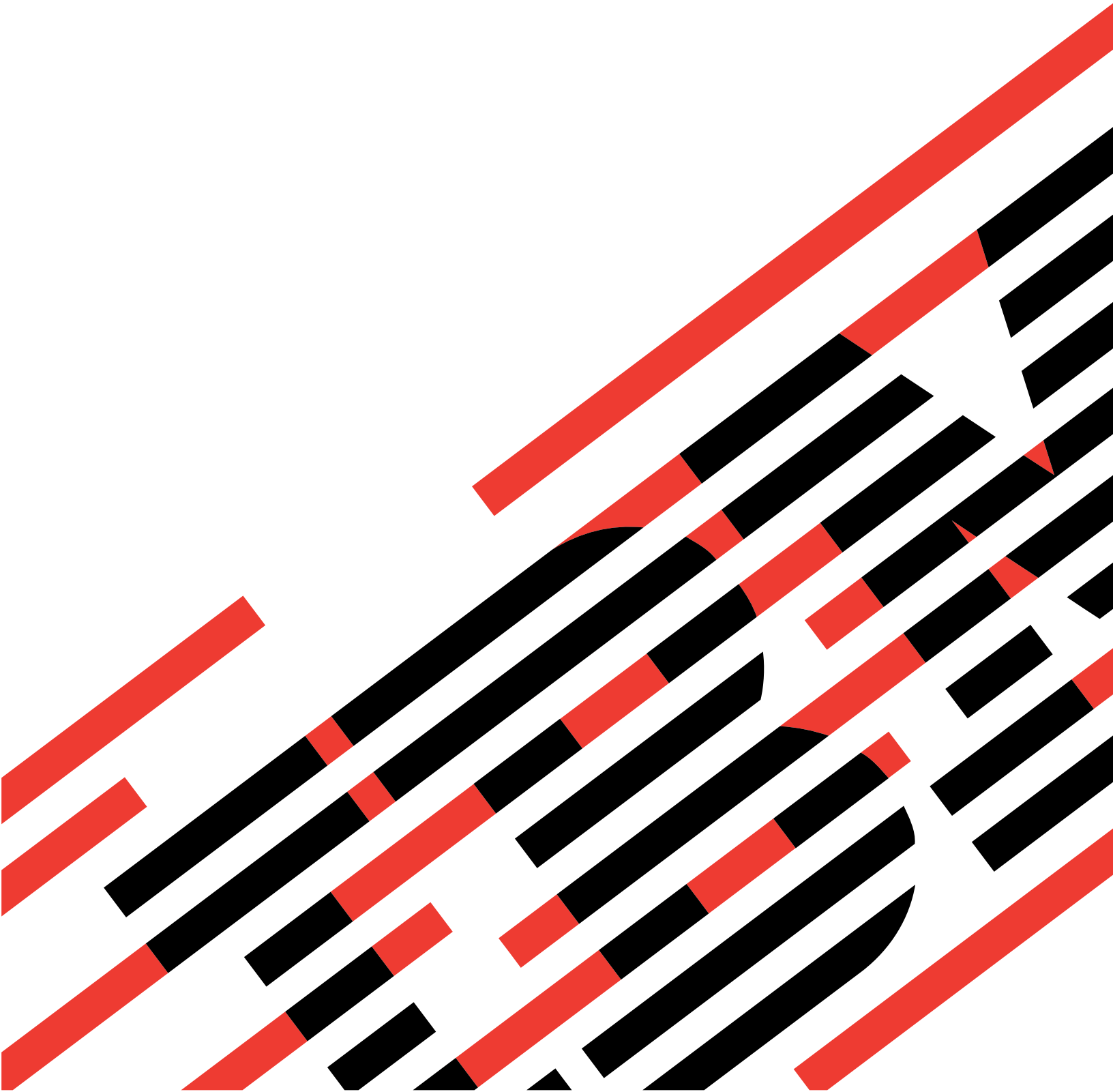
IBM

eserver

iSeries

Enterprise Identity Mapping (EIM)

Verzia 5, vydanie 3



IBM

@server

iSeries

Enterprise Identity Mapping (EIM)

Verzia 5, vydanie 3

Poznámka

Pred použitím týchto informácií a nimi podporovaného produktu si určite prečítajte informácie v časti “Právne vyhlásenia”, na strane 115.

Štvrté vydanie (August 2005)

Toto vydanie sa týka verzie 5, vydanie 3, modifikácia 0 operačného systému IBM OS/400 (číslo produktu 5722–SS1) a všetkých nasledujúcich vydaní a modifikácií, kým nebude v nových vydaniach uvedené inak. Táto verzia nie je určená pre všetky modely RISC (reduced instruction set computer) ani pre všetky modely CISC.

Obsah

EIM (Enterprise Identity Mapping)

EIM (Enterprise Identity Mapping) for iSeries je implementáciou v OS/400 infraštruktúry IBM @server , ktorá dovoľuje administrátorom a vývojárom aplikácií vyriešiť problém manažovania viacerých registrov užívateľov v ich podniku. Väčšina podnikov so sieťami čelí problému viacerých registrov užívateľov, čo vyžaduje, aby každá osoba alebo entita v podniku mala identitu užívateľa v každom registri. Potreba viacerých registrov užívateľov rýchlo prerastie do veľkého administratívneho problému, ktorý ovplyvňuje užívateľov, administrátorov a vývojárov aplikácií. EIM (Enterprise Identity Mapping) prináša nenákladné riešenia pre jednoduchší manažment viacerých registrov užívateľov a identít užívateľov vo vašom podniku.

EIM vám dovoľuje vytvoriť systém mapovaní identít, nazývaných priradenia, medzi rôznymi identitami užívateľa v rôznych registroch užívateľov pre osobu vo vašom podniku. EIM tiež poskytuje spoločnú množinu rozhraní API, ktoré sa dajú použiť medzi platformami na vývoj aplikácií, ktoré používajú mapovania identít, ktoré vytvoríte na vyhľadávanie vzťahov medzi identitami užívateľa. Okrem toho môžete použiť EIM v spojení so službou sieťovej autentifikácie, implementáciou Kerberos v OS/400 a poskytovať tak prostredie s jednoduchým prihlásením.

EIM môžete nakonfigurovať a manažovať cez iSeries, grafické užívateľské rozhranie iSeries. Server iSeries používa EIM na povolenie rozhraniam OS/400 autentifikovať užívateľov pomocou služby sieťovej autentifikácie. Aplikácie a tiež OS/400 môžu akceptovať lístky Kerberos a používať EIM na vyhľadanie užívateľského profilu, ktorý reprezentuje rovnakú osobu ako reprezentuje lístok Kerberos.

Ak sa chcete dozvedieť o fungovaní EIM, o konceptoch EIM a o používaní EIM vo vašom podniku, pozrite si nasledujúce časti:

Tlač tejto témy
Vytlačte si verziu PDF tejto témy a ľubovoľných súvisiacich tém.

Novinky vo V5R3
Dozviete sa tu o nových funkciách pre EIM v tomto vydaní.

Prehľad Enterprise Identity Mapping
Prečítajte si o problémoch, ktoré vám môže pomôcť vyriešiť EIM, o aktuálnych priemyselných prístupoch k týmto problémom a o dôvodoch, prečo je prístup cez EIM lepší.

Koncepty EIM
Dozviete sa tu o dôležitých konceptoch EIM, ktoré je nutné zohľadniť pri implementácii EIM.

Plán pre EIM
Dozviete sa tu, ako vytvoriť plán implementácie, potrebný pre úspešnú konfiguráciu EIM pre iSeries v prostredí so zmiešanými platformami.

Konfigurácia EIM
Dozviete sa tu, ako použiť sprievodcu konfiguráciou EIM na konfiguráciu EIM pre vaše servery iSeries.

Manažovanie EIM
Dozviete sa tu, ako manažovať vašu doménu EIM a údaje domény, vrátane spôsobu manažovania domén, identifikátorov, priradení, definícií registrov EIM, riadenia prístupu k EIM, atď.

Rozhrania API EIM
Dozviete sa tu o rozhraniach API EIM a o spôsobe ich využitia vo vašich aplikáciách a sieti.

Odstraňovanie problémov EIM
Dozviete sa tu o bežných problémoch a chybách, ku ktorým môže dôjsť pri konfigurovaní a používaní EIM a tiež o možných riešeniach.

Súvisiace informácie pre EIM
Dozviete sa tu o ostatných zdrojoch a informáciách týkajúcich sa EIM.

Novinky vo V5R3

Vylepšenia V5R3 EIM (Enterprise Identity Mapping) pre iSeries a súvisiace vylepšenia OS/400 zahrňujú:

Nová alebo vylepšená funkcia pre EIM

- **Sprievodca synchronizáciou funkcií**. Sprievodcu **synchronizáciou funkcií** môžete použiť v iSeries Navigator na rozšírenie sieťových autentifikačných služieb a konfigurácií EIM do skupiny systémov V5R3. Sprievodca duplikuje konfigurácie v modelovom systéme a kopíruje ich do iných systémov v skupine. Jedným nakonfigurovaním a rozšírením tejto konfigurácie do viacerých systémov ušetríte viac času, ako konfigurovaním každého systému zvlášť. Technické a konfiguračné detaily nájdete v scenári: Rozšírenie služby sieťovej autentifikácie a EIM do viacerých systémov.
- **Podpora politiky mapovania**. Podpora politiky mapovania EIM vám umožní použiť priradenia politiky a taktiež špecifické priradenia identifikátorov v doméne EIM. Priradenia politiky môžete vytvoriť a použiť na definovanie priamych vzťahov medzi identitami užívateľov a rôznymi registrami užívateľov. Priradenia politiky poskytujú prostriedky tvorby mapovaní typu veľa-jeden medzi zdrojovou množinou viacerých identít užívateľov v jednom registri užívateľov a jedinou cieľovou identitou užívateľa v zadanom cieľovom registri užívateľov. Priradenia politiky môžete použiť namiesto alebo v spojení s priradeniami identifikátorov.
- **Vylepšenie príkazu užívateľského profilu**. Do obidvoch príkazov CRTUSRPRF (Create user profile) a CHGUSRPRF (Change user profile) bol pridaný ďalší parameter s názvom EIMASSOC. Parameter EIMASSOC vám umožní definovať priradenia identifikátorov EIM pre špecifický užívateľský profil pre lokálny register. Ak chcete použiť tento parameter, zadajte identifikátor EIM, voľbu akcie pre priradenie, typ priradenia identifikátora a či chcete vytvoriť zadaný identifikátor EIM, ak ešte neexistuje. Ak sa chcete dozvedieť viac o tomto novom parametri, pozrite si časť “Aspekty užívateľských profilov systému OS/400 pre Enterprise Identity Mapping” na strane 42.

Vylepšenia informácií EIM

Toto vydanie obsahuje rozšírenú sekciu plánovania, ktorá pokrýva celkové potreby plánovania pre implementáciu EIM do platformy @server a taktiež špecifické informácie plánovania pre implementáciu EIM do OS/400.

Navyše, téma Jednoduché prihlásenie bola pridaná do Informačného centra, aby poskytla úplnú dokumentáciu o implementovaní EIM ako súčasti prostredia s jednoduchým prihlásením na zredukovanie manažmentu hesiel. Táto téma poskytuje množstvo detailných scenárov bežných situácií jednoduchého prihlásenia, s detailnými konfiguračnými pokynmi na ich implementáciu.

Ako zistiť, čo je nové alebo zmenené

Na označenie miest s technickými zmenami tieto informácie používajú:

- Obrázok » na označenie začiatku nových alebo zmenených informácií.
- Obrázok « na označenie konca nových alebo zmenených informácií.

Ak chcete nájsť ďalšie informácie o novinkách alebo zmenách v tomto vydaní, pozrite si časť Poznámka pre užívateľov.

Tlač tejto témy

Ak si chcete prezrieť alebo stiahnuť verziu PDF, vyberte Enterprise Identity Mapping (about 1389 KB).

Iné informácie

Môžete zobraziť alebo prevziať tieto súvisiace témy:

- Služby sieťovej autentifikácie (približne 1398 KB) obsahuje informácie o konfigurovaní služby sieťovej autentifikácie v spojení s EIM na vytvorenie prostredia s jednoduchým prihlásením.
- Adresárový server (LDAP) (približne 1700 KB) obsahuje informácie o konfigurovaní servera LDAP, ktorý môžete použiť ako radič domény EIM, spolu s informáciami o rozšírenej konfigurácii LDAP.

Ukladanie súborov PDF

Ak chcete za účelom zobrazenia alebo tlače prevziať súbor PDF do vašej pracovnej stanice:

1. Otvorte PDF vo vašom prehliadači (kliknite na odkaz hore).
2. V ponuke vášho prehliadača kliknite na **File**.
3. Kliknite na **Save As...**
4. Prejdite do adresára, kam chcete uložiť súbor PDF.
5. Kliknite na tlačidlo **Save**.

Prevzatie programu Adobe Acrobat Reader

Ak potrebujete na prezeranie alebo tlač dokumentov PDF program Adobe Acrobat Reader, môžete si prevziať kópiu z Webovej lokality Adobe (www.adobe.com/prodindex/acrobat/readstep.html) .

Prehľad EIM (Enterprise Identity Mapping)

Dnešné sieťové prostredia sú tvorené komplexnými skupinami systémov a aplikácií, čoho dôsledkom je potreba manažovať viac registrov užívateľov. Práca s viacerými registrami užívateľov rýchlo prerastie do veľkého administratívneho problému, ktorý ovplyvňuje užívateľov, administrátorov a vývojárov aplikácií. Navyše, mnoho spoločností sa snaží bezpečne manažovať autentifikáciu a autorizáciu pre systémy a aplikácie. EIM (Enterprise Identity Mapping) je technológia infraštruktúry IBM @server , ktorá umožňuje administrátorom a vývojárom aplikácií adresovať tento problém jednoduchšie a lacnejšie, než bolo možné v minulosti.

Nasledujúce informácie opisujú problémy, ukazujú aktuálne priemyselné prístupy a vysvetľujú, prečo je riešenie EIM lepšie.

Problém manažovania viacerých registrov užívateľov

Veľa administrátorov manažuje siete, ktoré obsahujú rôzne systémy a servery, pričom každý z nich má vlastný jedinečný spôsob manažovania užívateľov cez rôzne registre užívateľov. V takýchto komplexných sieťach sú administrátori zodpovední za manažovanie identít každého užívateľa a hesiel vo všetkých systémoch. Okrem toho, administrátori musia často synchronizovať tieto identity a heslá a užívatelia sú zaťažení pamätaním si viacerých identít a hesiel a ich neustálou synchronizáciou. Réžia užívateľa a administrátora je v tomto prostredí veľmi veľká. V dôsledku toho musia administrátori namiesto manažovania podniku stráviť veľa drahocenného času odstraňovaním problémov s neúspešnými pokusmi o prihlásenie a prestavovaním zabudnutých hesiel.

Problém manažovania viacerých registrov užívateľov tiež ovplyvňuje vývojárov aplikácií, ktorí chcú poskytovať viacvrstvové alebo heterogénne aplikácie. Vývojári vedia, že zákazníci majú dôležité obchodné údaje rozložené vo viacerých typoch systémov a každý z nich vlastní vlastné registre užívateľov. Okrem toho, vývojári musia vytvoriť vlastné registre užívateľov a súvisiace bezpečnostné sémantiky pre ich aplikácie. Rieši to problém pre vývojára aplikácie, ale zvyšuje to réžiu pre užívateľov a administrátorov.

Aktuálne prístupy

K dispozícii je niekoľko aktuálnych priemyselných prístupov pre riešenie problému manažovania viacerých registrov užívateľov, ale všetky poskytujú len neúplné riešenia. Napríklad LDAP (Lightweight Directory Access Protocol) poskytuje riešenie pre distribuované registre užívateľov. Používanie LDAP (alebo iných obľúbených riešení, napríklad Microsoft Passport) znamená, že administrátori musia manažovať ešte ďalší register užívateľov a bezpečnostnú sémantiku, alebo musia vymieňať existujúce aplikácie, ktoré sa vytvárajú na používanie týchto registrov.

Pri takomto riešení musia administrátori manažovať viac bezpečnostných mechanizmov pre jednotlivé prostriedky, čo zvyšuje réžiu správy a pravdepodobnosť narušenia bezpečnosti. Keď viacero mechanizmov podporuje jeden prostriedok, šanca, že v jednom mechanizme sa zmení autorita a na zmenu v jednej alebo viacerých ďalších

mechanizmov sa zabudne, je oveľa vyššia. Napríklad k narušeniu bezpečnosti môže dôjsť v prípade, ak má užívateľ zakázaný prístup cez jedno rozhranie, ale má povolený prístup cez jedno alebo viac iných rozhraní.

Po dokončení tejto práce administrátori zistia, že nevyriešili celý problém. Vo všeobecnosti, podniky investovali priveľa peňazí do súčasných registrov užívateľov a k nim priradeným bezpečnostným sémantikám, aby bolo použitie tohto riešenia praktické. Vytvorenie ďalšieho registra užívateľov a bezpečnostných sémantík rieši problém pre poskytovateľa aplikácií, ale nerieši problémy užívateľov ani administrátorov.

Ďalším možným riešením je používanie prístupu jednoduchého prihlásenia. K dispozícii je niekoľko produktov, ktoré umožňujú administrátorom manažovať súbory obsahujúce všetky identity a heslá užívateľov. Tento prístup má však niekoľko slabín:

- Adresuje len jeden z problémov užívateľov. Užívatelia sa môžu prihlásiť do viacerých systémov pomocou jednej identity a hesla, ale neodstraňuje to nutnosť, aby užívatelia mali heslá v iných systémoch, ani potrebu manažovať tieto heslá.
- Vzniká nový problém možného narušenia bezpečnosti v dôsledku ukladania hesiel do týchto súborov v normálnom textovom alebo nezašifrovanom tvare. Heslá by sa nikdy nemali ukladať do normálnych textových súborov a nemali by byť nikomu prístupné, vrátane administrátorov.
- Nerieši to problémy vývojárov aplikácií tretích strán, ktorí poskytujú heterogénne viacvrstvové aplikácie. Pre svoje aplikácie musia naďalej používať vlastné registre užívateľov.

Napriek týmto slabostiam sa niektoré podniky rozhodli pre používanie týchto prístupov, pretože čiastočne riešia problémy viacerých registrov užívateľov.

Prístup EIM

EIM ponúka nový prístup pre lacné budovanie riešení, aby sa dalo ľahšie manažovať viac registrov užívateľov a identít užívateľov v prostredí viacvrstvových, heterogénnych aplikácií. EIM je architektúra opisujúca vzťahy medzi jednotlivcami alebo entitami (akými sú súborové servery a tlačové servery) v podniku a mnohými identitami, ktoré ich v rámci podniku reprezentujú. Okrem toho, EIM poskytuje množinu rozhraní API, ktoré umožňujú aplikáciám zisťovať informácie o týchto vzťahoch.

Napríklad, ak poznáte identitu užívateľa zvolenej osoby v jednom registri užívateľov, môžete určiť, ktorá identita užívateľa v inom registri reprezentuje rovnakú osobu. Ak bol užívateľ autentifikovaný pomocou jednej identity užívateľa a túto identitu užívateľa môžete namapovať na príslušnú identitu v inom registri užívateľov, užívateľ nemusí znovu poskytovať prihlasovacie údaje na autentifikáciu. Viete, kto je tento užívateľ a stačí len vedieť, ktorá identita užívateľa reprezentuje tohto užívateľa v inom registri užívateľov. EIM tak poskytuje zovšeobecnenú funkciu mapovania identít pre podnik.

EIM umožňuje mapovania typu jeden-veľa (inými slovami, jeden užívateľ s viac ako jednou identitou užívateľa v jednom registri užívateľov). Administrátor však nemusí mať konkrétne mapovania jednotlivcov pre všetky identity užívateľov v registri užívateľov. EIM umožňuje aj mapovania typu jeden-viacero (inými slovami, viacerí užívatelia mapovaní na jednu identitu užívateľa v jednom registri užívateľov).

Schopnosť vytvárať mapovanie medzi identitami užívateľa v rôznych registroch užívateľov prináša mnoho výhod. Znamená to hlavne, že aplikácie môžu byť schopné používať jeden register užívateľov na autentifikáciu a zároveň úplne iný register užívateľov na autorizáciu. Administrátor by mohol napríklad mapovať identitu užívateľa Windows v registri Kerberos na užívateľský profil OS/400 v inom registri užívateľov, aby sa dostal k prostriedkom OS/400, na ktoré má užívateľský profil OS/400 oprávnenie.

EIM je otvorená architektúra, ktorú môžu administrátori používať na vytváranie vzťahov mapovania identít pre ľubovoľný register. Nevyžaduje kopírovanie existujúcich údajov do nových archívov ani synchronizáciu oboch kópií. Jediné nové údaje, ktoré zavádza EIM sú informácie o vzťahoch. EIM ukladá tieto údaje do adresára LDAP, čo umožňuje pružné manažovanie údajov na jednom mieste a všade, kde sa tieto informácie používajú, má kópie. Na záver, EIM umožňuje podnikom a vývojárom aplikácií jednoducho pracovať v širšom rozsahu prostredí s menšími nákladmi, než by bolo možné bez tejto podpory.

EIM používané spolu so službou sieťovej autentifikácie, čo je implementácia Kerberos pre OS/400, poskytuje riešenie jednoduchého prihlásenia. Je možné písať aplikácie, ktoré používajú rozhrania API GSS a EIM na akceptovanie lístkov Kerberos a na mapovanie na ďalšiu priradenú identitu užívateľa v inom registri užívateľov. Priradenie medzi identitami užívateľov, ktoré umožňuje toto mapovanie identít, možno uskutočniť vytvorením priradení identifikátora, ktoré nepriamo priraďujú jednu identitu užívateľa k inej prostredníctvom identifikátora EIM alebo vytvorením priradení politiky, ktoré priamo priraďujú jednu identitu užívateľa v skupine k jednej konkrétnej identite užívateľa.

Používanie mapovania identity vyžaduje, aby administrátori postupovali nasledovne:

1. Nakonfigurovanie domény EIM v sieti. Na vytvorenie radiča domény pre doménu a na nakonfigurovanie prístupu k tejto doméne môžete použiť Sprievodcu konfiguráciou EIM iSeries. Počas použitia tohto sprievodcu sa môžete rozhodnúť, či vytvoríte novú doménu EIM a v lokálnom alebo vzdialenom systéme vytvoríte radič domény. Prípadne, ak doména EIM už existuje, môžete sa rozhodnúť pre použitie existujúcej domény EIM.
2. Zistite, ktorí užívatelia zadefinovaní pre adresárový server, ktorý je hostiteľom radiča domény EIM, môžu manažovať alebo sa dostať ku konkrétnym informáciám v doméne EIM a zaraďte ich do príslušných skupín riadenia prístupu k EIM.
3. Vytvorte definície registra EIM pre tie registre užívateľov, ktoré budú patriť do domény EIM. Napriek tomu, že do domény EIM môžete zadefinovať akýkoľvek register užívateľov, musíte zadefinovať registre užívateľov pre aplikácie a operačné systémy s podporou pre EIM.
4. Podľa vašich požiadaviek na implementáciu EIM určite, ktoré z nasledujúcich úloh treba vykonať na nakonfigurovanie vášho EIM:
   - Vytvorenie identifikátorov EIM pre každého jedinečného užívateľa v doméne a vytvorenie priradení identifikátora pre týchto užívateľov.
   - Vytvorenie priradení politiky.
   - Vytvorenie ich kombinácie.

Viac informácií o konfigurovaní a používaní EIM na vytvorenie prostredia jednoduchého prihlásenia kvôli maximalizácii výhod zníženého manažovania hesiel nájdete v Jednoduché prihlásenie v Informačnom centre iSeries.

Scenáre Enterprise Identity Mapping

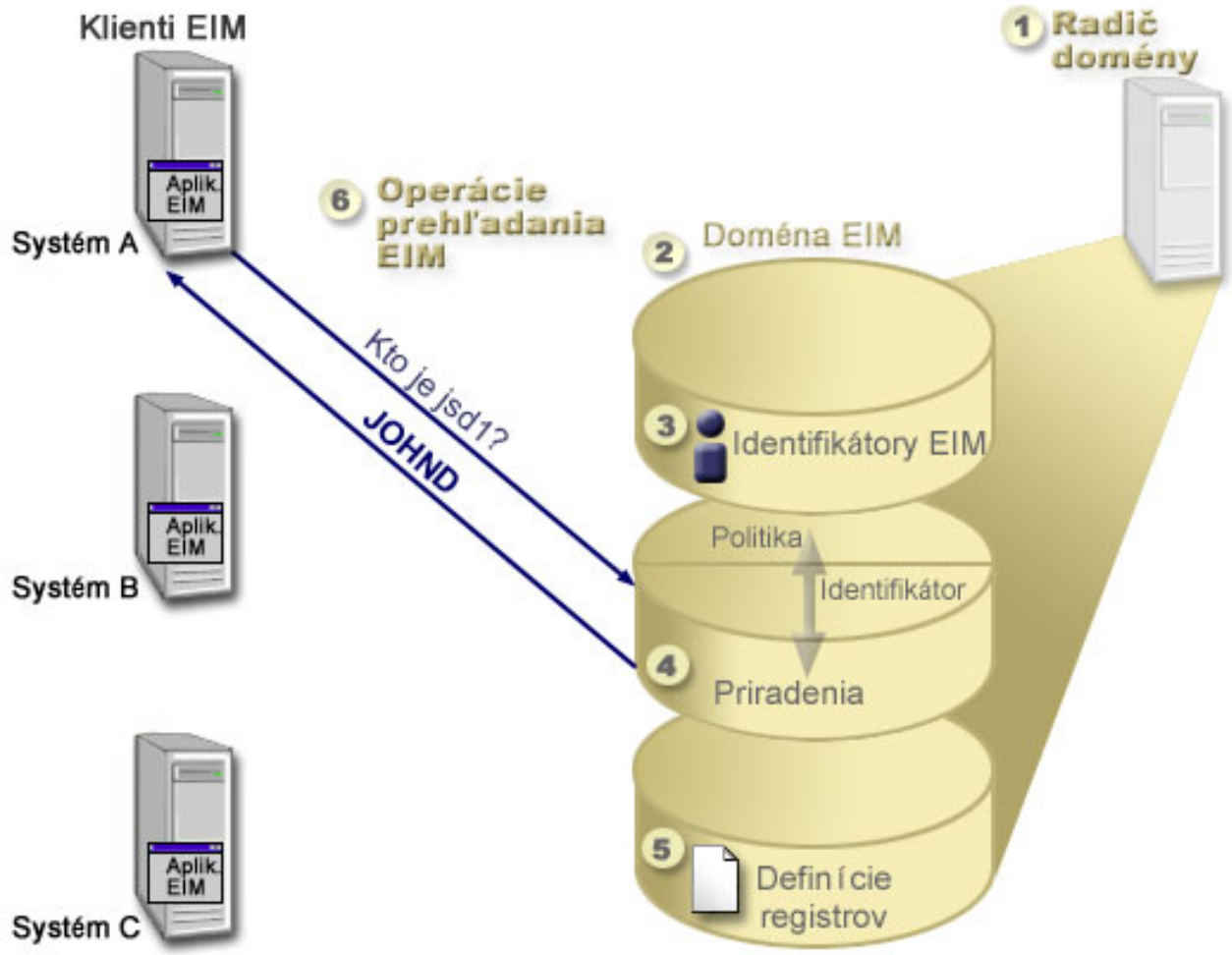
EIM (Enterprise Identity Mapping) je technológia infraštruktúry IBM, ktorá vám umožní sledovanie a manažovanie identít užívateľov v podniku. EIM zvyčajne používate spolu s technológiou autentifikácie, napríklad služba sieťovej autentifikácie, na implementovanie prostredia s jednoduchým prihlásením.

Ak sa zaujímate o širšie použitie EIM, mali by ste si pozrieť časť Scenár v téme Jednoduché prihlásenie v Informačnom centre.

Koncepty Enterprise Identity Mapping

Konceptuálne pochopenie spôsobu fungovania EIM (Enterprise Identity Mapping) je potrebné pre úplné pochopenie spôsobu možného využitia EIM vo vašom podniku. Hoci sa môžu nastavenia a implementácia rozhraní API EIM líšiť podľa platformy servera, koncepty EIM sú spoločné pre platformy IBM @server .

Obrázok 1 poskytuje príklad implementácie EIM v podniku. Tri servery vystupujú ako klienti EIM a obsahujú aplikácie podporujúce EIM, ktoré získavajú údaje EIM prostredníctvom operácií prehľadania EIM 6 . Radič domény 1 obsahuje informácie o doméne EIM 2 , vrátane identifikátora EIM 3 , priradení 4 medzi týmito identifikátormi EIM a identitami užívateľov, a definície registrov EIM 5 .



Obrázok 1. Príklad implementácie EIM

Ak sa chcete dozvedieť viac o týchto konceptoch EIM @server , pozrite si nasledujúce informácie:

- "Radič domény EIM"
- "Doména EIM" na strane 7
- "Identifikátor EIM" na strane 9
- "Definície registrov EIM" na strane 12
- "Priradenia EIM" na strane 16
- "Operácie prehľadania EIM" na strane 25
- "Enterprise Identity Mapping: Podpora a povolenie politiky mapovania" na strane 32
- "Riadenie prístupu EIM" na strane 33

Ak sa chcete dozvedieť viac o ďalších súvisiacich konceptoch, ktoré sú dôležité pre pochopenie použitia EIM, pozrite si nasledujúce informácie:

- "Koncepty LDAP pre EIM" na strane 39
- "Koncepty iSeries pre Enterprise Identity Mapping" na strane 41

Radič domény EIM

Radič domény EIM je server LDAP (Lightweight Directory Access Protocol), ktorý je nakonfigurovaný na riadenie jednej alebo viacerých domén EIM. *Doména EIM* je adresár LDAP, ktorý obsahuje všetky identifikátory EIM,

priradenia EIM a registre užívateľov, ktoré sú definované v danej doméne. Systémy (klienti EIM) sú spojené s doménou EIM tým, že používajú údaje domény pre operácie prehľadania EIM.

Aktuálne môžete nakonfigurovať adresárový server IBM v rovnakých platformách IBM @server tak, aby fungoval ako radič domény EIM. Klientom domény EIM môže byť ľubovoľný klient, ktorý podporuje rozhrania API EIM. Tieto klientske systémy používajú rozhrania API EIM na kontaktovanie radiča domény EIM, aby vykonali "Operácie prehľadania EIM" na strane 25. Umiestnenie klienta EIM určuje, či je radič domény EIM lokálny alebo vzdialený systém. Radič domény je *lokálny*, ak je klient EIM spustený v rovnakom systéme ako radič domény. Radič domény je *vzdialený*, ak je klient EIM spustený v inom systéme ako radič domény.

| **Poznámka:** Adresárový server, ktorý plánujete konfigurovať vo vzdialenom systéme, musí poskytovať podporu EIM.
| EIM vyžaduje, aby bol radič domény hosťovaný adresárovým serverom, ktorý podporuje LDAP (Lightweight Directory
| Access Protocol) verzia 3. Navyše, adresárový server musí byť nakonfigurovaný tak, aby akceptoval schému EIM. IBM
| Directory Server for iSeries a IBM Directory Server V5.1 poskytuje túto podporu.

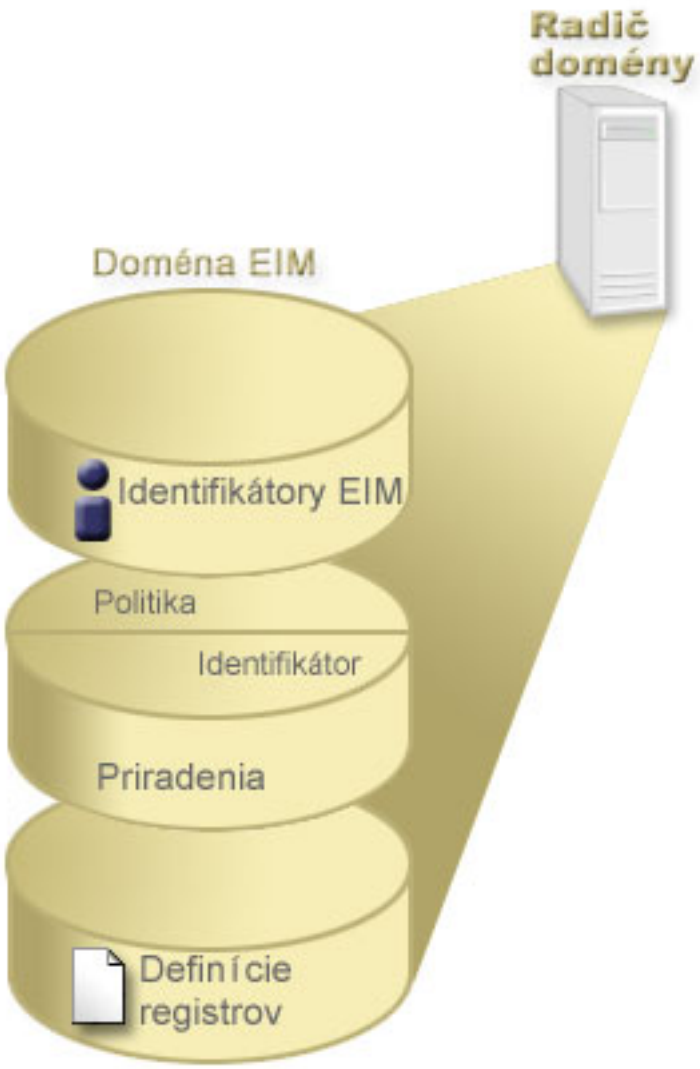
Doména EIM

Doména EIM je adresár v serveri LDAP (Lightweight Directory Access Protocol), ktorý obsahuje údaje EIM pre podnik. Doména EIM je kolekcia všetkých identifikátorov EIM, priradení EIM a registrov užívateľov, ktoré sú definované v tejto doméne a taktiež riadenia prístupu pre údaje. Systémy (klienti EIM) sú spojené s doménou tým, že používajú údaje domény pre operácie prehľadania EIM.

Doména EIM sa odlišuje od registra užívateľov. Register užívateľov definuje množinu identít užívateľov, ktoré konkrétna inštancia operačného systému alebo aplikácie pozná a dôveruje im. Register užívateľov tiež obsahuje informácie potrebné na autentifikáciu užívateľa danej identity. Navyše, register užívateľov často obsahuje iné atribúty, napríklad užívateľské preferencie, systémové privilégiá alebo osobné informácie pre danú identitu.

Naopak, doména EIM *používa* identity užívateľov, ktoré sú definované v registroch užívateľov. Doména EIM obsahuje informácie o *vzťahoch* medzi identitami v rôznych registroch užívateľov (meno užívateľa, typ registra a inštancia registra) a skutočnými osobami alebo entitami, ktoré sú reprezentované týmito identitami.

Obrázok 2 znázorňuje údaje, ktoré sú uložené v doméne EIM. K týmto údajom patria identifikátory EIM, definície registrov EIM a priradenia EIM. Údaje EIM definujú vzťah medzi identitami užívateľov a osobami alebo entitami v podniku, ktoré sú reprezentované týmito identitami.



Obrázok 2. Doména EIM a údaje, ktoré sú uložené v doméne

K údajom EIM patria:

- **Definície registra EIM.** Každá definícia registra EIM, ktorú vytvoríte, reprezentuje aktuálny register užívateľov (a obsahuje informácie o identite užívateľa), ktorý existuje v systéme v podniku. Keď zadefinujete špecifický register užívateľov v EIM, tento register užívateľov sa môže zaradiť do domény EIM. Môžete vytvoriť dva typy definícií registra, jeden typ sa týka systémových registrov užívateľov a druhý sa týka registrov užívateľov aplikácie. Viac informácií nájdete v časti “Definície registrov EIM” na strane 12.
- **Identifikátory EIM.** Každý identifikátor EIM, ktorý vytvoríte, jedinečne reprezentuje osobu alebo entitu (napríklad tlačový server alebo súborový server) v rámci podniku. Identifikátor EIM môžete vytvoriť, keď chcete mať mapovania typu jeden-jeden medzi identitami užívateľa, ktoré patria osobe alebo entite, s ktorou identifikátor EIM korešponduje. Viac informácií nájdete v časti “Identifikátor EIM” na strane 9.
- **Priradenia EIM.** Priradenia EIM, ktoré vytvoríte, reprezentujú vzťahy medzi identitami užívateľa. Priradenia musíte definovať, aby klienti EIM mohli použiť rozhrania API EIM na vykonávanie operácií prehľadania EIM. Tieto operácie prehľadania EIM hľadajú v doméne EIM definované priradenia. Viac informácií nájdete v časti “Operácie prehľadania EIM” na strane 25. Existujú tri rôzne typy priradení, ktoré môžete vytvoriť:
  - **Priradenia identifikátora.** Priradenia identifikátorov vám dovoľujú definovať vzťah typu jeden-jeden medzi identitami užívateľov cez identifikátor EIM, definovaný pre osobu. Každé priradenie identifikátora EIM, ktoré vytvoríte, reprezentuje jediný, špecifický vzťah medzi identifikátorom EIM a pridruženou identitou užívateľa v

rámci podniku. Priradenia identifikátorov poskytujú informácie, ktoré viažu identifikátor EIM k špecifickej identite užívateľa v špecifickom registri užívateľov a dovoľuje vám pre užívateľa vytvárať pripojenia typu jeden-jeden. Priradenia identity sú užitočné hlavne v prípade, keď osoby majú identity užívateľov so špeciálnymi oprávneniami a inými privilégiami, ktoré majú špecificky riadiť vytváranie mapovaní typu jeden-jeden medzi ich identitami užívateľa.

- **Priradenia politiky.** Priradenia politiky vám dovoľujú definovať vzťahy medzi skupinou identít užívateľa v jednom alebo viacerých registroch užívateľov a individuálnou identitou užívateľa v inom registri užívateľov. Každé vytvorenie priradenia politiky EIM vedie k mapovaniu typu veľa-jeden medzi zdrojovou skupinou identít užívateľa v jednom registri užívateľov a jednou cieľovou identitou užívateľa. Zvyčajne vytvárate priradenia politiky na mapovanie skupiny užívateľov, ktorí potrebujú rovnakú úroveň autorizácie k jednej identite užívateľa s danou úrovňou autorizácie.

Potom, ako vytvoríte vaše identifikátory EIM, definície registra a rôzne priradenia, môžete začať používať EIM, aby ste oveľa jednoduchšie organizovali a pracovali s identitami v rámci vášho podniku.

Identifikátor EIM

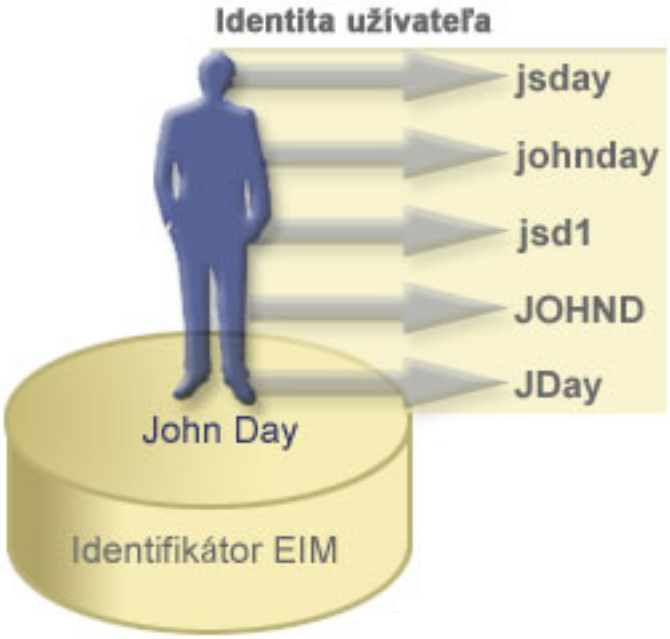
Identifikátor EIM reprezentuje osobu alebo entitu v podniku. Typická sieť obsahuje rôzne hardvérové platformy a aplikácie a k nim priradené registre užívateľov. Väčšina platforiem a veľa aplikácií používa registre užívateľov, špecifické pre platformu alebo aplikáciu. Tieto registre užívateľov obsahujú všetky identifikačné informácie užívateľov pre užívateľov, ktorí pracujú s týmito servermi alebo aplikáciami.

EIM môžete použiť na vytvorenie jedinečných identifikátorov EIM pre osoby alebo entity vo vašom podniku. Potom môžete vytvárať priradenia identifikátorov alebo mapovania identít typu jeden-jeden medzi identifikátorom EIM a rôznymi identitami užívateľov pre osobu alebo entitu, ktorú reprezentuje identifikátor EIM. Tento proces uľahčuje vytváranie heterogénnych, viacvrstvových aplikácií. Uľahčí sa aj vytváranie a používanie nástrojov, ktoré zjednodušujú správu súvisiacu s manažovaním každej identity užívateľa, ktorú má osoba alebo entita v rámci podniku.

Identifikátor EIM, reprezentujúci osobu

Obrázok 3 znázorňuje príklad identifikátora EIM, ktorý reprezentuje osobu pomenovanú *John Day* a jeho rôzne identity užívateľa v podniku. V tomto príklade má osoba *John Day* päť identít užívateľa v štyroch rozličných registroch užívateľov: johnday, jsd1, JOHND, jsday a JDay.

