljanja domene

Čeprav ni zahtevano, lahko odstranite domeno EIM iz mape Upravljanje domen, ko končate z izvajanjem sprememb.

Če želite odstraniti domeno, naredite naslednje:

1. Razširite **Omrežje** → **Preslikava identitete podjetja**.
2. Z desno tipko miške kliknite **Upravljanje domen** in izberite **Odstrani domeno....**
3. Izberite domeno EIM, ki jo želite odstraniti iz upravljanja domene.
4. Kliknite **Potrdi**, da odstranite domeno.

Upravljanje povezav

Povezava definira razmerje med identifikatorjem EIM in identiteto uporabnika v registru. Izdelate lahko na primer povezavo med profilom uporabnika OS/400 ali principalom Kerberos ter identifikatorjem EIM. To povezavo lahko nato uporabite za določitev, kateri identifikator EIM ustreza profilu uporabnika lokalnega iSeries ali principalu Kerberos.

Vzdrževanje povezav identitet uporabnikov z ustreznimi identifikatorji EIM je ključ do poenostavljanja upravnih nalog, ki so potrebne za sledenje, kateri uporabniki imajo račune v različnih sistemih v omrežju.

Upravljanje teh povezav omogoča tudi, da izkoristite prednost omogočanja enojne prijave v vašem omrežju. Če izvedete omrežje z varno enojno prijavo, morate ohranjati ažurnost povezav.

Izdelate lahko tri vrste povezav: izvorno, ciljno in upravno. Če želite izdelati ali vzdrževati povezave med identitetami uporabnikov z ustreznimi identifikatorji EIM, lahko izvedete eno od naslednjih nalog:

- Izdelava povezave
- Brisanje povezave

Izdelava povezave

Če želite omogočiti prijavno okolje, morate izdelati povezave med različnimi identitetami uporabnika osebe ali entitete s posameznim identifikatorjem EIM za to osebo ali entiteto. Izdelate lahko tri različne vrste povezave: ciljna, izvorna ali upravna.

Če želite izdelati izvorno ali upravno povezavo, morate imeti pooblastilo za upravljanje identifikatorjev ali pooblastilo za upravljanje EIM. Če želite izdelati ciljno povezavo, morate imeti pooblastilo za upravljanje registra za vse registra, upravljanje registra za posamezen register ali za upravljanje EIM.

Če želite izdelati povezavo za identifikator EIM, naredite naslednje:

1. Razširite **Omrežje** → **Preslikava identitete podjetja** → **Upravljanje domene**.
2. Povezani morate biti z domeno EIM, v kateri želite delati.
 - Če domena EIM, s katero želite delati, ni navedena pod mapo Upravljanje domene, preglejte Dodajanje domene EIM v Upravljanje domene.
 - Če trenutno niste povezani z domeno EIM, v kateri želite delati, preglejte Povezovanje s krmilnikom domene EIM.
3. Razširite domeno EIM, s katero ste zdaj povezani.
4. Kliknite **Identifikatorji**, da prikažete seznam identifikatorjev EIM.
5. Z desno tipko miške kliknite ustrezní identifikator EIM in izberite **Lastnosti....**

6. Kliknite jeziček **Povezave**.
7. Kliknite **Dodaj...**, da prikažete pogovorno okno **Dodajanje povezave**.
8. Kliknite **Pomoč**, če potrebujete več informacij za izpolnjevanje polj.
9. Ko podate zahtevane informacije, kliknite **Potrdi**.

Brisanje povezave

Če želite zbrisati upravno ali izvorno povezavo, morate imeti pooblastilo za upravljanje identifikatorjev ali pooblastilo za upravljanje EIM. Če želite zbrisati ciljno povezavo, morate imeti pooblastilo skrbnika za izbrane registre (vključno z registrom, s katerim želite delati), pooblastilo skrbnika za register ali pooblastilo za upravljanje EIM.

Povezavo zbrisete takole:

1. Razširite **Omrežje** → **Preslikava identitete podjetja** → **Upravljanje domene**.
2. Povezani morate biti z domeno EIM, v kateri želite delati:
 - Če domena EIM, s katero želite delati, ni navedena pod upravljanjem domene, preglejte Dodajanje domene EIM v upravljanje domene.
 - Če trenutno niste povezani z domeno EIM, v kateri želite delati, preglejte Povezovanje z domeno EIM.
3. Razširite domeno EIM, s katero ste zdaj povezani.
4. Kliknite **Identifikatorji**.
5. Z desno tipko miške kliknite zeleni identifikator in izberite **Lastnosti...**
6. Kliknite jeziček **Povezave**, da prikažete trenutne povezave za identifikator EIM.
7. Izberite povezavo, ki jo želite odstraniti.
8. Kliknite **Odstrani**, da odstranite povezave.
9. Kliknite **Potrdi**.

Upravljanje identifikatorjev EIM

Vzdrževanje identifikatorjev EIM, ki predstavljajo uporabnike v vašem omrežju, je odločilno pri varnostnih ukrepih. Uporabniki v podjetju se vedno spreminjajo, nekateri prihajajo, nekateri odhajajo in spet drugi se premikajo med področji. Skuaj s temi spremembami je potrebno slediti uporabniške račune ter njihove dostope do sistemov v omrežju. Z izdelavo identifikatorjev EIM ter povezavo z identiteto uporabnika za vsakega uporabnika poenostavite to nalogo sledenja.

Omogočanje enojne prijave poenostavi nalogo uporabnikom tudi takrat, ko preidejo v drug oddelek ali področje v podjetju. Njihovo čiščenje zaščite in dostop do sistemov se prav tako lahko spremeni. Omogočanje enojne prijave onemogoči potrebo, da bi si ti uporabniki morali zapomniti nova imena uporabnikov in gesla za nove sisteme.

Upravljanje EIM za vaše uporabnike v podjetju vključuje mnogo nalog, ki so običajno rutina. Za upravljanje identifikatorjev EIM v omrežjih in domenah lahko uporabite naslednje naloge:

- Izdelava identifikatorja EIM
- Dodajanje vzdevka identifikatorju EIM
- Brisanje identifikatorja EIM

Če želite informacije o upravljanju povezav, preglejte temo Upravljanje povezav.

Izdelava identifikatorja EIM

Če želite izdelati identifikator EIM, morate imeti pooblastilo za upravljanje identifikatorjev ali pooblastilo za upravljanje EIM.

Če želite izdelati identifikator EIM za osebo ali entiteto, naredite naslednje:

1. Razširite **Omrežje** → **Preslikava identitete podjetja** → **Upravljanje domene**.

2. Povezani morate biti z domeno EIM, v kateri želite delati:
 - Če domena EIM, s katero želite delati, ni navedena pod **Upravljanje domene**, preglejte Dodajanje domene EIM v Upravljanje domene.
 - Če trenutno niste povezani z domeno EIM, v kateri želite delati, preglejte Povezovanje z domeno EIM.
3. Razširite domeno EIM, s katero ste zdaj povezani.
4. Z desno tipko miške kliknite **Identifikatorji** in izberite **Nov identifikator...**
5. Kliknite **Pomoč**, če potrebujete več informacij za katerokoli polje.
6. Ko podate zahtevane informacije, kliknite **Potrdi**.

Dodajanje vzdevka identifikatorju EIM

Morda želite izdelati vzdevek, ki bo nudil dodatne razločevalne informacije za identifikator EIM. Vi ali ostali uporabniki lahko nato vzdevek uporabljajo za razločevanje enega identifikatorja EIM od drugega. Če imate na primer dve uporabnika z imenom Janez J. Novak, lahko na primer izdelate vzdevek Janez Jože Novak za enega ter vzdevek Janez Jure Novak za drugega uporabnika, s čimer boste lažje razločevali identiteto uporabnika.