Obrázok 3: Vzťah medzi identifikátorom EIM pre *John Day* a jeho rôzne identity užívateľa

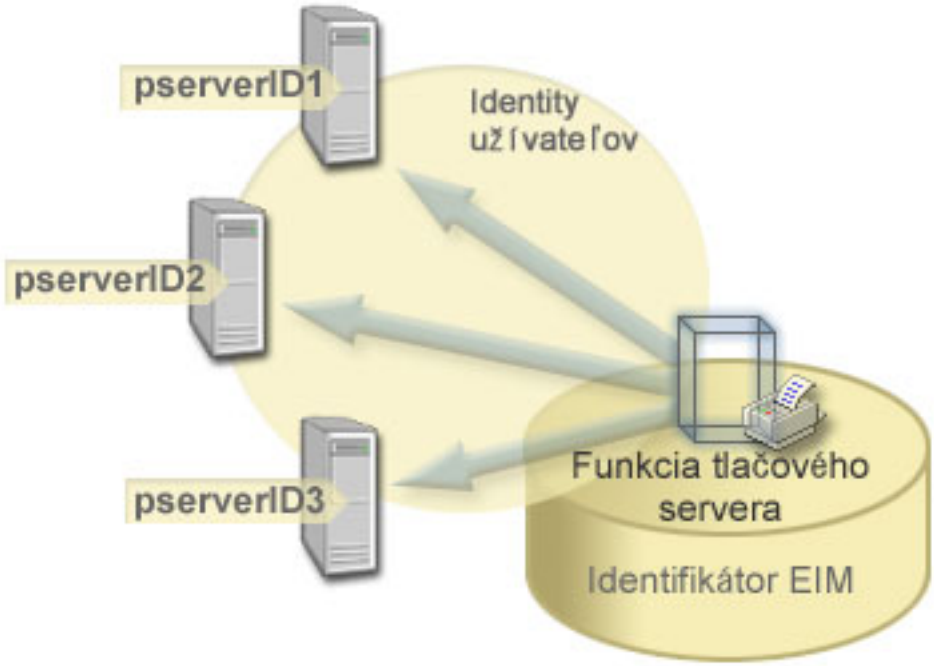


V EIM môžete vytvoriť priradenia, ktoré definujú vzťahy medzi identifikátorom John Day a každou z rôznych identít užívateľa pre *John Day*. Vytvorením týchto priradení na zadefinovanie týchto vzťahov môžete vy a ostatní písať aplikácie, ktoré používajú rozhrania API EIM na vyhľadanie potrebnej, ale neznámej identity užívateľa na základe známej identity užívateľa.

Identifikátor EIM, reprezentujúci entitu

Okrem reprezentácie užívateľov môžu identifikátory EIM reprezentovať entity vo vašom podniku, ako znázorňuje Obrázok 4. Napríklad funkcia tlačového servera v podniku prebieha vo viacerých systémoch. Na Obrázku 4 funkcia tlačového servera v podniku prebieha v troch odlišných systémoch pod tromi odlišnými identitami užívateľov: pserverID1, pserverID2 a pserverID3.

Obrázok 4: Vzťah medzi identifikátorom EIM, ktorý reprezentuje funkciu tlačového servera a rôzne identity užívateľov pre túto funkciu



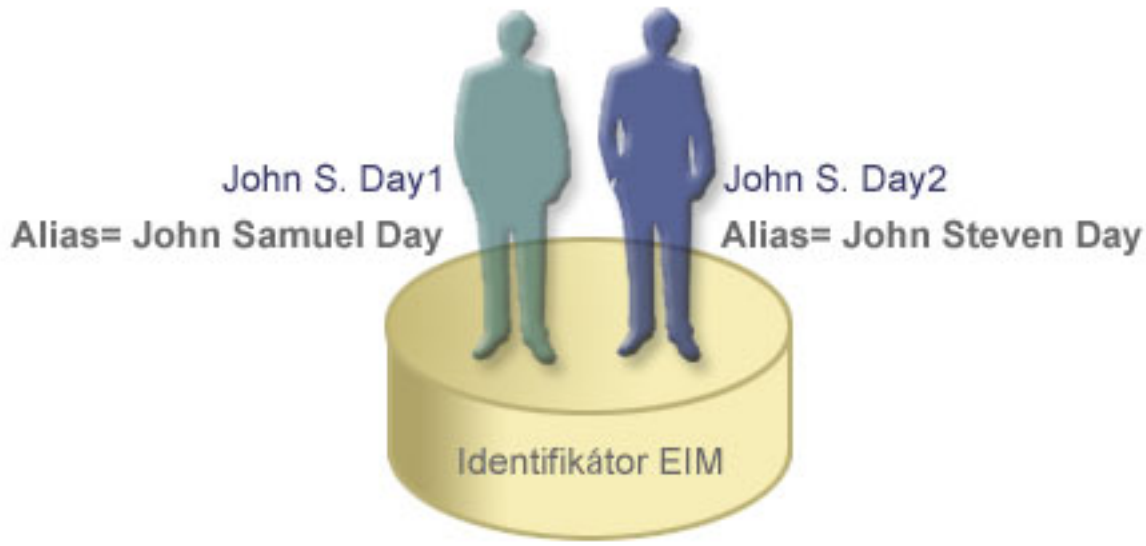
Pomocou EIM môžete vytvoriť jeden identifikátor, ktorý reprezentuje funkciu tlačového servera v celom podniku. Ako ukazuje príklad, identifikátor EIM Funkcia tlačového servera reprezentuje aktuálnu entitu funkcie tlačového servera v podniku. Na zadefinovanie vzťahu medzi identifikátorom EIM (Funkcia tlačového servera) a každou identitou užívateľa pre túto funkciu (pserverID1, pserverID2 a pserverID3) sa vytvárajú priradenia. Tieto priradenia umožňujú vývojárom aplikácií používať operácie prehľadania EIM na nájdenie špecifickej funkcie tlačového servera. Poskytovatelia aplikácií môžu písať distribuované aplikácie, ktoré manažujú funkciu tlačového servera v podniku oveľa jednoduchšie.

Identifikátory EIM a používanie aliasov

Názvy identifikátorov EIM musia byť jedinečné v doméne EIM. Aliasy môžu pomáhať riešiť situácie, pri ktorých môže byť použitie jedinečných názvov identifikátorov obtiažne. Príkladom užitočnosti aliasov identifikátorov EIM sú situácie, keď sa platné meno osoby odlišuje od mena, pod ktorým je táto osoba známa. Napríklad odlišné osoby v podniku môžu mať rovnaké meno, čo môže spôsobiť problémy, ak ako identifikátory EIM používate mená.

Obrázok 5 znázorňuje príklad, v ktorom má podnik dvoch užívateľov s menom *John S. Day*. Administrátor EIM vytvorí dva odlišné identifikátory EIM, aby ich rozlíšil: John S. Day1 a John S. Day2. Na prvý pohľad však nie je zrejmé, ktorý *John S. Day* je reprezentovaný každým z týchto identifikátorov.

Obrázok 5: Aliasy pre dva identifikátory EIM podľa zdieľaného vlastného mena *John S. Day*



Pomocou aliasov môže administrátor EIM poskytnúť ďalšie informácie o osobe pre každý identifikátor EIM. Každý identifikátor EIM môže mať viac aliasov na určenie, ktorého *John S. Day* reprezentuje daný identifikátor EIM. Napríklad dodatočné aliasy môžu obsahovať číslo zamestnanca, číslo oddelenia, pracovný titul alebo iný rozlišovací atribút. V tomto príklade aliasom pre John S. Day1 môže byť John Samuel Day a aliasom pre John S. Day2 môže byť John Steven Day.

Informácie o aliasoch môžete použiť ako pomôcku pri lokalizovaní konkrétneho identifikátora EIM. Napríklad aplikácia používajúca EIM, môže určiť alias, ktorý použije na vyhľadanie príslušného identifikátora EIM pre túto aplikáciu. Administrátor môže tento alias pridať do identifikátora EIM, takže aplikácia môže pre operácie EIM používať tento alias namiesto jedinečného názvu identifikátora. Aplikácia môže uvádzať tieto informácie, keď na vykonávanie operácií prehľadania EIM používa API eimGetTargetFromIdentifier() (Get EIM Target Identities from the Identifier), aby našla vhodnú identitu užívateľa, ktorú potrebuje.

Definície registrov EIM

Definícia registra EIM je položka v EIM, ktorú vytvoríte, aby reprezentovala aktuálny register užívateľov, ktorý existuje v systéme v podniku. Register užívateľov slúži ako adresár a obsahuje zoznam platných identít užívateľov pre konkrétny systém alebo aplikáciu. Základný register užívateľov obsahuje identity užívateľov a ich heslá. Jedným z príkladov registra užívateľov je register z/OS Security Server Resource Access Control Facility (RACF). Registre užívateľov tiež môžu obsahovať aj iné informácie. Napríklad adresár LDAP (Lightweight Directory Access Protocol) obsahuje prihlasovacie rozlišovacie názvy, heslá a riadenie prístupu k údajom, ktoré sú uložené v LDAP. Iným príkladom bežných registrov užívateľov sú principály v realme Kerberos alebo identity užívateľov v doméne Windows Active Directory a register užívateľských profilov OS/400.

Môžete tiež zadefinovať registre užívateľov, ktoré existujú v iných registroch užívateľov. Niektoré aplikácie používajú podmnožinu identít užívateľov z jednej inštancie registra užívateľov. Napríklad register z/OS Security Server (RACF) môže obsahovať určité registre užívateľov, ktoré sú podmnožinou užívateľov v rámci celkového registra užívateľov RACF. Na modelovanie tohto správania EIM umožňuje administrátorom vytvoriť dva druhy definícií registra EIM:

- Definície systémového registra
- Definície aplikačného registra

Definície registrov EIM poskytujú informácie o registroch užívateľov v podniku. Administrátor zadefinuje tieto registre v EIM zadaním týchto informácií:

- Jedinečný ľubovoľný názov registra EIM. Každá definícia registra reprezentuje špecifickú inštanciu registra užívateľov. Môžete vybrať taký názov definície registra EIM, ktorý vám pomôže identifikovať konkrétnu inštanciu

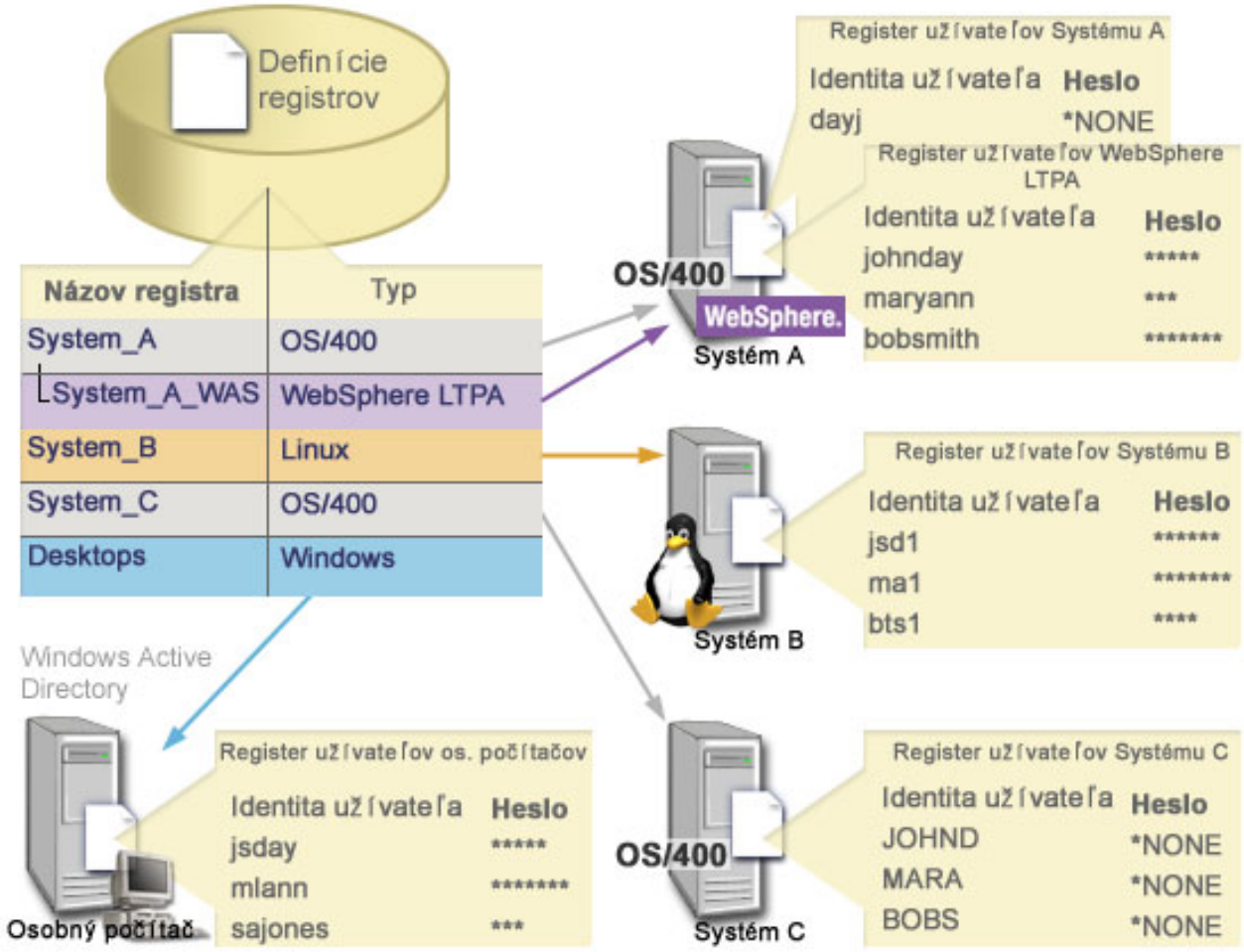
registra užívateľov. Napríklad pre systémový register užívateľov môžete vybrať názov hostiteľa TCP/IP alebo názov hostiteľa skombinovaný s názvom aplikácie pre register užívateľov aplikácie. Môžete použiť ľubovoľnú kombináciu alfanumerických znakov, veľké i malé písmená a medzery na vytvorenie jedinečných názvov definícií registrov EIM.

- Typ registra užívateľov. Existuje viacero preddefinovaných typov registrov užívateľov, ktoré EIM poskytuje na pokrytie väčšiny registrov užívateľov operačného systému. Sú to:
  - AIX
  - Domino - dlhý názov
  - Domino - krátky názov
  - Kerberos
  - Kerberos - rozlišujúci veľkosť písmen
  - LDAP
  - Linux
  - Novell
  - Adresárový server
  - OS/400
  - Tivoli Access Manager
  - RACF
  - Windows - lokálny
  - Windows doména (Kerberos) (Tento typ zohľadňuje veľkosť písmen.)
  - X.509

Poznámka: Hoci preddefinované typy definícií registrov pokrývajú väčšinu registrov užívateľov operačného systému, môžete si vytvoriť definíciu registra, pre ktorú EIM neposkytuje preddefinovaný typ registra. V tejto situácii máte dve možnosti. Môžete použiť existujúcu definíciu registra, ktorá sa zhoduje s charakteristikami vášho registra užívateľov alebo môžete zadefinovať súkromný typ registra užívateľov. Napríklad na obrázku 6 administrátor vykonal požadovaný postup a zadefinoval typ registra WebSphere LTPA pre definíciu registra aplikácie System_A_WAS.

Na obrázku 6 administrátor vytvoril definície systémového registra EIM pre registre užívateľov, reprezentujúce Systém A, Systém B, Systém C a Windows Active Directory, ktoré obsahujú užívateľské principály Kerberos, s ktorými sa užívatelia prihlasujú do svojich pracovných staníc. Okrem toho, administrátor vytvoril definíciu aplikačného registra pre WebSphere (R) Lightweight Third-Party Authentication (LTPA), ktorý sa vykonáva v systéme A. Tento názov definície registra, ktorý administrátor používa, pomáha identifikovať špecifický výskyt tohto typu registra užívateľov. Napríklad adresa IP alebo názov hostiteľa je často dostatočný pre veľa typov registrov užívateľov. V tomto príklade administrátor používa System_A_WAS ako názov definície aplikačného registra na identifikáciu tejto špecifickej inštancie aplikácie WebSphere LTPA . Tiež špecifikuje, že rodičovský systémový register pre definíciu aplikačného registra je register System_A.

Obrázok 6: Definície registra EIM pre päť registrov užívateľov v podniku



Poznámka: Kvôli ďalšiemu zníženiu potreby spravovania hesiel užívateľov administrátor na obrázku 6 nastaví heslá užívateľského profilu OS/400 v systéme A a v systéme C na *NONE. Administrátor v tomto prípade konfiguruje prostredie s jednoduchým prihlásením a jediné aplikácie, s ktorými pracujú jeho užívatelia, sú aplikácie podporujúce EIM, napríklad iSeries Navigator. Ďalej administrátor chce odstrániť heslá z ich užívateľských profilov OS/400, aby užívatelia aj on mali menej hesiel na spravovanie.

Definície registrov EIM a používanie aliasov

Pre definície registrov EIM tiež môžete vytvoriť aliasy. Pre definíciu registra môže byť špecifikovaný jeden alebo viac aliasov. Táto podpora aliasov umožňuje programátorom písať aplikácie bez toho, aby dopredu poznali názov registra EIM, vybratý administrátorom, ktorý nasadzuje danú aplikáciu. Dokumentácia k aplikácii môže administrátorovi EIM oznámiť alias, ktorý používa daná aplikácia. Vďaka tejto informácii môže administrátor priradiť tento alias k definícii registra EIM, reprezentujúcej skutočný register užívateľov, ktorý chce administrátor použiť pre aplikáciu.

Keď administrátor pridá alias do definície registra EIM, aplikácia môže použiť API eimGetRegistryFromAlias() EIM na vykonanie vyhľadania aliasu, aby sa pri inicializácii našiel názov registra EIM. Vyhľadanie aliasu umožňuje aplikácii určiť názov registra EIM alebo názvy, ktoré má použiť ako vstup pre rozhrania API, vykonávajúce operácie prehľadania EIM.

Napríklad aplikácia, ktorá je napísaná na používanie EIM, môže špecifikovať buď alias zdrojového registra alebo alias cieľového registra, alebo aliasy pre oba registre. Keď priradíte tieto aliasy k príslušným definíciám registra, aplikácia môže vykonať vyhľadanie aliasu na nájdenie definície registra EIM alebo definícií, ktoré vyhovujú aliasom v aplikácii. Toto vyhľadanie aliasu zabezpečí, že aplikácia použije register užívateľov alebo registre užívateľov, ktoré chce použiť administrátor. V závislosti od požiadaviek aplikácie môže administrátor priradiť viaceré aliasy jednej definícii registra.

Keď špecifikujete alias pre definíciu registra, musíte špecifikovať typ a názov pre tento alias. Môžete použiť preddefinované typy aliasov, alebo môžete zadefinovať vlastné typy aliasov. K preddefinovaným typom aliasov patria:

- Názov hostiteľa DNS (Domain Name System)
- Realm Kerberos
- Rozlišovací názov (DN) vydavateľa
- Koreňový rozlišovací názov (DN)
- Adresa TCP/IP
- Názov hostiteľa LDAP DNS
- Iné

Alias nemusí byť v špecifickom formáte. Pre typ môžete zadať hodnotu podľa vášho výberu.

Aplikácia môže napríklad špecifikovať, že administrátor priradí alias s typom appl a názov aliasu zdrojový register. Táto aplikácia môže potom používať API eimGetRegistryNameFromAlias() a špecifikovať typ aliasu a názov pre API na získanie registra užívateľov, ktorý aplikácia potrebuje.

Definície systémového registra

Definícia systémového registra je položka, ktorú vytvoríte v EIM na reprezentovanie a opísanie odlišných registrov užívateľov v rámci pracovnej stanice alebo servera. Definíciu systémového registra EIM pre register užívateľov môžete vytvoriť, ak má register v podniku jednu z nasledujúcich čŕt:

- Register poskytuje operačný systém, napríklad AIX, OS/400 alebo produkt na manažovanie bezpečnosti, napríklad z/OS Security Server Resource Access Control Facility (RACF).
- Register obsahuje identity užívateľov, ktoré sú jedinečné pre špecifickú aplikáciu, napríklad Lotus Notes.
- Tento register obsahuje distribuované identity užívateľov, napríklad princípály Kerberos alebo rozlišovacie názvy LDAP (Lightweight Directory Access Protocol).

Operácie prehľadania EIM sa vykonajú správne bez ohľadu na to, či administrátor EIM zadefinuje register ako systémový alebo aplikačný. Samostatné definície registrov však dovoľujú manažovanie mapovacích údajov pre jednotlivé aplikácie. Zodpovednosť za manažovanie mapovaní špecifických pre aplikáciu sa môže priradiť administrátorovi špecifického registra.

Definície registra aplikácií

Definícia registra aplikácií je položka v EIM, ktorú vytvoríte za účelom opísať a reprezentovať podmnožinu identít užívateľov, ktoré sú definované v systémovom registri. Tieto identity užívateľov zdieľajú spoločnú množinu atribútov alebo charakteristík, ktoré im umožňujú použiť konkrétnu aplikáciu alebo množinu aplikácií. Definície registra aplikácií reprezentujú registre užívateľov, ktoré existujú v rámci iných registrov užívateľov. Napríklad register z/OS Security Server (RACF) môže obsahovať určité registre užívateľov, ktoré sú podmnožinou užívateľov v rámci celkového registra užívateľov RACF. Kvôli tomuto vzťahu, musíte zadať pre každú definíciu registra aplikácií, ktorú vytvoríte, názov registra rodičovského systému.

Pokiaľ majú identity užívateľa v registri nasledujúce črty, môžete vytvoriť definíciu aplikačného registra EIM pre register užívateľov:

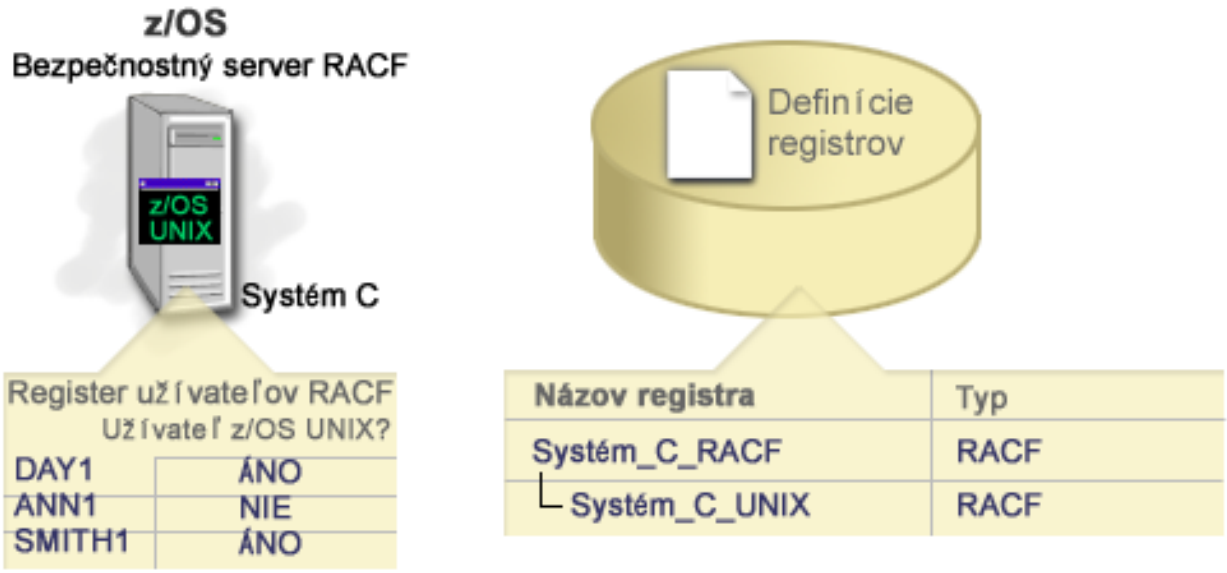
- Identity užívateľa pre aplikáciu nie sú uložené v registri užívateľov, špecifickom pre aplikáciu.
- Identity užívateľa pre aplikáciu sú uložené v systémovom registri, ktorý obsahuje identity užívateľa pre inú aplikáciu.

Operácie prehľadania EIM sa vykonajú správne bez ohľadu na to, či administrátor EIM vytvorí aplikáciu alebo definíciu systémového registra pre register užívateľov. Samostatné definície registrov však dovoľujú manažovanie mapovacích údajov pre jednotlivé aplikácie. Zodpovednosť za manažovanie mapovaní špecifických pre aplikáciu sa môže priradiť administrátorovi špecifického registra.

Napríklad obrázok 7 ukazuje, ako vytvoril administrátor EIM definíciu systémového registra na reprezentovanie registra z/OS Security Server RACF. Administrátor tiež vytvoril definíciu registra aplikácií na reprezentovanie identít

užívateľov v rámci registra RACF, ktorý používa z/OS(TM) UNIX systémové služby (z/OS UNIX). Systém C obsahuje register užívateľov RACF, ktorý obsahuje informácie pre tri identity užívateľov, DAY1, ANN1 a SMITH1. Dve z týchto identít užívateľov DAY1 a SMITH1) pristupujú z/OS UNIX k systému C. Tieto identity užívateľov sú vlastne užívatelia RACF s jedinečnými atribútmi, ktoré ich identifikujú ako užívateľov z/OS UNIX. V rámci definícii registrov EIM definoval administrátor EIM System_C_RACF na reprezentovanie celkového registra užívateľov RACF. Administrátor tiež definoval System_C_UNIX na preprezentovanie identít, ktoré majú atribúty z/OS UNIX.

Obrázok 7: Definície registrov EIM pre register užívateľov RACF a pre užívateľov z/OS UNIX



Priradenia EIM

Priradenie EIM je položka, ktorú vytvárate v doméne EIM na definovanie vzťahu medzi identitami užívateľa a rôznymi registrami užívateľov. Typ priradenia ktoré vytvárate závisí od toho, či je definovaný vzťah priamy alebo nepriamy. V EIM môžete vytvoriť dva typy priradení: priradenia identifikátora a priradenia politiky. Priradenia politiky môžete použiť namiesto alebo v kombinácií s priradeniami identifikátora. Spôsob, akým použijete priradenia závisí na vašom úplnom pláne implementácie EIM.

Ak sa chcete dozvedieť viac o práci s priradeniami, pozrite si nasledujúce informácie:

- Priradenia identifikátora
  Dozviete sa, ako používať priradenia identifikátorov na opis vzťahov medzi identifikátorom EIM a identitami užívateľov v registroch užívateľov, ktoré reprezentujú danú osobu. Priradenie identifikátora vytvára priame mapovanie typu jeden-jeden medzi identifikátorom EIM a špecifickou identitou užívateľa. Priradenia identifikátorov môžete použiť na nepriame definovanie vzťahu medzi identitami užívateľov pomocou identifikátora EIM.
- Priradenia politiky
  Dozviete sa, ako používať priradenia politiky, na opis vzťahu medzi viacerými identitami užívateľov a jednou identitou užívateľa v registri užívateľov. Priradenia politiky používajú podporu politiky mapovania EIM na vytvorenie mapovaní typu veľa-jeden medzi identitami užívateľov bez toho, aby vyžadovali identifikátor EIM.
- Informácie na vyhľadanie
  Dozviete sa, ako používať tieto voliteľné údaje na ďalšiu identifikáciu cieľovej identity užívateľa, ktorú rozhrania API EIM môžu použiť počas operácie vyhľadávania mapovania na ďalšie uspresnenie hľadania cieľovej identity užívateľa, ktorá je objektom operácie.

Priradenia identifikátorov

Identifikátor EIM predstavuje konkrétnu osobu alebo entitu v podniku. Priradenie identifikátora EIM opisuje vzťah medzi identifikátorom EIM a jednou identitou užívateľa v registri užívateľov, ktorá takisto predstavuje túto osobu. Keď vytvoríte priradenia medzi identifikátorom EIM a všetkými identitami užívateľa danej osoby alebo entity, vytvoríte jeden úplný opis spôsobu, akým táto osoba alebo entita používa prostriedky v podniku.

Identity užívateľov sa môžu používať na autentifikáciu, autorizáciu alebo na oboje. *Autentifikácia* je proces kontroly, či entita alebo osoba preukazujúca identitu užívateľa má právo používať danú identitu. Kontrola sa často vykonáva požiadaním osoby poskytujúcej identitu o zadanie tajných alebo súkromných informácií priradených k danej identite užívateľa, napríklad heslo. *Autorizácia* je proces zaistenia, že správne autentifikovaná identita užívateľa môže vykonať len funkcie alebo pristúpiť k prostriedkom, na ktoré má daná identita udelené privilégiá. V minulosti museli takmer všetky aplikácie na autentifikáciu aj autorizáciu používať identity v jednom registri užívateľov. Pomocou operácií prehľadania EIM môžu aplikácie používať identity v jednom registri užívateľov na autentifikáciu a priradené identity užívateľov v inom registri užívateľov na autorizáciu.

Identifikátor EIM poskytuje nepriame priradenie medzi takými identitami užívateľov, ktoré umožňujú aplikáciám nájsť na základe známej identity užívateľa inú identitu užívateľa pre identifikátor EIM. EIM poskytuje rozhrania API, ktoré umožňujú aplikáciám vyhľadať neznámu identitu užívateľa v špecifickom (cieľovom) registri užívateľov, ak poznajú identitu užívateľa v niektorom inom (zdrojovom) registri užívateľov. Tento proces sa nazýva mapovanie identity.

Pomocou EIM môže administrátor definovať tri rôzne typy priradení, ktoré opisujú vzťah medzi identifikátorom EIM a identitou užívateľa. Priradenia identifikátorov môžu byť tohto typu: zdrojové, cieľové alebo administratívne. Typ priradenia, ktoré vytvoríte, závisí od spôsobu použitia identity užívateľa. Napríklad vytvoríte zdrojové a cieľové priradenia pre tie identity užívateľov, ktoré sa majú zúčastniť operácií vyhľadávania mapovania. Typicky, ak sa identita užívateľa používa na autentifikáciu, vytvoríte pre ňu zdrojové priradenie. Potom vytvoríte cieľové priradenia pre tie identity užívateľov, ktoré sa používajú na autorizáciu.

Skôr ako môžete vytvoriť priradenie identifikátora, musíte najprv vytvoriť príslušný identifikátor EIM a príslušnú definíciu registra EIM pre register užívateľov, obsahujúci priradenú identitu užívateľa. Priradenie definuje vzťah medzi identifikátorom EIM a identitou užívateľa prostredníctvom týchto informácií:

- Názov identifikátora EIM
- Názov identity užívateľa
- Názov definície registra EIM
- Typ priradenia
- Voliteľné: Informácie na vyhľadanie na ďalšiu identifikáciu cieľovej identity užívateľa v cieľovom priradení.

Zdrojové priradenie

Zdrojové priradenie umožňuje použiť identitu užívateľa ako zdroj v operácii prehľadania EIM na nájdenie inej identity užívateľa, ktorá je priradená k rovnakému identifikátoru EIM.

Keď sa identita užívateľa použije na *autentifikáciu*, táto identita užívateľa by mala mať zdrojové priradenie k identifikátoru EIM. Napríklad môžete vytvoriť zdrojové priradenie pre principál Kerberos, pretože táto forma identity užívateľa sa používa na autentifikáciu. Ak chcete zabezpečiť úspešné operácie vyhľadávania mapovaní pre identifikátory EIM, zdrojové a cieľové priradenia sa musia použiť pre jeden identifikátor EIM spoločne.

Cieľové priradenie

Cieľové priradenie umožňuje vrátenie identity užívateľa ako výsledok operácie prehľadania EIM. Identity užívateľov, reprezentujúce koncových užívateľov sú zvyčajne len cieľové priradenia.

Keď sa identita užívateľa použije na *autorizáciu* namiesto autentifikácie, daná identita užívateľa by mala mať cieľové priradenie k identifikátoru EIM. Napríklad môžete vytvoriť cieľové priradenie pre užívateľský profil systému OS/400, pretože táto forma identity užívateľa určuje prostriedky a privilégiá užívateľa v konkrétnom systéme iSeries. Ak chcete

zabezpečiť úspešné operácie vyhľadávania mapovaní pre identifikátory EIM, zdrojové a cieľové priradenia sa musia použiť pre jeden identifikátor EIM spoločne.

Vzťah zdrojového a cieľového priradenia

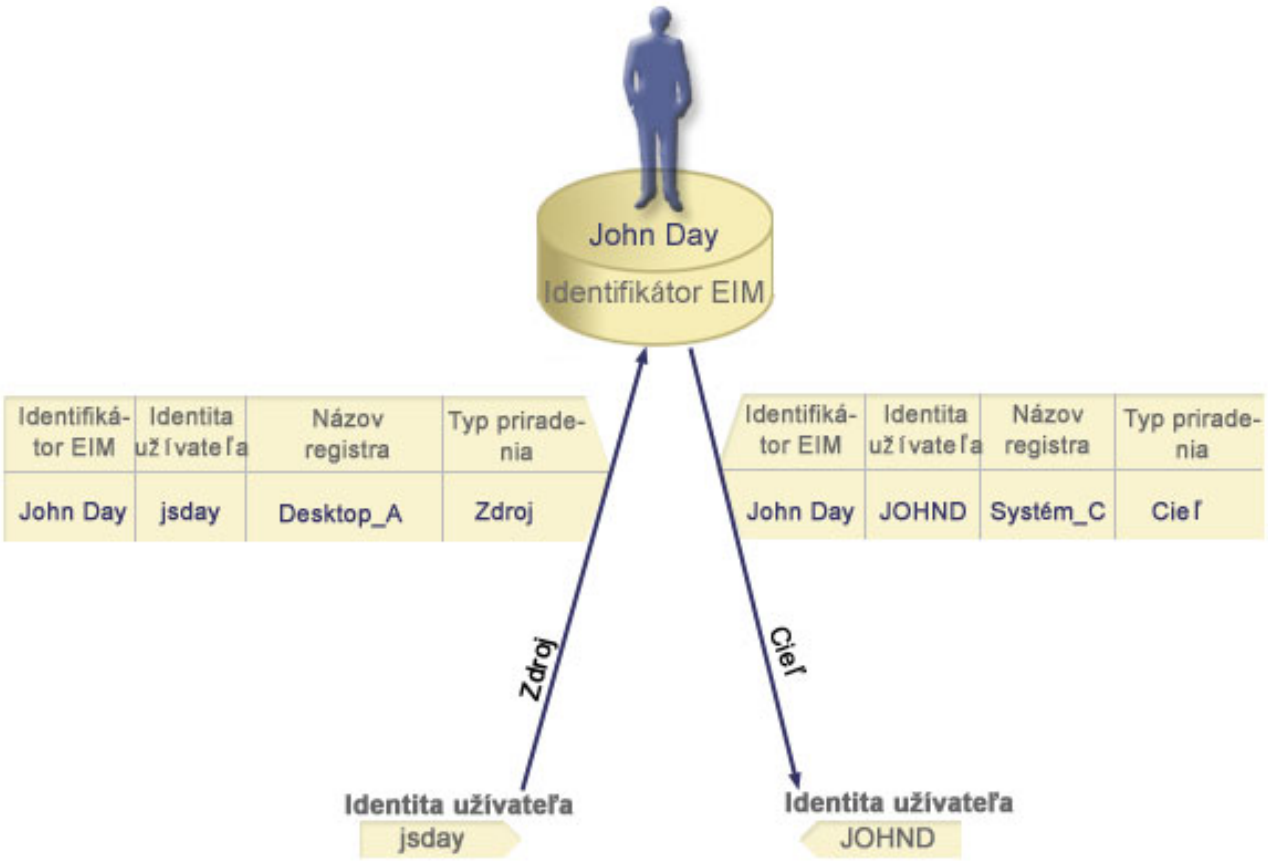
Ak chcete zabezpečiť úspešné operácie vyhľadávania mapovaní, musíte pre jeden identifikátor EIM vytvoriť aspoň jedno zdrojové a jedno alebo viac cieľových priradení. Typicky vytvoríte cieľové priradenie pre každú identitu užívateľa v registri užívateľov, ktorý daná osoba používa na autorizáciu do systému alebo aplikácie, ktorej zodpovedá register užívateľov.

Napríklad užívatelia vo vašom podniku sa bežne prihlasujú a autentifikujú do osobných počítačov so systémom Windows (R) a pristupujú k serveru iSeries, kde vykonávajú množstvo úloh. Užívatelia sa prihlasujú do ich osobných počítačov pomocou principálu Kerberos a do servera iSeries pomocou užívateľského profilu systému OS/400. Chcete vytvoriť prostredie s jednoduchým prihlásením, v ktorom sa užívatelia autentifikujú do ich osobných počítačov pomocou principálu Kerberos a viac sa nemusia manuálne autentifikovať do servera iSeries.

Na splnenie tohto cieľa stačí vytvoriť zdrojové priradenie pre principál Kerberos pre každého užívateľa k identifikátoru EIM užívateľa. Potom vytvoríte cieľové priradenie pre užívateľský profil systému OS/400 každého užívateľa k identifikátoru EIM užívateľa. Táto konfigurácia zabezpečuje, že systém OS/400 môže vykonávať operácie vyhľadávania mapovaní na určenie správneho užívateľského profilu, ktorý je potrebný pre užívateľa pristupujúceho do servera iSeries po autentifikácii do pracovnej plochy. Systém OS/400 potom umožní užívateľovi pristupovať k prostriedkom servera na základe zodpovedajúceho užívateľského profilu bez potreby manuálnej autentifikácie užívateľa do servera.

Obrázok 6 znázorňuje ďalší príklad, kde administrátor EIM vytvoril dve priradenia, zdrojové a cieľové, pre identifikátor EIM John Day na definovanie vzťahu medzi týmto identifikátorom a dvoma priradenými identitami užívateľov. Administrátor vytvoril zdrojové priradenie pre principál Kerberos jsday v registri užívateľov Desktops. Okrem toho vytvoril cieľové priradenie pre užívateľský profil systému OS/400 (R) JOHND v registri užívateľov System_C. Tieto priradenia poskytujú aplikáciám prostriedky na získanie neznámej identity užívateľa (cieľ JOHND) na základe známej identity užívateľa (zdroj jsday) ako časti operácie prehľadania EIM.

Obrázok 6: Cieľové a zdrojové priradenia EIM pre identifikátor EIM John Day



Pre niektorých užívateľov môže byť potrebné vytvoriť aj cieľové aj zdrojové priradenie pre tú istú identitu užívateľa. Je to potrebné, ak niekto používa jeden systém ako klienta aj server, alebo ak dotyčný vystupuje ako administrátor.

Poznámka: Identity užívateľov, ktoré predstavujú obyčajných užívateľov potrebujú za normálnych okolností len cieľové priradenie.

Napríklad administrátor používa funkciu Centrálne riadenie v programe iSeries Navigator na riadenie centrálneho systému a niekoľkých koncových systémov. Vykonáva rozličné funkcie, ktoré môžu mať pôvod v centrálnom alebo v koncovom systéme. V tejto situácii by ste mali vytvoriť aj zdrojové aj cieľové priradenie pre každú jeho identitu užívateľa v každom systéme. Toto zabezpečí, že pri prístupe administrátora do iných systémov z ľubovoľného systému sa identita užívateľa použitá pri vzniku prístupu do iných systémov môže namapovať k príslušnej identite užívateľa pre nasledujúce systémy, ku ktorým bude administrátor pristupovať.

Administratívne priradenie

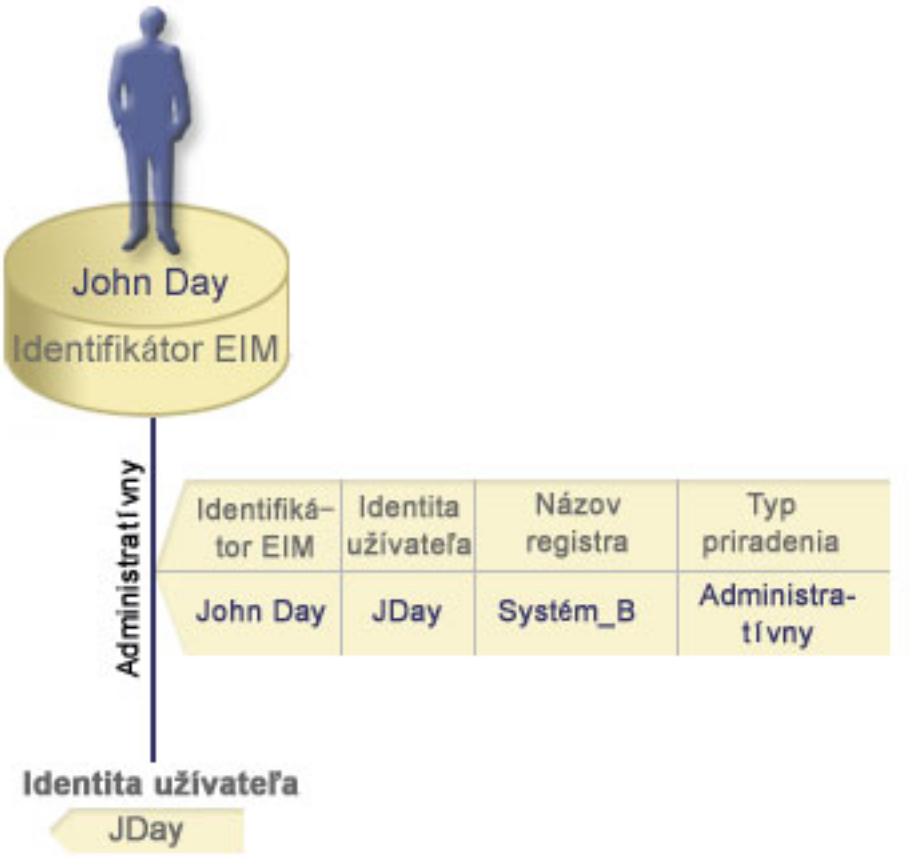
Administratívne priradenie pre identifikátor EIM sa typicky používa na označenie, že osoba alebo entita reprezentovaná daným identifikátorom EIM vlastní identitu užívateľa, ktorá vyžaduje zvláštnu pozornosť v zadanom systéme. Tento typ priradenia sa môže použiť napríklad s veľmi dôležitými registrami užívateľov.

Vzhľadom na špeciálnu povahu administratívnych priradení sa tento typ priradení nemôže zúčastňovať operácií vyhľadávania mapovaní EIM. Operácia prehľadania EIM poskytujúca zdrojovú identitu užívateľa s administratívnym priradením preto nevracia žiadne výsledky. Podobne, identita užívateľa s administratívnym priradením sa nikdy nevráti ako výsledok operácie prehľadania EIM.

Obrázok 7 znázorňuje príklad administratívneho priradenia. V tomto príklade má zamestnanec John Day identitu užívateľa John_Day v systéme A a identitu užívateľa JDay v systéme B, ktorý predstavuje vysoko bezpečný systém.

Administrátor systému chce zaistiť, aby sa užívatelia autentifikovali pre System B len pomocou lokálneho registra užívateľov tohto systému. Administrátor nechce povoliť aplikácii autentifikovať zamestnanca s menom John Day do systému pomocou iného autentifikačného mechanizmu. Použitím administratívneho priradenia pre identitu užívateľa JDay v System B môže administrátor EIM zistiť, že John Day vlastní konto v System B, ale EIM v operáciách prehľadania EIM nevráti žiadne informácie o identite JDay. Aplikácie nenájdu pomocou operácií prehľadania EIM identity užívateľov s administratívnymi priradeniami ani v prípade, ak existujú v tomto systéme.

Obrázok 7: Administratívne priradenie EIM pre identifikátor EIM John Day



Priradenia politiky

Od verzie 5, vydania 3 umožňuje podpora politík mapovania v EIM (Enterprise Identity Mapping) vytvorenie a používanie priradení politiky na definovanie vzťahu medzi viacerými identitami užívateľov v jednom alebo viacerých registroch užívateľov a jednou identitou užívateľa v inom registri užívateľov. Priradenia politiky používajú podporu politík mapovania EIM na vytvorenie mapovaní typu veľa-jeden medzi identitami užívateľov bez použitia identifikátora EIM. Priradenia politiky môžete používať namiesto alebo v kombinácii s priradeniami identifikátorov, ktoré poskytujú mapovania typu veľa-jeden medzi identifikátorom EIM a jednou identitou užívateľa.

Priradenie politiky ovplyvňuje len identity užívateľov, pre ktoré neexistujú konkrétne samostatné priradenia EIM. Ak existujú konkrétne priradenia identifikátorov medzi identifikátorom EIM a identitami užívateľov, aplikácii vykonávajúcej operáciu vyhľadávania sa vráti cieľová identita užívateľa z priradenia identifikátora, aj keď existuje priradenie politiky a priradenia politiky sú povolené. Viac informácií o spôsobe spracovania priradení operáciami vyhľadávania sa môžete dozvedieť v časti “Operácie prehľadania EIM” na strane 25.

Môžete vytvoriť tri rôzne typy priradení politiky:

- Predvolené priradenia politiky domény, ktoré umožňujú vytvorenie vzťahu pomocou mapovania pre všetky identity užívateľov v doméne.

- Predvolené priradenia politiky registrov, ktoré umožňujú vytvorenie vzťahu pomocou mapovania pre všetky identity užívateľov v jednom registri.
- Priradenia politiky filtra certifikátov, ktoré umožňujú vytvorenie vzťahu pomocou mapovania pre množinu identít užívateľov (vo forme digitálnych certifikátov) v jednom registri X.509.

Predvolené priradenia politiky domény: Predvolené priradenie politiky domény predstavuje jeden typ priradenia politiky, ktorý môžete použiť na vytvorenie mapovaní typu veľa-jeden medzi identitami užívateľov. Predvolené priradenie politiky domény môžete použiť na namapovanie zdrojovej množiny viacerých identít užívateľov (v tomto prípade všetkých užívateľov v doméne) k jednej cieľovej identite užívateľa v konkrétnom cieľovom registri užívateľov. Pri predvolenom priradení politiky domény predstavujú všetci užívatelia v doméne zdroj priradenia politiky a sú namapovaní k jednému cieľovému registru a jednej cieľovej identite užívateľa.

Ak chcete používať predvolené priradenie politiky domény, musíte povoliť vyhľadávanie mapovaní pomocou priradení politiky pre doménu. Okrem toho musíte povoliť vyhľadávanie mapovaní pre cieľový register užívateľov priradenia politiky. Po nakonfigurovaní tohto povolenia sa môžu registre užívateľov v priradení politiky zúčastniť na operáciách vyhľadávania mapovaní.

Predvolené priradenie politiky domény nadobudne účinnosť, keď operáciu vyhľadávania mapovaní nesplnia priradenia identifikátorov, priradenia politiky filtra certifikátov ani predvolené priradenia politiky registrov pre cieľový register. Výsledkom je namapovanie všetkých identít užívateľov v doméne k jednej cieľovej identite užívateľa podľa predvoleného priradenia politiky domény.

Napríklad vytvoríte predvolené priradenie politiky domény s cieľovou identitou užívateľa John_Day v cieľovom registri Registry_xyz a zatiaľ ste nevytvorili žiadne priradenia identifikátorov ani iné priradenia politiky, ktoré sú namapované k tejto identite užívateľa. Pri zadaní hodnoty Registry_xyz ako cieľového registra v operáciách vyhľadávania predvolená politika domény zabezpečuje vrátenie cieľovej identity užívateľa John_Day pre všetky identity užívateľov v doméne, ktoré nemajú definované žiadne ďalšie priradenia.

Ak chcete definovať predvolené priradenie politiky domény, musíte zadať nasledujúce dve položky:

- **Cieľový register**. Cieľový register, ktorý zadáte predstavuje názov definície registra EIM (Enterprise Identity Mapping) obsahujúceho identitu užívateľa, na ktorú sú namapované všetky identity užívateľov v doméne.
- **Cieľový užívateľ**. Cieľový užívateľ predstavuje názov identity užívateľa, ktorá sa vráti ako cieľ operácie vyhľadávania mapovaní EIM na základe tohto priradenia politiky.

Predvolené priradenie politiky domény môžete definovať pre každý register v doméne. Ak dve alebo viac priradení politiky domény odkazuje na ten istý cieľový register, musíte pre každé z nich definovať jedinečné informácie na vyhľadanie na zabezpečenie rozlíšiteľnosti pri operáciách vyhľadávania mapovaní. V opačnom prípade môžu operácie vyhľadávania mapovaní vrátiť viacero cieľových identít užívateľov. Následkom týchto nejednoznačných výsledkov môže byť neschopnosť aplikácií spoliehajúcich sa na EIM určiť presnú cieľovú identitu užívateľa, ktorá sa má použiť.

Priradenia politiky sa dajú použiť množstvom prekrývajúcich sa spôsobov a preto by ste mali mať pred vytváraním a používaním priradení politiky dôkladné vedomosti o podpore politiky mapovania a spôsobe práce operácií vyhľadávania.

Predvolené priradenia politiky registrov: Predvolené priradenie politiky registra predstavuje jeden typ priradenia politiky, ktorý môžete použiť na vytvorenie mapovaní typu veľa-jeden medzi identitami užívateľov. Predvolené priradenie politiky registra môžete použiť na namapovanie zdrojovej množiny viacerých identít užívateľov (v tomto prípade sa nachádzajú v jednom registri) k jednej cieľovej identite užívateľa v konkrétnom cieľovom registri užívateľov. Pri predvolenom priradení politiky registra predstavujú všetci užívatelia v jednom registri zdroj priradenia politiky a sú namapovaní k jednému cieľovému registru a cieľovému užívateľovi.

Ak chcete používať predvolené priradenia politiky registrov, musíte povoliť vyhľadávanie mapovaní pomocou priradení politiky pre doménu. Okrem toho musíte povoliť vyhľadávanie mapovaní pre zdrojový register a povoliť vyhľadávanie mapovaní a používanie priradení politiky pre cieľový register užívateľov priradenia politiky. Po nakonfigurovaní tohto povolenia sa môžu registre užívateľov v priradení politiky zúčastniť na operáciách vyhľadávania mapovaní.

Predvolené priradenie politiky registra nadobudne účinnosť, keď operáciu vyhľadávania mapovaní nesplnia priradenia identifikátorov, priradenia politiky filtra certifikátov ani iné predvolené priradenia politiky registrov pre cieľový register. Výsledkom je namapovanie všetkých identít užívateľov v zdrojovom registri k jednej cieľovej identite užívateľa podľa predvoleného priradenia politiky registra.

Napríklad vytvoríte predvolené priradenie politiky registra so zdrojovým registrom my_realm.com, ktorý predstavuje principály v konkrétnom realme Kerberos. Pre toto priradenie politiky takisto zadáte cieľovú identitu užívateľa general_user1 v cieľovom registri os/400_system_reg, ktorý predstavuje konkrétny užívateľský profil v registri užívateľov systému OS/400. V tomto prípade ste nevytvorili žiadne priradenia identifikátorov ani priradenia politiky, týkajúce sa identít užívateľov v zdrojovom registri. Pri zadaní hodnoty os/400_system_reg ako cieľového registra a hodnoty my_realm.com ako zdrojového registra v operáciách vyhľadávania predvolené priradenie politiky registra zabezpečuje vrátenie cieľovej identity užívateľa general_user1 pre všetky identity užívateľov v registri my_realm.com, ktoré nemajú definované žiadne špecifické priradenia identifikátorov ani priradenia politiky filtra certifikátov.

Ak chcete definovať predvolené priradenie politiky registra, musíte zadať nasledujúce tri položky:

- **Zdrojový register**. Predstavuje definíciu registra, ktorú má priradenie politiky používať ako zdroj mapovania. Všetky identity užívateľov v tomto zdrojovom registri užívateľov sa namapujú na zadaného cieľového užívateľa priradenia politiky.
- **Cieľový register**. Cieľový register, ktorý zadáte predstavuje názov definície registra EIM (Enterprise Identity Mapping). Cieľový register musí obsahovať cieľovú identitu užívateľa, na ktorú sa majú namapovať všetky identity užívateľov v zdrojovom registri.
- **Cieľový užívateľ**. Cieľový užívateľ predstavuje názov identity užívateľa, ktorá sa vráti ako cieľ operácie vyhľadávania mapovaní EIM na základe tohto priradenia politiky.

Môžete definovať viac ako jedno predvolené priradenie politiky registra. Ak dve alebo viac priradení politiky s tým istým zdrojovým registrom odkazuje na ten istý cieľový register, musíte definovať jedinečné informácie na vyhľadanie pre každé z týchto priradení politiky na zabezpečenie rozlíšiteľnosti pri operáciách vyhľadávania mapovaní. V opačnom prípade môžu operácie vyhľadávania mapovaní vrátiť viacero cieľových identít užívateľov. Následkom týchto nejednoznačných výsledkov môže byť neschopnosť aplikácií spoliehajúcich sa na EIM určiť presnú cieľovú identitu, ktorá sa má použiť.

Priradenia politiky sa dajú použiť množstvom prekrývajúcich sa spôsobov a preto by ste mali mať pred vytváraním a používaním priradení politiky dôkladné vedomosti o podpore politiky mapovania a spôsobe práce operácií vyhľadávania.

Priradenia politiky filtra certifikátov: Priradenie politiky filtra certifikátov predstavuje jeden typ priradenia politiky, ktorý môžete použiť na vytvorenie mapovaní typu 1 k N medzi identitami užívateľa. Priradenie politiky filtra certifikátov môžete použiť na namapovanie zdrojovej množiny certifikátov k jednej cieľovej identite užívateľa v konkrétnom cieľovom registri užívateľov.

V priradení politiky filtra certifikátov musíte ako jej zdroj zadať množinu certifikátov v jednom registri X.509. Tieto certifikáty sa namapujú k jednému cieľovému registru a k cieľovému užívateľovi, ktorého zadáte. Na rozdiel od predvoleného priradenia politiky registra, kde všetci užívatelia v jednom registri predstavujú zdroj priradenia politiky, rozsah priradenia politiky filtra certifikátov je flexibilnejší. Ako zdroj môžete zadať podmnožinu certifikátov v registri. Filter certifikátov, ktorý zadáte pre priradenie politiky určuje jeho rozsah.

Poznámka: Ak chcete namapovať všetky certifikáty v registri užívateľov X.509 k jednej cieľovej identite užívateľa, vytvorte a použite predvolené priradenie politiky registra.

Ak chcete používať priradenia politiky filtra certifikátov, musíte povoliť vyhľadávanie mapovaní pomocou priradení politiky pre doménu. Okrem toho musíte povoliť vyhľadávanie mapovaní pre zdrojový register a povoliť vyhľadávanie mapovaní a používanie priradení politiky pre cieľový register užívateľov priradenia politiky. Po nakonfigurovaní tohto povolenia sa môžu registre užívateľov v priradení politiky zúčastniť na operáciách vyhľadávania mapovaní.

Ak digitálny certifikát predstavuje zdrojovú identitu užívateľa v operácii vyhľadávania mapovaní EIM (po tom, ako žiadajúca aplikácia použije API EIM eimFormatUserIdentity() na naformátovanie názvu identity užívateľa), EIM najprv skontroluje, či existuje priradenie identifikátora medzi identifikátorom EIM a zadanou identitou užívateľa. Ak neexistuje, EIM porovná informácií o DN v certifikáte s hodnotou DN alebo s čiastočnými informáciami zadanými vo filtri pre priradenie politiky. Ak informácie DN v certifikáte spĺňajú kritérium filtra, EIM vráti cieľovú identitu užívateľa, zadanú priradením politiky. Výsledkom je namapovanie tých certifikátov v zdrojovom registri X.509, ktoré spĺňajú kritérium filtra certifikátov, k jednej cieľovej identite užívateľa podľa priradenia politiky filtra certifikátov.

Napríklad vytvoríte priradenie politiky filtra certifikátov so zdrojovým registrom certificates.x509. Tento register obsahuje certifikáty pre všetkých zamestnancov spoločnosti, vrátane tých, ktoré všetci manažéri v oddelení ľudských zdrojov používajú na prístup k určitým súkromným interným webovým stránkam a k iným prostriedkom prostredníctvom servera iSeries. Pre toto priradenie politiky takisto zadáte cieľovú identitu užívateľa hr_managers v cieľovom registri system_abc, ktorý predstavuje konkrétny užívateľský profil v registri užívateľov systému OS/400. Ak chcete skontrolovať, že toto priradenie politiky pokrýva len certifikáty patriace manažérom ľudských zdrojov, zadajte filter certifikátov s rozlišovacím názvom subjektu (SDN) ou=hrmgr,o=myco.com,c=us.

V tomto prípade ste nevytvorili žiadne priradenia identifikátorov ani ďalšie priradenia politiky filtra certifikátov týkajúce sa identít užívateľov v zdrojovom registri. Pri zadaní hodnoty system_abc ako cieľového registra a hodnoty certificates.x509 ako zdrojového registra v operáciách vyhľadávania zabezpečuje priradenie politiky filtra certifikátov vrátenie cieľovej identity užívateľa hr_managers pre všetky certifikáty v registri certificates.x509, ktoré sa zhodujú so zadaným filtrom certifikátov a ktoré nemajú definované žiadne špecifické priradenia identifikátorov.

Ak chcete definovať priradenie politiky filtra certifikátov, zadajte nasledujúce informácie:

- **Zdrojový register**. Definícia zdrojového registra, ktorú zadáte musí predstavovať register užívateľov typu X.509. Politika filtra certifikátov vytvorí priradenie medzi identitami užívateľov v registri užívateľov X.509 a jednou konkrétnou cieľovou identitou užívateľa. Priradenie sa týka len tých identít užívateľov v registri, ktoré spĺňajú kritérium filtra certifikátov zadaného pre túto politiku.
- **Filter certifikátov**. Filter certifikátov definuje množinu podobných atribútov užívateľských certifikátov. Priradenie politiky filtra certifikátov mapuje certifikáty s týmito definovanými atribútmi v registri užívateľov X.509 ku konkrétnej cieľovej identite užívateľa. Filter zadáte na základe kombinácie rozlišovacieho názvu subjektu (SDN) a rozlišovacieho názvu vydavateľa (IDN), ktorý sa zhoduje s certifikátmi, ktoré chcete použiť ako zdroj mapovania. Filter certifikátov, ktorý zadáte pre politiku, už musí existovať v doméne EIM.
- **Cieľový register**. Definícia cieľového registra, ktorú zadáte predstavuje register užívateľov, obsahujúci identitu užívateľa, na ktorú chcete namapovať certifikáty zhodujúce sa s filtrom certifikátov.
- **Cieľový užívateľ**. Cieľový užívateľ predstavuje identitu užívateľa, ktorá sa vráti ako cieľ operácií vyhľadávania mapovaní EIM na základe tohto priradenia politiky.

Priradenia politiky certifikátov a ostatné priradenia sa dajú použiť množstvom prekrývajúcich sa spôsobov a preto by ste mali mať pred vytváraním a používaním priradení politiky certifikátov dôkladné vedomosti o podpore politiky mapovania EIM a spôsobe práce operácií vyhľadávania.

Filtre certifikátov: Filter certifikátov definuje množinu podobných atribútov certifikátov s rozlišovacím názvom pre skupinu užívateľských certifikátov v zdrojovom registri užívateľov X.509. Filter certifikátov môžete použiť ako základ priradenia politiky filtra certifikátov. Filter certifikátov v priradení politiky určuje, ktoré certifikáty v zadanom zdrojovom registri X.509 sa majú namapovať k zadanému cieľovému užívateľovi. Certifikáty, ktoré majú DN subjektu a vydavateľa, spĺňajúce kritérium filtra sa počas operácií vyhľadávania mapovaní EIM namapujú na zadaného cieľového užívateľova.

Napríklad vytvoríte filter certifikátov s rozlišovacím názvom subjektu (SDN) o=ibm,c=us. Všetky certifikáty s týmito názvami DN, tvoriacimi časť ich informácií SDN spĺňajú kritérium filtra, napríklad certifikát s hodnotou SDN cn=JohnDay,ou=LegalDept,o=ibm,c=us. Ak existuje viac ako jeden filter certifikátov, ktorého kritérium certifikát spĺňa, prioritu má hodnota viac špecifického filtra certifikátov, s ktorým sa certifikát najviac zhoduje. Napríklad máte jeden filter certifikátov s hodnotou SDN o=ibm,c=us a ďalší filter certifikátov s hodnotou SDN ou=LegalDept,o=ibm,c=us. Ak máte v zdrojovom registri X.509 certifikát s hodnotou SDN cn=JohnDay,ou=LegalDept,o=ibm,c=us, použije sa druhý, teda viac špecifický filter certifikátov. Ak máte v

zdrojovom registri X.509 certifikát s hodnotou SDN cn=SharonJones,o=ibm,c=us, použije sa menej špecifický filter certifikátov, pretože certifikát sa najviac zhoduje s jeho kritériom.

Ak chcete definovať filter certifikátov, zadajte jedno alebo oboje z nasledujúceho:

- Rozlišovací názov subjektu (SDN). Úplný alebo čiastočný názov DN, ktorý zadáte pre filter, musí zodpovedať časti DN subjektu v digitálnom certifikáte, ktorý určuje vlastník certifikátu. Môžete poskytnúť úplný reťazec DN subjektu alebo môžete poskytnúť jedno alebo viac čiastočných DN tvoriacich úplné SDN.
- Rozlišovací názov vydavateľa (IDN). Úplný alebo čiastočný názov DN, ktorý zadáte pre filter, musí zodpovedať časti DN vydavateľa v digitálnom certifikáte, ktorý určuje Certifikačná autorita, ktorý vydala certifikát. Môžete poskytnúť úplný reťazec DN vydavateľa alebo môžete poskytnúť jedno alebo viac čiastočných DN tvoriacich úplné IDN.

Existuje niekoľko metód, ktoré môžete použiť na vytvorenie filtra certifikátov, vrátanie použitia rozhrania API Format EIM Policy Filter (eimFormatPolicyFilter()) na vygenerovanie filtrov certifikátov pomocou certifikátu ako šablóny pre vytvorenie potrebných DN v správnom poradí a formáte pre SND a IDN.

Informácie na vyhľadanie

Od verzie V5R3 môžete poskytovať *voliteľné* údaje nazývané informácie na vyhľadanie pre ďalšiu identifikáciu cieľovej identity užívateľa. Táto cieľová identita užívateľa môže byť špecifikovaná buď v priradení identifikátora alebo v priradení politiky. Informácie na vyhľadanie sú jedinečným znakovým reťazcom, ktorý môže buď API eimGetTargetFromSource EIM, alebo API eimGetTargetFromIdentifier EIM používať pri operácii vyhľadávania mapovaní na ďalšie zjemnenie hľadania cieľovej identity užívateľa, ktorá je objektom operácie. Údaje, ktoré špecifikujete pre informácie na vyhľadanie korešpondujú s parametrom dodatočných informácií užívateľov z registra pre tieto rozhrania API EIM.

Informácie vyhľadávania sú potrebné, len keď operácia vyhľadávania mapovaní môže vrátiť viac ako jednu cieľovú identitu užívateľa. Operácia vyhľadávania mapovaní môže vrátiť viaceré cieľové identity užívateľa, keď nastane jedna alebo viac z týchto situácií:

- Identifikátor EIM má viaceré individuálne cieľové priradenia do rovnakého cieľového registra.
- Viac ako jeden identifikátor EIM má rovnakú identita užívateľa špecifikovanú v zdrojovom priradení a každý z týchto identifikátorov EIM má cieľové priradenie do rovnakého cieľového registra, hoci identita užívateľa, špecifikovaná pre každé cieľové priradenie môže byť rôzna.
- Viac ako jedno predvolené priradenie politiky domény špecifikuje rovnaký cieľový register.
- Viac ako jedno predvolené priradenie politiky registra špecifikuje rovnaký zdrojový register a rovnaký cieľový register.
- Viac ako jedno priradenie politiky filtra certifikátov špecifikuje rovnaký zdrojový register X.509, filter certifikátov a cieľový register.

Poznámka: Operácia vyhľadávania mapovaní, ktorá vracia viac ako jednu cieľovú identitu užívateľa môže spôsobiť problémy aplikáciám podporovaných EIM, vrátane aplikácií a produktov OS/400, ktoré nie sú navrhnuté na spracovanie týchto nejednoznačných výsledkov. Avšak základné aplikácie OS/400, ako je iSeries Access for Windows, nemôžu používať informácie na vyhľadanie na rozlišovanie medzi viacerými cieľovými identitami užívateľa vrátenými operáciou vyhľadávania. Ďalej by ste mohli zvážiť predefinovanie priradení pre doménu, aby ste zabezpečili, že operácia vyhľadávania mapovaní vráti jednu cieľovú identitu užívateľa, aby základné aplikácie OS/400 mohli úspešne vykonať operácie vyhľadávania a mapovať identity.

Informácie na vyhľadanie môžete použiť na predídenie situáciám, kde je možné, že operácie vyhľadávania mapovaní vrátia viac ako jednu cieľovú identitu užívateľa. Ak chcete zabrániť operáciám vyhľadávania mapovaní vracať viaceré cieľové identity užívateľa, musíte definovať jedinečné informácie na vyhľadanie pre každú cieľovú identitu užívateľa v každom priradení. Tieto informácie na vyhľadanie musia byť poskytnuté operácii vyhľadávania mapovaní na zaistenie, že operácia môže vrátiť jedinečnú cieľovú identitu užívateľa. Inak aplikácie, ktoré sa spoliehajú na EIM nebudú schopné určiť presnú cieľovú identitu na použitie.

Máte napríklad identifikátor EIM s názvom John Day, ktorý má dva užívateľské profily v systéme A. Jeden z týchto užívateľských profilov je JDUSER v systéme A a druhý je JDSECADM, ktorý má špeciálne oprávnenie administrátora bezpečnosti. Existujú dve cieľové priradenia pre identifikátor John Day. Jedno z týchto cieľových priradení je pre identitu užívateľa JDUSER v cieľovom registri systému A a má zadané informácie na vyhľadanie s oprávnením užívateľa pre JDUSER. Druhé cieľové priradenie je pre identitu užívateľa JDSECADM v cieľovom registri systému A a má zadané informácie na vyhľadanie správcu bezpečnosti pre JDSECADM.

Ak operácia vyhľadávania mapovaní nešpecifikuje žiadne informácie na vyhľadanie, operácia vyhľadávania vráti obe identity užívateľa JDUSER aj JDSECADM. Ak operácia vyhľadávania mapovaní špecifikuje informácie na vyhľadanie oprávnenie užívateľa, operácia vyhľadávania vráti len identitu užívateľa JDUSER. Ak operácia vyhľadávania mapovaní špecifikuje informácie na vyhľadanie správca bezpečnosti, operácia vyhľadávania vráti len identitu užívateľa JDSECADM.

Poznámka: Ak vymažete posledné cieľové priradenie pre identitu užívateľa (či je to priradenie identifikátora alebo priradenie politiky), cieľová identita užívateľa a všetky informácie na vyhľadanie sa tiež vymažú z domény.

Priradenia politiky certifikátov a ostatné priradenia sa dajú použiť množstvom prekrývajúcich sa spôsobov a preto by ste mali mať pred vytváraním a používaním priradení politiky certifikátov dôkladné vedomosti o podpore politiky mapovania EIM a spôsobe práce operácií vyhľadávania.

Operácie prehľadania EIM

Aplikácia alebo operačný systém používa API EIM na vykonávanie *operácie vyhľadávania*, aby aplikácia alebo operačný systém mohol mapovať z jednej identity užívateľa v jednom registri do inej identity užívateľa v inom registri. Operácia prehľadania EIM je proces, prostredníctvom ktorého aplikácia alebo operačný systém vyhľadáva neznámu priradenú užívateľskú identitu v určitom cieľovom registri pomocou niektorých známych a dôveryhodných informácií. Aplikácie používajúce rozhrania API EIM môžu vykonávať tieto operácie prehľadania EIM na informáciách len vtedy, ak sú tieto informácie uložené v doméne EIM. Aplikácia môže vykonať jeden z dvoch typov operácií prehľadania EIM podľa typu informácií, ktoré aplikácia poskytne ako zdroj operácie prehľadania EIM: identita užívateľa alebo identifikátor EIM.

Keď aplikácie alebo operačné systémy používajú API eimGetTargetFromSource() na získanie identity cieľového užívateľa pre daný cieľový register, musia poskytnúť *identitu užívateľa ako zdroj* operácie vyhľadávania. Keď sa má použiť identita užívateľa ako zdroj v operácii prehľadania EIM, musí mať pre ňu definované buď zdrojové priradenie identifikátora, alebo byť pokrytá priradením politiky. Keď aplikácia alebo operačný systém používa toto API, táto aplikácia alebo operačný systém musia poskytnúť tri časti informácií:

- Identitu užívateľa ako zdroj alebo štartovací bod operácie.
- Názov definície registra EIM pre identitu zdrojového užívateľa.
- Názov definície registra EIM, ktorá je cieľom operácie prehľadania EIM. Táto definícia registra opisuje register užívateľov, ktorý obsahuje identitu užívateľa, ktorú aplikácia hľadá.

Keď aplikácie alebo operačné systémy používajú API eimGetTargetFromIdentifier() na získanie identity užívateľa pre daný cieľový register, musia poskytnúť *identifikátor EIM ako zdroj* operácie prehľadania EIM. Keď aplikácia používa toto API, táto aplikácia musí poskytnúť dve časti informácií:

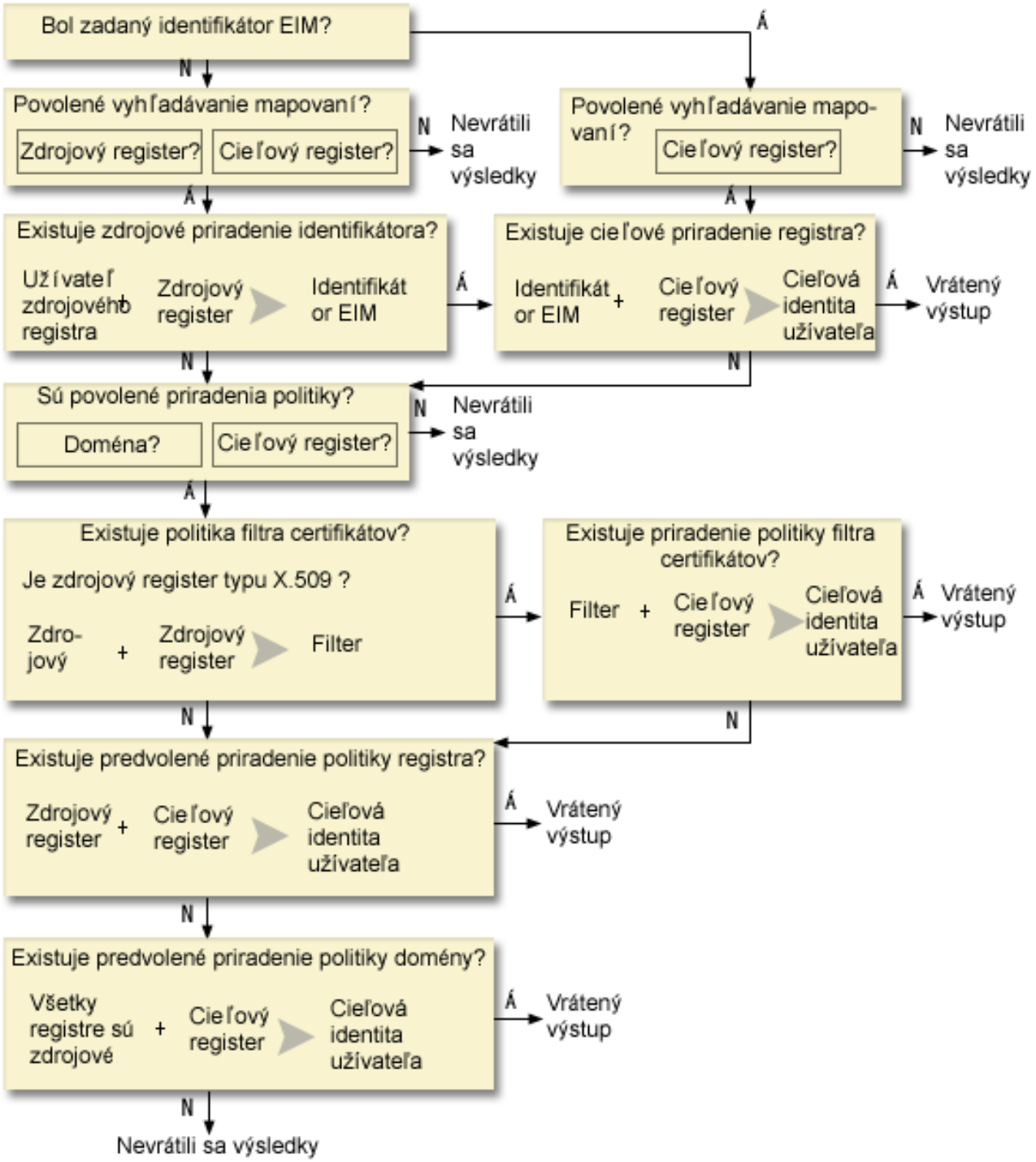
- Identifikátor EIM ako zdroj alebo štartovací bod operácie.
- Názov definície registra EIM, ktorá je cieľom operácie prehľadania EIM. Táto definícia registra opisuje register užívateľov, ktorý obsahuje identitu užívateľa, ktorú aplikácia hľadá.

Ak sa má identita užívateľa vrátiť ako cieľ ľubovoľného typu operácie prehľadania EIM, pre danú identitu užívateľa musí byť definované cieľové priradenie. Toto cieľové priradenie môže mať formu priradenia identifikátora alebo priradenia politiky.

Poskytnuté informácie sú postúpené EIM a operácia prehľadania EIM vyhľadá a vráti všetky cieľové identity užívateľov, pričom prehľadáva údaje EIM v nasledujúcom poradí, ako ilustruje obrázok 10:

1. Cieľové priradenie identifikátora pre identifikátor EIM. Identifikátor EIM je identifikovaný jedným z týchto dvoch spôsobov: Je poskytnutý prostredníctvom API eimGetTargetFromIdentifier(). Alebo je identifikátor EIM určený z informácií poskytnutých prostredníctvom API eimGetTargetFromSource().
2. Priradenie politiky filtra certifikátov.
3. Priradenie politiky štandardného registra.
4. Priradenie politiky štandardnej domény.

Obrázok 10: Základný diagram postupu operácie prehľadania EIM



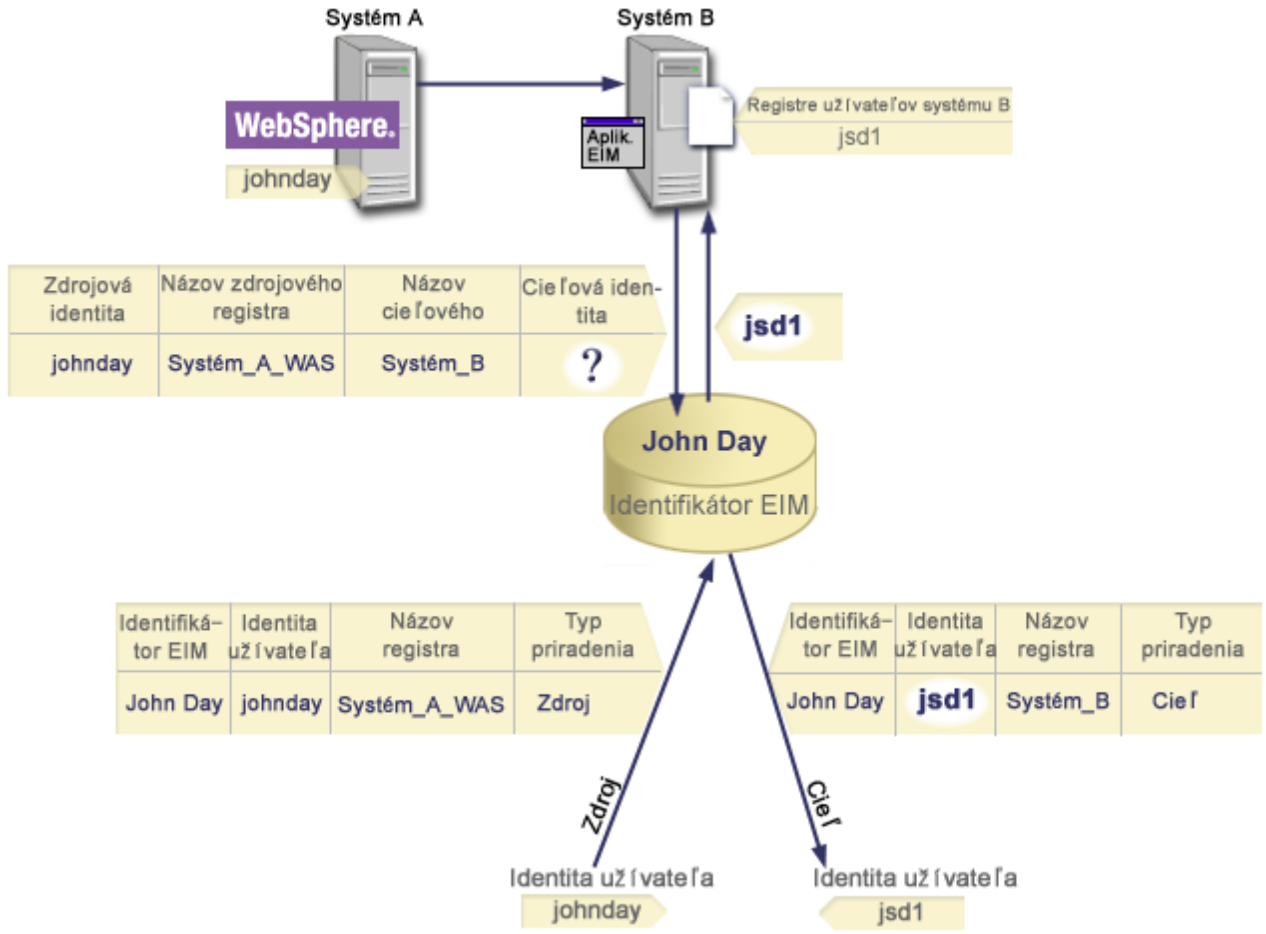
Operácia vyhľadávania prebieha týmto spôsobom:

1. Operácia vyhľadávania skontroluje, či je povolené vyhľadávanie mapovaní. Operácia vyhľadávania určí, či sú povolené vyhľadávanie mapovaní pre určený zdrojový register, určený cieľový register alebo obidva určené registre. Ak nie je vyhľadávanie mapovaní povolené pre jeden alebo oba registre, operácia vyhľadávania skončí bez vrátenia cieľovej identity užívateľa.
2. Operácia vyhľadávania skontroluje, či existujú priradenia identifikátora, ktoré vyhovujú vyhľadávacím kritériám.Ak bol poskytnutý identifikátor EIM, operácia vyhľadávania použije uvedený názov identifikátora EIM. Inak operácia vyhľadávania skontroluje, či existuje zdrojové priradenie konkrétneho identifikátora, ktorý sa zhoduje s dodanou identitou zdrojového užívateľa a zdrojovým registrom. Ak existuje, operácia vyhľadávania ho použije na určenie príslušného názvu identifikátora EIM. Vyhľadávacia operácia potom použije názov identifikátora EIM na vyhľadanie cieľového priradenia identifikátora pre identifikátor EIM, ktorý sa zhoduje s uvedeným názvom definície cieľového registra EIM. Ak existuje cieľové priradenie identifikátora, ktoré sa zhoduje, operácia vyhľadávania vráti cieľovú identitu užívateľa, definovanú v cieľovom priradení.
3. Vyhľadávacia operácia skontroluje, či je povolené použitie priradení politiky. Operácia vyhľadávania skontroluje, či doména umožňuje vyhľadávanie mapovaní pomocou priradení politiky. Vyhľadávacia operácia tiež skontroluje, či je povolený cieľový register na použitie priradení politiky. Ak doména nie je povolená pre priradenia politiky alebo register nie je povolený pre priradenia politiky, operácia vyhľadávania skončí bez vrátenia cieľovej identity užívateľa.
4. Operácia vyhľadávania skontroluje priradenia politiky filtra certifikátov. Operácia vyhľadávania skontroluje, či je zdrojový register registrom typu X.509. Ak je tento register typu X.509, operácia vyhľadávania skontroluje, či existuje priradenie politiky filtra certifikátov, ktoré sa zhoduje s názvami definícií zdrojového a cieľového registra. Operácia vyhľadávania skontroluje, či existujú certifikáty v zdrojovom registri X.509, ktoré spĺňajú kritéria špecifikované v priradení politiky filtra certifikátov. Ak existuje zhodné priradenie politiky a existujú certifikáty, ktoré vyhovujú ktirériám filtra certifikátov, operácia vyhľadávania vráti príslušnú cieľovú identitu užívateľa pre toto priradenie politiky.
5. Operácia vyhľadávania skontroluje predvolené priradenia politiky registra. Operácia vyhľadávania skontroluje, či existuje predvolené priradenie politiky registra, ktoré sa zhoduje s názvami definícií zdrojového a cieľového registra. Ak existuje vhodné priradenie politiky, operácia vyhľadávania vráti príslušnú cieľovú identitu užívateľa pre toto priradenie politiky.
6. Operácia vyhľadávania skontroluje predvolené priradenia politiky domény. Operácia vyhľadávania skontroluje, či je definované predvolené priradenie politiky domény pre definíciu cieľového registra. Ak existuje zhodné priradenia politiky, operácia vyhľadávania vráti priradenú identitu cieľového užívateľa pre toto priradenie politiky.
7. Operácia vyhľadávania nie je schopná vrátiť žiadne výsledky.

Príklady operácie vyhľadávania: Príklad 1

Na obrázku 11 sa identita užívateľa johnday autentifikuje do WebSphere Application Server pomocou Lightweight Third-Party Authentication (LPTA) v systéme A. WebSphere Application Server v systéme A zavolá natívny program v systéme B kvôli prístupu k údajom v systéme B. Natívny program používa API EIM na vykonanie operácie prehľadania EIM, založenej na identite užívateľa v systéme A ako zdroja operácie. Aplikácia poskytne tieto informácie na vykonanie operácie: johnday ako zdrojová identita užívateľa, System_A_WAS ako zdrojový názov definície registra EIM a System_B ako cieľový názov definície registra EIM. Tieto zdrojové informácie sú postúpené do EIM a operácia prehľadania EIM nájde zdrojové priradenie identifikátora, ktoré vyhovuje týmto informáciám. Pomocou názvu identifikátora EIM John Day operácia prehľadania EIM vyhľadá cieľové priradenie identifikátora pre identifikátor, ktorý sa zhoduje s cieľovým názvom definície registra EIM pre System_B. Keď sa nájde vyhovujúce cieľové priradenie, operácia prehľadania EIM vráti aplikácii identitu užívateľa jsd1.