Če želite dodati vzdevek identifikatorju, morate imeti pooblastilo za upravljanje identifikatorjev ali pooblastilo za upravljanje EIM.

Če želite vzdevek dodati identifikatorju EIM, naredite naslednje:

1. Razširite **Omrežje** → **Preslikava identitete podjetja** → **Upravljanje domene**.
2. Povezani morate biti z domeno EIM, v kateri želite delati:
 - Če domena EIM, s katero želite delati, ni navedena pod Upravljanje domene, preglejte Dodajanje domene EIM v Upravljanje domene.
 - Če trenutno niste povezani z domeno EIM, v kateri želite delati, preglejte Povezovanje s krmilnikom domene EIM.
3. Razširite domeno EIM, s katero ste povezani.
4. Z desno tipko miške kliknite zeleni identifikator in izberite **Lastnosti**. Če ne obstaja noben identifikator EIM, preglejte Izdelava identifikatorja EIM.
5. Podajte ime vzdevka, ki ga želite dodati temu identifikatorju EIM, in kliknite **Dodaj**.
6. Kliknite **Potrdi**, da shranite spremembe.

Brisanje identifikatorja EIM

Če želite zbrisati identifikator EIM, morate imeti za upravljanje EIM.

Če želite zbrisati identifikator EIM, naredite naslednje:

1. Razširite **Omrežje** → **Preslikava identitete podjetja** → **Upravljanje domene**.
2. Povezani morate biti z domeno EIM, v kateri želite delati:
 - Če domena EIM, s katero želite delati, ni navedena pod Upravljanje domene, preglejte Dodajanje domene EIM v Upravljanje domene.
 - Če trenutno niste povezani z domeno EIM, v kateri želite delati, preglejte Povezovanje s krmilnikom domene EIM.
3. Razširite domeno EIM, s katero ste zdaj povezani.
4. Kliknite **Identifikatorji**.
5. Izberite enega ali več identifikatorjev, ki jih želite zbrisati.
6. Z desno tipko miške kliknite izbrane identifikatorje EIM in izberite **Zbriši**.
7. V pogovornem oknu **Potrditev brisanja** kliknite **Da**, da odstranite izbrane identifikatorje EIM.

Upravljanje pooblastil uporabnikov EIM

EIM definira različna pooblastila EIM, ki so potrebna za izvajanje različnih operacij v domeni. Ta vključujejo funkcije upravljanja domen, kot so izdelava identifikatorjev, izpis registrov ter izvajanje operacij iskanja preslikav. Le uporabniki s pooblastili skrbnika EIM lahko podeljujejo ali odvzemajo pooblastila za druge uporabnike.

Preglejte temo pooblastila EIM, kjer boste našli kratek opis definicij za vsako skupino pooblastil ter podrobnosti o določenem dostopu, ki ga ima vsak od teh pooblastil do določenih funkcij EIM.

Če želite spremeniti pooblastila za uporabnika, naredite naslednje:

1. V Navigatorju iSeries razširite **Omrežje** → **Preslikava identitete podjetja** → **Upravljanje domene**.
2. Razširite domeno EIM, v kateri želite delati. Če trenutno s to domeno niste povezani, boste pozvani k povezavi. Zagotovite, da ste z domeno povezani s pooblastilom skrbnika EIM.
3. Z desno tipko miške kliknite domeno EIM in izberite **Pooblastila....**
4. V pogovornem oknu **Urejanje pooblastila EIM** podajte uporabnika, za katerega spreminjate pooblastila EIM.
5. Kliknite **Potrdi**.
6. V pogovornem oknu **Urejanje pooblastila EIM** izvedite ustrezne spremembe v pooblastilih za uporabnika.
7. Ko končate, kliknite **Potrdi**, da shranite spremembe v pooblastilih.

Upravljanje registrov uporabnikov

Preden lahko izdelate povezave med identitetami, ki so vsebovane v registrih uporabnikov ter ustreznimi identifikatorji EIM, morate najprej definirati register uporabnikov v domeni EIM:

Naslednje naloge so del upravljanja registrov uporabnikov v domeni EIM.

- Dodajanje registra uporabnikov
- Dodajanje vzdevka registru uporabnikov
- Definiranje zasebnega tipa registra uporabnikov v EIM
- Odstranjevanje registra uporabnikov
- Odstranjevanje vzdevka iz registra uporabnikov

Dodajanje registra uporabnikov

Če želite dodati register uporabnikov, morate imeti pooblastilo skrbnika EIM. Če želite podrobne informacije o tem pooblastilu ter o tem, do česa lahko dostopa uporabnik s tem pooblastilom, preglejte pooblastila EIM .

Če želite v domeno EIM dodati register uporabnikov, naredite naslednje:

1. Razširite **Omrežje** → **Preslikava identitete podjetja** → **Upravljanje domene**.
2. V domeno EIM se povežite z uporabnikom, ki ima pooblastilo skrbnika EIM.
 - Če domena EIM, s katero želite delati, ni navedena pod mapo Upravljanje domene, preglejte Dodajanje domene EIM v upravljanje domene.
 - Če trenutno niste povezani z domeno EIM, v kateri želite delati, preglejte Povezovanje s krmilnikom domene EIM.
3. Razširite domeno EIM, s katero ste zdaj povezani.
4. Z desno tipko miške kliknite **Registri uporabnikov** in izberite **Dodaj register...**
5. Podajte zahtevane informacije za register uporabnikov. Za register uporabnika lahko podate tudi informacije o vzdevku.
6. Kliknite **Potrdi**, da shranite informacije in register uporabnikov dodate v domeno EIM.

Dodajanje vzdevka registru uporabnikov

Vi ali razvijalec aplikacij boste morda želeli izdelati vzdevek, s katerim boste podali dodatne razločevalne informacije za register uporabnikov. Vi ali uporabniki lahko nato vzdevek uporabijo za razločevanje enega registra uporabnikov od drugega. Razvijalci aplikacij in skrbniki na primer uporabljajo vzdevek na registru uporabnikov za komuniciranje, katere registre EIM naj uporablja aplikacija. Če želite informacije o uporabi vzdevkov z registri uporabnikov, preglejte definicije registra EIM.

Če želite vzdevek dodati registru uporabnikov, morate uporabiti enega od naslednjih pooblastil: skrbnik EIM, skrbnik registra za vse registre ali skrbnik registra za specifični register, za katerega izvajate to opravilo.

Če želite vzdevek dodati registru uporabnikov v domeni EIM, naredite naslednje:

1. Razširite **Omrežje** → **Preslikava identitete podjetja** → **Upravljanje domene**.
2. Povezani morate biti z domeno EIM, v kateri želite delati:
 - Če domena EIM, s katero želite delati, ni navedena pod mapo Upravljanje domene, preglejte Dodajanje domene EIM v upravljanje domene.
 - Če trenutno niste povezani z domeno EIM, v kateri želite delati, preglejte Povezovanje s krmilnikom domene EIM.
3. Razširite domeno EIM, s katero ste zdaj povezani.
4. Kliknite **Registri uporabnikov**, da prikažete seznam registrov v domeni.
5. Z desno tipko miške kliknite register uporabnikov, v katerega želite dodati vzdevek, in izberite **Lastnosti...**
6. Kliknite jeziček **Vzdevek** v pogovornem oknu **Lastnosti**.
7. Podajte ime in tip vzdevka, ki ga želite dodati. Podate lahko tip vzdevka, ki ni vključen na seznamu tipov.
8. Kliknite **Dodaj**.
9. Kliknite **Potrdi**, da shranite spremembe.