Obrázok 11: Operácia prehľadania EIM vracia cieľovú identitu užívateľa z určitých priradení identifikátora, založených na známej identite užívateľa johnday



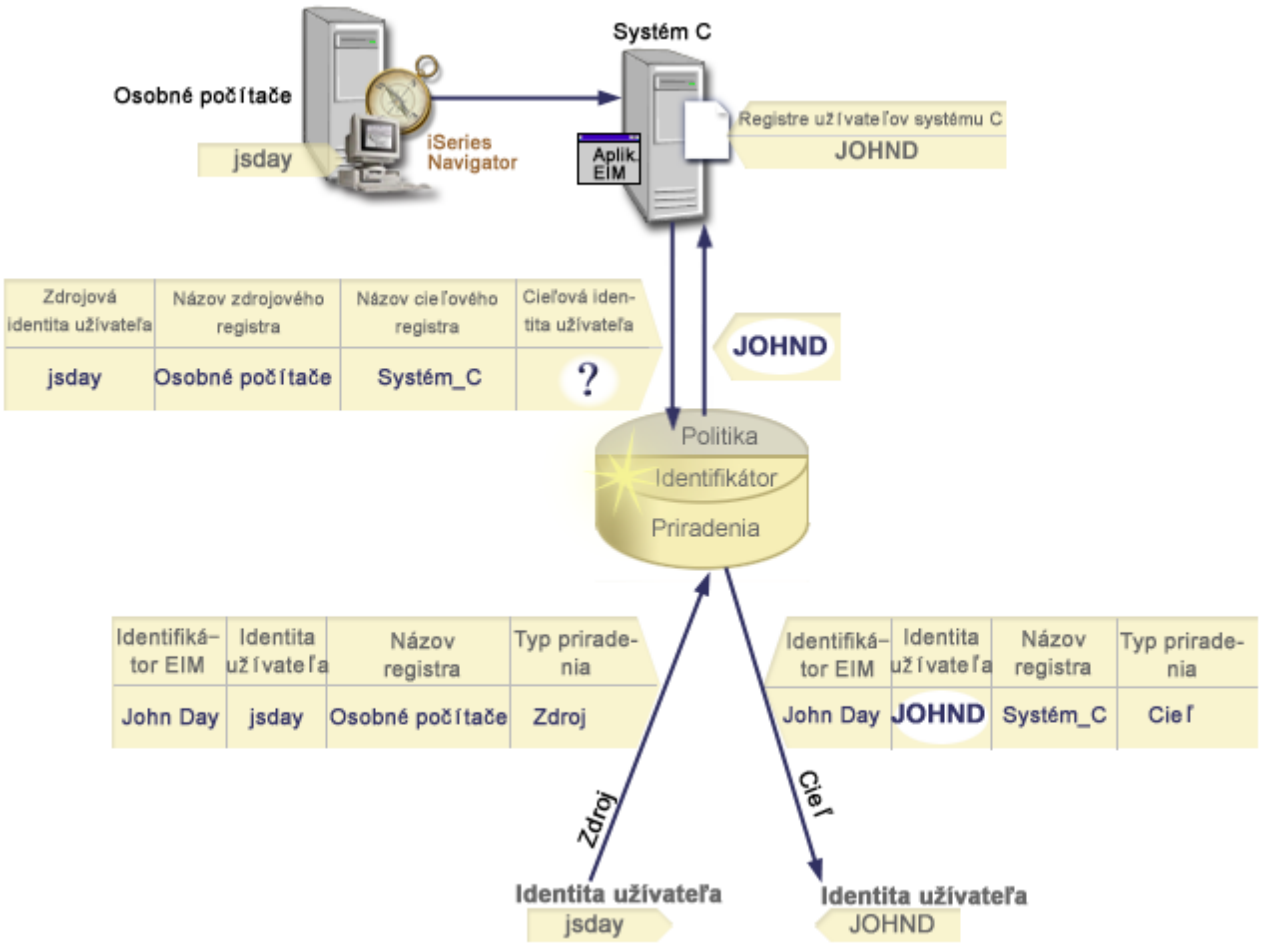
Príklady operácie vyhľadávania: Príklad 2

Na obrázku 12 chce administrátor namapovať užívateľa Windows v registri Windows Active Directory na užívateľský profil OS/400. Autentifikačnou metódou, ktorú používa Windows je Kerberos a názov registra Windows Active Directory, ako ho definoval administrátor v EIM je Desktops. Identita užívateľa, z ktorej chce administrátor namapovať, je principál Kerbera s názvom jsday. Názov registra OS/400 ako ho administrátor definoval v EIM, je System_C a identita užívateľa, do ktorej chce administrátor mapovať, je užívateľský profil s názvom JOHND.

Administrátor vytvorí identifikátor EIM s názvom John Day. Potom pridá dve priradenia k tomuto identifikátoru EIM:

- Zdrojové priradenie pre principál Kerberos s názvom jsday v registri Desktops.
- Zdrojové priradenie pre užívateľský profil OS/400 s názvom JOHND v registri System_C.

Obrázok 12: Operácia prehľadania EIM vráti cieľovú identitu užívateľa z určitých priradení identifikátora, založených na známom principále Kerberos jsday



Táto konfigurácia dovoľuje operáciu vyhľadávania mapovaní, ktorá mapuje z principálu Kerberos na užívateľský profil OS/400 nasledujúcim spôsobom:

Zdrojová identita užívateľa a register	**--->**	**Identifikátor EIM**	**--->**	**Cieľová identita užívateľa**
jsday v registri Desktops	--->	John Day	--->	JOHND (v registri System_C)

Operácia vyhľadávania prebieha týmto spôsobom:

1. Užívateľ jsday sa prihlasuje a autentifikuje do Windows pomocou svojho principálu Kerberos v registri Windows Active Directory Desktops.
2. Užívateľ otvára iSeries Navigator na prístup k údajom v systéme System_C.
3. OS/400 použije API EIM na vykonanie operácie prehľadania EIM so zdrojovou identitou užívateľa jsday, zdrojovým registrom Desktops a cieľovým registrom System_C.
4. Operácia prehľadania EIM kontroluje, či je vyhľadávanie mapovaní povolené pre zdrojový register Desktops a cieľový register System_C. Sú povolené.
5. Operácia vyhľadávania kontroluje zdrojové priradenie špecifického identifikátora, ktoré sa zhoduje s dodanou zdrojovou identitou užívateľa jsday v zdrojovom registri Desktops.
6. Operácia vyhľadávania používa porovnanie zdrojového priradenia identifikátora na určenie príslušného názvu identifikátora EIM, ktorý je John Day.

7. Operácia vyhľadávania používa tento názov identifikátora EIM na hľadanie cieľového priradenia identifikátora pre identifikátor EIM, ktorý sa zhoduje so špecifikovaným cieľovým názvom definície registra EIM systému System_C.
8. Také cieľové priradenie identifikátora existuje a operácia vyhľadávania vráti cieľovú identitu užívateľa JOHND ako je definovaná v cieľovom priradení.
9. Keď operácia vyhľadávania mapovaní skončí, iSeries Navigator sa začne vykonávať pod užívateľským profilom JOHND. Oprávnenie užívateľa na prístup k prostriedkom a vykonávanie akcií v iSeries Navigator je určované oprávnením definovaným pre užívateľský profil JOHND a nie pre oprávnenie definované pre identitu užívateľa jsday.

Nasledujúci príklad ilustruje priebeh hľadania operácie vyhľadávania, keď sú dostupné priradenia politiky, ale neexistujú priradenia identifikátorov pre identitu užívateľa.

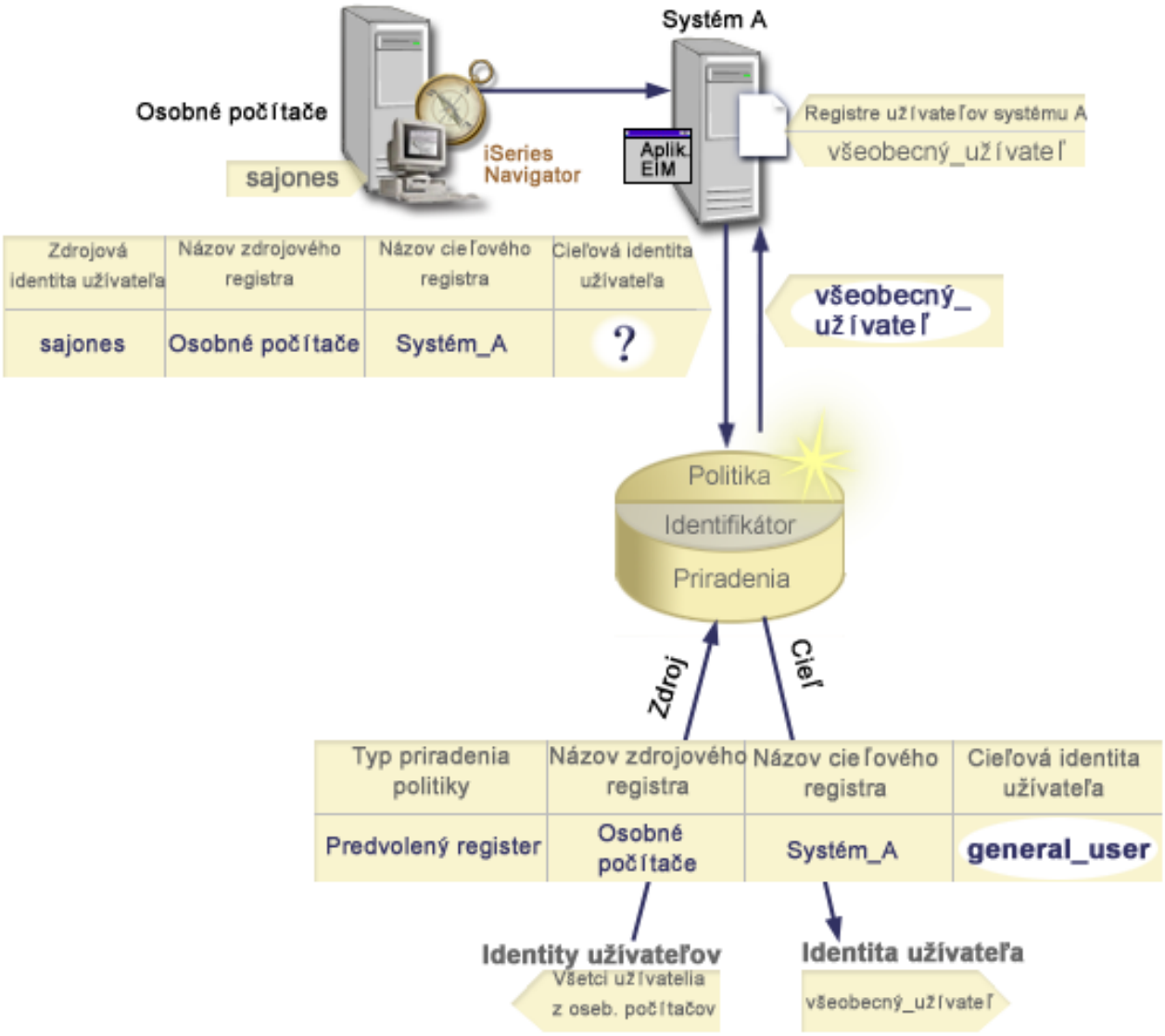
Príklady operácie vyhľadávania: Príklad 3

Na obrázku 13 chce administrátor namapovať všetkých užívateľov pracovných staníc v registri a Windows Active Directory do jedného užívateľského profilu OS/400 s názvom general_user v registri OS/400, ktorý je v EIM nazvaný System_A. Autentifikačnou metódou, ktorú používa Windows je Kerberos a názov registra Windows Active Directory, ako ho definoval administrátor v EIM je Desktops. Jednou z identít užívateľa, z ktorých chce administrátor mapovať, je principál Kerberos s názvom sajones.

Administrátor vytvorí predvolené priradenie politiky registra s nasledujúcimi informáciami:

- Zdrojový register Desktops.
- Cieľový register System_A.
- Cieľová identita užívateľa general_user.

Obrázok 13: Operácia vyhľadávania vráti cieľovú identitu užívateľa z predvoleného priradenia politiky registra.



Táto konfigurácia umožňuje, aby operácia vyhľadávania mapovaní namapovala všetky principály Kerberos v registri Desktops, vrátane principálu sajones, na užívateľský profil OS/400 s názvom general_user týmto spôsobom:

Zdrojová identita užívateľa a register	--->	Predvolené priradenie politiky registra	--->	Cieľová identita užívateľa
sajones v Desktops registry	--->	Predvolené priradenie politiky registra	--->	general_user (v registri System_A)

Operácia vyhľadávania prebieha týmto spôsobom:

1. Užívateľ sajones sa prihlási a autentifikuje do jeho prostredia Windows prostredníctvom principálu Kerberos v registri Desktops.
2. Užívateľ otvorí iSeries Navigator pre prístup k údajom v systéme A.
3. OS/400 použije API EIM na vykonanie operácie prehľadania EIM so zdrojovou identitou užívateľa sajones v zdrojovom registri Desktops a cieľovom registri System_A.
4. Operácia prehľadania EIM kontroluje, či je vyhľadávanie mapovaní povolené pre zdrojový register Desktops a cieľový register System_A. Sú povolené.

5. Operácia vyhľadávania skontroluje špecifické zdrojové priradenie identifikátora, ktoré sa zhoduje s dodanou zdrojovou identitou užívateľa sajones v zdrojovom registri Desktops. Nenájde zhodné priradenie identifikátora.
6. Operácia vyhľadávania skontroluje, či má doména povolenie na používanie priradení politiky. Má povolenie.
7. Operácia vyhľadávania skontroluje, či má cieľový register (System_A) povolenie na používanie priradení politiky. Má povolenie.
8. Operácia vyhľadávania skontroluje, či zdrojový register (Desktops) je registrom X.509. Nie je.
9. Operácia vyhľadávania skontroluje, či existuje predvolené priradenie politiky registra, ktoré sa zhoduje s názvom definície zdrojového registra (Desktops) a názvom definície cieľového registra (System_A).
10. Operácia vyhľadávania určí, že existuje jedno a vráti general_user ako cieľovú identitu užívateľa.

Niekedy operácia prehľadania EIM vráti nejednoznačný výsledok. Môže sa to stať napríklad, keď viac ako jedna cieľová identita užívateľa vyhovuje zadaným kritériám operácie vyhľadávania. Niektoré aplikácie podporujúce EIM, vrátane aplikácií a produktov OS/400, nie sú navrhnuté na spracovanie týchto nejednoznačných výsledkov a môžu zlyhať alebo poskytnúť neočakávané výsledky. Pre vyriešenie tejto situácie budete musieť vykonať príslušné akcie. Napríklad budete musieť zmeniť vašu konfiguráciu EIM alebo definovať informácie na vyhľadanie pre každú cieľovú identitu užívateľa, aby sa predišlo viacerým zhodám v cieľovej identite užívateľa. Môžete tiež otestovať mapovanie, aby ste určili, či zmeny, ktoré ste vykonali fungujú tak, ako ste očakávali.

Enterprise Identity Mapping: Podpora a povolenie politiky mapovania

Podpora politiky mapovania v EIM (Enterprise Identity Mapping) umožňuje používať v doméne EIM priradenia politiky a tiež špecifické priradenia identifikátorov. Priradenia politiky môžete používať namiesto alebo v kombinácii s priradeniami identifikátorov.

Podpora politiky mapovania EIM poskytuje prostriedky na povolenie a zakázanie používania priradení politiky pre celú doménu a takisto pre každý konkrétny cieľový register užívateľov. EIM takisto umožňuje nastaviť, či sa môže konkrétny register vo všeobecnosti zúčastniť operácií vyhľadávania mapovaní. Následne môžete použiť podporu politiky mapovania na presnejšie riadenie spôsobu vracania výsledkov operácií vyhľadávania mapovaní.

Predvolené nastavenie pre doménu EIM je zakázanie vyhľadávaní mapovaní, ktoré používajú priradenia politiky. Ak je používanie priradení politiky v doméne zakázané, všetky operácie vyhľadávania mapovaní v doméne vracajú výsledky len s použitím špecifických priradení identifikátorov medzi identitami užívateľov a identifikátormi EIM.

Pri predvolených nastaveniach je pre každý samostatný register povolená účasť na vyhľadávaní mapovaní a zakázané používanie priradení politiky. Ak povolíte používanie priradení politiky pre konkrétny cieľový register, musíte zabezpečiť aj povolenie tohto nastavenia pre doménu.

Účasť na vyhľadávaní mapovaní a používanie priradení politiky môžete pre každý register nakonfigurovať jedným z troch spôsobov:

- Pre zadaný register sa nesmú používať žiadne operácie vyhľadávania mapovaní. Inými slovami aplikácia vykonávajúca operáciu vyhľadávania mapovaní zahŕňajúcu tento register zlyhá pri vracaní výsledkov.
- Operácie vyhľadávania mapovaní môžu používať len špecifické priradenia identifikátorov medzi identitami užívateľov a identifikátormi EIM. Vyhľadávanie mapovaní je pre register povolené, ale používanie priradení politiky je zakázané.
- Operácie vyhľadávania mapovaní môže používať špecifické priradenia identifikátorov, ak existujú a priradenia politiky, ak špecifické priradenia identifikátorov neexistujú (všetky nastavenia sú povolené).

Viac informácií o spôsobe povolenia politiky mapovania a nastavení účasti na vyhľadávaní mapovaní si môžete pozrieť v častiach:

- Povolenie priradení politiky pre doménu
- Povolenie podpory vyhľadávania mapovaní a používania priradení politiky pre cieľový register

Riadenie prístupu EIM

Užívateľ EIM je užívateľ, ktorý vlastní oprávnenie na riadenie prístupu k EIM na základe členstva v preddefinovanej skupine užívateľov LDAP (Lightweight Directory Access Protocol) v konkrétnej doméne. Špecifikovanie *riadenia prístupu* EIM pre užívateľa pridáva tohto užívateľa do konkrétnej skupiny užívateľov LDAP v konkrétnej doméne. Každá skupina LDAP má oprávnenie vykonávať konkrétne administračné úlohy EIM v tejto doméne. Jednotlivé administratívne úlohy a ich typy, vrátane operácií vyhľadávania, ktoré môže užívateľ EIM vykonať, sú určené skupinou riadenia prístupu, do ktorej patrí užívateľ EIM.

Poznámka: Ak chcete nakonfigurovať EIM, musíte dokázať, že ste dôveryhodný v rámci kontextu siete, nie v jednom konkrétnom systéme. Oprávnenie na konfigurovanie EIM nie je založené na vašom oprávnení užívateľského profilu OS/400, ale skôr na vašom oprávnení na riadenie prístupu k EIM. EIM je sieťový prostriedok, nie prostriedok pre jeden konkrétny systém; takže EIM nerozoznáva zvláštne oprávnenia na konfiguráciu, charakteristické pre OS/400, akými sú *ALLOBJ a *SECADM. Po nakonfigurovaní EIM, oprávnenie na vykonávanie úloh môže byť založené na mnohých rozličných užívateľských profiloch, napríklad na užívateľských profiloch OS/400. Napríklad IBM Directory Server for iSeries (LDAP) považuje užívateľské profily OS/400 so zvláštnym oprávnením *ALLOBJ a *IOSYSCFG za administrátorov adresára.

Pridávať ďalších užívateľov do skupiny riadenia prístupu k EIM alebo meniť nastavenia riadenia prístupu pre iných užívateľov môžu len užívatelia s oprávnením administrátora riadenia prístupu k EIM. Skôr, ako sa užívateľ stane členom skupiny riadenia prístupu k EIM, musí mať záznam v adresárovom serveri, ktorý sa správa ako radič domény EIM. Rovnako, len konkrétne typy užívateľov sa môžu stať členmi skupiny riadenia prístupu k EIM. Identita užívateľa môže byť v tvare principálu Kerberos, rozlišovacieho názvu LDAP alebo užívateľského profilu OS/400 tak dlho, kým je táto identita užívateľa definovaná pre adresárový server.

Poznámka: Ak má byť typ užívateľa principál Kerberos dostupný v EIM, v systéme musí byť nakonfigurovaná služba sieťovej autentifikácie. Ak má byť typ užívateľského profilu OS/400 dostupný v EIM, musíte v adresárovom serveri nakonfigurovať príponu systémového objektu. Toto umožňuje adresárovému serveru odkazovať na systémové objekty OS/400, napríklad na užívateľské profily OS/400.

Nasledujú krátke opisy funkcií, ktoré môže vykonávať každá skupina oprávnení EIM:

- **Administrátor LDAP (Lightweight Directory Access Protocol).** Administrátor LDAP je špeciálny rozlišovací názov (DN) v adresári, ktorý je administrátorom pre celý adresár. Administrátor LDAP má preto prístup k všetkým administračným funkciám EIM aj k celému adresáru. Užívateľ s týmto oprávnením na riadenie prístupu môže vykonávať nasledujúce funkcie:
  - Vytváranie domény.
  - Vymazávanie domény.
  - Vytváranie a odstraňovanie identifikátorov EIM.
  - Vytváranie a odstraňovanie definícií registra EIM.
  - Vytváranie a odstraňovanie zdrojových, cieľových a administratívnych priradení.
  - Vytváranie a odstraňovanie priradení politiky.
  - Vytváranie a odstraňovanie filtrov certifikátov.
  - Aktivovanie a deaktivovanie používania priradení politiky pre doménu.
  - Aktivovanie a deaktivovanie vyhľadávania mapovaní pre register.
  - Aktivovanie a deaktivovanie používania priradení politiky pre register.
  - Vykonávanie operácií prehľadania EIM.
  - Načítavanie priradení identifikátora, priradení politiky, filtrov certifikátov, identifikátorov EIM a definícií registra EIM.
  - Pridávanie, odstraňovanie a vypisovanie informácií o riadení prístupu k EIM.
- **Administrátor EIM.** Členstvo v tejto skupine riadenia prístupu umožňuje užívateľovi manažovať všetky údaje EIM v rámci tejto domény EIM. Užívateľ s týmto oprávnením na riadenie prístupu môže vykonávať nasledujúce funkcie:

- Vymazávanie domény.
- Vytváranie a odstraňovanie identifikátorov EIM.
- Vytváranie a odstraňovanie definícií registra EIM.
- Vytváranie a odstraňovanie zdrojových, cieľových a administratívnych priradení.
- Vytváranie a odstraňovanie priradení politiky.
- Vytváranie a odstraňovanie filtrov certifikátov.
- Aktivovanie a deaktivovanie používania priradení politiky pre doménu.
- Aktivovanie a deaktivovanie vyhľadávania mapovaní pre register.
- Aktivovanie a deaktivovanie používania priradení politiky pre register.
- Vykonávanie operácií prehľadania EIM.
- Načítavanie priradení identifikátora, priradení politiky, filtrov certifikátov, identifikátorov EIM a definícií registra EIM.
- Pridávanie, odstraňovanie a vypisovanie informácií o riadení prístupu k EIM.

• **Administrátor identifikátorov.** Členstvo v tejto skupine riadenia prístupu umožňuje užívateľovi pridávať a meniť identifikátory EIM a manažovať zdrojové a administratívne priradenia. Užívateľ s týmto oprávnením na riadenie prístupu môže vykonávať nasledujúce funkcie:
- Vytváranie identifikátorov EIM.
- Pridávanie a odstraňovanie zdrojových priradení.
- Pridávanie a odstraňovanie administratívnych priradení.
- Vykonávanie operácií prehľadania EIM.
- Načítavanie priradení identifikátora, priradení politiky, filtrov certifikátov, identifikátorov EIM a definícií registra EIM.

• **Operácie mapovania EIM.** Členstvo v tejto skupine riadenia prístupu umožňuje užívateľovi vykonávať operácie vyhľadávania mapovaní EIM. Užívateľ s týmto oprávnením na riadenie prístupu môže vykonávať nasledujúce funkcie:
- Vykonávanie operácií prehľadania EIM.
- Načítavanie priradení identifikátora, priradení politiky, filtrov certifikátov, identifikátorov EIM a definícií registra EIM.

• **Administrátor registrov.** Členstvo v tejto skupine riadenia prístupu umožňuje užívateľovi manažovať všetky definície registra EIM. Užívateľ s týmto oprávnením na riadenie prístupu môže vykonávať nasledujúce funkcie:
- Pridávanie a odstraňovanie cieľových priradení.
- Vytváranie a odstraňovanie priradení politiky.
- Vytváranie a odstraňovanie filtrov certifikátov.
- Aktivovanie a deaktivovanie vyhľadávania mapovaní pre register.
- Aktivovanie a deaktivovanie používania priradení politiky pre register.
- Vykonávanie operácií prehľadania EIM.
- Načítavanie priradení identifikátora, priradení politiky, filtrov certifikátov, identifikátorov EIM a definícií registra EIM.

• **Administrátor pre vybraté registre.** Členstvo v tejto skupine riadenia prístupu umožňuje užívateľovi manažovať informácie o EIM len pre určenú definíciu registra užívateľov (napríklad Registry_X). Členstvo v tejto skupine riadenia prístupu umožňuje užívateľovi tiež pridávať a odstraňovať cieľové priradenia len pre určenú definíciu registra užívateľov. Ak má užívateľ s týmto oprávnením na riadenie prístupu plne využívať operácie vyhľadávania mapovaní a priradenia politiky, mal by mať aj oprávnenie na riadenie prístupu k **operáciám mapovania EIM**. Toto oprávnenie na riadenie prístupu umožňuje užívateľovi vykonávať nasledujúce funkcie pre konkrétne autorizované definície registra:
- Vytváranie, odstraňovanie a vypisovanie cieľových priradení len pre určené definície registra EIM.
- Pridávanie a odstraňovanie predvolených priradení politiky domény.
- Pridávanie a odstraňovanie priradení politiky len pre určené definície registra.

- Pridávanie filtrov certifikátov len pre určené definície registra.
- Aktivovanie a deaktivovanie vyhľadávaní mapovania len pre určené definície registra.
- Aktivovanie a deaktivovanie používania priradení politiky len pre určené definície registra.
- Načítavanie identifikátorov EIM.
- Načítavanie priradení identifikátorov a filtrov certifikátov len pre určené definície registra.
- Načítavanie informácií o definícii registra EIM len pre určené definície registra.

Poznámka: Užívateľ, ktorý má oprávnenie **Administrátora na riadenie prístupu k vybratým registrom** aj oprávnenie na riadenie prístupu k **operáciám vyhľadávania mapovania EIM** získa schopnosť vykonávať nasledujúce funkcie:

- Pridávanie a odstraňovanie priradení politiky len pre určené registre.
- Vykonávanie operácií prehľadania EIM.
- Načítavanie všetkých priradení identifikátora, priradení politiky, filtrov certifikátov a definícií registra EIM.

Ak chcete zistiť, či má konkrétna skupina riadenia prístupu k EIM oprávnenie na vykonávanie konkrétnej akcie, pozrite si tieto časti:

- Skupina riadenia prístupu k EIM: Oprávnenie na API
- Skupina riadenia prístupu k EIM: Oprávnenie na úlohy EIM

Skupina riadenia prístupu k EIM: Oprávnenie rozhrania API

Každá z nasledujúcich tabuliek je organizovaná podľa operácie EIM, ktorú vykonáva rozhranie API. Každá tabuľka zobrazuje všetky rozhrania API EIM, rôzne skupiny riadenia prístupu k EIM a či má skupina riadenia prístupu oprávnenie vykonávať konkrétnu funkciu EIM.

Tabuľka 1. Práca s doménami

API EIM	Administrátor LDAP	Administrátor EIM	Administrátor identifikátorov	Hľadanie mapovaní EIM	Administrátor registrov	Administrátor pre vybraté registre
eimChangeDomain	X	X	-	-	-	-
eimCreateDomain	X	-	-	-	-	-
eimDeleteDomain	X	X	-	-	-	-
eimListDomains	X	X	-	-	-	-

Tabuľka 2. Práca s identifikátormi

API EIM	Administrátor LDAP	Administrátor EIM	Administrátor identifikátorov EIM	Hľadanie mapovaní EIM	Administrátor registrov EIM	X administrátor registrov EIM
eimAddIdentifier	X	X	X	-	-	-
eimChangeIdentifier	X	X	X	-	-	-
eimListIdentifiers	X	X	X	X	X	X
eimRemoveIdentifier	X	X	-	-	-	-
eimGetAssociated Identifiers	X	X	X	X	X	X

Tabuľka 3. Práca s registrami

API EIM	Administrátor LDAP	Administrátor EIM	Administrátor identifikátorov EIM	Hľadanie mapovaní EIM	Administrátor registrov EIM	X administrátor registrov EIM
eimAddApplication Registry	X	X	-	-	-	-
eimAddSystemRegistry	X	X	-	-	-	-

Tabuľka 3. Práca s registrami (pokračovanie)

API EIM	Administrátor LDAP	Administrátor EIM	Administrátor identifikátorov EIM	Hľadanie mapovaní EIM	Administrátor registrov EIM	X administrátor registrov EIM
eimChangeRegistry	X	X	-	-	X	X
eimChange RegistryUser	X	X	-	-	X	X
eimChangeRegistryAlias	X	X	-	-	X	X
eimGetRegistry NameFromAlias	X	X	X	X	X	X
eimListRegistries	X	X	X	X	X	X
eimListRegistry Associations	X	X	X	X	X	X
eimListRegistryAliases	X	X	X	X	X	X
eimListRegistry Users	X	X	X	X	X	X
eimRemoveRegistry	X	X	-	-	-	-

Tabuľka 4. Práca s priradeniami identifikátorov. Pre rozhrania API eimAddAssociation() a eimRemoveAssociation() existujú štyri parametre, ktoré určujú typ priradenia, ktoré sa pridáva alebo odstraňuje. Oprávnenie na tieto rozhrania API závisí na type priradenia zadaného v týchto parametroch. V tejto tabuľke je pre každé z týchto rozhraní API zahrnutý aj typ priradenia.

API EIM	Administrátor LDAP	Administrátor EIM	Administrátor identifikátorov EIM	Hľadanie mapovaní EIM	Administrátor registrov EIM	X administrátor registrov EIM
eimAddAssociation (administratívne)	X	X	X	-	-	-
eimAddAssociation (zdrojové)	X	X	X	-	-	-
eimAddAssociation (source and target)	X	X	X	-	X	X
eimAddAssociation (cieľové)	X	X	-	-	X	X
eimListAssociations	X	X	X	X	X	X
eimRemoveAssociation (administratívne)	X	X	X	-	-	-
eimRemoveAssociation (zdrojové)	X	X	X	-	-	-
eimRemoveAssociation (source and target)	X	X	X	-	X	X
eimRemoveAssociation (cieľové)	X	X	-	-	X	X

Tabuľka 5. Práca s priradeniami politiky

API EIM	Administrátor LDAP	Administrátor EIM	Administrátor identifikátorov EIM	Hľadanie mapovaní EIM	Administrátor registrov EIM	X administrátor registrov EIM
eimAddPolicyAssociation	X	X	-	-	X	X
eimAddPolicyFilter	X	X	-	-	X	X
eimListPolicyFilters	X	X	X	X	X	X
eimRemove PolicyAssociation	X	X			X	X
eimRemovePolicyFilter	-	-	-	-	-	

Tabuľka 6. Práca s mapovaniami

API EIM	Administrátor LDAP	Administrátor EIM	Administrátor identifikátorov EIM	Hľadanie mapovaní EIM	Administrátor registrov EIM	X administrátor registrov EIM
eimGetAssociatedIdentifier	X	X	X	X	X	X
eimGetTargetFromIdentifier	X	X	X	X	X	X
eimGetTargetFromSource	X	X	X	X	X	X

Tabuľka 7. Práca s prístupom

API EIM	Administrátor LDAP	Administrátor EIM	Administrátor identifikátorov EIM	Hľadanie mapovaní EIM	Administrátor registrov EIM	X administrátor registrov EIM
eimAddAccess	X	X	-	-	-	-
eimListAccess	X	X	-	-	-	-
eimListUserAccess	X	X	-	-	-	-
eimQueryAccess	X	X	-	-	-	-
eimRemoveAccess	X	X	-	-	-	-

Skupina riadenia prístupu k Enterprise Identity Mapping: Oprávnenie na úlohy EIM

Nasledujúca tabuľka zobrazuje vzťahy medzi rôznymi skupinami riadenia prístupu k EIM (Enterprise Identity Mapping) a úlohami EIM, ktoré môžu vykonať.

Aj keď sa administrátor LDAP nenachádza v tabuľke, vyžaduje sa táto úroveň riadenia prístupu na vytvorenie novej domény EIM. Okrem toho má administrátor LDAP také isté riadenie prístupu ako administrátor EIM, ale administrátor EIM nemá automaticky riadenie prístupu Administrátor LDAP.

Tabuľka 8. Tabuľka 1: Skupiny riadenia prístupu k EIM

Úloha EIM	Administrátor EIM	Administrátor identifikátorov	Operácie vyhľadávania mapovaní EIM	Administrátor registrov	Administrátor pre vybraté registre
Vytvoriť doménu	-	-	-	-	-
Vymazať doménu	X	-	-	-	-
Upraviť doménu	X	-	-	-	-
Povoliť/Zakázať priradenia politiky pre doménu	X	-	-	-	-
Hľadať domény	X	-	-	-	-
Pridať systémový register	X	-	-	-	-
Pridať register aplikácií	X	-	-	-	-
Odstrániť register	X	-	-	-	-
Upraviť register	X	-	-	X	X
Povoliť/Zakázať vyhľadávanie mapovaní pre register	X	-	-	X	X

Tabuľka 8. Tabuľka 1: Skupiny riadenia prístupu k EIM (pokračovanie)

Úloha EIM	Administrátor EIM	Administrátor identifikátorov	Operácie vyhľadávania mapovaní EIM	Administrátor registrov	Administrátor pre vybraté registre
Povoliť/Zakázať priradenia politiky pre register	X	-	-	X	X
Hľadať registre	X	X	X	X	X
Pridať identifikátor	X	X	-	-	-
Odstrániť identifikátor	X	-	-	-	-
Upraviť identifikátor	X	X	-	-	-
Hľadať identifikátory	X	X	X	X	X
Opakovane získať priradené identifikátory	X	X	X	X	X
Pridať/Odstrániť administratívne priradenie	X	X	-	-	-
Pridať/Odstrániť zdrojové priradenie	X	X	-	-	-
Pridať/Odstrániť cieľové priradenie	X	-	-	X	X
Pridať/Odstrániť priradenie politiky	X	-	-	X	X
Pridať/Odstrániť filter certifikátov	X	-	-	X	X
Hľadať filter certifikátov	X	X	X	X	X
Hľadať priradenia	X	X	X	X	X
Hľadať priradenia politiky	X	X	X	X	X
Opakovane získať cieľové priradenie zo zdrojového priradenia	X	X	X	X	-
Opakovane získať cieľové priradenie z identifikátora	X	X	X	X	X
Upraviť užívateľov registrov	X	-	-	X	X
Hľadať užívateľov registrov	X	X	X	X	X
Upraviť alias registra	X	-	-	X	X

Tabuľka 8. Tabuľka 1: Skupiny riadenia prístupu k EIM (pokračovanie)

Úloha EIM	Administrátor EIM	Administrátor identifikátorov	Operácie vyhľadávania mapovaní EIM	Administrátor registrov	Administrátor pre vybraté registre
Hľadať aliasy registrov	X	X	X	X	X
Opakovane získať register z aliasu	X	X	X	X	X
Pridať/Odstrániť riadenie prístupu k EIM	X	-	-	-	-
Zobraziť členov skupiny riadenia prístupu	X	-	-	-	-
Zobraziť riadenie prístupu k EIM pre konkrétneho užívateľa	X	-	-	-	-
Dotazovať riadenie prístupu k EIM	X	-	-	-	-

Koncepty LDAP pre EIM

EIM (Enterprise Identity Mapping) požíva na ukladanie údajov server LDAP (Lightweight Directory Access Protocol) ako radič domény. V dôsledku toho by ste mali pochopiť niektoré koncepty LDAP, ktoré sa vzťahujú na konfigurovanie a používanie EIM vo vašom podniku. Napríklad rozlišovací názov LDAP môžete použiť ako identitu užívateľa na nakonfigurovanie EIM a autentifikovanie do radiča domén EIM.

Ak chcete lepšie pochopiť konfigurovanie a používanie EIM, mali by ste pochopiť nasledujúce koncepty LDAP:

- Rozlišovací názov
- Rodičovský rozlišovací názov
- Schéma LDAP a iné úvahy o EIM

Rozlišovací názov

DN (distinguished name) je položka LDAP (Lightweight Directory Access Protocol), ktorá jedinečne identifikuje a opisuje položku v adresárovom serveri (LDAP). Použite sprievodcu konfiguráciou na nakonfigurovanie adresárového servera na ukladanie informácií domény EIM. EIM používa adresárový server na ukladanie údajov EIM, preto môžete použiť rozlišovacie názvy ako prostriedky autentifikácie do radiča doemény EIM.

Rozlišovacie názvy obsahujú názov samotnej entity a názvy objektov nad ňou v adresári LDAP (v poradí odspodu nahor). Úplný rozlišovací názov môže byť napríklad cn=Tim Jones, o=IBM, c=US. Každá položka má aspoň jeden atribút, ktorý sa používa na pomenovanie danej položky. Tento pomenovací atribút sa nazýva relatívny rozlišovací názov (RDN) položky. Položka nad daným RDN sa nazýva rodičovský rozlišovací názov. V tomto príklade cn=Tim Jones pomenúva položku, preto je RDN. o=IBM, c=US je rodičovské DN pre cn=Tim Jones. Ak sa chcete dozvedieť viac o tom, ako EIM používa názvy DN, pozrite si časť “Rodičovský rozlišovací názov” na strane 40.

EIM používa adresárový server na ukladanie údajov EIM, preto môžete použiť rozlišovacie názvy pre identitu užívateľa, ktorá ho autentifikuje do radiča domény. Môžete tiež použiť rozlišovací názov pre identitu užívateľov, ktorý konfiguruje EIM pre váš server iSeries. Napríklad rozlišovací názov môžete použiť, keď robíte nasledujúce:

- Konfigurujete adresárový server, aby vystupoval ako radič domény EIM. Toto vykonáte vytvorením a použitím rozlišovacieho názvu, ktorý identifikuje administrátora LDAP pre adresárový server. Ak ešte nebol adresárový server nakonfigurovaný, môžete ho nakonfigurovať, keď použijete sprievodcu konfiguráciou EIM na vytvorenie a pripojenie novej domény.
- Používate Sprievodcu konfiguráciou EIM na výber typu identity užívateľa, ktorý má sprievodca použiť pri pripájaní k radiču domény EIM. Rozlišovací názov je jeden z typov užívateľov, ktorý môžete vybrať. Rozlišovací názov musí reprezentovať užívateľa, ktorý je autorizovaný vytvárať objekty v lokálnom názvovom priestore adresárového servera.
- Používate Sprievodcu konfiguráciou EIM na výber typu užívateľa na vykonávanie operácií EIM v mene funkcií operačného systému. Tieto operácie zahrňujú operácie vyhľadávania mapovaní a vymazávanie priradení počas vymazávania lokálneho užívateľského profilu OS/400. Rozlišovací názov je jeden z typov užívateľov, ktorý môžete vybrať.
- Pripájate sa k radiču domény kvôli správe EIM, napríklad kvôli manažovaniu registrov a identifikátorov a vykonaniu operácií vyhľadávania mapovaní.
- Vytvárate filtre certifikátov na určenie rozsahu priradenia politiky filtra certifikátov. Keď vytvoríte filter certifikátov, musíte poskytnúť informácie o rozlišovacom názve pre DN subjektu alebo DN vydavateľa alebo certifikát na určenie kritéria, ktoré filter používa na určenie certifikátov ovplyvnených priradením politiky.

Ak sa chcete dozvedieť viac o rozlišovacích názvoch a o tom ako ich LDAP používa, pozrite si Koncepty adresárového servera.

Rodičovský rozlišovací názov

Rodičovský rozlišovací názov (DN) je položka v názvovom priestore adresárového servera LDAP (Lightweight Directory Access Protocol). Položky servera LDAP sú usporiadané v hierarchickej štruktúre, ktorá môže zodpovedať politickým, geografickým alebo organizačným hraniciam alebo hraniciam domény. Rozlišovací názov sa považuje za rodičovské DN, keď toto DN je adresárová položka priamo nadradená danému DN.

Úplný rozlišovací názov môže byť napríklad cn=Tim Jones, o=IBM, c=US. Každá položka má aspoň jeden atribút, ktorý sa používa na pomenovanie danej položky. Tento pomenovací atribút sa nazýva relatívny rozlišovací názov (RDN) položky. Položka nad daným RDN sa nazýva rodičovský rozlišovací názov. V tomto príklade cn=Tim Jones pomenúva položku, preto je RDN. o=IBM, c=US je rodičovské DN pre cn=Tim Jones.

EIM používa adresárový server ako radič domény na ukladanie údajov domény EIM. Rodičovské DN kombinované s názvom domény EIM určuje umiestnenie údajov domény EIM v názvovom priestore adresárového servera. Počas používania sprievodcu konfiguráciou EIM na vytvorenie a pripojenie novej domény, môžete zadať rodičovské DN pre doménu, ktorú vytvárate. Pomocou rodičovského DN môžete určiť, kde sa v názvovom priestore LDAP majú uložiť údaje EIM pre doménu. Ak nezadáte rodičovské DN, údaje EIM sa uložia do vlastnej prípony v názvovom priestore a predvolené umiestnenie údajov domény EIM je **ibm-eimDomainName=EIM**.

Ak sa chcete dozvedieť viac o rozlišovacích názvoch a o tom, ako sú použité, pozrite si časťKoncepty adresárového servera.

Schéma LDAP a ďalšie aspekty pre Enterprise Identity Mapping

Vo verzii 5, vydanie 3 vyžaduje EIM (Enterprise Identity Mapping), aby hostiteľom radiča domény bol adresárový server, ktorý podporuje protokol Lightweight Directory Access Protocol (LDAP) verzie 3. Okrem toho musí byť adresárový server schopný prijať schému EIM a podporovať nasledujúce atribúty a triedy objektov:

- Atribút ibm-entryUUID.
- ibmattributetypes:
  - acIEntry
  - acIPropagate
  - acISource
  - entryOwner
  - ownerPropagate

- ownerSource
- Atribúty EIM, vrátane troch nových atribútov pre podporu priradenia politiky:
  - ibm-eimAdditionalInformation
  - ibm-eimAdminUserAssoc
  - ibm-eimDomainName, ibm-eimDomainVersion,
  - ibm-eimRegistryAliases
  - ibm-eimRegistryEntryName
  - ibm-eimRegistryName
  - ibm-eimRegistryType
  - ibm-eimSourceUserAssoc
  - ibm-eimTargetIdAssoc
  - ibm-eimTargetUserName
  - ibm-eimUserAssoc
  - ibm-eimFilterType
  - ibm-eimFilterValue
  - ibm-eimPolicyStatus
- Triedy objektov EIM, vrátane troch nových tried pre podporu priradenia politiky:
  - ibm-eimApplicationRegistry
  - ibm-eimDomain
  - ibm-eimIdentifier
  - ibm-eimRegistry
  - ibm-eimRegistryUser
  - ibm-eimSourceRelationship
  - ibm-eimSystemRegsitry
  - ibm-eimTargetRelationship
  - ibm-eimFilterPolicy
  - ibm-eimDefaultPolicy
  - ibm-eimPolicyListAux

Verzia 5, vydanie 3 produktu IBM Directory Server for iSeries poskytuje túto podporu. Viac informácií o produktoch adresárových serverov spoločnosti IBM poskytujúcich potrebnú podporu pre EIM a ďalšie aspekty radičov domén EIM nájdete v časti Plánovanie radiča domény EIM.

Ak v súčasnosti používate ako radič domény EIM adresárový server v systéme iSeries verzie 5, vydanie 2, musíte aktualizovať schému LDAP a podporu EIM pre tento adresárový server, aby ste ho mohli pokračovať používať na manažovanie údajov domény EIM. Ak sa chcete dozvedieť viac, pozrite si stránku iSeries LDAP na webovej lokalite spoločnosti IBM.

Koncepty iSeries pre Enterprise Identity Mapping

EIM (Enterprise Identity Mapping) môžete implementovať na každej platforme IBM @server . Avšak, ak ju implementujete v serveri iSeries, mali by ste si byť vedomý niektorých informácií, ktoré sú špecifické pre implementáciu v serveri iSeries. Pozrite si nasledujúce informácie, kde sa dozviete o aplikáciách systému OS/400, podporujúcich EIM, aspektoch užívateľských profilov a o ďalších témach, ktoré vám môžu pomôcť efektívne používať EIM v systéme iSeries.

- Aspekty užívateľských profilov systému OS/400 pre EIM
- Auditovanie systému OS/400 pre EIM
- Aplikácie OS/400, podporujúce EIM

Aspekty užívateľských profilov systému OS/400 pre Enterprise Identity Mapping

Schopnosť vykonávať úlohy v EIM (Enterprise Identity Mapping) nie je založená na vašom oprávnení užívateľského profilu systému OS/400, ale na oprávnení "Riadenie prístupu EIM" na strane 33. Existuje niekoľko dodatočných úloh, ktoré je potrebné vykonať na nastavenie systému OS/400 pre používanie EIM. Tieto dodatočné úlohy vyžadujú užívateľský profil systému OS/400 s vhodnými špeciálnymi oprávneniami.

Ak chcete nastaviť systém OS/400 pre používanie EIM pomocou programu iSeries Navigator, musí mať váš užívateľský profil nasledujúce špeciálne oprávnenia:

- Špeciálne oprávnenie administrátora bezpečnosti (*SECADM).
- Špeciálne oprávnenie na všetky objekty (*ALLOBJ).
- Špeciálne oprávnenie na konfiguráciu systému (*IOSYSCFG).

Vylepšenia príkazov užívateľských profilov systému OS/400 pre identifikátory EIM

Po nakonfigurovaní EIM pre váš systém môžete využívať výhody nového parametra pre príkazy CRTUSRPRF (Create user profile) a CHGUSRPRF (Change user profile), nazvaného EIMASSOC. Tento parameter môžete použiť na definovanie priradení identifikátorov EIM pre konkrétny užívateľský profil pre lokálny register.

Pri používaní tohto parametra môžete zadať nasledujúce informácie:

- Názov identifikátora EIM, ktorý môže predstavovať nový alebo existujúci názov identifikátora.
- Voľbu akcie pre priradenie, ktorá môže pridať (*ADD), nahradiť (*REPLACE) alebo odstrániť (*REMOVE) zadané priradenie.

  Poznámka: Na vytvorenie nových priradení použite voľbu *ADD. Voľbu *REPLACE môžete použiť napríklad, ak ste už definovali priradenia pre nesprávny identifikátor. Voľba *REPLACE odstráni všetky existujúce priradenia lokálneho registra so zadaným typom k ľubovoľnému inému identifikátoru a následne pridá priradenie zadané ako parameter. Voľbu *REMOVE použite na odstránenie zadaných priradení zo zadaného identifikátora.
- Typ priradenia identifikátora, ktoré môže byť: cieľové, zdrojové, zdrojové aj cieľové alebo administratívne.
- Má sa zadaný identifikátor EIM vytvoriť, ak ešte neexistuje?

Typicky vytvárate cieľové priradenie pre profil systému OS/400 a to najmä v prostredí s jednoduchým prihlásením. Po tom, čo príkaz vytvorí potrebné cieľové priradenie pre užívateľský profil (a identifikátor EIM, ak to je potrebné), budete zrejme potrebovať vytvoriť zodpovedajúce zdrojové priradenie. Na vytvorenie zdrojového priradenia pre ďalšiu identitu užívateľa, napríklad princípál Kerberos, ktorý užívateľ používa na prihlásenie do siete, môžete použiť program iSeries Navigator.

Pri konfigurovaní EIM pre váš systém ste do systému zadali identitu a heslo užívateľa, ktorá sa má používať pri vykonávaní operácií EIM operačným systémom. Táto identita užívateľa musí mať dostatočné oprávnenie riadenia prístupu EIM na vytváranie identifikátorov a pridávanie priradení.

Heslá užívateľských profilov systému OS/400 a EIM

Vašim primárnym cieľom, ako administrátora, pre konfiguráciu EIM ako časti prostredia s jednoduchým prihlásením je redukcia manažmentu hesiel užívateľov, ktorý musíte vykonávať pre typických koncových užívateľov vo vašom podniku. Viete, že pri používaní mapovania identity, ktoré poskytuje EIM, v kombinácií s autentifikáciou protokolom Kerberos budú užívatelia musieť vykonávať menej prihlásení a pamätať a manažovať menej hesiel. Je to výhoda, pretože ste menej často volaný riešiť problémy s namapovanými identitami užívateľov, akými je napríklad prestavenie hesiel, keď ich užívatelia zabudnú. Napriek tomu sú vaše pravidlá bezpečnostnej politiky pre heslá účinné a stále musíte manažovať užívateľské profily pre užívateľov vždy, keď heslo exspiruje.

Ďalšie výhody plynúce z prostredia s jednoduchým prihlásením môžu vzniknúť, ak zvážite nastavenia hesiel pre užívateľské profily, ktoré sú cieľmi mapovaní identít. Ako cieľ mapovania identity užívateľ nemusí poskytovať heslo pre užívateľský profil pri prístupe k systému iSeries alebo k prostriedku systému OS/400 podporujúceho EIM. Pre

typických užívateľov môžete zmeniť nastavenie hesla na hodnotu *NONE a s užívateľským profilom sa nebude môcť použiť žiadne heslo. Vlastník užívateľského profilu viac heslo nepotrebuje a to vďaka mapovaniu identity a jednoduchému prihláseniu. Nastavením hesla na hodnotu *NONE získate ďalšie výhody, pretože ani vy, ani užívatelia sa nemusíte viac zaoberať exspiráciou hesiel; navyše, nikto nemôže použiť profil na priame prihlásenie do systému iSeries ani na prístup k prostriedkom systému OS/400, podporujúcim EIM. Avšak, administrátori by mali mať heslá pre ich užívateľské profily pre prípad, že sa niekedy budú musieť priamo prihlásiť do systému iSeries. Napríklad, ak má váš radič domény EIM poruchu a nedá sa vykonať mapovanie identity, administrátor môže potrebovať priame prihlásenie do systému iSeries, kým sa problém s radičom domény nevyrieši.

Audit systému OS/400 pre Enterprise Identity Mapping

Na celkový bezpečnostný plán má významný vplyv výber auditu, ktorý vykonávate. Ak nakonfigurujete a budete používať EIM (Enterprise Identity Mapping), budete možno chcieť nakonfigurovať podporu auditovania pre adresárový server na zabezpečenie, že poskytujete vhodnú úroveň sledovateľnosti, ktorú vyžaduje vaša bezpečnostná politika. Napríklad podpora auditovania môže byť pomocná pri zisťovaní, ktorý z užívateľov namapovaný pomocou priradenia politiky vykonal akciu vo vašom systéme, alebo zmenil objekt.

Ak sa chcete dozvedieť viac o podpore auditovania pre produkt IBM Directory Server for iSeries (LDAP), pozrite si časť Auditovanie v téme Informačného centra IBM Directory Server for iSeries (LDAP). Tieto informácie takisto poskytujú vhodné referencie na aspekty auditovania systému OS/400 a na nastavenia, ktoré musíte povoliť na kontrolu správnosti konfigurácie auditovania adresárového servera.

Aplikácie systému OS/400, podporujúce Enterprise Identity Mapping

Nasledujúce aplikácie systému OS/400 sa dajú nakonfigurovať na používanie EIM (Enterprise Identity Mapping):

- Hostiteľské servery OS/400 (v súčasnosti používané produktom iSeries Access for Windows a programom iSeries Navigator)
- Telnet Server (v súčasnosti používaný emuláciou PC5250 a hostiteľom IBM Websphere na požiadanie)
- QFileSrv.400 ODBC (umožňuje používanie jednoduchého prihlásenia prostredníctvom jazyka SQL)
- JDBC (umožňuje používanie EIM prostredníctvom jazyka SQL)
- Distributed Relational Database Architecture (DRDA) (umožňuje používanie EIM prostredníctvom jazyka SQL)
- IBM WebSphere Host On-Demand verzia 8 (vlastnosť prihlásenia produktu Web Express)
- NetServer
- QFileSvr.400

Plán pre Enterprise Identity Mapping

Plán implementácie je nevyhnutný pre úspešné nakonfigurovanie a používanie EIM (Enterprise Identity Mapping) vo vašom podniku. Ak chcete vytvoriť plán, potrebujete zhromaždiť údaje o systémoch, aplikáciách a užívateľoch, ktorí budú EIM používať. Informácie, ktoré získate použijete pri rozhodovaní o najlepšej konfigurácii EIM pre váš podnik.

EIM je technológia infraštruktúry IBM @server dostupná pre všetky platformy IBM, preto spôsob, akým naplánujete implementáciu závisí od toho, aké platformy sú vo vašom podniku. Hoci je mnoho aktivít plánovania, ktoré sú špecifické pre jednotlivé platformy, veľa aktivít plánovania EIM sa používa na všetky platformy IBM. Mali by ste sa prepracovať cez bežné aktivity plánovania EIM, aby ste vytvorili celkový plán implementácie. Ak sa chcete dozvedieť viac o pláne implementácie EIM, pozrite si tieto časti:

- Plán EIM pre @server Ak chcete vytvoriť celkový plán implementácie EIM, prečítajte si tento materiál.
- Plán EIM pre OS/400 Ak chcete vytvoriť plán konfigurácie pre vašu implementáciu EIMOS/400, prečíatajte si tento materiál.

Plánovanie Enterprise Identity Mapping pre eServer

Plán implementácie je nevyhnutný pre úspešnú konfiguráciu a používanie EIM (Enterprise Identity Mapping) v podniku s viacerými platformami. Na vývoj vášho plánu implementácie potrebujete zhromaždiť informácie o

systémoch, aplikáciách a užívateľoch EIM. Tieto získané informácie neskôr použijete pri rozhodnutiach o najlepšom spôsobe konfigurácie EIM pre prostredie s viacerými platformami.

Nasledujúci zoznam poskytuje rýchleho sprievodcu úlohami plánovania, ktoré by ste mali dokončiť pred konfigurovaním a používaním EIM v prostredí s viacerými platformami. Prečítajte si informácie na týchto stránkach a zistite, ako úspešne naplánovať vaše potreby konfigurácie EIM, vrátane potrebných zručností implementačného tímu, informácií, ktoré potrebujete získať a rozhodnutí o konfigurácií, ktoré musíte urobiť. Pomôcť vám môže aj vytlačenie pracovných listov plánovania EIM (číslo 8 v zozname nižšie), aby ste ich mohli použiť počas procesu plánovania.

1. Požiadavky nastavení EIM
2. Identifikácia potrebných zručností, rolí a oprávnení
3. Plánovanie domény EIM
4. Plánovanie radiča domény EIM
5. Vývoj plánu pomenovania definícií registrov EIM
6. Vývoj plánu mapovania identity EIM
7. Aspekty vývoja aplikácií
8. Pracovné listy plánovania implementácie EIM

Požiadavky na nastavenie Enterprise Identity Mapping pre server eServer

Ak chcete vo vašom podniku úspešne implementovať EIM, musíte zabezpečiť splnenie troch množín požiadaviek:

1. Požiadavky na úrovni podniku alebo siete
2. Systémové požiadavky
3. Aplikačné požiadavky

Požiadavky na úrovni podniku alebo siete

Musíte nakonfigurovať jeden zo systémov vo vašom podniku alebo sieti tak, aby vystupoval ako adič domény EIM, čo je špeciálne nakonfigurovaný server LDAP, ktorý ukladá a poskytuje údaje domény EIM. Na voľbu produktu adresárových služieb, ktorý sa bude používať ako radič domény, vplýva veľa faktorov vrátane faktu, že nie všetky servery LDAP poskytujú podporu radiča domény EIM.

Ďalším aspektom je dostupnosť administratívnych nástrojov. Jednou voľbou je použitie rozhraní API EIM vo vašich vlastných aplikáciách na vykonanie administratívnych funkcií. Ak plánujete ako radič domény EIM použiť produkt Directory Server for iSeries (LDAP), môžete na riadenie EIM použiť program iSeries Navigator. Ak plánujete použiť produkt IBM Directory, môžete použiť pomocný program eimadmin, ktorý je súčasťou LDAP SPE verzie 1, vydania 4.

Nasledujúce informácie poskytujú základné informácie o platformách spoločnosti IBM, poskytujúcich produkt adresárového servera, ktorý podporuje EIM. Detailné informácie k voľbe adresárového servera na poskytnutie podpory radiča domény EIM nájdete v časti Plánovanie radiča domény EIM.

Systémové a aplikačné požiadavky

Každý systém nachádzajúci sa v doméne EIM musí spĺňať nasledujúce požiadavky:

- Mať nainštalovaný softvér klienta LDAP.
- Mať implementáciu rozhraní API EIM.

Každá aplikácia v doméne EIM musí byť schopná používať rozhrania API EIM na vykonávanie operácií vyhľadávania mapovaní a ďalších.

Poznámka: V prípade distribuovanej aplikácie nemusí byť potrebné, aby aj strana servera aj strana klienta bola schopná používať rozhrania API EIM. Väčšinou len aplikácia na strane servera potrebuje používať rozhrania API EIM.

Nasledujúca tabuľka poskytuje informácie o podpore EIM, ktorú poskytujú platformy servera eserver. Informácie sú usporiadané podľa platformy, stĺpce majú nasledujúci význam:

- Klient EIM, potrebný pre podporu rozhraní API EIM platformou.
- Typ dostupných konfiguračných a administratívnych nástrojov EIM pre platformu.
- Produkt adresárového servera, ktorý môže byť nainštalovaný, aby platforma fungovala ako radič domény EIM.

Platforma nemusí byť schopná fungovať ako radič domény EIM, aby sa mohla nachádzať v doméne EIM.

Tabuľka 9. Podpora EIM servera eServer

Platforma	Klient EIM (podpora rozhrania API)	Radič domény	Administratívne nástroje EIM
Systém AIX v serveri pSeries	AIX R5.2	IBM Directory V5.1	Nedostupné
LINUX • SLES8 na PPC64 • Red Hat 7.3 na i386 • SLES7 v serveri zSeries	Prevezmite jedno z tohto: • Klient IBM Directory V4.1 • Klient IBM Directory V5.1 • Klient LDAP v2.0.23	IBM Directory V5.1	Nedostupné
Systém OS/400 v serveri iSeries	OS/400 V5R2 a OS/400 V5R3	OS/400 V5R2 a V5R3 Directory Server	Program iSeries Navigator V5R2 a V5R3
Windows 2000 v serveri xSeries	Prevezmite jedno z tohto: • Klient IBM Directory V4.1 • Klient IBM Directory V5.1	Klient IBM Directory V5.1	Nedostupné
z/OS v serveri zSeries	z/OS V1R4 LDAP SPE OW57137	z/OS V1R4 LDAP	V1R4 LDAP SPE OW57137

Poznámka: Viac informácií o produkte IBM Directory Server si môžete pozrieť na webovej lokalite produktu spoločnosti IBM na adrese http://www-3.ibm.com/software/network/help-directory/

Pokiaľ platforma poskytuje podporu klienta EIM (API), môže sa systém nachádzať v doméne EIM. Nie je potrebné, aby platforma poskytovala podporu radiča domény EIM, kým ju nechcete použiť ako radič domény EIM vo vašom podniku.

Ak ste skontrolovali splnenie všetkých požiadaviek EIM, môžete začať identifikovať potrebné zručnosti, roly a oprávnenia na konfiguráciu EIM.

Identifikácia potrebných zručností a rolí

Návrh EIM umožňuje, aby v malej organizácii bola za konfiguráciu aj správu zodpovedná jedna osoba. Vo väčšej organizácii môžete uprednostniť väčší počet rôznych osôb. Počet ľudí, ktorých potrebujete vo vašom tíme závisí od vyžadovaných zručností jednotlivých členov tímu, typov platforiem zahrnutých vo vašej implementácii EIM a preferovanom spôsobe rozdelenia bezpečnostných rolí a zodpovednosti vo vašej organizácii.

Úspešná implementácia EIM vyžaduje konfiguráciu a interakciu niekoľkých softvérových produktov. Každý z týchto produktov vyžaduje špecifické zručnosti a roly a preto môžete zvoliť vytvorenie implementačného tímu EIM, skladajúceho sa z ľudí z niekoľkých rôznych disciplín, najmä ak pracujete vo veľkej organizácii.

Nasledujúce informácie opisujú zručnosti a oprávnenia vyžadované na úspešnú implementáciu EIM. Tieto zručnosti sú uvedené v zmysle pracovných zaradení jednotlivých ľudí, ktorí sa v nich špecializujú. Napríklad úloha administrátora adresárového servera odkazuje na úlohu vyžadujúcu zručnosti týkajúce sa protokolu Lightweight Directory Access Protocol (LDAP).

Členovia tímu a ich roly

Nasledujúce informácie opisujú zodpovednosti a vyžadované oprávnenia rolí potrebných na riadenie EIM. Tento zoznam rolí môžete použiť na určenie členov tímu, ktorých potrebujete na inštaláciu a konfiguráciu vyžadovaných produktov a na konfiguráciu EIM a jednej alebo viacerých domén EIM.

Jedna z prvých množín rolí, ktoré potrebujete definovať, predstavuje počet a typy administrátorov pre vašu doménu EIM. Každá osoba s administratívnymi úlohami a oprávneniami EIM musí byť zahrnutá v procese plánovania EIM ako člen implementačného tímu EIM.

Poznámka: Administrátori EIM zohrávajú vo vašej organizácii dôležitú rolu a majú takú istú moc ako osoby, ktoré môžu vo vašich systémoch vytvárať identity užívateľov. Keď vytvoria priradenia EIM pre identity užívateľov, určia, kto môže pristupovať do vašich počítačových systémov a aké má pri prístupe privilégiá. Spoločnosť IBM odporúča, aby ste toto oprávnenie udelili osobám, ktorým dôverujete na základe bezpečnostnej politiky vašej spoločnosti.

Nasledujúca tabuľka obsahuje zoznam možných rolí členov tímu, úloh a zručnosti potrebných na konfiguráciu a riadenie EIM. Viac detailných informácií o administratívnych úlohách EIM, ktoré môže každá rola vykonávať si môžete pozrieť v časti “Riadenie prístupu EIM” na strane 33.

Poznámka: Ak bude vo vašej organizácii jedna osoba zodpovedná za všetky konfiguračné a administratívne úlohy EIM, mala by mať rolu a oprávnenie administrátora EIM.

Tabuľka 10. Roly, úlohy a zručnosti pre konfiguráciu EIM

Rola	Autorizovaná úloha	Vyžadované zručnosti
Administrátor EIM	• Koordinácia operácií v doméne • Pridanie, odstránenie a zmena definícií registrov, identifikátorov EIM a priradení pre identity užívateľov • Oprávnenie radiča pre údaje v rámci domény EIM	Znalosť administratívnych nástrojov EIM
Administrátor identifikátorov EIM	• Vytvorenie a zmena identifikátorov EIM • Pridanie a odstránenie administratívnych a zdrojových priradení (nemôže pridať ani odstrániť cieľové priradenia)	Znalosť administratívnych nástrojov EIM
Administrátor registrov EIM	Riadenie všetkých definícií registrov EIM: • Pridanie a odstránenie cieľových priradení (nemôže pridať ani odstrániť zdrojové a administratívne priradenia) • Aktualizácia definícií registrov EIM	Znalosti: • Všetkých registrov užívateľov, definovaných pre doménu EIM (napríklad informácie o identitách užívateľov) • Administratívnych nástrojov EIM
X administrátor registrov EIM	Riadenie konkrétnej definície registra EIM: • Pridanie a odstránenie cieľových priradení pre konkrétny register užívateľov (napríklad register X) • Aktualizácia konkrétnej definície registra EIM	Znalosti: • Konkrétneho registra užívateľov, definovaného pre doménu EIM (napríklad informácie o identitách užívateľov) • Administratívnych nástrojov EIM

Tabuľka 10. Roly, úlohy a zručnosti pre konfiguráciu EIM (pokračovanie)

Rola	Autorizovaná úloha	Vyžadované zručnosti
Administrátor adresárového servera (LDAP)	• Inštalácia a konfigurácia adresárového servera (ak je to potrebné) • Prispôsobenie konfigurácie adresárového servera pre EIM • Vytvorenie domény EIM (pozrite si poznámku) • Definovanie užívateľov autorizovaných pre prístup k radiču domény EIM • Voliteľné: Definovanie prvého administrátora EIM **Poznámka:** Administrátor adresárového servera môže vykonávať všetky činnosti administrátora EIM.	Znalosti: • Inštalácie, konfigurácie a prispôsobenia adresárového servera • Administratívnych nástrojov EIM
Administrátor registrov užívateľov	• Nastavenie užívateľských profilov alebo identít užívateľov pre konkrétny register užívateľov • Voliteľné: Môže zastupovať administrátora registrov EIM pre konkrétny register užívateľov	Znalosti: • Nástrojov pre spravovanie registra užívateľov • Administratívnych nástrojov EIM
Systémový programátor alebo administrátor systému	Inštalácia potrebných softvérových produktov (môže zahŕňať inštaláciu EIM)	Znalosti: • Systémového programovania alebo administratívnych zručností • Inštalačných procedúr pre platformu
Aplikačný programátor	Písanie aplikácií používajúcich rozhrania API EIM	Znalosti: • Platformy • Programovacích zručností • Kompilácie programov

Po identifikovaní rolí, ktoré chcete používať pre konfigurovanie a riadenie EIM vo vašom podniku, môžete začať plánovať doménu EIM.

Plánovanie domény Enterprise Identity Mapping

Časť úvodného procesu plánovania implementácie EIM (Enterprise Identity Mapping) vyžaduje definovanie domény EIM. Ak chcete získať maximálne výhody z vlastníctva centralizovaného archívu informácií o mapovaniach, musíte naplánovať zdieľanie domény medzi aplikáciami a systémami.

Pomocou témy plánovania EIM získate informácie, ktoré potrebujete na definovanie domény a na ich zaznamenanie v pracovných listoch plánovania. Časti s príkladmi v pracovných listoch vám môžu pomôcť získať a zaznamenať tieto informácie v každej etape plánovania tejto témy.

Nasledujúca tabuľka obsahuje zoznam informácií, ktoré potrebujete získať pri plánovaní vašej domény a návrhy roly alebo rolí implementačného tímu EIM, ktoré môžu byť zodpovedné za každú potrebnú informáciu.

Poznámka: Aj keď tabuľka obsahuje zoznam konkrétnych rolí ako návrhov pre priradenie zodpovednosti za získanie opísaných informácií, roly by ste mali priraďovať na základe potrieb a bezpečnostnej politiky vašej organizácie. Napríklad v menšej organizácii môžete uprednostniť určenie jednej osoby ako administrátora EIM, ktorý bude zodpovedný za všetky aspekty plánovania, konfigurácie a riadenia EIM.

Tabuľka 11. Informácie potrebné na plánovanie domény EIM

Potrebné informácie	Rola
1. Existuje doména spĺňajúca potreby alebo je potrebné vytvoriť novú?	Administrátor EIM
2. Ktorý adresárový server bude predstavovať radič domény EIM? (Pozrite si časť Plánovanie radiča domény EIM, kde nájdete detailné informácie k voľbe radiča domény.)	Administrátor adresárového servera (LDAP) alebo administrátor EIM
3. Názov domény. (Môžete poskytnúť aj nepovinný opis.)	Administrátor EIM
4. Kde sa nachádza adresár na uloženie údajov domény EIM? **Poznámka:** V závislosti od vašej voľby systému hostiteľa adresárového servera a v závislosti od vašej voľby adresára na uloženie údajov domény EIM budete zrejme musieť vykonať niektoré konfiguračné úlohy adresárových služieb pred vytvorením domény.	Administrátor adresárového servera (LDAP) alebo administrátor EIM
5. Aplikácie a operačné systémy, ktoré sa budú nachádzať v doméne. Ak konfigurujete vašu prvú doménu, môže to byť len jeden systém. (Pozrite si časť Vývoj plánu pomenovania definícií registrov EIM, kde nájdete viac informácií.)	Tím EIM
6. Ľudia a entity, ktoré sa budú nachádzať doméne. **Poznámka:** Ak chcete, aby bolo úvodné testovanie ľahšie, môžete obmedziť počet účastníkov na jedného alebo dvoch.	Tím EIM

Teraz, keď už viete, čo budete potrebovať na definovanie vašej domény EIM, môžete začať plánovať radič domény EIM na uloženie údajov domény EIM.

Plánovanie radiča domény Enterprise Identity Mapping

Počas zhromažďovania informácií potrebných na definovanie vašej domény EIM (Enterprise Identity Mapping) musíte určiť, ktorý produkt adresárového servera bude fungovať ako radič domény EIM. EIM vyžaduje, aby hostiteľom radiča domény bol adresárový server, ktorý podporuje protokol Lightweight Directory Access Protocol (LDAP) verzie 3. Okrem toho musí byť adresárový server schopný prijať schému LDAP a ďalšie faktory týkajúce sa EIM a podporovať určité atribúty a triedy objektov.

Ak váš podnik vlastní viac adresárových serverov schopných hosťovať radič domény EIM, mali by ste zvážiť aj použitie sekundárnych replikačných radičov domény. Napríklad, ak očakávate veľký počet operácií vyhľadávania mapovaní EIM, repliky môžu zvýšiť ich výkon.

Takisto by ste mali zvážiť, či chcete, aby radič domény bol *lokálny* alebo *vzdialený* vo vzťahu k systému, v ktorom očakávate spustenie najväčšieho počtu operácií vyhľadávania mapovaní. Ak bude radič domény lokálny voči systému s veľkým zaťažením, môže sa zvýšiť výkon operácií vyhľadávania pre lokálny systém. Na zaznamenanie týchto plánovacích rozhodnutí použite pracovné listy plánovania a takisto tie, ktoré obsahujú informácie o vašej doméne a ďalšie informácie o adresároch.

Po rozhodnutí, ktorý adresárový server vo vašom podniku bude hosťovať váš radič domény EIM, musíte urobiť niekoľko rozhodnutí o prístupe k radiču domény.

Plánovanie prístupu k radiču domény

Potrebujete naplánovať, ako budete vy, aplikácie a operačné systémy podporujúce EIM pristupovať k adresárovému serveru, ktorý je hostiteľom radiča domény EIM. Ak chcete pristupovať k doméne EIM, musíte:

1. Byť schopný vytvoriť viazanie k radiču domény EIM
2. Skontrolovať, že subjekt viazania je členom skupiny riadenia prístupu k EIM alebo je administrátorom LDAP. Viac informácií nájdete v časti Manažovanie riadenia prístupu k EIM.

Rozhrania API EIM podporujú niekoľko rôznych mechanizmov vytvorenia pripojenia, tiež známych ako viazanie, s radičom domény EIM. Každý typ mechanizmu viazania poskytuje pre pripojenie inú úroveň autentifikácie a šifrovania. Možné voľby sú:

- **Jednoduché viazania** Jednoduché viazanie je pripojenie LDAP, pri ktorom klient LDAP poskytuje na autentifikáciu rozlišovací názov a heslo viazania k serveru LDAP. Rozlišovací názov a heslo viazania definuje administrátor LDAP v adresári LDAP. Ide o najslabšiu a najmenej bezpečnú formu autentifikácie, pretože rozlišovací názov a heslo viazania sa odosielajú nešifrované a dajú sa ľahko zistiť odpočúvaním. Na zvýšenie ochrany pre heslo viazania o jednu úroveň môžete použiť mechanizmus CRAM-MD5 (autentifikačný mechanizmus otázka-odpoveď). Pri použití protokolu CRAM-MD5 klient odošle serveru na autentifikáciu hašovaciu hodnotu namiesto čistého hesla.
- **Autentifikácia serverom pomocou protokolu Secure Sockets Layer (SSL) - autentifikácia na strane servera** Server LDAP sa dá nakonfigurovať na podporu pripojení pomocou SSL alebo TSL (Transport Layer Security). Server LDAP používa na svoju autentifikáciu klientovi LDAP digitálny certifikát a vytvorí medzi nimi zašifrovanú komunikačnú reláciu. Pomocou certifikátu sa autentifikuje len server LDAP. Koncový užívateľ sa autentifikuje pomocou rozlišovacieho názvu a hesla viazania. Sila autentifikácie je taká istá ako v prípade jednoduchého viazania, ale všetky údaje sú zašifrované (vrátane rozlišovacieho názvu a hesla viazania).
- **Autentifikácia klientom pomocou protokolu SSL** Server LDAP sa dá nakonfigurovať tak, aby od koncového užívateľa vyžadoval autentifikáciu pomocou digitálneho certifikátu, a nie rozlišovacieho názvu a hesla viazania pre zabezpečené pripojenia SSL alebo TLS k serveru LDAP. Autentifikuje sa klient aj server a relácia je zašifrovaná. Táto voľba poskytuje silnejšiu úroveň autentifikácie užívateľa a chráni súkromie všetkých prenášaných údajov.
- **Autentifikácia pomocou Kerberos** Klient LDAP sa môže autentifikovať serveru pomocou lístka Kerberos ako voliteľnej náhrady rozlišovacieho názvu a hesla viazania. Protokol Kerberos je dôveryhodný systém sieťovej autentifikácie tretej strany, ktorý umožňuje, aby princípál (užívateľ alebo služba) preukázal svoju identitu inej službe v rámci nezabezpečenej siete. Autentifikácia princípálov sa dokončí prostredníctvom centrálneho servera nazvaného distribučné centrum kľúčov (KDC). Centrum KDC autentifikuje užívateľa s lístkom Kerberos. Tieto lístky preukazujú identitu princípálu iným službám v sieti. Po autentifikácii princípálu týmito lístkami si môže princípál a služba vymieňať zašifrované informácie s cieľovou službou. Táto voľba poskytuje silnejšiu úroveň autentifikácie užívateľa a chráni súkromie autentifikačných informácií.

Voľba mechanizmu viazania závisí od úrovne bezpečnosti vyžadovanej aplikáciou podporujúcou EIM a autentifikačného mechanizmu podporovaného serverom LDAP, ktorý je hostiteľom domény EIM.

Okrem toho budete zrejme musieť na aktivovanie zvoleného autentifikačného mechanizmu vykonať ďalšie konfiguračné úlohy servera LDAP. Pozrite si dokumentáciu servera LDAP, ktorý je hostiteľom vášho radiča domény, kde sa dozviete, aké ďalšie konfiguračné úlohy potrebujete vykonať.

Príklad pracovného listu plánovania: Informácie o radiči domény

Po vykonaní rozhodnutí týkajúcich sa vášho radiča domény EIM môžete použiť pracovné listy plánovania na zaznamenanie informácií o radiči domény EIM, potrebných pre operačné systémy a aplikácie podporujúce EIM. Informácie, ktoré zhromaždíte v tejto časti procesu môže použiť administrátor LDAP na definovanie identity viazania aplikácie alebo operačného systému pre adresárový server LDAP, ktorý je hostiteľom radiča domény EIM.

Nasledujúca vzorová časť pracovného listu plánovania znázorňuje typy informácií, ktoré potrebujete získať. Takisto zahŕňa vzorové hodnoty, ktoré môžete použiť pri konfigurácii radiča domény EIM.

Tabuľka 12. Informácie o doméne a radiči domény pre pracovný list plánovania EIM

Informácie potrebné na konfiguráciu domény EIM a radiča domény EIM	Príklady odpovedí
Zmysluplný názov domény. Môže to byť názov spoločnosti, oddelenia alebo aplikácie používajúcej doménu.	MyDomain

Tabuľka 12. Informácie o doméne a radiči domény pre pracovný list plánovania EIM (pokračovanie)

Informácie potrebné na konfiguráciu domény EIM a radiča domény EIM	**Príklady odpovedí**
Voliteľné: Ak konfigurujete doménu EIM v existujúcom adresári LDAP, zadajte rodičovský rozlišovací názov domény. Toto je rozlišovací názov, ktorý reprezentuje položku bezprostredne nad položkou názvu vašej domény v stromovej hierarchii informácií v adresároch, napríklad o=ibm,c=us.	o=ibm,c=us
Výsledný úplný rozlišovací názov domény EIM. Toto je úplne definovaný názov domény EIM, ktorý opisuje umiestnenie adresára pre údaje domény EIM. Úplný rozlišovací názov domény sa skladá minimálne z doménového DN (ibm-eimDomainName=) a názvu domény, ktorý ste zadali. Ak používate rodičovské DN, bude sa úplné doménové DN skladať z relatívneho doménového DN (ibm-eimDomainName=), názvu domény (MyDomain) a rodičovského DN (o=ibm,c=us). **Poznámka:**	Jedno z týchto, v závislosti od voľby rodičovského DN: • ibm-eimDomainName=MyDomain • ibm-eimDomainName=MyDomain,o=ibm,c=us
Adresa pripojenia pre radič domény. Obsahuje typ pripojenia (základné ldap alebo bezpečné ldap, napríklad ldap:// alebo ldaps://) a nasledujúce informácie:	ldap://
• Voliteľné: Názov alebo adresa IP hostiteľa • Voliteľné: Číslo portu	• some.ldap.host • 389
Výsledná úplná adresa pripojenia pre radič domény.	ldap://some.ldap.host:389
Mechanizmus viazania, vyžadovaný aplikáciami alebo systémami. Voľby zahŕňajú: • Jednoduché viazanie • CRAM MD5 • Autentifikácia serverom • Autentifikácia klientom • Kerberos	Kerberos

Ak má váš tím konfigurácie a správy EIM viacero členov, budete musieť určiť identitu a mechanizmus viazania, ktorý musí každý člen používať pri prístupe k doméne EIM v závislosti od jeho roly. Okrem toho potrebujete určiť identitu a mechanizmus viazania pre koncových užívateľov aplikácií EIM. Nasledujúci pracovný list vám môže pomôcť ako príklad pri získavaní týchto informácií.

Tabuľka 13. Príklad pracovného listu plánovania identít viazania

Oprávnenie alebo rola EIM	**Identita viazania**	**Mechanizmus viazania**	**Potrebný dôvod**
Administrátor EIM	eimadmin@krbrealm1.com	kerberos	konfigurácia a riadenie EIM
Administrátor LDAP	cn=administrator	jednoduché viazanie	konfigurácia radiča domény EIM
X administrátor registrov EIM	cn=admin2	CRAM MD5	riadenie konkrétnych definícií registrov
Vyhľadávanie mapovania EIM	cn=MyApp,c=US	jednoduché viazanie	vykonávanie operácií vyhľadávania mapovaní v aplikáciách

Po získaní potrebných informácií na konfiguráciu vášho radiča domény môžete začať vyvíjať plán mapovania identity.

Vývoj plánu pomenovania definícií registrov Enterprise Identity Mapping

Ak chcete používať EIM (Enterprise Identity Mapping) na mapovanie identity užívateľa v jednom registri užívateľov k ekvivalentnej identite užívateľa v inom registri užívateľov, musia byť oba registre užívateľov pre EIM definované. Musíte vytvoriť definíciu registra EIM pre každý register užívateľov aplikácie alebo operačného systému, ktorý sa bude nachádzať v doméne EIM. Registre užívateľov môžu reprezentovať registre operačného systému, napríklad Resource Access Control Facility (RACF) alebo OS/400, distribuovaný register ako napríklad Kerberos alebo podmnožinu systémového registra, ktorý exkluzívne používa iná aplikácia.

Doména EIM môže obsahovať definície registrov pre registre užívateľov, existujúce v inej platforme. Napríklad doména riadená radičom domény v systéme OS/400 môže obsahovať definície registrov pre platformy iné ako OS/400 (napríklad register AIX). Aj keď môžete pre doménu EIM definovať ľubovoľný register užívateľov, musíte definovať registre užívateľov pre aplikácie a operačné systémy podporujúce EIM.

Definícii registra EIM môžete dať ľubovoľný názov, ktorý však musí byť v doméne EIM jedinečný. Napríklad definíciu registra EIM môžete pomenovať na základe názvu systému, ktorý je hostiteľom registra užívateľov. Ak to je nie dostačujúce na rozlíšenie definície registra od podobných definícií, môžete použiť bodku (.) alebo znak podčiarknutia (_) na pridanie typu registra užívateľov, ktorý definujete. Bez ohľadu na kritérium, ktoré budete používať, by ste mali zvážiť vyvinutie názvovej konvencie pre vaše definície registrov EIM. Týmto zabezpečíte konzistenciu názvov definícií v rámci domény a adekvátny opis typu, inštancie a spôsobu použitia definovaného registra užívateľov. Napríklad názov každej definície registra môžete zvoliť ako kombináciu názvu aplikácie alebo operačného systému používajúceho register a fyzického umiestnenia registra užívateľov vo vašom podniku.

Aplikácia používajúca EIM môže zadať alias zdrojového registra, alias cieľového registra alebo oboch. Pri vytváraní definícií registrov EIM by ste mali skontrolovať dokumentáciu vašich aplikácií, aby ste zistili, či potrebujete zadať jeden alebo viac aliasov pre definície registrov. Ak priradíte tieto aliasy vhodným definíciám registrov, aplikácia môže vykonať hľadanie aliasu, aby našla definíciu alebo definície registrov EIM, zhodujúce sa s aliasmi v aplikácii.

Nasledujúca vzorová časť pracovného listu plánovania vám môže pomôcť ako návod pre zaznamenanie informácií o zúčastnených registroch užívateľov. Skutočný pracovný list môžete použiť na zadanie názvu definície registra pre každý register užívateľov, na zadanie, či používa alias a na opis jeho umiestnenia a použitia. Niektoré informácie, ktoré potrebujete pre pracovný list, vám poskytne dokumentácia k inštalácii a konfigurácii aplikácie.