Definiranje zasebnega tipa registra uporabnikov v EIM

Če želite definirati tip registra uporabnikov, ki ni vnaprej definiran za prepoznavanje v EIM, morate podati tip registra v obliki **IdentifikatorObjekta-normalizacija**, kjer je **IdentifikatorObjekta** identifikator objekta, zapisan v decimalni obliki s pikami, kot je 1.2.3.4.5.6.7, **normalizacija** pa je vrednost **caseExact** ali vrednost **caseIgnore**. Identifikator objekta (OID) za OS/400 je na primer 1.3.18.0.2.33.2-caseIgnore.

Od pooblaščenca službe za registracijo OID si morate pridobiti vse OID-e, ki jih potrebujete, da zagotovite, da izdelujete in uporabljate unikatne OID-e. Z unikatnimi OID-i se boste izognili morebitnim navzkrižjem z OID-i, ki jih izdelajo druge organizacije ali aplikacije.

OID-e si lahko pridobite na dva načina:

- **Registriranje objektov s pooblaščenno službo.**
Ta metoda predstavlja dobro izbiro, ko za predstavitev informacij potrebujete majhno število fiksnih OID-ov. Ti OID-i lahko predstavljajo načela potrdil za uporabnike v vašem podjetju.
- **Pridobitev dodelitve dela od službe za registriranje in dodelitev svojih lastnih OID-ov, ko je to potrebno.**
Ta metoda, ki predstavlja dodelitev območja identifikatorjev objektov v decimalnem zapisu s pikami, je dobra izbira, če potrebujete večje število OID-ov ali se vaše dodelitve OID-ov spreminjajo. Dodelitev dela je sestavljena iz začetnih števil v decimalnem zapisu s pikami, na katerih mora temeljiti osnova **IdentifikatorjaObjekta**. Dodelitev dela je lahko na primer 1.2.3.4.5.. Svoje lastne OID-e lahko izdelate tako, da dodajate temu osnovnemu delu. Na primer, izdelate lahko OID-e v obliki 1.2.3.4.5.x.x.x).

Več o registriranju OID-ov pri službi za registracijo lahko dobite, tako da pregledate naslednje internetne vire:

- American National Standards Institute (ANSI) je služba za registriranje za imena organizacij v Združenih državah, ki upošteva globalni proces registracije, ki sta ga vzpostavili organizaciji International Standards Organization (ISO) in International Telecommunication Union (ITU). List s podatki ter povezavo na

obrazec prošnje se nahaja na ANSI-jevi spletni strani http://web.ansi.org/public/services/reg_org.html



. Del OID-a ANSI za organizacije je 2.16.840.1. ANSI zaračuna določeno vrednost za dodelitve delov OID. Približno dva tedna traja, do prejmete dodelitev dela OID-a od ANSI-ja. ANSI bo dodelil številko (NEWNUM) z izdelavo novega dela OID-a: 2.16.840.1.NEWNUM.

- V večini držav ali regij nacionalne organizacije za standarde vzdržujejo register OID-ov. Kot pri delu ANSI, so ti deli običajno dodeljeni pod OID-om 2.16. Nekoliko boste morali povprašati, če boste želeli najti pooblaščenico službo OID za posamezno državo ali regijo. Naslove državnih teles članov ISO lahko najdete na naslovu <http://www.iso.ch/adresse/membodies.html>



. Informacije zajemajo pošti naslov ter elektronsko pošto. V večini primerov je podana tudi spletna stran.

- Drug možna začetna točka je mednarodni register shem ISO DCC NSAP. NSAP pomeni Network Service Access Point in se uporablja v različnih mednarodnih standardih. Register za sheme lahko pridobite na naslovu <http://www.fei.org.uk> pod naslovom ISO DCC NSAP



. Spletna stran trenutno navaja kontaktne informacije za 13 pooblaščenih služb za poimenovanje, nekatere od njih bodo dodeljevale tudi OID-e.

- IANA (Internet Assigned Numbers Authority) dodeljuje zasebne številke podjetja, ki so OID-i v delu 1.3.6.1.4.1. IANA je do zdaj dodelila dele za več kot 7500 podjetij. Stran s prošnjo najdete na naslovu <http://www.iana.org/cgi-bin/enterprise.pl>



, pod Zasebne številke podjetja. Registracija pri IANA običajno traja približno en teden. OID pri IANA je brezplačen. IANA bo dodelil novo številko (NEWNUM), tako da bo novi del OID-a enak 1.3.6.1.4.1.NEWNUM.

- Zvezna vlada v ZDA vzdržuje CSOR (Computer Security Objects Registry). CSOR je pooblaščenica služba za poimenovanje za del 2.16.840.1.101.3 in trenutno registrira objekte za varnostne oznake, šifrirne algoritme ter načela za potrdila. OID-i načel za potrdila so definirane v delu 2.16.840.1.101.3.2.1. CSOR nudi OID-je načel tudi agencijam za zvezno vlado ZDA. Če želite podrobnejše informacije o CSOR, preglejte <http://csrc.nist.gov/csor/>



Če želite podrobnejše informacije o OID-ih za načela o potrdilih, preglejte spletno stran <http://csrc.nist.gov/csor/pkireg.htm>



Odstranjevanje registra uporabnikov

Odstranjevanje registra uporabnikov iz domene EIM povzroči, da bodo izgubljene vse povezave z identifikatorji EIM za te identitete uporabnikov v registru uporabnikov. Ponovno dodajanje registra uporabnikov nazaj v domeno EIM, potem ko ga odstranite, ne zažene ponovno razmerij povezav.

Če želite odstraniti register uporabnikov, morate imeti pooblastilo skrbnika EIM.

Če želite odstraniti register uporabnikov, naredite naslednje:

1. Razširite **Omrežje** → **Preslikava identitete podjetja** → **Upravljanje domene**.

2. Povezani morate biti z domeno EIM, v kateri želite delati.
 - Če domena EIM, s katero želite delati, ni navedena pod mapo Upravljanje domene, preglejte Dodajanje domene EIM v upravljanje domene.
 - Če trenutno niste povezani z domeno EIM, v kateri želite delati, preglejte Povezovanje s krmilnikom domene EIM.
3. Razširite domeno EIM, s katero ste zdaj povezani.
4. Kliknite **Registri uporabnikov**, da prikažete seznam registrov v domeni.
5. Z desno tipko miške kliknite register uporabnikov, ki ga želite zbrisati, in kliknite **Zbriši...**
6. V pogovornem oknu **Potrditev** kliknite **Da**, da zbrisete register uporabnikov.

Odstranjevanje vzdevka iz registra uporabnikov

Če želite odstraniti vzdevek iz registra uporabnikov, morate imeti pooblastilo skrbnika registra in pooblastilo skrbnika za izbrane registre (vključno z registrom, s katerim želite delati) ali pooblastilo za upravljanje EIM.

Če želite vzdevek odstraniti iz registra uporabnikov v domeni EIM, naredite naslednje:

1. Razširite **Omrežje** → **Preslikava identitete podjetja** → **Upravljanje domene**.
2. Povezani morate biti z domeno EIM, v kateri želite delati:
 - Če domena EIM, s katero želite delati, ni navedena pod mapo Upravljanje domene, preglejte Dodajanje domene EIM v upravljanje domene.
 - Če trenutno niste povezani z domeno EIM, v kateri želite delati, preglejte Povezovanje s krmilnikom domene EIM.
3. Razširite domeno EIM, s katero ste zdaj povezani.
4. Kliknite **Registri uporabnikov**, da prikažete seznam registrov v domeni.
5. Z desno tipko miške kliknite register uporabnikov, iz katerega želite odstraniti vzdevek, in izberite **Lastnosti**.
6. Kliknite jeziček **Vzdevek** v pogovornem oknu **Lastnosti**.
7. Izberite vzdevek, ki ga želite odstraniti, in kliknite **Odstrani**.
8. Kliknite **Potrdi**, da shranite spremembe.