Tabuľka 14. Vzor pracovného listu plánovania informácií o definícii registra EIM

Názov definície registra	Typ registra užívateľov	Alias definície registra	Opis registra
System_C	Register užívateľov systému OS/400	Pozrite si dokumentáciu k aplikácii	Hlavný systémový register užívateľov pre operačný systém OS/400 v systéme C
System_A_WAS	WebSphere LTPA	app_23_alias_source	Register užívateľov WebSphere LTPA v systéme A
System_B	Linux	Pozrite si dokumentáciu k aplikácii	Register užívateľov systému Linux v systéme B
System_A	Register užívateľov systému OS/400	app_23_alias_target app_xx_alias_target	Hlavný systémový register užívateľov pre operačný systém OS/400 v systéme A
System_D	Register užívateľov Kerberos	app_xx_alias_source	legal.mydomain.com Kerberos realm
System_4	Register užívateľov systému Windows 2000	Pozrite si dokumentáciu k aplikácii	Register užívateľov aplikácie ľudských zdrojov v systéme 4

Poznámka: Typy priradení pre každý register sa určia neskôr v procese plánovania.

Po dokončení tejto časti pracovného listu plánovania by ste mali začať vyvíjať váš plán mapovania identity na určenie, či budete používať na vytvorenie mapovaní potrebných pre identity užívateľov v každom definovanom registri užívateľov priradenia identifikátorov, priradenia politiky alebo oba typy priradení.

Vývoj plánu mapovania identity

Kritická časť úvodného procesu plánovania implementácie EIM (Enterprise Identity Mapping) vyžaduje určenie spôsobu používania mapovania identity vo vašom podniku. Na mapovanie identít v EIM môžete použiť dve metódy:

- **Priradenia identifikátorov** opisujú vzťahy medzi identifikátorom EIM a identitami užívateľov v registroch užívateľov, ktoré reprezentujú danú osobu. Priradenie identifikátora vytvorí priame mapovanie typu veľa-jeden medzi identifikátorom EIM a konkrétnou identitou užívateľa. Priradenia identifikátorov môžete použiť na nepriame definovanie vzťahu medzi identitami užívateľov pomocou identifikátora EIM.

  Ak vaša bezpečnostná politika vyžaduje vysoký stupeň sledovateľnosti, budete zrejme musieť pre vašu implementáciu mapovania identít používať výhradne priradenia identifikátorov. Priradenia identít používate na vytvorenie mapovaní typu veľa-jeden pre identity užívateľov, ktoré vlastnia užívatelia a preto môžete vždy presne určiť, kto vykonal akciu na objekte alebo v systéme.
- **Priradenia politiky** opisujú vzťah medzi viacerými identitami užívateľov a jednou identitou užívateľa v registri užívateľov. Priradenia politiky používajú podporu politík mapovania EIM na vytvorenie mapovaní typu veľa-jeden medzi identitami užívateľov bez použitia identifikátora EIM.

  Priradenia politiky môžu byť použiteľné, ak máte jednu alebo viac veľkých skupín užívateľov, ktorí potrebujú pristupovať k systémom alebo aplikáciám vo vašom podniku, ale nechcete im pre získanie tohto prístupu vytvárať vlastné identity užívateľov. Napríklad udržiavate webovú aplikáciu, ktorá pristupuje ku konkrétnej internej aplikácii. Zrejme nebudete chcieť nastavovať stovky alebo tisícky identít užívateľov na autentifikáciu užívateľov pre túto internú aplikáciu. V tejto situácii je vhodné nakonfigurovať mapovanie identity tak, aby všetci užívatelia webovej aplikácie boli namapovaní k jednej identite užívateľa s minimálnou úrovňou autorizácie, potrebnou na spustenie aplikácie. Tento typ mapovania identity môžete vytvoriť pomocou priradení politiky.

Môžete sa rozhodnúť pre použitie priradenia identifikátorov na poskytnutie najlepšieho riadenia identít užívateľov vo vašom podniku a získanie najvyššieho stupňa efektívneho manažmentu hesiel. Alebo sa môžete rozhodnúť pre použitie kombinácie priradení politiky a priradení identifikátorov na zavedenie jednoduchého prihlásenia a udržiavanie špecifického riadenia identít užívateľov pre administrátorov. Bez ohľadu na výber mapovania identity, ktoré podľa vášho rozhodnutia najlepšie spĺňa vaše obchodné potreby a bezpečnostnú politiku, musíte vytvoriť plán mapovania identít na zabezpečenie vhodnej implementácie.

Ak chcete vytvoriť plán mapovania identít, musíte vykonať toto:

- "Vývoj plánu pomenovania identifikátorov EIM" na strane 54
- "Plánovanie priradení v Enterprise Identity Mapping"

Plánovanie priradení v Enterprise Identity Mapping: Priradenia sú položky vytvorené v doméne EIM, ktoré definujú vzťah medzi identitami užívateľov v rôznych registroch užívateľov. V EIM môžete vytvoriť jeden z dvoch typov priradení: priradenia identifikátorov, ktoré definujú mapovania typu veľa-jeden a priradenia politiky, ktoré definujú mapovania typu veľa-jeden. Priradenia politiky môžete používať namiesto alebo v kombinácii s priradeniami identifikátorov.

Špecifické typy priradení, ktoré chcete vytvoriť závisia od spôsobu používania konkrétnej identity užívateľa užívateľom a takisto od celkového plánu mapovania identity.

Môžete vytvoriť ľubovoľný z nasledujúcich typov priradení identifikátorov:

- **Cieľové priradenia**

  Cieľové priradenia definujete pre užívateľov, ktorí za normálnych okolností pristupujú k tomuto systému ako k serveru z iného klientskeho systému. Tento typ priradenia sa používa, keď aplikácia vykonáva operácie vyhľadávania mapovaní.
- **Zdrojové priradenia**

  Zdrojové priradenia definujete, keď identita užívateľa predstavuje prvú identitu užívateľa, ktorú užívateľ poskytne na prihlásenie do systému alebo siete. Tento typ priradenia sa používa, keď aplikácia vykonáva operácie vyhľadávania mapovaní.
- **Administratívne priradenia**

Administratívne priradenia definujete, ak chcete mať možnosť sledovať fakt, že identita užívateľa patrí konkrétnemu užívateľovi, ale nechcete, aby bola dostupná pre operácie vyhľadávania mapovaní. Tento typ priradenia môžete použiť na sledovanie všetkých identít užívateľov, ktoré jedna osoba používa v podniku.

Priradenie politiky vždy definuje cieľové priradenie.

Je možné, aby jedna definícia registra mala viac ako jeden typ priradenia, v závislosti od spôsobu používania registra užívateľov, na ktorý odkazuje. Aj keď neexistuje žiadne obmedzenie počtu alebo kombinácií priradení, ktoré môžete definovať, mal by byť ich počet z dôvodu zjednodušenia správy vašej domény EIM minimálny.

Aplikácia typicky poskytne informácie o definíciách registrov, ktoré očakáva pre zdrojové a cieľové registre, ale nie pre typy priradení. Každý koncový užívateľ aplikácie musí byť namapovaný k aplikácii prostredníctvom aspoň jedného priradenia. Toto priradenie môže byť mapovanie typu veľa-jeden medzi jedinečným identifikátorom EIM a identitou užívateľa vo vyžadovanom cieľovom registri alebo mapovanie typu veľa-jeden medzi zdrojovým registrom, ktorého členom je identita užívateľa a vyžadovaným cieľovým registrom. Typ priradenia, ktorý použijete závisí od vašich požiadaviek na mapovanie identity a kritériu poskytnutom aplikáciou.

Ako časť procesu plánovania ste už dokončili dva pracovné listy plánovania pre identity užívateľov vo vašej organizácii, obsahujúce informácie o potrebných identifikátoroch EIM a definíciách registrov EIM. Teraz potrebujete tieto informácie spojiť pomocou určenia typov priradení, ktoré chcete použiť na mapovanie identít užívateľov vo vašom podniku. Musíte určiť, či sa má definovať priradenie politiky pre konkrétnu aplikáciu a jej registre užívateľov, alebo či sa majú definovať špecifické priradenia identifikátorov (zdrojové, cieľové alebo administratívne) pre každú identitu užívateľa v systéme alebo registri aplikácií. Môžete to dosiahnuť zaznamenaním informácií o vyžadovaných typoch priradení v pracovnom liste plánovania definícií registrov a v zodpovedajúcich riadkoch každého pracovného listu priradení.

Na dokončenie vášho plánu mapovania identity môžete ako návod použiť nasledujúce príklady pracovných listov, ktoré vám pomôžu zaznamenať informácie o priradení, ktoré potrebujete na opis celkového obrazu plánu implementácie mapovania identity.

Tabuľka 15. Príklad pracovného listu plánovania informácií o definícii registra EIM

Názov definície registra	Typ registra užívateľov	Alias definície registra	Opis registra	Typy priradení
System_C	Register užívateľov systému OS/400	Pozrite si dokumentáciu k aplikácii	Hlavný systémový register užívateľov pre operačný systém OS/400 v systéme C	Cieľové
System_A_WAS	WebSphere LTPA	app_23_alias_source	Register užívateľov WebSphere LTPA v systéme A	Primárne zdrojové
System_B	Linux	Pozrite si dokumentáciu k aplikácii	Register užívateľov systému Linux v systéme B	Zdrojové a cieľové
System_A	Register užívateľov systému OS/400	app_23_alias_target app_xx_alias_target	Hlavný systémový register užívateľov pre operačný systém OS/400 v systéme A	Cieľové
System_D	Register užívateľov Kerberos	app_xx_alias_source	legal.mydomain.com Kerberos realm	Zdrojové
System_4	Register užívateľov systému Windows 2000	Pozrite si dokumentáciu k aplikácii	Register užívateľov aplikácie ľudských zdrojov v systéme 4	Administratívne

Tabuľka 15. Príklad pracovného listu plánovania informácií o definícii registra EIM (pokračovanie)

Názov definície registra	Typ registra užívateľov	Alias definície registra	Opis registra	Typy priradení
order.mydomain.com	Register užívateľov systému Windows 2000		Hlavný prihlasovací register pre zamestnancov oddelenia objednávok	Predvolená politika registra (zdrojový register)
System_A_order_app	Aplikácia oddelenia objednávok		Špecifický register aplikácie pre aktualizácie objednávok	Predvolená politika registra (cieľový register)
System_C_order_app	Aplikácia oddelenia objednávok		Špecifický register aplikácie pre aktualizácie objednávok	Predvolená politika registra (cieľový register)

Tabuľka 16. Príklad pracovného listu plánovania identifikátorov EIM

Jedinečný názov identifikátora	Opis identifikátora alebo identity užívateľa	Alias identifikátora
John S Day	Manažér ľudských zdrojov	app_23_admin
John J Day	Právne oddelenie	app_xx_admin
Sharon A. Jones	Administrátor oddelenia objednávok	

Tabuľka 17. Príklad pracovného listu plánovania priradení identifikátorov

Jedinečný názov identifikátora: _____John S Day_____		
Register užívateľov	**Identita užívateľa**	**Typy priradení**
WAS systému A	johnday	Zdrojové
Operačný systém Linux v systéme B	jsd1	Zdrojové a cieľové
OS/400 v systéme C	JOHND	Cieľové
Register 4 v systéme ľudských zdrojov Windows 2000	JDAY	Administratívne

Tabuľka 18. Príklad pracovného listu plánovania priradení politiky

Typ priradenia politiky	Zdrojový register užívateľov	Cieľový register užívateľov	Identita užívateľa	Opis
Predvolený register	order.mydomain.com	System_A_order_app	SYSUSERA	Mapuje autentifikovaného užívateľa oddelenia objednávok systému Windows na vhodnú identitu užívateľa aplikácie
Predvolený register	order.mydomain.com	System_C_order_app	SYSUSERB	Mapuje autentifikovaného užívateľa oddelenia objednávok systému Windows na vhodnú identitu užívateľa aplikácie

Vývoj plánu pomenovania identifikátorov EIM: Pri plánovaní vašich potrieb mapovania identity EIM môžete vytvoriť jedinečné identifikátory EIM pre užívateľov aplikácií podporujúcich EIM a operačných systémov vo vašom

podniku, ak chcete vytvoriť mapovania typu veľa-jeden medzi identitami užívateľa a samotným užívateľom. Používaním priradení identifikátorov na vytvorenie mapovaní typu veľa-jeden môžete maximalizovať výhody manažmentu hesiel, ktoré EIM poskytuje.

Plán pomenovania, ktorý vyvíjate, závisí od vašich obchodných potrieb a preferencií; jediná požiadavka je jedinečnosť názvov identifikátorov EIM. Niektoré spoločnosti môžu uprednostniť použitie celého mena osoby; iné spoločnosti môžu uprednostniť iný typ údajov, napríklad číslo zamestnanca. Ak chcete vytvoriť názvy identifikátorov EIM na základe celého mena osoby, musíte brať do úvahy aj možné duplicitné mená. Spôsob, akým sa vysporiadate s duplicitnými názvami identifikátorov, závisí len od vašich rozhodnutí. Na zabezpečenie jedinečnosti budete možno chcieť pridať ku každému názvu identifikátora dopredu určený znakový reťazec; môžete sa napríklad rozhodnúť pridať číslo oddelenia každej osoby.

Ako časť vývoja plánu pomenovania identifikátorov EIM sa musíte rozhodnúť o vašom celkovom pláne mapovania identity. Môže vám to pomôcť pri rozhodovaní o potrebe použitia identifikátorov a priradení identifikátorov alebo priradení politiky na mapovanie identít v rámci vášho podniku. Pri vývoji vášho plánu pomenovania identifikátorov EIM môžete použiť nižšie uvedené pracovné listy, ktoré vám pomôžu so zhromaždením informácií o identitách užívateľov vo vašej organizácii a s plánovaním identifikátorov pre identity užívateľov. Pracovný list predstavuje informácie, ktoré administrátor EIM potrebuje vedieť pri vytváraní identifikátorov EIM alebo priradení politiky pre užívateľov aplikácie.

Tabuľka 19. Príklad pracovného listu plánovania identifikátorov EIM

Jedinečný názov identifikátora	**Opis identifikátora alebo identity užívateľa**	**Alias identifikátora**
John S Day	Manažér ľudských zdrojov	app_23_admin
John J Day	Právne oddelenie	app_xx_admin
Sharon A. Jones	Administrátor oddelenia objednávok	

Aplikácia používajúca EIM môže zadať alias, ktorý bude používať pri hľadaní vhodného identifikátora EIM pre aplikáciu, ktorú môže použiť na určenie konkrétnej identity užívateľa na použitie. Mali by ste skontrolovať dokumentáciu vašich aplikácií, ak chcete zistiť, či potrebujete pre identifikátor zadať jeden alebo viac aliasov. Polia identifikátora EIM a opisu identity užívateľa majú voľnú formu a používajú sa na poskytnutie opisných informácií o užívateľovi.

Identifikátory EIM nemusíte vytvárať pre všetkých členov vášho podniku naraz. Po vytvorení úvodného identifikátora EIM a jeho použití na testovanie vašej konfigurácie EIM, môžete ďalšie identifikátory EIM vytvárať na základe cieľov vašej organizácie pre používanie EIM. Identifikátory EIM môžete pridať napríklad pre jednotlivé oddelenia alebo oblasti. Alebo ich môžete pridávať počas nasadenia ďalších aplikácií EIM.

Po dokončení zhromažďovania informácií potrebných na vývoj plánu pomenovania identifikátorov EIM môžete začať plánovať priradenia pre vaše identity užívateľov.

Pracovné listy plánovania implementácie Enterprise Identity Mapping

Počas procesu plánovania EIM (Enterprise Identity Mapping) môžete zistiť, že tieto pracovné listy pomáhajú pri zhromažďovaní informácií, ktoré budete potrebovať na konfiguráciu a používanie EIM vo vašom podniku. Príklady dokončených častí pracovných listov sú poskytnuté na stránkach plánovania pri vhodnej príležitosti.

Tieto pracovné listy sú poskytnuté ako príklad typov pracovných listov, ktoré potrebujete pre váš plán implementácie EIM. Počet poskytnutých položiek je menší ako počet, ktorý budete pravdepodobne potrebovať pre vaše informácie o EIM. Tieto pracovné listy môžete editovať, aby boli vo vašej situácii užitočnejšie.

Tabuľka 20. Pracovné listy s informáciami o doméne a radiči domény

Informácie potrebné na konfiguráciu domény EIM a radiča domény EIM	**Odpovede**
Zmysluplný názov domény. Môže to byť názov spoločnosti, oddelenia alebo aplikácie používajúcej doménu.	
Voliteľné: Rodičovský rozlišovací názov domény. Toto je rozlišovací názov, ktorý reprezentuje položku bezprostredne nad položkou názvu vašej domény v stromovej hierarchii informácií v adresároch, napríklad o=ibm,c=us.	
Výsledný úplný rozlišovací názov domény EIM. Toto je úplne definovaný názov domény EIM, ktorý opisuje umiestnenie adresára pre údaje domény EIM. Úplný rozlišovací názov domény sa skladá minimálne z doménového DN (ibm-eimDomainName=) a názvu domény, ktorý ste zadali. Ak používate rodičovské DN, bude sa úplné doménové DN skladať z relatívneho doménového DN (ibm-eimDomainName=), názvu domény (MyDomain) a rodičovského DN (o=ibm,c=us).	
Adresa pripojenia pre radič domény. Obsahuje typ pripojenia (základné ldap alebo bezpečné ldap, napríklad ldap:// alebo ldaps://) a nasledujúce informácie:	
• Voliteľné: Názov alebo adresa IP hostiteľa • Voliteľné: Číslo portu	
Výsledná úplná adresa pripojenia pre radič domény.	
Mechanizmus viazania, vyžadovaný aplikáciami alebo systémami. Voľby zahŕňajú: • Jednoduché viazanie • CRAM MD5 • Autentifikácia serverom • Autentifikácia klientom • Kerberos	

Príklad použitia tohto pracovného listu si môžete pozrieť v časti Plánovanie radiča domény EIM.

Tabuľka 21. Pracovný list plánovania identít viazania

Oprávnenie alebo rola EIM	**Identita viazania**	**Mechanizmus viazania**	**Potrebný dôvod**

Príklad použitia tohto pracovného listu si môžete pozrieť v časti Plánovanie radiča domény EIM.

Tabuľka 22. Pracovný list plánovania informácií o definícii registra EIM

Názov definície registra	Typ registra užívateľov	Alias definície registra	Opis registra	Typy priradení

Príklad použitia tohto pracovného listu si môžete pozrieť v časti Vývoj plánu pomenovania definícií registrov EIM.

Tabuľka 23. Pracovný list plánovania identifikátorov EIM

Jedinečný názov identifikátora	Opis identifikátora alebo identity užívateľa	Alias identifikátora

Príklad použitia tohto pracovného listu si môžete pozrieť v časti Vývoj plánu pomenovania identifikátorov EIM.

Tabuľka 24. Pracovný list plánovania priradení identifikátorov

Jedinečný názov identifikátora: _____John S Day_____		
Register užívateľov	**Identita užívateľa**	**Typy priradení**

Tabuľka 24. Pracovný list plánovania priradení identifikátorov (pokračovanie)

Jedinečný názov identifikátora: _____John S Day_____		
Register užívateľov	**Identita užívateľa**	**Typy priradení**

Príklad použitia tohto pracovného listu si môžete pozrieť v časti Plánovanie priradení EIM.

Tabuľka 25. Pracovný list plánovania priradení politiky

Typ priradenia politiky	**Zdrojový register užívateľov**	**Cieľový register užívateľov**	**Identita užívateľa**	**Opis**

Príklad použitia tohto pracovného listu si môžete pozrieť v časti Plánovanie priradení EIM.

Plánovanie vývoja aplikácií podporujúcich Enterprise Identity Mapping

Aplikácia musí byť schopná používať rozhrania API EIM, aby mohla používať EIM (Enterprise Identity Mapping) a aby sa mohla nachádzať v doméne. Mali by ste si pozrieť dokumentáciu rozhraní API EIM a takisto dokumentáciu EIM, špecifickú pre vašu platformu, aby ste vedeli určiť, či existujú špeciálne aspekty plánovania, ktorým by ste mali rozumieť pri písaní alebo prispôsobovaní aplikácií na používanie rozhraní API EIM. Napríklad môžu existovať faktory týkajúce sa kompilácie aplikácií vytvorených v jazyku C alebo C++, ktoré obsahujú volania rozhraní API EIM. Takisto, v závislosti od platformy aplikácie môžu existovať ďalšie faktory týkajúce sa procesu zostavovania aplikácie.

Plánovanie Enterprise Identity Mapping pre OS/400

Existuje viacero technológií a služieb, ktoré EIM (Enterprise Identity Mapping) zahŕňa v serveri iSeries. Pred konfigurovaním EIM vo vašom serveri by ste sa mali rozhodnúť, ktorú funkčnosť chcete implementovať pomocou EIM a schopností jednoduchého prihlásenia.

Pred implementáciou EIM by ste mali vybrať základné bezpečnostné požiadavky pre vašu sieť a implementovať ich. EIM poskytuje administrátorom a užívateľom jednoduchší manažment identít v podniku. Pri používaní so službou sieťovej autentifikácie EIM poskytuje pre váš podnik schopnosti jednoduchého prihlásenia.

Ak sa chcete dozvedieť viac o plánovaní vašej konfigurácie EIM pre server iSeries, pozrite si nasledujúce informácie:

- "Požiadavky inštalácie EIM pre iSeries"
- "Inštalácia vyžadovaných volieb iSeries Navigator" na strane 59
- "Aspekty zálohy a obnovy pre Enterprise Identity Mapping" na strane 59

Ak plánujte používať protokol Kerberos na autentifikáciu užívateľov ako súčasť implementácie jednoduchého prihlásenia, mali by ste takisto nakonfigurovať službu sieťovej autentifikácie. Pozrite si tému Plánovanie služby sieťovej autentifikácie, kde nájdete informácie o plánovaní služby sieťovej autentifikácie a dokument Plánovanie jednoduchého prihlásenia, kde nájdete informácie o plánovaní prostredia s jednoduchým prihlásením.

Požiadavky inštalácie EIM pre iSeries

Nasledujúci plánovací pracovný list identifikuje služby, ktoré by ste mali nainštalovať pred konfiguráciou EIM.

Tabuľka 26. Plánovací pracovný list inštalácie EIM

Pracovný list pre plánovanie požiadaviek pre EIM	**Odpovede**
Je váš OS/400 V5R2 (5722-SS1) alebo novší?	

Tabuľka 26. Plánovací pracovný list inštalácie EIM (pokračovanie)

Pracovný list pre plánovanie požiadaviek pre EIM	Odpovede
Sú nasledujúce voľby a licenčné produkty nainštalované na iSeries™? • OS/400 Hostiteľské servery (5722-SS1, voľba 12) • iSeries Access for Windows® (5722-XE1) • Cryptographic Access Provider (5722-AC3) • Qshell Interpreter (5722-SS1, voľba 30) Potrebné, ak plánujte konfigurovať službu sieťovej autentifikácie spolu s EIM.	
Zahrňuje iSeries Navigator nainštalovaný v PC administrátora tieto podkomponenty? • Bezpečnosť Potrebné, ak plánujte konfigurovať službu sieťovej autentifikácie spolu s EIM. • Sieť	
Máte nainštalovaný najnovší servisný balík pre iSeries Access for Windows? Ak chcete najnovší servisný balík, pozrite si iSeries Access .	
Ak je adresárový server, napríklad IBM Directory Server pre iSeries (LDAP,) aktuálne nakonfigurovaný a chcete ho použiť ako radič domény EIM, poznáte rozlišovacie meno a heslo administrátora LDAP?	
Ak je adresárový server aktuálne nakonfigurovaný, môže byť dočasne zastavený? (Bude to potrebné kvôli dokončeniu procesu konfigurácie EIM.)	
Máte špeciálne oprávnenia *SECADM, *ALLOBJ a *IOSYSCFG?	
Aplikovali ste najnovšie dočasné opravy programu (PTF)?	

Inštalácia vyžadovaných volieb iSeries Navigator

Ak chcete aktivovať prostredie s jednoduchým prihlásením s EIM a službu sieťovej autentifikácie, musíte nainštalovať obidve, voľbu **Sieť** a voľbu **Bezpečnosť** programu iSeries Navigator. EIM sa nachádza pod voľbou **Sieť** a služba sieťovej autentifikácie sa nachádza pod voľbou **Bezpečnosť**. Ak neplánujete používať vo vašej sieti službu sieťovej autentifikácie, nepotrebujete nainštalovať voľbu **Bezpečnosť** programu iSeries Navigator.

Ak chcete nainštalovať voľbu Sieť programu iSeries Navigator alebo overiť, že už máte túto voľbu nainštalovanú, zaistite aby bol program iSeries Access for Windows nainštalovaný v PC, ktoré používate na spravovanie servera iSeries.

Ak chcete nainštalovať voľbu **Sieť**, vykonajte tieto kroky:

1. Kliknite na **Start > Programs > IBM iSeries Access for Windows > Selektívne nastavovanie**.
2. Riaďte sa inštrukciami z dialógového okna. V dialógovom okne **Výber komponentov** rozviňte **iSeries Navigator** a potom vyberte voľbu **Sieť**. Ak plánujete používať službu sieťovej autentifikácie, mali by ste tiež vybrať voľbu **Bezpečnosť**.
3. Pokračujte cez zvyšok **Selektívneho nastavovania**.

Aspekty zálohy a obnovy pre Enterprise Identity Mapping

Musíte vyvinúť plán zálohovania a obnovy pre vaše údaje EIM (Enterprise Identity Mapping), aby ste zabezpečili ich ochranu a možnú obnovu v prípade problému s adresárovým serverom, ktorý je hostiteľom radiča domény EIM. Okrem toho potrebujete dôležité informácie o konfigurácii EIM, aby ste porozumeli obnove.

Záloha a obnova údajov domény EIM

Spôsob uloženia vašich údajov EIM závisí od vášho rozhodnutia o spôsobe riadenia tohto aspektu adresárového servera, ktorý predstavuje radič domény pre vaše údaje EIM.

Jedným zo spôsobov zálohovania údajov, vhodným najmä na účely obnovy pri nehode, je uloženie databázovej knižnice. Pri predvolených nastaveniach to je QUSRDIRDB. Ak je povolený protokol zmien changelog, mali by ste

uložiť aj knižnicu QUSRDIRCL. Adresárový server v systéme, kde chcete obnoviť knižnicu, musí mať takú istú schému a konfiguráciu LDAP ako pôvodný adresárový server. Súbory, ktoré ukladajú tieto informácie sa nachádzajú v adresári /QIBM/UserData/OS400/DirSrv. Ďalšie konfiguračné údaje sú uložené v QUSRSYS/QGLDCFG (objekt *USRSPC) a QUSRSYS/QGLDVLDL (objekt *VLDL). Ak chcete mať kompletnú zálohu všetkého pre váš adresárový server, musíte uložiť obe knižnice, súbory integrovaného súborového systému a objekty QUSRSYS.

Vhodné je pozrieť si dokument Informácie adresárového servera pre uloženie a obnovu v téme Informačného centra pre produkt IBM Directory Server for iSeries (LDAP), kde sa dozviete viac o spôsobe uloženia a obnovy základných údajov adresárového servera.

Napríklad na uloženie celého obsahu adresárového servera alebo jeho časti môžete použiť súbor LDIF. Ak chcete zálohovať doménové informácie pre radič domény produktu IBM Directory Server for iSeries, vykonajte tieto kroky:

- V programe iSeries Navigator, rozviňte **Sieť > Servery > TCP/IP**.
- Pravým tlačidlom myši kliknite na **Adresárový server IBM**, vyberte **Nástroje** a potom vyberte **Exportovať súbor**, aby sa zobrazila strana, ktorá vám umožní zadať časti obsahu adresárového servera, ktoré chcete exportovať do súboru.
- Preneste súbor pre export do servera iSeries, ktorý chcete používať ako záložný adresárový server.
- V programe iSeries Navigator v záložnom serveri rozviňte **Sieť > Servery > TCP/IP**.
- Pravým tlačidlom myši kliknite na **Adresárový server IBM**, vyberte **Nástroje** a potom vyberte **Importovať**, aby sa načítal obsah preneseného súboru do nového adresárového servera.

Ďalšou metódou, ktorú môžete zvážiť pri ukladaní vašich údajov EIM, je konfigurácia a používanie replikačného adresárového servera. Všetky zmeny údajov domény EIM sú automaticky postúpené replikačnému adresárovému serveru, čo znamená, že pri zlyhaní alebo strate údajov EIM adresárovým serverom, ktorý predstavuje hostiteľa radiča domény, ich môžete opakovane získať z replikačného servera.

Spôsob konfigurácie a používania replikačného adresárového servera závisí od typu replikačného modelu, ktorý budete používať. Viac informácií o replikácii a konfigurovaní adresárového servera na replikáciu si môžete pozrieť v častiach Replikácia a Riadenie replikácií v téme Informačného centra produktu IBM Directory Server for iSeries (LDAP).

Záloha a obnova konfiguračných informácií EIM

V prípade zlyhania systému budete možno potrebovať obnoviť jeho konfiguračné informácie EIM. Tieto informácie sa nedajú jednoducho ukladať a obnovovať medzi systémami.

Pri ukladaní a obnove konfigurácie EIM sú dostupné tieto voľby:

- Na uloženie konfiguračných informácií EIM a ďalších dôležitých konfiguračných informácií použite príkaz SAVSECDTA (Save Security Data). Potom obnovte objekt užívateľského profilu QSYS v každom systéme.

  Poznámka: V každom systéme s konfiguráciou EIM musíte použiť príkaz SAVSCEDTA a obnoviť objekt užívateľského profilu QSYS samostatne. Ak sa pokúsite obnoviť objekt užívateľského profilu QSYS v systéme, v ktorom nebol uložený, môžu sa vyskytnúť problémy.
- Znovu spustite sprievodcu konfiguráciou EIM alebo manuálne zaktualizujte vlastnosti konfiguračnej zložky EIM. Ak chcete tento proces zjednodušiť, mali by ste uložiť váš plán implementácie EIM alebo zaznamenať konfiguračné informácie EIM v každom systéme.

Okrem toho musíte zvážiť a naplánovať zálohu a obnovu údajov vašej služby sieťovej autentifikácie, ak ste ju nakonfigurovali ako súčasť implementácie prostredia s jednoduchým prihlásením.

Konfigurácia Enterprise Identity Mapping

Sprievodca konfiguráciou EIM umožňuje vykonať základnú konfiguráciu EIM (Enterprise Identity Mapping) pre vaše iSeries rýchlo a jednoducho. Sprievodca vám poskytuje tri voľby pre konfiguráciu systému EIM. Spôsob použitia sprievodcu pre konfiguráciu EIM v špecifickom systéme závisí na vašom celkovom pláne používania EIM vo vašom podniku a na vašich potrebách konfigurácie EIM. Napríklad veľa administrátorov chce používať EIM v spojení so službou sieťovej autentifikácie, aby vytvorili prostredie s jednoduchým prihlásením vo viacerých systémoch a platformách bez potreby vykonania zmien v závislých bezpečnostných politikách. Sprievodca konfiguráciou EIM vám ich preto umožňuje konfigurovať službu sieťovej autentifikácie ako súčasť vašej konfigurácie EIM. Konfigurácia a používanie služby sieťovej autentifikácie však nie je nevyhnutné a povinné pre konfiguráciu a používanie EIM.

Predtým, než začnete s procesom konfigurácie EIM pre jeden alebo viac systémov, naplánujete vašu implementáciu EIM, aby ste získali všetky potrebné informácie. Napríklad musíte vykonať rozhodnutia ohľadom tohto:

- Ktorý server iSeries chcete nakonfigurovať ako radič domény EIM pre doménu EIM? Najprv použite Sprievodcu konfiguráciou EIM pre vytvorenie novej domény v tomto systéme a potom sprievodcu použite pre konfiguráciu všetkých dodatočných serverov iSeries pre ich pripojenie k tejto doméne.
- Chcete nakonfigurovať službu sieťovej autentifikácie vo všetkých systémoch, ktoré konfigurujete pre EIM? Ak to chcete vykonať, môžete použiť Sprievodcu konfiguráciou EIM pre vytvorenie základnej konfigurácie služby sieťovej autentifikácie v každom serveri iSeries. Musíte však vykonať aj iné úlohy pre dokončenie konfigurácie služby sieťovej autentifikácie.

Po použití Sprievodcu konfiguráciou EIM pre vytvorenie základnej konfigurácie pre každý server iSeries však stále ostáva ešte niekoľko konfiguračných úloh EIM, ktoré musíte vykonať pred dokončením konfigurácie EIM. Pozrite si Scenár: Povolenie jednoduchého prihlásenia, kde nájdete príklad zobrazujúci spôsob konfigurácie prostredia s jednoduchým prihlásením použitím služby sieťovej autentifikácie a EIM fiktívnou spoločnosťou.

Ak chcete konfigurovať EIM, musíte mať všetky tieto špeciálne oprávnenia:

- Administrátor bezpečnosti (*SECADM).
- Všetky objekty (*ALLOBJ).
- Konfigurácia systému (*IOSYSCFG).

Pred použitím Sprievodcu konfiguráciou EIM musíte dokončiť všetky kroky pre “Plán pre Enterprise Identity Mapping” na strane 43, aby ste mohli presne určiť spôsob používania EIM. Ak konfigurujete EIM ako súčasť vytvárania prostredia s jednoduchým prihlásením, rovnako vykonajte všetky kroky pre plánovanie jednoduchého prihlásenia.

Po dokončení vášho plánovania môžete použiť Sprievodcu konfiguráciou EIM, aby ste vytvorili jednu z troch základných konfigurácií EIM. Sprievodcu môžete použiť na pripojenie k existujúcej doméne, alebo na vytvorenie a pripojenie k novej doméne. Pri použití Sprievodcu konfiguráciou EIM pre vytvorenie a pripojenie k novej doméne môžete zvoliť, či chcete nakonfigurovať radič domény EIM v lokálnom alebo vo vzdialenom systéme. Nasledujúce informácie poskytujú pokyny ku konfigurácii EIM podľa typu základnej konfigurácie EIM:

“Vytvorenie a pripojenie k novej lokálnej doméne” na strane 62 Zvoľte túto úlohu, ak chcete pre váš podnik vytvoriť novú doménu EIM a konfigurovať lokálny adresárový server, aby fungoval ako radič domény EIM pre túto novú doménu. Ak protokol Kerberos nie je aktuálne nakonfigurovaný v serveri iSeries, sprievodca vás vyzve na spustenie Sprievodcu konfiguráciou služby sieťovej autentifikácie. Po dokončení tejto úlohy môžete nakonfigurovať iné servery iSeries pre pripojenie k tejto doméne. Ak chcete nakonfigurovať iné servery ako účastníkov domény, ku každému z nich sa pripojte a použite Sprievodcu konfiguráciou EIM, aby ste daný server nakonfigurovali na pripojenie k existujúcej doméne EIM.

“Vytvorenie a pripojenie k novej vzdialenej doméne” na strane 66 Zvoľte túto úlohu, ak chcete pre váš podnik vytvoriť novú doménu EIM a konfigurovať vzdialený adresárový server, aby fungoval ako radič domény EIM pre túto novú doménu. Ak protokol Kerberos nie je aktuálne nakonfigurovaný v serveri iSeries, sprievodca vás vyzve na spustenie Sprievodcu konfiguráciou služby sieťovej autentifikácie. Po dokončení tejto úlohy môžete nakonfigurovať iné servery iSeries pre pripojenie k tejto doméne. Ak chcete nakonfigurovať iné servery ako

účastníkov domény, ku každému z nich sa pripojte a použite Sprievodcu konfiguráciou EIM, aby ste daný server nakonfigurovali na pripojenie k existujúcej doméne EIM.

"Pripojenie k existujúcej doméne" na strane 72 Po použití Sprievodcu konfiguráciou EIM v jednom systéme iSeries pre konfiguráciu radiča domény a vytvorenie domény EIM zvoľte túto úlohu sprievodcu pre konfiguráciu iných serverov iSeries ako účastníkov domény. Tohto sprievodcu musíte spustiť a túto úlohu musíte vykonať v každom serveri iSeries v sieti, ktorý bude používať EIM. Musíte poskytnúť informácie o spojovanej doméne, vrátane informácií o pripojení (ako číslo portu a či sa má pre radič domény EIM použiť protokol TLS (Transport Layer Security) alebo SSL (Secure Sockets Layer)). Ak protokol Kerberos nie je aktuálne nakonfigurovaný v serveri iSeries, sprievodca vás vyzve na spustenie Sprievodcu konfiguráciou služby sieťovej autentifikácie.

Ako sprístupniť Sprievodcu konfiguráciou EIM

Ak chcete spustiť Sprievodcu konfiguráciou EIM, vykonajte tieto kroky:

1. Spustite program iSeries Navigator.
2. Prihláste sa do servera iSeries, pre ktorý chcete nakonfigurovať EIM. Ak konfigurujete EIM pre viac než jeden server iSeries, začnite s tým serverom, v ktorom chcete nakonfigurovať radič domény pre EIM.
3. Rozviňte **Sieť → Enterprise Identity Mapping**.
4. Pravým tlačidlom myši kliknite na **Konfigurácia** a vyberte **Konfigurovať...**, aby sa spustil Sprievodca konfiguráciou EIM.
5. Vyberte konfiguračnú voľbu EIM a postupujte podľa pokynov sprievodcu, potrebných pre jeho dokončenie.
6. Ak potrebujete zistiť, aké informácie treba zadať do jednotlivých polí sprievodcu, kliknite na tlačidlo **Pomoc**.

Vytvorenie a pripojenie k novej lokálnej doméne

Pri použití Sprievodcu konfiguráciou EIM pre vytvorenie a pripojenie k novej doméne môžete zvoliť, či chcete ako súčasť vytvorenia vašej konfigurácie EIM nakonfigurovať radič domény EIM v lokálnom systéme. Ak treba, Sprievodca konfiguráciou EIM skontroluje, či poskytujete základné konfiguračné informácie pre adresárový server. Ak protokol Kerberos nie je aktuálne nakonfigurovaný v serveri iSeries, sprievodca vás vyzve na spustenie Sprievodcu konfiguráciou služby sieťovej autentifikácie.

Po dokončení Sprievodcu konfiguráciou EIM môžete vykonať tieto úlohy:

- Vytvoriť novú doménu EIM.
- Konfigurovať lokálny adresárový server, aby fungoval ako radič domény EIM.
- Konfigurovať službu sieťovej autentifikácie pre systém.
- Vytvoriť definície registrov EIM pre lokálny register OS/400 a register Kerberos.
- Konfigurovať systém, aby sa stal účastníkom novej domény EIM.

Ak chcete konfigurovať váš systém pre vytvorenie a pripojenie k novej doméne EIM, musíte mať všetky tieto špeciálne oprávnenia:

- Administrátor bezpečnosti (*SECADM).
- Všetky objekty (*ALLOBJ).
- Konfigurácia systému (*IOSYSCFG).

Ak chcete použiť Sprievodcu konfiguráciou EIM pre vytvorenie a pripojenie k novej lokálnej doméne, vykonajte tieto kroky:

1. V programe iSeries Navigator vyberte systém, pre ktorý chcete nakonfigurovať EIM a rozviňte **Sieť > Enterprise Identity Mapping**.
2. Pravým tlačidlom myši kliknite na **Konfigurácia** a vyberte **Konfigurovať...**, aby sa spustil Sprievodca konfiguráciou EIM.

Poznámka: Táto voľba je označená ako **Prekonfigurovať...**, ak už bolo EIM predtým v systéme nakonfigurované.

3. Na strane sprievodcu **Vitajte** vyberte **Vytvoriť a pripojiť k novej doméne** a kliknite na tlačidlo **Ďalej**.
4. Na strane **Zadanie umiestnenia domény EIM** vyberte **V lokálnom adresárovom serveri** a kliknite na tlačidlo **Ďalej**.

   Poznámka: Táto voľba nakonfiguruje lokálny adresárový server, aby fungoval ako radič domény EIM. Tento adresárový server ukladá všetky údaje EIM pre doménu, preto musí byť aktívny a zostať aktívny, aby mohol podporovať vyhľadanie mapovania EIM a iné operácie.

   Poznámka: Ak služba sieťovej autentifikácie práve nie je nakonfigurovaná v serveri iSeries, alebo pre konfiguráciu prostredia s jednoduchým prihlásením je treba poskytnúť ďalšie konfiguračné informácie o sieťovej autentifikácii, zobrazí sa strana **Konfigurácia služby sieťovej autentifikácie**. Táto strana vám umožní spustiť Sprievodcu konfiguráciou služby sieťovej autentifikácie, aby ste mohli nakonfigurovať službu sieťovej autentifikácie. Službu sieťovej autentifikácie môžete nakonfigurovať neskôr použitím sprievodcu konfiguráciou pre túto službu prostredníctvom programu iSeries Navigator. Po dokončení konfigurácie služby sieťovej autentifikácie pokračujete ďalej v Sprievodcovi konfiguráciou EIM.
5. Ak chcete konfigurovať službu sieťovej autentifikácie, vykonajte tieto kroky:
   a. Na strane **Konfigurácia služby sieťovej autentifikácie** vyberte **Áno**, aby sa spustil Sprievodca konfiguráciou služby sieťovej autentifikácie. Pomocou tohto sprievodcu môžete konfigurovať viacero rozhraní a služieb OS/400 ako účastníkov realmu Kerberos a tiež môžete konfigurovať prostredie s jednoduchým prihlásením, používajúce EIM a službu sieťovej autentifikácie.
   b. Na strane **Zadanie informácií o realme** zadajte názov predvoleného realmu v poli **Predvolený realm**. Ak používate Microsoft Active Directory pre autentifikáciu pomocou Kerberos, vyberte **Microsoft Active Directory sa používa pre autentifikáciu pomocou Kerberos** a kliknite na tlačidlo **Ďalej**.
   c. Na strane **Zadanie informácií o KDC** zadajte plne kvalifikovaný názov servera Kerberos pre tento realm v poli **KDC**, potom v poli **Port** zadajte hodnotu 88 a kliknite na tlačidlo **Ďalej**.
   d. Na strane **Zadanie informácií o serveri hesiel** vyberte **Áno** alebo **Nie** pre nastavenie servera hesiel. Server hesiel umožňuje principálom meniť heslá v serveri Kerberos. Ak vyberiete voľbu **Áno**, zadajte názov servera hesiel v poli **Server hesiel**. V poli **Port** použite predvolenú hodnotu 464 a kliknite na tlačidlo Ďalej.
   e. Na strane **Výber položiek súboru kľúčov** vyberte **Autentifikácia pomocou Kerberos OS/400** a kliknite na tlačidlo **Ďalej**.

      Poznámka: Tiež môžete vytvoriť položky súboru kľúčov pre IBM Directory Server pre iSeries (LDAP), iSeries NetServer a server iSeries HTTP, ak chcete, aby tieto služby používali autentifikáciu pomocou Kerberos. Najskôr budete musieť vykonať ďalšiu konfiguráciu pre tieto služby predtým, než môžu používať autentifikáciu pomocou Kerberos.
   f. Na strane **Vytvorenie položky súboru kľúčov OS/400** zadajte a potvrďte heslo a kliknite na tlačidlo **Ďalej**. Toto isté heslo neskôr použijete pri pridávaní principálov OS/400 pre server Kerberos.
   g. Na strane **Vytvorenie dávkového súboru** vyberte **Áno**, potom zadajte nasledujúce informácie a kliknite na tlačidlo **Ďalej**:
      - V poli **Dávkový súbor** zaktualizujte adresárovú cestu. Kliknite na tlačidlo **Prehľadať**, ak chcete vyhľadať správnu adresárovú cestu alebo upravte cestu v poli **Dávkový súbor**.
      - V poli **Zahrnúť heslo** vyberte **Áno**. Toto zaručuje, že všetky heslá priradené k principálu služieb OS/400 sa zahrnú do dávkového súboru. Je dôležité nezabudnúť, že heslá sa zobrazujú ako čitateľný text a môže ich prečítať ktokoľvek s prístupom na čítanie toho dávkového súboru. Je preto dôležité ihneď po jeho použití dávkový súbor vymazať zo servera Kerberos aj z PC. Ak heslo nezahrniete, budete vyzvaný na zadanie hesla pri spustení dávkového súboru.

        Poznámka: Môžete tiež manuálne pridať principály služieb, vygenerované sprievodcom do Microsoft Active Directory. Ak chcete zistiť, ako toto spraviť, pozrite si tému Pridanie principálov OS/400 do servera Kerberos

- Na strane **Sumár** zobrazte detaily konfigurácie služby sieťovej autentifikácie a kliknite na tlačidlo **Dokončiť** pre návrat do Sprievodcu konfiguráciou EIM.

6. Ak lokálny adresárový server nie je práve nakonfigurovaný, po pokračovaní Sprievodcu konfiguráciou EIM sa zobrazí strana **Konfigurácia adresárového servera**. Ak chcete konfigurovať lokálny adresárový server, poskytnite tieto informácie:

   Poznámka: Ak lokálny adresárový server nakonfigurujete pred použitím Sprievodcu konfiguráciou EIM, namiesto predošlého sa zobrazí strana **Zadanie užívateľa pre pripojenie**. Túto stranu použite pre špecifikáciu rozlišovacieho mena a hesla administrátora LDAP, aby ste zaručili, že sprievodca bude mať dostatočné oprávnenie na správu domény EIM a objektov v nej obsiahnutých a pokračujte ďalším krokom v tejto procedúre. Ak potrebujete zistiť, aké informácie treba zadať na tejto strane, kliknite na tlačidlo **Pomoc**.

   - V poli **Port** použite predvolené číslo portu 389, alebo zadajte odlišné číslo portu, ak chcete používať nezabezpečené komunikácie EIM s adresárovým serverom.
   - V poli **Rozlišovací názov** zadajte rozlišovací názov LDAP (DN), identifikujúci administrátora LDAP pre adresárový server. Sprievodca konfiguráciou EIM toto DN administrátora LDAP vytvorí a použije to pre konfiguráciu adresárového servera, aby fungoval ako radič domény pre novú vytváranú doménu.
   - V poli **Heslo** zadajte heslo pre administrátora LDAP.
   - V poli **Potvrdenie hesla** zadajte heslo druhýkrát za účelom overenia.
   - Kliknite na tlačidlo **Ďalej**.

7. Na strane **Zadanie domény** poskytnite tieto informácie:
   - V poli **Doména** zadajte názov domény EIM, ktorú chcete vytvoriť. Použite predvolený názov EIM, alebo použite ľubovoľný znakový reťazec, ktorý vám vyhovuje. Nemôžete však použiť špeciálne znaky ako **= + < > , # ;** \ a *****.
   - V poli **Opis** zadajte opisný text domény.
   - Kliknite na tlačidlo **Ďalej**.

8. Na strane **Špecifikácia rodičovského DN pre doménu** vyberte **Áno** pre špecifikovanie rodičovského DN pre práve vytváranú doménu, alebo zadajte **Nie**, ak chcete údaje EIM uložiť do adresára s príponou, ktorej názov je odvodený z názvu domény EIM.

   Poznámka: Pri vytvorení domény v lokálnom adresárovom serveri je špecifikácia rodičovského DN voliteľná. Ak zadáte rodičovské DN, môžete určiť, kam v lokálnom názvovom priestore LDAP sa majú uložiť údaje EIM pre doménu. Ak nezadáte rodičovské DN, údaje EIM sa uložia do vlastnej prípony v názvovom priestore. Ak vyberiete **Áno**, vyberte rodičovské DN pre lokálnu príponu LDAP zo zoznamu, alebo zadajte text, aby sa vytvorilo nové rodičovské DN. Pre novú doménu nie je nutné zadať rodičovské DN. Ak chcete získať viac informácií o používaní rodičovského DN, kliknite na **Pomoc**.

9. Na strane **Informácie o registroch** špecifikujte, či chcete pridať lokálne registre užívateľov do domény EIM ako definície registrov. Vyberte jeden alebo oba typy registra užívateľov:

   Poznámka: Teraz nemusíte vytvárať definície registrov. Ak vyberiete neskoršie vytvorenie definícií registrov, musíte pridať definície systémových registrov a zaktualizovať vlastnosti konfigurácie EIM.

   - Vyberte **Lokálne OS/400**, ak chcete pridať definíciu registra pre lokálny register. V poskytnutom poli pre názov definície registra použite buď predvolenú hodnotu registra, alebo pre názov definície registra zadajte odlišnú hodnotu. Názov registra EIM je ľubovoľný reťazec reprezentujúci typ registra a špecifickú inštanciu tohto registra.
   - Vyberte **Kerberos**, ak chcete pridať definíciu registra pre register Kerberos. V poskytnutom poli pre názov definície registra použite buď predvolenú hodnotu registra, alebo pre názov definície registra zadajte odlišnú hodnotu. Predvolený názov definície registra je rovnaký ako názov realmu. Použitím predvoleného názvu a teda použitím názvu registra Kerberos, ktorý je rovnaký ako je názov realmu, môžete zvýšiť výkon získavania informácií z tohto registra. Ak treba, vyberte **Identity užívateľa Kerberos rozlišujú veľkosť písmen**.
   - Kliknite na tlačidlo **Ďalej**.

10. Na strane **Zadanie užívateľa systému EIM** vyberte **Typ užívateľa**, ktorého systém použije pri vykonávaní operácií EIM v mene funkcií operačného systému. Tieto operácie zahrňujú operácie vyhľadávania mapovaní a vymazania priradení pri vymazaní lokálneho užívateľského profilu OS/400. Môžete vybrať jeden z týchto typov užívateľov: **Rozlišovací názov a heslo**, **Súbor kľúčov a principál Kerberos** alebo **Principál a heslo Kerberos**. Typy užívateľov, ktoré môžete vybrať sa líšia podľa aktuálnej konfigurácie systému. Napríklad, ak Služba sieťovej autentifikácie nie je pre systém nakonfigurovaná, typy užívateľov Kerberos nemusia byť dostupné vo výbere. Vybratý typ užívateľa predurčuje ďalšie informácie, ktoré musíte poskytnúť pre dokončenie strany podľa týchto pokynov:

    Poznámka: Musíte špecifikovať užívateľa aktuálne definovaného v adresárovom serveri, ktorý je hostiteľom pre radič domény EIM. Vami zadaný užívateľ musí mať privilégiá minimálne na vykonanie vyhľadávania mapovaní a správu registra pre lokálny register užívateľov. Ak špecifikovaný užívateľ nemá tieto privilégiá, určité funkcie operačného systému súvisiace s používaním jednoduchého prihlásenia a vymazania užívateľských profilov môžu zlyhať.

    Ak ste pred spustením tohto sprievodcu nenakonfigurovali adresárový server, jediný typ užívateľa, ktorý môžete vybrať, je **Rozlišovací názov a heslo** a jediný rozlišovací názov, ktorý môžete zadať, je DN administrátora LDAP.

    - Ak vyberiete **Rozlišovací názov a heslo**, poskytnite tieto informácie:
      - V poli **Rozlišovací názov** zadajte rozlišovací názov LDAP (DN), identifikujúci užívateľa, ktorého systém použije pri vykonávaní operácií EIM.
      - V poli **Heslo** zadajte heslo pre rozlišovací názov.
      - V poli **Potvrdenie hesla** zadajte heslo druhýkrát za účelom overenia.
    - Ak vyberiete **Principál Kerberos a heslo**, zadajte tieto informácie:
      - V poli **Principál** zadajte názov principálu Kerberos, ktorého systém použije pri vykonávaní operácií EIM
      - V poli **Realm** zadajte plne kvalifikovaný názov realmu Kerberos, ktorého je principál členom. Názov principálu a realmu jedinečne identifikujú užívateľov Kerberos v súbore kľúčov. Napríklad principál jsmith v realme ordept.myco.com je reprezentovaný v súbore kľúčov ako jsmith@ordept.myco.com.
      - V poli **Heslo** zadajte heslo pre daného užívateľa.
      - V poli **Potvrdenie hesla** zadajte heslo druhýkrát za účelom overenia.
    - Ak vyberiete **Súbor kľúčov a principál Kerberos**, poskytnite tieto informácie:
      - V poli **Súbor kľúčov** zadajte úplnú cestu a názov súboru kľúčov, obsahujúceho principál Kerberos, ktorého systém použije pri vykonávaní operácií EIM. Alebo kliknite na tlačidlo **Prehľadať...**, ak chcete prehľadať adresáre integrovaného súborového systému iSeries a vybrať súbor kľúčov.
      - V poli **Principál** špecifikujte názov principálu Kerberos, ktorého systém použije pri vykonávaní operácií EIM.
      - V poli **Realm** zadajte plne kvalifikovaný názov realmu Kerberos, ktorého je principál členom. Názov principálu a realmu jedinečne identifikujú užívateľov Kerberos v súbore kľúčov. Napríklad principál jsmith v realme ordept.myco.com je reprezentovaný v súbore kľúčov ako jsmith@ordept.myco.com.
    - Kliknite na **Skontrolovať pripojenie**, aby ste sa uistili, že sprievodca dokáže použiť zadané informácie o užívateľovi pre úspešné vytvorenie pripojenia k radiču domény EIM.
    - Kliknite na tlačidlo **Ďalej**.
11. Na paneli **Sumár** skontrolujte vami zadané konfiguračné informácie. Ak sú všetky informácie správne, kliknite na tlačidlo **Dokončiť**.

Sprievodca pri svojom dokončení pridá novú doménu do zložky **Správa domén**, čím ste vytvorili základnú konfiguráciu EIM pre tento server. Ak chcete dokončiť vašu konfiguráciu EIM pre doménu, musíte však vykonať ešte tieto úlohy:

1. Použite Sprievodcu konfiguráciou EIM v každom ďalšom serveri, ktorý chcete pripojiť k doméne.
2. Ak treba, do domény EIM pridajte definície registrov EIM pre ďalšie servery a aplikácie iného typu ako iSeries, ak chcete, aby boli účastníkmi domény EIM. Tieto definície registra odkazujú na aktuálne registre užívateľov, ktoré

musia byť účastníkmi domény. Môžete buď pridať definície systémových registrov alebo môžete pridať definície aplikačných registrov v závislosti na potrebách vašej implementácie EIM.

3. Na základe vašich potrieb implementácie EIM určite, či chcete:
   - Vytvoriť identifikátory EIM pre každého jedinečného užívateľa alebo entitu v doméne a vytvoriť priradenia pre tieto identifikátory.
   - Vytvoriť priradenia politiky pre mapovanie skupiny užívateľov do samostatnej cieľovej identity užívateľa.
   - Vytvoriť kombináciu z predošlých volieb.
4. Použite funkciu testovanie mapovania EIM, aby ste otestovali mapovania identít pre vašu konfiguráciu EIM.
5. Ak jediný vami vytvorený užívateľ EIM je DN pre administrátora LDAP, potom váš užívateľ EIM má vysokú úroveň oprávnenia pre všetky údaje v adresárovom serveri. Zvážte preto vytvorenie jedného alebo viacerých DN ako ďalších užívateľov, ktorí budú mať vhodnejšie a obmedzenejšie riadenie prístupu pre údaje EIM. Ak sa chcete dozvedieť viac o vytváraní názvov DN, pozrite si časť Rozlišovacie názvy v téme IBM Directory Server for iSeries (LDAP). Počet dodatočných užívateľov EIM, ktorých definujete závisí od prístupu vašej bezpečnostnej politiky k oddeleniu úloh týkajúcich sa bezpečnosti od zodpovednosti. Typicky môžete vytvoriť minimálne tieto dva typy DN:
   - **Užívateľa s riadením prístupu Administrátor EIM**

     Toto DN administrátora EIM poskytuje príslušnú úroveň oprávnenia pre administrátora, ktorý je zodpovedný za správu domény EIM. Toto DN administrátora EIM sa dá použiť pre pripojenie k radiču domény pri manažovaní všetkých aspektov domény EIM prostredníctvom programu iSeries Navigator.
   - **Aspoň jedného užívateľa, ktorý má všetky tieto riadenia prístupu**:
     - Administrátor identifikátorov
     - Administrátor registrov
     - Operácie s mapovaním EIM

     Tento užívateľ poskytuje príslušnú úroveň riadenia prístupu vyžadovanú pre užívateľa systému vykonávajúceho operácie EIM v mene operačného systému.

   Poznámka: Ak chcete pre užívateľa systému použiť toto nové DN namiesto DN administrátora LDAP, musíte zmeniť vlastnosti konfigurácie EIM pre server iSeries. Pozrite si Správa vlastností konfigurácie EIM, kde sa dozviete, ako meniť DN užívateľa systému.

Ďalej možno budete chcieť používať protokol SSL (Secure Sockets Layer) alebo protokol TLS (Transport Layer Security) pre konfiguráciu bezpečného pripojenia k radiču domény EIM, aby ste ochránili prenos údajov EIM. Ak povolíte SSL pre adresárový server, musíte zaktualizovať vlastnosti konfigurácie EIM pre špecifikáciu používania bezpečného pripojenia pomocou protokolu SSL v serveri iSeries. Tiež budete musieť zaktualizovať vlastnosti pre doménu, aby ste špecifikovali, že EIM používa pripojenia SSL pre správu domény prostredníctvom programu iSeries Navigator.

Poznámka: Po vytvorení základnej konfigurácie služby sieťovej autentifikácie možno budete musieť vykonať ešte ďalšie úlohy hlavne v prípade, ak implementujete prostredie s jednoduchým prihlásením. Informácie o týchto ďalších krokoch získate zobrazením krokov pre kompletnú konfiguráciu, uvedených v scenári Povolenie jednoduchého prihlásenia pre OS/400.

Vytvorenie a pripojenie k novej vzdialenej doméne

Pri použití Sprievodcu konfiguráciou EIM pre vytvorenie a pripojenie k novej lokálnej doméne môžete zvoliť, či chcete ako súčasť vytvorenia vašej konfigurácie EIM nakonfigurovať adresárový server vo vzdialenom systéme, aby fungoval ako radič domény EIM. Ak chcete nakonfigurovať EIM vo vzdialenom serveri, musíte zadať príslušné informácie pre pripájanie k vzdialenému adresárovému serveru. Ak protokol Kerberos nie je aktuálne nakonfigurovaný v serveri iSeries, sprievodca vás vyzve na spustenie Sprievodcu konfiguráciou služby sieťovej autentifikácie.

Poznámka: Adresárový server vo vzdialenom systéme musí poskytovať podporu pre EIM. EIM vyžaduje, aby hostiteľom radiča domény bol adresárový server podporujúci protokol LDAP (Lightweight Directory Access Protocol) verzie 3. Produkt adresárového servera musí mať nakonfigurovanú schému EIM.

Napríklad produkt IBM Directory Server V5.1 poskytuje túto podporu. Pozrite si tému Plánovanie radiča domény EIM, kde nájdete detailné informácie o požiadavkách na radič domény EIM.

Po dokončení Sprievodcu konfiguráciou EIM môžete vykonať tieto úlohy:

- Vytvoriť novú doménu EIM.
- Konfigurovať vzdialený adresárový server, aby fungoval ako radič domény EIM.
- Konfigurovať službu sieťovej autentifikácie pre systém.
- Vytvoriť definície registrov EIM pre lokálny register OS/400 a register Kerberos.
- Konfigurovať systém, aby sa stal účastníkom novej domény EIM.

Ak chcete konfigurovať váš systém pre vytvorenie a pripojenie k novej lokálnej doméne EIM, musíte mať všetky tieto špeciálne oprávnenia:

- Administrátor bezpečnosti (*SECADM).
- Všetky objekty (*ALLOBJ).
- Konfigurácia systému (*IOSYSCFG).

Ak chcete použiť Sprievodcu konfiguráciou EIM pre vytvorenie a pripojenie k doméne vo vzdialenom systéme, vykonajte tieto kroky:

1. Skontrolujte, či je adresárový server vo vzdialenom systéme aktívny. Pozrite si dokumentáciu pre produkt adresárového servera, aby ste zistili, ako to spraviť.
2. V programe iSeries Navigator vyberte systém, pre ktorý chcete nakonfigurovať EIM a rozviňte **Sieť > Enterprise Identity Mapping**.
3. Pravým tlačidlom myši kliknite na **Konfigurácia** a vyberte **Konfigurovať...**, aby sa spustil Sprievodca konfiguráciou EIM.

   Poznámka: Táto voľba je označená ako **Prekonfigurovať...**, ak už bolo EIM predtým v systéme nakonfigurované.
4. Na strane sprievodcu **Vitajte** vyberte **Vytvoriť a pripojiť k novej doméne** a kliknite na tlačidlo **Ďalej**.
5. Na strane **Zadanie umiestnenia domény EIM** vyberte **Vo vzdialenom adresárovom serveri** a kliknite na tlačidlo **Ďalej**.

   Poznámka: Táto voľba nakonfiguruje vzdialený adresárový server, aby fungoval ako radič domény EIM. Ak chcete, aby vzdialený adresárový server fungoval ako radič domény EIM, vami špecifikovaný vzdialený adresárový server musí poskytovať podporu pre EIM a musí byť aktívny, aby sa táto konfigurácia EIM mohla úspešne dokončiť. Tiež musí ostať aktívna pre podporu operácie vyhľadávania mapovaní EIM a iných operácií.

   Poznámka: Ak služba sieťovej autentifikácie práve nie je nakonfigurovaná v serveri iSeries, alebo pre konfiguráciu prostredia s jednoduchým prihlásením je treba poskytnúť ďalšie konfiguračné informácie o sieťovej autentifikácii, zobrazí sa strana **Konfigurácia služby sieťovej autentifikácie**. Táto strana vám umožní spustiť Sprievodcu konfiguráciou služby sieťovej autentifikácie, aby ste mohli nakonfigurovať službu sieťovej autentifikácie. Službu sieťovej autentifikácie nakonfigurovať neskôr použitím sprievodcu konfiguráciou pre túto službu prostredníctvom programu iSeries Navigator. Po dokončení konfigurácie služby sieťovej autentifikácie pokračujete ďalej v Sprievodcovi konfiguráciou EIM.
6. Ak chcete konfigurovať službu sieťovej autentifikácie, vykonajte tieto kroky:
   a. Na strane **Konfigurácia služby sieťovej autentifikácie** vyberte **Áno**, aby sa spustil Sprievodca konfiguráciou služby sieťovej autentifikácie. Pomocou tohto sprievodcu môžete konfigurovať viacero rozhraní a služieb OS/400 ako účastníkov realmu Kerberos a tiež môžete konfigurovať prostredie s jednoduchým prihlásením, používajúce EIM a službu sieťovej autentifikácie.

b. Na strane **Zadanie informácií o realme** zadajte názov predvoleného realmu v poli **Predvolený realm**. Ak používate Microsoft Active Directory pre autentifikáciu pomocou Kerberos, vyberte **Microsoft Active Directory sa používa pre autentifikáciu pomocou Kerberos** a kliknite na tlačidlo **Ďalej**.

c. Na strane **Zadanie informácií o KDC** zadajte plne kvalifikovaný názov servera Kerberos pre tento realm v poli **KDC**, potom v poli **Port** zadajte hodnotu 88 a kliknite na tlačidlo **Ďalej**.

d. Na strane **Zadanie informácií o serveri hesiel** vyberte **Áno** alebo **Nie** pre nastavenie servera hesiel. Server hesiel umožňuje principálom meniť heslá v serveri Kerberos. Ak vyberiete voľbu **Áno**, zadajte názov servera hesiel v poli **Server hesiel**. V poli **Port** použite predvolenú hodnotu 464 a kliknite na tlačidlo Ďalej.

e. Na strane **Výber položiek súboru kľúčov** vyberte **Autentifikácia pomocou Kerberos OS/400** a kliknite na tlačidlo **Ďalej**.

Poznámka: Tiež môžete vytvoriť položky súboru kľúčov pre IBM Directory Server pre iSeries (LDAP), iSeries NetServer a server iSeries HTTP, ak chcete, aby tieto služby používali autentifikáciu pomocou Kerberos. Najskôr budete musieť vykonať ďalšiu konfiguráciu pre tieto služby predtým, než môžu používať autentifikáciu pomocou Kerberos.

f. Na strane **Vytvorenie položky súboru kľúčov OS/400** zadajte a potvrďte heslo a kliknite na tlačidlo **Ďalej**. Toto isté heslo neskôr použijete pri pridávaní principálov OS/400 pre server Kerberos.

g. Na strane **Vytvorenie dávkového súboru** vyberte **Áno**, potom zadajte nasledujúce informácie a kliknite na tlačidlo **Ďalej**:

- V poli **Dávkový súbor** zaktualizujte adresárovú cestu. Kliknite na tlačidlo **Prehľadať**, ak chcete vyhľadať správnu adresárovú cestu alebo upravte cestu v poli **Dávkový súbor**.
- V poli **Zahrnúť heslo** vyberte **Áno**. Toto zaručuje, že všetky heslá priradené k principálu služieb OS/400 sa zahrnú do dávkového súboru. Je dôležité nezabudnúť, že heslá sa zobrazujú ako čitateľný text a môže ich prečítať ktokoľvek s prístupom na čítanie toho dávkového súboru. Je preto dôležité ihneď po jeho použití dávkový súbor vymazať zo servera Kerberos aj z PC. Ak heslo nezahrniete, budete vyzvaný na zadanie hesla pri spustení dávkového súboru.

  Poznámka: Môžete tiež manuálne pridať principály služieb, vygenerované sprievodcom do Microsoft Active Directory. Ak chcete zistiť, ako toto spraviť, pozrite si tému Pridanie principálov OS/400 do servera Kerberos

- Na strane **Sumár** zobrazte detaily konfigurácie služby sieťovej autentifikácie a kliknite na tlačidlo **Dokončiť** pre návrat do Sprievodcu konfiguráciou EIM.

7. Stranu **Zadanie radiča domény EIM** použite pre zadanie informácií o pripojení podľa týchto pokynov pre vzdialený radič domény, ktorý chcete konfigurovať:
   - V poli **Názov radiča domény** zadajte názov vzdialeného adresárového servera, ktorý chcete konfigurovať ako radič domény EIM pre doménu, ktorú vytvárate. Názvom radiča domény EIM môže byť názov domény a hostiteľa adresárového servera TCP/IP alebo adresa adresárového servera.
   - Informácie o pripojení k radiču domény zadajte podľa týchto pokynov:
     – Vyberte **Použiť bezpečné pripojenie (SSL alebo TLS)**, ak chcete používať bezpečné pripojenie k radiču domény EIM. Pri výbere tejto voľby použije pripojenie buď protokol SSL (Secure Sockets Layer), alebo TLS (Transport Layer Security) pre vytvorenie bezpečného pripojenia, aby ochránilo prenos údajov EIM cez nedôveryhodnú sieť, napríklad Internet.

       Poznámka: Overte, že radič domény EIM je nakonfigurovaný pre používanie bezpečného pripojenia. V opačnom prípade môže pripojenie k radiču domény zlyhať.

     – V poli **Port** zadajte port TCP/IP, na ktorom adresárový server počúva. Ak je vybraté **Použiť bezpečné pripojenie**, predvoleným portom je port 636; v opačnom prípade je predvoleným portom port 389.
   - Kliknite na **Skontrolovať pripojenie**, aby ste otestovali, či sprievodca dokáže zadané informácie použiť pre vytvorenie pripojenia k vzdialenému radiču domény EIM.
   - Kliknite na tlačidlo **Ďalej**.
8. Na strane **Zadanie užívateľa pre pripojenie** vyberte **Typ užívateľa** pre pripojenie. Môžete vybrať jeden z týchto typov užívateľov: **Rozlišovací názov a heslo**, **Súbor kľúčov a principál Kerberos**, **Principál a heslo Kerberos**

alebo **Užívateľský profil a heslo**. Tieto dva typy užívateľa Kerberos sú dostupné len v prípade, ak je služba sieťovej autentifikácie nakonfigurovaná pre systém iSeries. Vami vybratý typ užívateľa určuje ostatné informácie, ktoré musíte poskytnúť v tomto dialógovom okne:

Poznámka: Ak chcete zaručiť, aby mal sprievodca dostatočné oprávnenie na vytvorenie potrebných objektov EIM v adresári, ako typ užívateľa vyberte **Rozlišovací názov a heslo** a ako užívateľa špecifikujte administrátora LDAP pomocou jeho DN a hesla.

Môžete zadať aj iného užívateľa pre pripojenie; avšak vami špecifikovaný užívateľ musí mať pre vzdialený adresárový server rovnaké oprávnenie administrátora.

- Ak vyberiete **Rozlišovací názov a heslo**, poskytnite tieto informácie:
  - Do poľa **Rozlišovací názov** zadajte rozlišovací názov administrátora LDAP (DN) a heslo, ktoré zabezpečí sprievodcovi dostatočné oprávnenia na administráciu domény EIM a objektov v tejto doméne.
  - V poli **Heslo** zadajte heslo pre rozlišovací názov.
  - V poli **Potvrdenie hesla** zadajte heslo druhýkrát za účelom overenia.
- Ak vyberiete **Súbor kľúčov a principál Kerberos**, poskytnite tieto informácie:
  - V poli **Súbor kľúčov** zadajte úplnú cestu a názov súboru kľúčov, obsahujúceho principál Kerberos, ktorého sprievodca použije pri pripájaní k doméne EIM. Alebo kliknite na tlačidlo **Prehľadať...**, ak chcete prehľadať adresáre integrovaného súborového systému iSeries a vybrať súbor kľúčov.
  - V poli **Principál** zadajte názov principálu Kerberos, ktorý sa použije pre identifikáciu užívateľa.
  - V poli **Realm** zadajte plne kvalifikovaný názov realmu Kerberos, ktorého je principál členom. Názov principálu a realmu jedinečne identifikujú užívateľov Kerberos v súbore kľúčov. Napríklad principál jsmith v realme ordept.myco.com je reprezentovaný v súbore kľúčov ako jsmith@ordept.myco.com.
- Ak vyberiete **Principál Kerberos a heslo**, zadajte tieto informácie:
  - V poli **Principál** zadajte názov principálu Kerberos, ktorého sprievodca použije pri pripájaní k doméne EIM.
  - V poli **Realm** zadajte plne kvalifikovaný názov realmu Kerberos, ktorého je principál členom. Názov principálu a realmu jedinečne identifikujú užívateľov Kerberos v súbore kľúčov. Napríklad principál jsmith v realme ordept.myco.com je reprezentovaný v súbore kľúčov ako jsmith@ordept.myco.com.
  - V poli **Heslo** zadajte heslo pre principál Kerberos.
  - V poli **Potvrdenie hesla** zadajte heslo druhýkrát za účelom overenia.
- Ak vyberiete **Užívateľský profil a heslo**, poskytnite tieto informácie:
  - V poli **Užívateľský profil a heslo** zadajte názov užívateľského profilu, ktorého sprievodca použije pri pripájaní k doméne EIM.
  - V poli **Heslo** zadajte heslo pre užívateľský profil.
  - V poli **Potvrdenie hesla** zadajte heslo druhýkrát za účelom overenia.
- Kliknite na **Skontrolovať pripojenie**, aby ste otestovali, či sprievodca dokáže zadané informácie o užívateľovi použiť pre úspešné vytvorenie pripojenia k radiču domény EIM.
- Kliknite na tlačidlo **Ďalej**.

9. Na strane **Zadanie domény** poskytnite tieto informácie:
   - V poli **Doména** zadajte názov domény EIM, ktorú chcete vytvoriť. Použite predvolený názov EIM, alebo použite ľubovoľný znakový reťazec, ktorý vám vyhovuje. Nemôžete však použiť špeciálne znaky ako **= + < > , # ;** \ a *****.
   - V poli **Opis** zadajte opisný text domény.
   - Kliknite na tlačidlo **Ďalej**.
10. V dialógovom okne **Špecifikácia rodičovského DN pre doménu** vyberte **Áno** pre špecifikáciu rodičovského DN, ktoré sprievodca použije pre umiestnenie domény EIM, ktorú vytvárate. Toto DN predstavuje položku, ktorá sa v stromovej hierarchii informácií v adresároch nachádza hneď nad položkou domény s vašim názvom. Môžete zadať **Nie**, ak chcete údaje EIM uložiť do adresára s príponou, ktorej názov je odvodený z názvu domény EIM.

Poznámka: Pri použití sprievodcu pre konfiguráciu domény vo vzdialenom radiči domény musíte pre danú doménu zadať príslušné rodičovské DN. Všetky potrebné objekty konfigurácie musia pre rodičovské DN existovať, inak môže konfigurácia EIM zlyhať, preto uprednostnite radšej prehľadanie pre príslušné rodičovské DN pred manuálnym zadaním informácií o DN. Ak chcete získať viac informácií o používaní rodičovského DN, kliknite na **Pomoc**.

11. Na strane **Informácie o registroch** špecifikujte, či chcete pridať lokálne registre užívateľov do domény EIM ako definície registrov. Vyberte jeden alebo oba typy registra užívateľov:

    Poznámka: Teraz nemusíte vytvárať definície registrov. Ak vyberiete neskoršie vytvorenie definícií registrov, musíte pridať definície systémových registrov a zaktualizovať vlastnosti konfigurácie EIM.

    - Vyberte **Lokálne OS/400**, ak chcete pridať definíciu registra pre lokálny register. V poskytnutom poli pre názov definície registra použite buď predvolenú hodnotu registra, alebo pre názov definície registra zadajte odlišnú hodnotu. Názov registra EIM je ľubovoľný reťazec reprezentujúci typ registra a špecifickú inštanciu tohto registra.
    - Vyberte **Kerberos**, ak chcete pridať definíciu registra pre register Kerberos. V poskytnutom poli pre názov definície registra použite buď predvolenú hodnotu registra, alebo pre názov definície registra zadajte odlišnú hodnotu. Predvolený názov definície registra je rovnaký ako názov realmu. Použitím predvoleného názvu a teda použitím názvu registra Kerberos, ktorý je rovnaký ako je názov realmu, môžete zvýšiť výkon získavania informácií z tohto registra. Ak treba, vyberte **Identity užívateľa Kerberos rozlišujú veľkosť písmen**.
    - Kliknite na tlačidlo **Ďalej**.

12. Na strane **Zadanie užívateľa systému EIM** vyberte **Typ užívateľa**, ktorého systém použije pri vykonávaní operácií EIM v mene funkcií operačného systému. Tieto operácie zahrňujú operácie vyhľadávania mapovaní a vymazania priradení pri vymazaní lokálneho užívateľského profilu OS/400. Môžete vybrať jeden z týchto typov užívateľov: **Rozlišovací názov a heslo**, **Súbor kľúčov a principál Kerberos** alebo **Principál a heslo Kerberos**. Typy užívateľov, ktoré môžete vybrať sa líšia podľa aktuálnej konfigurácie systému. Napríklad, ak Služba sieťovej autentifikácie nie je pre systém nakonfigurovaná, typy užívateľov Kerberos nemusia byť dostupné vo výbere. Vybratý typ užívateľa predurčuje ďalšie informácie, ktoré musíte poskytnúť pre dokončenie strany podľa týchto pokynov:

    Poznámka: Musíte špecifikovať užívateľa aktuálne definovaného v adresárovom serveri, ktorý je hostiteľom pre radič domény EIM. Vami zadaný užívateľ musí mať privilégiá minimálne na vykonanie vyhľadávania mapovaní a správu registra pre lokálny register užívateľov. Ak špecifikovaný užívateľ nemá tieto privilégiá, určité funkcie operačného systému súvisiace s používaním jednoduchého prihlásenia a vymazania užívateľských profilov môžu zlyhať.

    Ak ste pred spustením tohto sprievodcu nenakonfigurovali adresárový server, jediný typ užívateľa, ktorý môžete vybrať, je **Rozlišovací názov a heslo** a jediný rozlišovací názov, ktorý môžete zadať, je DN administrátora LDAP.

    - Ak vyberiete **Rozlišovací názov a heslo**, poskytnite tieto informácie:
      - V poli **Rozlišovací názov** zadajte rozlišovací názov LDAP (DN), identifikujúci užívateľa, ktorého systém použije pri vykonávaní operácií EIM.
      - V poli **Heslo** zadajte heslo pre rozlišovací názov.
      - V poli **Potvrdenie hesla** zadajte heslo druhýkrát za účelom overenia.
    - Ak vyberiete **Principál Kerberos a heslo**, zadajte tieto informácie:
      - V poli **Principál** zadajte názov principálu Kerberos, ktorého systém použije pri vykonávaní operácií EIM
      - V poli **Realm** zadajte plne kvalifikovaný názov realmu Kerberos, ktorého je principál členom. Názov principálu a realmu jedinečne identifikujú užívateľov Kerberos v súbore kľúčov. Napríklad principál jsmith v realme ordept.myco.com je reprezentovaný v súbore kľúčov ako jsmith@ordept.myco.com.
      - V poli **Heslo** zadajte heslo pre daného užívateľa.
      - V poli **Potvrdenie hesla** zadajte heslo druhýkrát za účelom overenia.
    - Ak vyberiete **Súbor kľúčov a principál Kerberos**, poskytnite tieto informácie:

– V poli **Súbor kľúčov** zadajte úplnú cestu a názov súboru kľúčov, obsahujúceho principál Kerberos, ktorého systém použije pri vykonávaní operácií EIM. Alebo kliknite na tlačidlo **Prehľadať...**, ak chcete prehľadať adresáre integrovaného súborového systému iSeries a vybrať súbor kľúčov.

– V poli **Principál** špecifikujte názov principálu Kerberos, ktorého systém použije pri vykonávaní operácií EIM.

– V poli **Realm** zadajte plne kvalifikovaný názov realmu Kerberos, ktorého je principál členom. Názov principálu a realmu jedinečne identifikujú užívateľov Kerberos v súbore kľúčov. Napríklad principál jsmith v realme ordept.myco.com je reprezentovaný v súbore kľúčov ako jsmith@ordept.myco.com.

- Kliknite na **Skontrolovať pripojenie**, aby ste sa uistili, že sprievodca dokáže použiť zadané informácie o užívateľovi pre úspešné vytvorenie pripojenia k radiču domény EIM.
- Kliknite na tlačidlo **Ďalej**.

13. Na paneli **Sumár** skontrolujte vami zadané konfiguračné informácie. Ak sú všetky informácie správne, kliknite na tlačidlo **Dokončiť**.

Sprievodca pri svojom dokončení pridá novú doménu do zložky **Správa domén**, čím ste vytvorili základnú konfiguráciu EIM pre tento server. Ak chcete dokončiť vašu konfiguráciu EIM pre doménu, musíte však vykonať ešte tieto úlohy:

1. Použite Sprievodcu konfiguráciou EIM v každom ďalšom serveri, ktorý chcete pripojiť k novej doméne.
2. Ak treba, do domény EIM pridajte definície registrov EIM pre ďalšie servery a aplikácie iného typu ako iSeries, ak chcete, aby boli účastníkmi domény EIM. Tieto definície registra odkazujú na aktuálne registre užívateľov, ktoré musia byť účastníkmi domény. Môžete buď pridať definície systémových registrov alebo môžete pridať definície aplikačných registrov v závislosti na potrebách vašej implementácie EIM.
3. Na základe vašich potrieb implementácie EIM určite, či chcete:
   - Vytvoriť identifikátory EIM pre každého jedinečného užívateľa alebo entitu v doméne a vytvoriť priradenia pre tieto identifikátory.
   - Vytvoriť priradenia politiky pre mapovanie skupiny užívateľov do samostatnej cieľovej identity užívateľa.
   - Vytvoriť kombináciu z predošlých volieb.
4. Použite funkciu testovanie mapovania EIM, aby ste otestovali mapovania identít pre vašu konfiguráciu EIM.
5. Ak jediný vami vytvorený užívateľ EIM je DN pre administrátora LDAP, potom váš užívateľ EIM má vysokú úroveň oprávnenia pre všetky údaje v adresárovom serveri. Zvážte preto vytvorenie jedného alebo viacerých DN ako ďalších užívateľov, ktorí budú mať vhodnejšie a obmedzenejšie riadenie prístupu pre údaje EIM. Ak sa chcete dozvedieť viac o vytváraní názvov DN, pozrite si časť Rozlišovacie názvy v téme IBM Directory Server for iSeries (LDAP). Počet dodatočných užívateľov EIM, ktorých definujete závisí od prístupu vašej bezpečnostnej politiky k oddeleniu úloh týkajúcich sa bezpečnosti od zodpovednosti. Typicky môžete vytvoriť minimálne tieto dva typy DN:
   - **Užívateľa s riadením prístupu Administrátor EIM**

     Toto DN administrátora EIM poskytuje príslušnú úroveň oprávnenia pre administrátora, ktorý je zodpovedný za správu domény EIM. Toto DN administrátora EIM sa dá použiť pre pripojenie k radiču domény pri manažovaní všetkých aspektov domény EIM prostredníctvom programu iSeries Navigator.
   - **Aspoň jedného užívateľa, ktorý má všetky tieto riadenia prístupu**:
     – Administrátor identifikátorov
     – Administrátor registrov
     – Operácie s mapovaním EIM

     Tento užívateľ poskytuje príslušnú úroveň riadenia prístupu vyžadovanú pre užívateľa systému vykonávajúceho operácie EIM v mene operačného systému.

Poznámka: Ak chcete pre užívateľa systému použiť toto nové DN namiesto DN administrátora LDAP, musíte zmeniť vlastnosti konfigurácie EIM pre server iSeries. Pozrite si Správa vlastností konfigurácie EIM, kde sa dozviete, ako meniť DN užívateľa systému.

Poznámka: Po vytvorení základnej konfigurácie služby sieťovej autentifikácie možno budete musieť vykonať ešte ďalšie úlohy hlavne v prípade, ak implementujete prostredie s jednoduchým prihlásením. Informácie o týchto ďalších krokoch získate zobrazením krokov pre kompletnú konfiguráciu, uvedených v scenári Povolenie jednoduchého prihlásenia pre OS/400.

Pripojenie k existujúcej doméne

Po vytvorení domény EIM a nakonfigurovaní adresárového servera ako radiča domény v jednom zo systémov môžete nakonfigurovať všetky ďalšie servery iSeries (verzie V5R2 alebo novšej) na pripojenie k existujúcej doméne EIM. Pri prechode sprievodcom musíte zadávať informácie o doméne, vrátane informácií o pripojení k radiču domény EIM. Ak na pripojenie k existujúcej doméne použijete Sprievodcu konfiguráciou EIM, sprievodca vám stále poskytuje možnosť spustenia Sprievodcu konfiguráciou služby sieťovej autentifikácie, ak si ako súčasť konfigurácie EIM v systéme zvolíte konfiguráciu Kerberos.