API-ji za EIM

EIM ima več aplikacijskih programerskih vmesnikov (API-jev), ki jih aplikacije lahko uporabijo za operacije EIM v imenu aplikacije ali uporabnika aplikacije. S temi API-ji lahko izvedete iskanje preslikav istovetnosti, različne funkcije za konfiguriranje in upravljanje EIM in spreminjate informacije in poizvedbe.

API-ji EIM so razdeljeni v več kategorij:

- Operacije za povezave in delo z EIM
- Upravljanje domen EIM
- Operacije registra
- Operacije identifikatorja EIM
- Upravljanje povezav EIM
- Operacije iskanja preslikav EIM
- Upravljanje pooblastil EIM

Aplikacije, ki uporabljajo te API-je za upravljanje ali uporabo informacij EIM v domeni EIM, se ponavadi držijo naslednjega programskega modela:

1. Pridobivanje ročke EIM
2. Povezovanje z domeno EIM
3. Običajna obdelava aplikacij

4. Uporaba API-ja za upravljanje EIM ali iskanje preslikav istovetnosti EIM
5. Običajna obdelava aplikacij
6. Pred zaključkom uniči ročko EIM

Za podrobnejše informacije o popoln seznam API-jev EIM, ki so na voljo za strežnik iSeries preglejte temo API-ji EIM (Enterprise Identity Mapping).

Odpravljanje težav v EIM

EIM je sestavljen iz številnih tehnologij, aplikacij in funkcij. Ker se lahko lotite odpravljanja težav na več načinov, vsebujejo naslednje teme podrobne informacije in navodila za odpravljanje nekaterih najpogostejših napak, na katere lahko naletite, kot so naslednje:

- Povezava s krmilnikom domene ni mogoča
- Dolgotrajen izpis identifikatorjev EIM
- Čarovnik za konfiguracijo EIM se pri zaključni obdelavi obes
- Ročka EIM ni več veljavna
- Sporočila Kerberos za overjanje in diagnosticiranje

Povezava s krmilnikom domene ni mogoča

Težave pri povezovanju s krmilnikom domene lahko povzročajo številni faktorji. Preglejte naslednje postavke, ki vam bodo pomagale določiti vzrok težave:

- Preverite, ali so informacije, podane za naslednje postavke, pravilne:
 - Ime krmilnika domene
 - Podana vrata
 - ID uporabnika in geslo
- Preverite, ali je krmilnik domene aktiven. Če je krmilnik domene strežnik iSeries, lahko uporabite Navigator iSeries in opravite naslednje korake:
 1. Razširite ikono **Omrežje** → **Strežniki** → **TCP/IP**.
 2. Preverite, ali je status imeniškega strežnika **Zagnan**. Če je strežnik zaustavljen, z desno tipko miške kliknite možnost **Imeniški strežnik** in izberite **Zaženi...**

Ko je krmilnik domene aktiven, se poskusite znova povezati z domeno.

1. Razširite ikono **Omrežje** → **Preslikava identitete podjetja** → **Upravljanje domen**.
2. Izberite domeno, s katero se želite povezati. Če ni navedena nobena domena EIM ali domena EIM, s katero želite delati, ni navedena v mapi Upravljanje domen, morate dodati domeno EIM v upravljanje domen.
3. Z desno tipko miške kliknite domeno EIM, s katero se želite povezati in izberite **Poveži...**
4. Podajte tip uporabnika in zahtevane uporabniške informacije, ki bodo uporabljene pri povezavi s krmilnikom domene EIM.
5. Kliknite **Potrdi**.

Dolgotrajen izpis identifikatorjev EIM

Če odprete mapo Identifikatorji v Navigatorju iSeries, je lahko tvorba seznama identifikatorjev dolgotrajna. Če imate v domeni veliko število identifikatorjev EIM, lahko zožite iskalni kriterij za prikaz seznama identifikatorjev EIM.

Prikaz identifikatorjev EIM prilagodite takole:

1. V Navigatorju iSeries razširite ikono **Omrežje** → **Preslikava identitete podjetja** → **Upravljanje domen**.
2. Razširite domeno, v kateri želite prikazati identifikatorje EIM.

3. Z desno tipko miške kliknite **Identifikatorji** in izberite **Prilagodi ta pogled** → **Vključi....**
4. Podajte zelen kriterij prikaza. Kot univerzalni znak lahko uporabite zvezdico (*).
5. Kliknite **Potrdi**.

Ko boste naslednjič kliknili možnost **Identifikatorji**, bodo prikazani samo tisti identifikatorji EIM, ki ustrezajo podanemu kriteriju. Če želite prikazati vse identifikatorje EIM, uporabite zgornje korake in izberite kot možnost za prikaz **Vsi identifikatorji**.

Čarovnik za konfiguracijo EIM se pri zaključni obdelavi obesil

Če se zdi, da se je čarovnik pri zaključni obdelavi obesil, morda čaka na zagon krmilnika domene. Preverite, ali je prišlo pri zagonu strežnika LDAP do kakšne napake. Za strežnike iSeries preverite dnevnik opravil za opravilo QDIRSRV v podsistemu QSYSWRK.

Dnevnik opravil preverite takole:

1. V Navigatorju iSeries razširite ikono **Upravljanje dela** → **Podsistemi** → **Qsyswrk**.
2. Z desno tipko miške kliknite **Qdirsrv** in izberite **Dnevnik opravil**.

Ročka EIM ni več veljavna

Če prejme uporabnik pri upravljanju EIM prek Navigatorja iSeries napako, ki kaže, da ročka EIM ni več veljavna, je bila povezava s krmilnikom domene prekinjena.

S krmilnikom domene se znova povežete takole:

1. V Navigatorju iSeries razširite ikono **Omrežje** → **Preslikava identitete podjetja** → **Upravljanje domen**.
2. Z desno tipko miške kliknite domeno, s katero želite delati in izberite **Znova poveži....**
3. Podajte informacije o povezavi.
4. Kliknite **Potrdi**.

Sporočila Kerberos za overjanje in diagnosticiranje

Če uporabljate pri overjanju z EIM protokol Kerberos, se pri vsaki neuspehi operaciji overjanja ali preslikave identitete zapiše v dnevnik opravil diagnostično sporočilo CPD3E3F. Diagnostično sporočilo vsebuje glavno in pomožno statusno kodo, ki kažeta, kje je prišlo do težave. Najpogostejše napake so navedene v sporočilu skupaj z obnovitvenim dejanjem.

Za začetek odpravljanja težave preglejte informacije pomoči, povezane z diagnostičnim sporočilom.

Informacije, povezane z EIM

Morda boste želeli spoznati tudi druge tehnologije, ki so povezane z EIM. Naslednje teme Informacijskega centra vam bodo pomagale razumeti te povezane tehnologije:

- **Omrežna storitev overjanja**

Ta tema vsebuje informacije o konfiguriranju omrežne storitve overjanja na strežniku iSeries. Omrežna storitev overjanja omogoča sodelovanje strežnika iSeries v obstoječem omrežju Kerberos. Če uporabite omrežno storitev overjanja skupaj z EIM, nudi enotno prijavo za omrežje.

- **Imeniške storitve (LDAP)**

Ta tema vsebuje konfiguracijske in konceptne informacije o imeniških storitvah (LDAP). EIM uporablja strežnik LDAP za shranitev podatkov EIM in povezav v preslikavah.



Natisnjeno na Danskem