Po dokončení pripojenia k existujúcej doméne pomocou Sprievodcu konfiguráciou EIM môžete vykonať tieto úlohy:

- Konfigurovať službu sieťovej autentifikácie pre systém.
- Vytvoriť definície registrov EIM pre lokálny register OS/400 a register Kerberos.
- Konfigurovať systém, aby sa stal účastníkom domény EIM.

Ak chcete konfigurovať váš systém na pripojenie k existujúcej doméne EIM, musíte mať všetky tieto špeciálne oprávnenia:

- Administrátor bezpečnosti (*SECADM).
- Všetky objekty (*ALLOBJ).

Ak chcete spustiť Sprievodcu konfiguráciou EIM pre pripojenie k existujúcej doméne EIM, vykonajte tieto kroky:

1. Skontrolujte, či je adresárový server vo vzdialenom systéme aktívny. Pozrite si dokumentáciu pre produkt adresárového servera, aby ste zistili, ako to spraviť.
2. V programe iSeries Navigator vyberte systém, pre ktorý chcete nakonfigurovať EIM a rozviňte **Sieť > Enterprise Identity Mapping**.
3. Pravým tlačidlom myši kliknite na **Konfigurácia** a vyberte **Konfigurovať...**, aby sa spustil Sprievodca konfiguráciou EIM.

   Poznámka: Táto voľba je označená ako **Prekonfigurovať...**, ak už bolo EIM predtým v systéme nakonfigurované.
4. Na **Uvítacej** strane sprievodcu vyberte **Pripojiť k existujúcej doméne** a kliknite na tlačidlo **Ďalej**.

   Poznámka: Ak služba sieťovej autentifikácie práve nie je nakonfigurovaná v serveri iSeries, alebo pre konfiguráciu prostredia s jednoduchým prihlásením je treba poskytnúť ďalšie konfiguračné informácie o sieťovej autentifikácii, zobrazí sa strana **Konfigurácia služby sieťovej autentifikácie**. Táto strana vám umožní spustiť Sprievodcu konfiguráciou služby sieťovej autentifikácie, aby ste mohli nakonfigurovať službu sieťovej autentifikácie. Službu sieťovej autentifikácie nakonfigurovať neskôr použitím sprievodcu konfiguráciou pre túto službu prostredníctvom programu iSeries Navigator. Po dokončení konfigurácie služby sieťovej autentifikácie pokračujete ďalej v Sprievodcovi konfiguráciou EIM.
5. Ak chcete konfigurovať službu sieťovej autentifikácie, vykonajte tieto kroky:
   a. Na strane **Konfigurácia služby sieťovej autentifikácie** vyberte **Áno**, aby sa spustil Sprievodca konfiguráciou služby sieťovej autentifikácie. Pomocou tohto sprievodcu môžete konfigurovať viacero rozhraní a služieb OS/400 ako účastníkov realmu Kerberos a tiež môžete konfigurovať prostredie s jednoduchým prihlásením, používajúce EIM a službu sieťovej autentifikácie.
   b. Na strane **Zadanie informácií o realme** zadajte názov predvoleného realmu v poli **Predvolený realm**. Ak používate Microsoft Active Directory pre autentifikáciu pomocou Kerberos, vyberte **Microsoft Active Directory sa používa pre autentifikáciu pomocou Kerberos** a kliknite na tlačidlo **Ďalej**.

c. Na strane **Zadanie informácií o KDC** zadajte plne kvalifikovaný názov servera Kerberos pre tento realm v poli **KDC**, potom v poli **Port** zadajte hodnotu 88 a kliknite na tlačidlo **Ďalej**.

d. Na strane **Zadanie informácií o serveri hesiel** vyberte **Áno** alebo **Nie** pre nastavenie servera hesiel. Server hesiel umožňuje principálom meniť heslá v serveri Kerberos. Ak vyberiete voľbu **Áno**, zadajte názov servera hesiel v poli **Server hesiel**. V poli **Port** použite predvolenú hodnotu 464 a kliknite na tlačidlo Ďalej.

e. Na strane **Výber položiek súboru kľúčov** vyberte **Autentifikácia pomocou Kerberos OS/400** a kliknite na tlačidlo **Ďalej**.

Poznámka: Tiež môžete vytvoriť položky súboru kľúčov pre IBM Directory Server pre iSeries (LDAP), iSeries NetServer a server iSeries HTTP, ak chcete, aby tieto služby používali autentifikáciu pomocou Kerberos. Najskôr budete musieť vykonať ďalšiu konfiguráciu pre tieto služby predtým, než môžu používať autentifikáciu pomocou Kerberos.

f. Na strane **Vytvorenie položky súboru kľúčov OS/400** zadajte a potvrďte heslo a kliknite na tlačidlo **Ďalej**. Toto isté heslo neskôr použijete pri pridávaní principálov OS/400 pre server Kerberos.

g. Na strane **Vytvorenie dávkového súboru** vyberte **Áno**, potom zadajte nasledujúce informácie a kliknite na tlačidlo **Ďalej**:

- V poli **Dávkový súbor** zaktualizujte adresárovú cestu. Kliknite na tlačidlo **Prehľadať**, ak chcete vyhľadať správnu adresárovú cestu alebo upravte cestu v poli **Dávkový súbor**.
- V poli **Zahrnúť heslo** vyberte **Áno**. Toto zaručuje, že všetky heslá priradené k principálu služieb OS/400 sa zahrnú do dávkového súboru. Je dôležité nezabudnúť, že heslá sa zobrazujú ako čitateľný text a môže ich prečítať ktokoľvek s prístupom na čítanie toho dávkového súboru. Je preto dôležité ihneď po jeho použití dávkový súbor vymazať zo servera Kerberos aj z PC. Ak heslo nezahrniete, budete vyzvaný na zadanie hesla pri spustení dávkového súboru.

  Poznámka: Môžete tiež manuálne pridať principály služieb, vygenerované sprievodcom do Microsoft Active Directory. Ak chcete zistiť, ako toto spraviť, pozrite si tému Pridanie principálov OS/400 do servera Kerberos

- Na strane **Sumár** zobrazte detaily konfigurácie služby sieťovej autentifikácie a kliknite na tlačidlo **Dokončiť** pre návrat do Sprievodcu konfiguráciou EIM.

6. Na strane **Zadanie radiča domény** poskytnite tieto informácie:

   Poznámka: Adresárový server fungujúci ako radič domény musí byť aktívny, aby sa táto konfigurácia EIM mohla úspešne dokončiť.

   - V poli **Názov radiča domény** zadajte názov systému fungujúceho ako radič domény pre doménu EIM, s ktorou sa má server iSeries spojiť.
   - Kliknite na **Použiť bezpečné pripojenie (SSL alebo TLS)**, ak chcete použiť bezpečné pripojenie k radiču domény EIM. Pri výbere tejto voľby použije pripojenie buď protokol SSL (Secure Sockets Layer), alebo TLS (Transport Layer Security) pre vytvorenie bezpečného pripojenia, aby ochránilo prenos údajov EIM cez nedôveryhodnú sieť, napríklad Internet.

     Poznámka: Overte, že radič domény EIM je nakonfigurovaný pre používanie bezpečného pripojenia. V opačnom prípade môže pripojenie k radiču domény zlyhať.

   - V poli **Port** zadajte port TCP/IP, na ktorom adresárový server počúva. Ak je vybraté **Použiť bezpečné pripojenie**, predvoleným portom je port 636; v opačnom prípade je predvoleným portom port 389.
   - Kliknite na **Skontrolovať pripojenie**, aby ste otestovali, či sprievodca dokáže zadané informácie použiť pre vytvorenie pripojenia k radiču domény EIM.
   - Kliknite na tlačidlo **Ďalej**.

7. Na strane **Zadanie užívateľa pre pripojenie** vyberte **Typ užívateľa** pre pripojenie. Môžete vybrať jeden z týchto typov užívateľov: **Rozlišovací názov a heslo**, **Súbor kľúčov a principál Kerberos**, **Principál a heslo Kerberos** alebo **Užívateľský profil a heslo**. Tieto dva typy užívateľa Kerberos sú dostupné len v prípade, ak je služba sieťovej autentifikácie nakonfigurovaná pre systém iSeries. Vami vybratý typ užívateľa určuje ostatné informácie, ktoré musíte poskytnúť v tomto dialógovom okne:

Poznámka: Ak chcete zaručiť, aby mal sprievodca dostatočné oprávnenie na vytvorenie potrebných objektov EIM v adresári, ako typ užívateľa vyberte **Rozlišovací názov a heslo** a ako užívateľa špecifikujte administrátora LDAP pomocou jeho DN a hesla.

Môžete zadať aj iného užívateľa pre pripojenie; avšak vami špecifikovaný užívateľ musí mať pre vzdialený adresárový server rovnaké oprávnenie administrátora.

- Ak vyberiete **Rozlišovací názov a heslo**, poskytnite tieto informácie:
  - V poli **Rozlišovací názov** zadajte rozlišovací názov LDAP (DN), identifikujúci užívateľa s oprávnením na vytvorenie objektov v lokálnom názvovom priestore servera LDAP. Ak ste tohto sprievodcu už použili pre konfiguráciu servera LDAP v niektorom z predošlých krokov, zadajte rozlišovací názov administrátora LDAP, ktorý ste vtedy vytvorili.
  - V poli **Heslo** zadajte heslo pre rozlišovací názov.
  - V poli **Potvrdenie hesla** zadajte heslo druhýkrát za účelom overenia.
- Ak vyberiete **Súbor kľúčov a principál Kerberos**, poskytnite tieto informácie:
  - V poli **Súbor kľúčov** zadajte úplnú cestu a názov súboru kľúčov, obsahujúceho principál Kerberos, ktorého sprievodca použije pri pripájaní k doméne EIM. Alebo kliknite na tlačidlo **Prehľadať...**, ak chcete prehľadať adresáre integrovaného súborového systému iSeries a vybrať súbor kľúčov.
  - V poli **Principál** zadajte názov principálu Kerberos, ktorý sa použije pre identifikáciu užívateľa.
  - V poli **Realm** zadajte plne kvalifikovaný názov realmu Kerberos, ktorého je principál členom. Názov principálu a realmu jedinečne identifikujú užívateľov Kerberos v súbore kľúčov. Napríklad principál jsmith v realme ordept.myco.com je reprezentovaný v súbore kľúčov ako jsmith@ordept.myco.com.
- Ak vyberiete **Principál Kerberos a heslo**, zadajte tieto informácie:
  - V poli **Principál** zadajte názov principálu Kerberos, ktorého sprievodca použije pri pripájaní k doméne EIM.
  - V poli **Realm** zadajte plne kvalifikovaný názov realmu Kerberos, ktorého je principál členom. Názov principálu a realmu jedinečne identifikujú užívateľov Kerberos v súbore kľúčov. Napríklad principál jsmith v realme ordept.myco.com je reprezentovaný v súbore kľúčov ako jsmith@ordept.myco.com.
  - V poli **Heslo** zadajte heslo pre principál Kerberos.
  - V poli **Potvrdenie hesla** zadajte heslo druhýkrát za účelom overenia.
- Ak vyberiete **Užívateľský profil a heslo**, poskytnite tieto informácie:
  - V poli **Užívateľský profil a heslo** zadajte názov užívateľského profilu, ktorého sprievodca použije pri pripájaní k doméne EIM.
  - V poli **Heslo** zadajte heslo pre užívateľský profil.
  - V poli **Potvrdenie hesla** zadajte heslo druhýkrát za účelom overenia.
- Kliknite na **Skontrolovať pripojenie**, aby ste otestovali, či sprievodca dokáže zadané informácie o užívateľovi použiť pre úspešné vytvorenie pripojenia k radiču domény EIM.
- Kliknite na tlačidlo **Ďalej**.

8. Na strane **Zadanie domény** vyberte názov domény, do ktorej sa chcete pripojiť a kliknite na tlačidlo **Ďalej**.
9. Na strane **Informácie o registroch** špecifikujte, či chcete pridať lokálne registre užívateľov do domény EIM ako definície registrov. Vyberte jeden alebo oba typy registra užívateľov:
   - Vyberte **Lokálne OS/400**, ak chcete pridať definíciu registra pre lokálny register. V poskytnutom poli pre názov definície registra použite buď predvolenú hodnotu registra, alebo pre názov definície registra zadajte odlišnú hodnotu. Názov registra EIM je ľubovoľný reťazec reprezentujúci typ registra a špecifickú inštanciu tohto registra.

     Poznámka: Teraz nemusíte vytvárať definície registrov OS/400. Ak vyberiete neskoršie vytvorenie definícií registrov OS/400, musíte pridať definície systémových registrov a zaktualizovať vlastnosti konfigurácie EIM.
   - Vyberte **Kerberos**, ak chcete pridať definíciu registra pre register Kerberos. V poskytnutom poli pre názov definície registra použite buď predvolenú hodnotu registra, alebo pre názov definície registra zadajte odlišnú

hodnotu. Predvolený názov definície registra je rovnaký ako názov realmu. Použitím predvoleného názvu a teda použitím názvu registra Kerberos, ktorý je rovnaký ako je názov realmu, môžete zvýšiť výkon získavania informácií z tohto registra. Ak treba, vyberte **Identity užívateľa Kerberos rozlišujú veľkosť písmen**.

Poznámka: Ak ste Sprievodcu konfiguráciou EIM alebo iný systém použili pre pridanie definície registra pre register Kerberos, pre ktorý má tento systém iSeries vytvorený principál služieb, ako súčasť tejto konfigurácie už nemusíte pridať definíciu registra Kerberos. Po dokončení tohto sprievodcu však budete musieť zadať názov tohto registra Kerberos vo vlastnostiach konfigurácie pre tento systém.

- Kliknite na tlačidlo **Ďalej**.

10. Na strane **Zadanie užívateľa systému EIM** vyberte **Typ užívateľa**, ktorého systém použije pri vykonávaní operácií EIM v mene funkcií operačného systému. Tieto operácie zahrňujú operácie vyhľadávania mapovaní a vymazania priradení pri vymazaní lokálneho užívateľského profilu OS/400. Môžete vybrať jeden z týchto typov užívateľov: **Rozlišovací názov a heslo**, **Súbor kľúčov a principál Kerberos** alebo **Principál a heslo Kerberos**. Typy užívateľov, ktoré môžete vybrať sa líšia podľa aktuálnej konfigurácie systému. Napríklad, ak Služba sieťovej autentifikácie nie je pre systém nakonfigurovaná, typy užívateľov Kerberos nemusia byť dostupné vo výbere. Vybratý typ užívateľa predurčuje ďalšie informácie, ktoré musíte poskytnúť pre dokončenie strany podľa týchto pokynov:

Poznámka: Musíte špecifikovať užívateľa aktuálne definovaného v adresárovom serveri, ktorý je hostiteľom pre radič domény EIM. Vami zadaný užívateľ musí mať privilégiá minimálne na vykonanie vyhľadávania mapovaní a správu registra pre lokálny register užívateľov. Ak špecifikovaný užívateľ nemá tieto privilégiá, určité funkcie operačného systému súvisiace s používaním jednoduchého prihlásenia a vymazania užívateľských profilov môžu zlyhať.

- Ak vyberiete **Rozlišovací názov a heslo**, poskytnite tieto informácie:
  - V poli **Rozlišovací názov** zadajte rozlišovací názov LDAP (DN), identifikujúci užívateľa, ktorého systém použije pri vykonávaní operácií EIM.
  - V poli **Heslo** zadajte heslo pre rozlišovací názov.
  - V poli **Potvrdenie hesla** zadajte heslo druhýkrát za účelom overenia.
- Ak vyberiete **Principál Kerberos a heslo**, zadajte tieto informácie:
  - V poli **Principál** zadajte názov principálu Kerberos, ktorého systém použije pri vykonávaní operácií EIM
  - V poli **Realm** zadajte plne kvalifikovaný názov realmu Kerberos, ktorého je principál členom. Názov principálu a realmu jedinečne identifikujú užívateľov Kerberos v súbore kľúčov. Napríklad principál jsmith v realme ordept.myco.com je reprezentovaný v súbore kľúčov ako jsmith@ordept.myco.com.
  - V poli **Heslo** zadajte heslo pre daného užívateľa.
  - V poli **Potvrdenie hesla** zadajte heslo druhýkrát za účelom overenia.
- Ak vyberiete **Súbor kľúčov a principál Kerberos**, poskytnite tieto informácie:
  - V poli **Súbor kľúčov** zadajte úplnú cestu a názov súboru kľúčov, obsahujúceho principál Kerberos, ktorého systém použije pri vykonávaní operácií EIM. Alebo kliknite na tlačidlo **Prehľadať...**, ak chcete prehľadať adresáre integrovaného súborového systému iSeries a vybrať súbor kľúčov.
  - V poli **Principál** špecifikujte názov principálu Kerberos, ktorého systém použije pri vykonávaní operácií EIM.
  - V poli **Realm** zadajte plne kvalifikovaný názov realmu Kerberos, ktorého je principál členom. Názov principálu a realmu jedinečne identifikujú užívateľov Kerberos v súbore kľúčov. Napríklad principál jsmith v realme ordept.myco.com je reprezentovaný v súbore kľúčov ako jsmith@ordept.myco.com.
- Kliknite na **Skontrolovať pripojenie**, aby ste sa uistili, že sprievodca dokáže použiť zadané informácie o užívateľovi pre úspešné vytvorenie pripojenia k radiču domény EIM.
- Kliknite na tlačidlo **Ďalej**.

11. Na strane **Sumár** zobrazte vami poskytnuté konfiguračné informácie. Ak sú všetky informácie správne, kliknite na tlačidlo **Dokončiť**.

Sprievodca pri svojom dokončení pridá doménu do zložky **Správa domén**, čím ste vytvorili základnú konfiguráciu EIM pre tento server. Ak chcete dokončiť vašu konfiguráciu EIM pre doménu, musíte však vykonať ešte tieto úlohy:

1. Ak treba, do domény EIM pridajte definície registrov EIM pre ďalšie servery a aplikácie iného typu ako iSeries, ak chcete, aby boli účastníkmi domény EIM. Tieto definície registra odkazujú na aktuálne registre užívateľov, ktoré musia byť účastníkmi domény. Môžete buď pridať definície systémových registrov alebo môžete pridať definície aplikačných registrov v závislosti na potrebách vašej implementácie EIM.
2. Na základe vašich potrieb implementácie EIM určite, či chcete:
   - Vytvoriť identifikátory EIM pre každého jedinečného užívateľa alebo entitu v doméne a vytvoriť priradenia pre tieto identifikátory.
   - Vytvoriť priradenia politiky pre mapovanie skupiny užívateľov do samostatnej cieľovej identity užívateľa.
   - Vytvoriť kombináciu z predošlých volieb.
3. Použite funkciu testovanie mapovania EIM, aby ste otestovali mapovania identít pre vašu konfiguráciu EIM.
4. Ak jediný vami vytvorený užívateľ EIM je DN pre administrátora LDAP, potom váš užívateľ EIM má vysokú úroveň oprávnenia pre všetky údaje v adresárovom serveri. Zvážte preto vytvorenie jedného alebo viacerých DN ako ďalších užívateľov, ktorí budú mať vhodnejšie a obmedzenejšie riadenie prístupu pre údaje EIM. Ak sa chcete dozvedieť viac o vytváraní názvov DN, pozrite si časť Rozlišovacie názvy v téme IBM Directory Server for iSeries (LDAP). Počet dodatočných užívateľov EIM, ktorých definujete závisí od prístupu vašej bezpečnostnej politiky k oddeleniu úloh týkajúcich sa bezpečnosti od zodpovednosti. Typicky môžete vytvoriť minimálne tieto dva typy DN:
   - **Užívateľa s riadením prístupu Administrátor EIM**

     Toto DN administrátora EIM poskytuje príslušnú úroveň oprávnenia pre administrátora, ktorý je zodpovedný za správu domény EIM. Toto DN administrátora EIM sa dá použiť pre pripojenie k radiču domény pri manažovaní všetkých aspektov domény EIM prostredníctvom programu iSeries Navigator.
   - **Aspoň jedného užívateľa, ktorý má všetky tieto riadenia prístupu**:
     - Administrátor identifikátorov
     - Administrátor registrov
     - Operácie s mapovaním EIM

     Tento užívateľ poskytuje príslušnú úroveň riadenia prístupu vyžadovanú pre užívateľa systému vykonávajúceho operácie EIM v mene operačného systému.

   Poznámka: Ak chcete pre užívateľa systému použiť toto nové DN namiesto DN administrátora LDAP, musíte zmeniť vlastnosti konfigurácie EIM pre server iSeries. Pozrite si Správa vlastností konfigurácie EIM, kde sa dozviete, ako meniť DN užívateľa systému.

Poznámka: Po vytvorení základnej konfigurácie služby sieťovej autentifikácie možno budete musieť vykonať ešte ďalšie úlohy hlavne v prípade, ak implementujete prostredie s jednoduchým prihlásením. Informácie o týchto ďalších krokoch získate zobrazením krokov pre kompletnú konfiguráciu, uvedených v scenári Povolenie jednoduchého prihlásenia pre OS/400.

Konfigurovanie bezpečného pripojenia k radiču domény EIM

Možno budete chcieť použiť SSL (Secure Sockets Layer) alebo TSL (Transport Layer Security Protocol) na vytvorenie bezpečného pripojenia k radiču domény EIM, kvôli ochrane prenášaných údajov.

Ak chcete nakonfigurovať SSL alebo TLS pre EIM, musíte vykonať tieto úlohy:

1. Ak to je potrebné, pomocou správcu digitálnych certifikátov (DCM) vytvorte certifikát pre adresárový server na použitie pre SSL.
2. Aktivujte SSL v lokálnom adresárovom serveri, ktorý hosťuje radič domény EIM.
3. Zaktualizujte vlastnosti konfigurácie EIM, aby ste určili, že server iSeries používa bezpečné pripojenie SSL.

   Ak chcete zaktualizovať konfiguračné vlastnosti EIM, vykonajte tieto kroky:

   a. V programe iSeries Navigator vyberte systém, v ktorom ste nakonfigurovali EIM a rozviňte **Sieť → Enterprise Identity Mapping**.

b. Pravým tlačidlom myši kliknite na **Konfigurácia** a vyberte **Vlastnosti**.
c. Na strane **Doména**, vyberte **Použitie bezpečného pripojenia (SSL alebo TLS)**, zadajte bezpečný port, na ktorom počúva adresárový server alebo akceptujte predvolenú hodnotu 636 v poli **Port** a kliknite na tlačidlo **OK**.

4. Zaktualizujte vlastnosti domény EIM pre každú doménu, aby ste určili, že EIM používa pripojenie SSL pri manažovaní domény cez iSeries Navigator.

   Ak chcete zaktualizovať vlastnosti domény EIM, vykonajte tieto kroky:

   a. V programe iSeries Navigator vyberte systém, v ktorom ste nakonfigurovali EIM a rozviňte **Sieť → Enterprise Identity Mapping → Správa domén**.
   b. Vyberte doménu EIM, v ktorej chcete pracovať.
      - V prípade, že doména EIM, v ktorej chcete pracovať sa nenachádza v **Správe domén**, pozrite si časť Pridanie domény EIM do Správy domén.
      - Pokiaľ nie ste pripojený k doméne EIM, v ktorej chcete pracovať, pozrite si časť Pripojenie k radiču domény EIM.
   c. Pravým tlačidlom myši kliknite na doménu EIM, ku ktorej ste teraz pripojený a vyberte **Vlastnosti**.
   d. Na strane **Doména**, vyberte **Použitie bezpečného pripojenia (SSL alebo TLS)**, zadajte bezpečný port, na ktorom počúva adresárový server alebo akceptujte predvolenú hodnotu 636 v poli **Port** a kliknite na tlačidlo **OK**.

Manažovanie Enterprise Identity Mapping

Po konfigurácii EIM (Enterprise Identity Mapping) vo vašom serveri iSeries budete musieť vykonávať administratívne úlohy, ktoré manažujú vašu doménu EIM a údaje v nej. Ak sa chcete dozvedieť viac o manažovaní EIM vo vašom podniku, pozrite si tieto strany:

“Manažovanie domén Enterprise Identity Mapping” Manažovanie domén EIM a ich vlastností.

“Manažovanie definícií registrov Enterprise Identity Mapping” na strane 82 Tvorba a manažment definícií registrov EIM pre registre užívateľov nachádzajúce sa v EIM vo vašom podniku.

“Manažovanie identifikátorov Enterprise Identity Mapping” na strane 87 Tvorba a manažment identifikátorov EIM pre doménu.

“Manažovanie priradení” na strane 90 Tvorba a vymazanie priradení identifikátorov a priradení politiky a manažment ďalších vlastností informácií o priradení v doméne EIM.

“Manažovanie vlastností konfigurácie EIM” na strane 105 Manažovanie konfigurácie EIM vo vašom systéme, vrátane vlastností užívateľov systému a ďalších vlastností.

“Manažovanie riadenia prístupu užívateľa EIM” na strane 104 Manažovanie skupín riadenia prístupu užívateľov za účelom riadenia prístupu užívateľov k údajom EIM, administratívnym úlohám EIM a ďalších operáciám.

Manažovanie domén Enterprise Identity Mapping

| Na manažovanie všetkých vašich domén EIM (Enterprise Identity Mapping) môžete použiť program iSeries Navigator.
| Ak chcete manažovať doménu EIM, táto doména sa musí nachádzať v zozname, alebo ju musíte pridať do zložky
| **Správa domén**, umiestnenej pod zložkou **Sieť** v programe iSeries Navigator. Pri použití sprievodcu konfiguráciou EIM
| pre vytvorenie a konfigurovanie novej domény EIM bude doména automaticky pridaná do zložky **Správa domén**, aby
| ste mohli manažovať túto doménu a informácie v nej obsiahnuté.

| Ak chcete manažovať doménu EIM, nachádzajúcu sa kdekoľvek v tej istej sieti, môžete použiť ľubovoľné pripojenie
| iSeries, aj keď vami používané iSeries nemusí byť účastníkom tejto domény.

Pri manažovaní domény môžete vykonávať tieto úlohy:

- "Pridanie domény Enterprise Identity Mapping do zložky Správa domén"
- "Pripojenie k doméne Enterprise Identity Mapping"
- "Aktivovanie priradení politiky pre doménu" na strane 79
- "Testovanie mapovaní EIM" na strane 79
- "Odstránenie domény Enterprise Identity Mapping zo zložky Správa domén" na strane 81
- "Vymazanie domény Enterprise Identity Mapping a všetkých objektov konfigurácie" na strane 82

Tiež môžete manažovať prístup užívateľov k doméne a k informáciám v doméne podľa týchto pokynov:

- "Manažovanie riadenia prístupu užívateľa EIM" na strane 104
- "Manažovanie definícií registrov Enterprise Identity Mapping" na strane 82
- "Manažovanie priradení" na strane 90
- "Manažovanie identifikátorov Enterprise Identity Mapping" na strane 87

Pridanie domény Enterprise Identity Mapping do zložky Správa domén

Ak chcete vykonať túto úlohu, musíte mať špeciálne oprávnenie *SECADM a vami pridávaná doména musí existovať pred pridaním do zložky **Správa domén**.

Ak chcete pridať existujúcu doménu EIM (Enterprise Identity Mapping) do zložky **Správa domén**, vykonajte tieto kroky:

1. Rozviňte **Sieť > Enterprise Identity Mapping**.
2. Pravým tlačidlom myši kliknite na **Správa domén** a vyberte **Pridať doménu...**.
3. V dialógovom okne **Pridanie domény** špecifikujte požadovanú doménu a zadajte informácie o pripojení. Tiež môžete kliknúť na tlačidlo **Prehľadať...**, ak chcete zobraziť zoznam domén, ktoré špecifikovaný radič domény manažuje.

   Poznámka: Ak kliknete na tlačidlo **Prehľadať...**, zobrazí sa dialógové okno **Pripojenie k radiču domény EIM**. Ak chcete zobraziť zoznam domén, musíte sa pripojiť k radiču domény buď s riadením prístupu administrátora LDAP, alebo s riadením prístupu Administrátor EIM. Obsah zoznamu domén sa líši na základe vášho riadenia prístupu k EIM. Ak máte riadenie prístupu Administrátor LDAP, môžete zobraziť zoznam domén, ktoré radič domény manažuje. V opačnom prípade sa v zozname zobrazia len tie domény, pre ktoré máte riadenie prístupu Administrátor EIM.
4. Ak potrebujete zistiť, aké informácie treba zadať do jednotlivých polí, kliknite na tlačidlo **Pomoc**.
5. Kliknite na tlačidlo **OK**, aby sa pridala doména.

Pripojenie k doméne Enterprise Identity Mapping

Predtým, ako môžete pracovať s doménou EIM (Enterprise Identity Mapping), musíte sa najprv pripojiť k radiču domény EIM pre túto doménu. K doméne EIM sa môžete pripojiť aj v prípade, ak váš server iSeries nie je práve nakonfigurovaný ako účastník tejto domény.

Ak sa chcete pripojiť k radiču domény EIM, užívateľ, pod ktorým sa pripájate musí byť členom skupiny "Riadenie prístupu EIM" na strane 33. Vaše členstvo v skupine riadenia prístupu k EIM určuje, aké úlohy môžete v doméne vykonávať a aké údaje EIM môžete zobraziť alebo meniť.

Ak sa chcete pripojiť k doméne EIM, vykonajte tieto kroky:

1. Rozviňte **Sieť > Enterprise Identity Mapping > Správa domén**.
2. Pravým tlačidlom myši kliknite na doménu, ku ktorej sa chcete pripojiť.

   Poznámka: Ak sa doména EIM, s ktorou chcete pracovať nenachádza v zozname pod zložkou **Správa domén**, musíte vykonať "Pridanie domény Enterprise Identity Mapping do zložky Správa domén".
3. Pravým tlačidlom myši kliknite na doménu EIM, ku ktorej sa chcete pripojiť a vyberte **Pripojiť...**.

4. V dialógovom okne **Pripojenie k radiču domény EIM** zadajte **Typ užívateľa**, poskytnite vyžadované informácie o identifikácii užívateľa a vyberte voľbu hesla pre pripojenie k radiču domény.
5. Ak potrebujete zistiť, aké informácie treba zadať do jednotlivých polí dialógového okna, kliknite na tlačidlo **Pomoc**.
6. Kliknite na tlačidlo **OK** pre pripojenie k radiču domény.

Aktivovanie priradení politiky pre doménu

Priradenie politiky poskytuje prostriedky na vytvorenie mapovaní typu veľa-jeden v situáciách, kedy neexistujú priradenia medzi identitami užívateľa a identifikátorom EIM. Priradenie politiky môžete použiť na mapovanie zdrojovej množiny viacerých identít užívateľa (namiesto jednej identity užívateľa) na jednu cieľovú identitu užívateľa v zadanom cieľovom registri užívateľov. Skôr, ako budete môcť použiť priradenia politiky sa musíte uistiť, že ste povolili doméne používať priradenia politiky pre operácie vyhľadávania mapovaní.

Ak chcete aktivovať podporu pre politiku mapovania na použitie priradení politiky pre doménu, musíte byť najprv pripojený k doméne EIM, v ktorej chcete pracovať a musíte mať riadenie prístupu administrátora EIM.

Ak chcete povoliť podpore vyhľadávania mapovaní používať priradenia politiky pre doménu, vykonajte tieto kroky:

1. Rozviňte **Sieť > Enterprise Identity Mapping > Správa domén**.
2. Pravým tlačidlom myši kliknite na doménu EIM, v ktorej chcete pracovať a vyberte **Politika mapovania...**
   - V prípade, že doména EIM, v ktorej chcete pracovať sa nenachádza v **Správe domén**, pozrite si časť “Pridanie domény Enterprise Identity Mapping do zložky Správa domén” na strane 78.
   - Pokiaľ nie ste pripojený k doméne EIM, v ktorej chcete pracovať, pozrite si časť Pripojenie k radiču domény EIM. (Voľba **Politika mapovania...** je nedostupná, kým sa nepripojíte k doméne.)
3. Na strane **Všeobecné** vyberte **Povoliť vyhľadávanie mapovaní pomocou priradení politiky pre doménu**.
4. Kliknite na tlačidlo **OK**.

Poznámka: Musíte povoliť vyhľadávanie mapovaní a použiť priradenia politiky pre definíciu každého cieľového registera, pre ktorý sú definované priradenia politiky. Ak nepovolíte vyhľadávanie mapovaní pre definíciu cieľového registra, daný register sa nedá použiť v operáciách vyhľadávania mapovaní EIM. Ak neurčíte, že cieľový register môže používať priradenia politiky, všetky priradenia politiky, definované pre daný register budú operácie vyhľadávania mapovaní EIM ignorovať.

Testovanie mapovaní EIM

Podpora testovania mapovania EIM vám umožňuje spustiť mapovacie operácie vyhľadávania EIM s vašou konfiguráciou EIM. Testovaním si môžete overiť, či sa konkrétna identita zdrojového užívateľa správne mapuje na príslušnú identitu cieľového užívateľa. Takéto testovanie zabezpečuje, že operácie vyhľadávania mapovania EIM môžu vrátiť správnu identitu cieľového užívateľa na základe poskytnutých informácií.

Ak chcete použiť mohli funkciu testovania mapovania na testovanie vašej konfigurácie EIM, musíte byť pripojený k doméne EIM, v ktorej chcete pracovať a musíte mať oprávnenie na riadenie prístupu k EIM na jednej z týchto úrovní:

- Administrátor EIM
- Administrátor identifikátorov
- Administrátor registrov
- Operácie vyhľadávania mapovaní EIM

Ak chcete podporu testovania mapovania použiť na otestovanie vašej konfigurácie EIM, postupujte nasledovne:

1. Rozviňte **Sieť > Enterprise Identity Mapping > Správa domén**.
2. Vyberte doménu EIM, v ktorej chcete pracovať.
   - Ak doména EIM, s ktorou chcete pracovať nie je uvedená pod **Správa domén**, pozrite si časť Pridanie domény EIM do Správy domén.
   - Ak nie ste pripojený k doméne, v ktorej chcete pracovať, pozrite si časť Pripojenie k radiču domény EIM.

3. Pravým tlačidlom myši kliknite na doménu EIM, ku ktorej ste pripojený a vyberte **Otestovať mapovanie...**
4. V dialógovom okne **Otestovanie mapovania** uveďte nasledujúce informácie:
   - V poli **Zdrojový register** zadajte názov definície registra, týkajúcej sa registra užívateľov, ktorý chcete použiť ako zdroj testu operácie vyhľadávania mapovaní.
   - V poli **Zdrojový užívateľ** zadajte názov užívateľskej identity, ktorú chcete použiť ako zdroj testu operácie vyhľadávania mapovaní.
   - V poli **Cieľový register** zadajte názov definície registra, týkajúcej sa registra užívateľov, ktorý chcete použiť ako cieľ testu operácie vyhľadávania mapovaní.
   - Voliteľné. V poli **Informácie na vyhľadanie** uveďte všetky informácie na vyhľadanie, zadefinované pre cieľového užívateľa.
5. Ak potrebujete zistiť, aké informácie treba zadať do jednotlivých polí dialógového okna, kliknite na tlačidlo **Pomoc**.
6. Kliknite na **Otestovať** a pozrite si výsledky operácie vyhľadávania mapovania, ktoré sa vám zobrazia.
7. Pokračujte v testovaní vašej konfigurácie alebo kliknite na **Zatvoriť**, ak chcete ukončiť testovanie.

Práca s výsledkami testu a riešenie problémov

Ak proces testovania nájde počas testovania priradenie medzi identitou zdrojového užívateľa a cieľovým registrom užívateľov, ktoré poskytol administrátor, vráti sa identita cieľového užívateľa. Test indikuje aj typ priradenia, ktoré našiel medzi dvoma identitami užívateľa. Ak proces testovania nenájde priradenie podľa poskytnutých informácií, test vráti identitu cieľového užívateľa s hodnotou none.

Test, podobne ako operácia vyhľadávania mapovania EIM, vyhľadáva a vracia prvú vhodnú identitu cieľového užívateľa vyhľadávaním v nasledujúcom poradí:

1. Priradenie konkrétneho identifikátora
2. Priradenie politiky filtra certifikátov
3. Predvolené priradenie politiky registra
4. Predvolené priradenie politiky domény

V niektorých prípadoch test nevracia žiadne výsledky vyhľadávania identity cieľového užívateľa, hoci pre túto doménu sú priradenia nakonfigurované. Skontrolujte, či ste pre test poskytli správne informácie. Ak sú informácie správne a test nevráti žiadne výsledky, problém mohla zapríčiniť niektorá z nasledujúcich okolností:

- Podpora priradenia politiky nie je aktivovaná na úrovni domény. Pravdepodobne budete musieť aktivovať priradenia politiky pre doménu.
- Podpora vyhľadávania mapovania alebo podpora priradenia politiky nie je aktivovaná na úrovni jednotlivých registrov. Pravdepodobne budete musieť aktivovať podporu vyhľadávania mapovania a používanie priradenia politiky pre cieľový register.
- Cieľové alebo zdrojové priradenie pre identifikátor EIM nie je správne nakonfigurované. Napríklad pre principálu Kerberos (alebo užívateľa Windows) zdrojové priradenie neexistuje alebo je nesprávne. Prípadne cieľové priradenie špecifikuje nesprávnu identitu užívateľa. Zobrazením všetkých priradení identifikátora pre identifikátor EIM skontrolujte priradenia pre konkrétny identifikátor.
- Priradenie politiky nie je správne nakonfigurované. Zobrazením všetkých priradení politiky pre doménu skontrolujte informácie o zdroji a cieli pre všetky priradenia politiky, zadefinované v doméne.
- Definícia registra a identity užívateľa sa nezhodujú v dôsledku zohľadňovania veľkosti písmen. Register alebo priradenie môžete vymazať a znova vytvoriť so správnou veľkosťou písmen.

V opačnom prípade môžu byť výsledky testu nejednoznačné. V takom prípade sa zobrazí chybová správa, oznamujúca tento problém. Ak sa s určenými kritériami testu zhoduje viac ako jedna identita cieľového užívateľa, test vráti nejednoznačné výsledky. Operácia vyhľadávania mapovania môže vrátiť viacero identít cieľového užívateľa v prípade jednej alebo viacerých nasledujúcich situácií:

- Identifikátor EIM má viaceré individuálne cieľové priradenia k rovnakému cieľovému registru.

- Viac ako jeden identifikátor EIM má rovnakú identita užívateľa špecifikovanú v zdrojovom priradení a každý z týchto identifikátorov EIM má cieľové priradenie do rovnakého cieľového registra, hoci identita užívateľa, špecifikovaná pre každé cieľové priradenie môže byť rôzna.
- Viac ako jedno predvolené politiky domény určuje rovnaký cieľový register.
- Viac ako jedno predvolené priradenie politiky registra určuje rovnaký zdrojový register a rovnaký cieľový register.
- Viac ako jedno priradenie politiky filtra certifikátov určuje rovnaký zdrojový register X.509, filter certifikátov a cieľový register.

Operácia vyhľadávania mapovania, ktorá vráti viac ako jednu identitu cieľového užívateľa môže spôsobiť problémy v aplikáciách s podporou EIM, vrátane aplikácií a produktov OS/400. Musíte preto určiť príčinu nejednoznačných výsledkov a druh akcie, potrebnej na vyriešenie tejto situácie. V závislosti od príčiny môžete vykonať niektoré z nasledujúcich krokov:

- Test vráti viaceré nežiadúce identity cieľového užívateľa. To znamená, že konfigurácia priradenia pre túto doménu nie je správna pretože:
  - Cieľové alebo zdrojové priradenie pre identifikátor EIM nie je správne nakonfigurované. Napríklad pre principálu Kerberos (alebo užívateľa Windows) zdrojové priradenie neexistuje alebo je nesprávne. Prípadne cieľové priradenie špecifikuje nesprávnu identitu užívateľa. Zobrazením všetkých priradení identifikátora pre identifikátor EIM skontrolujte priradenia pre konkrétny identifikátor.
  - Priradenie politiky nie je správne nakonfigurované. Zobrazením všetkých priradení politiky pre doménu skontrolujte informácie o zdroji a cieli pre všetky priradenia politiky, zadefinované v doméne.
- Test vráti viaceré identity cieľového užívateľa a tieto výsledky zodpovedajú spôsobu, akým ste nakonfigurovali priradenia, takže pre každú identitu cieľového užívateľa musíte špecifikovať informácie na vyhľadanie. Jedinečné informácie na vyhľadanie musíte zadefinovať pre všetky identity cieľového užívateľa, ktoré majú rovnaký zdroj (buď identifikátor EIM pre priradenia identifikátora alebo zdrojový register užívateľov pre priradenia politiky). Zadefinovaním informácií na vyhľadanie pre každú identitu cieľového užívateľa zabezpečujete, že operácia vyhľadávania vráti jednu identitu cieľového užívateľa namiesto všetkých možných identít cieľového užívateľa. Pozrite si tému Pridanie informácií na vyhľadanie k cieľovej identite užívateľa. Tieto informácie na vyhľadanie musíte uviesť v operácii vyhľadávania mapovania.

Poznámka: Tento prístup funguje len v prípade, ak má aplikácia povolené používať informácie na vyhľadanie. Základné aplikácie OS/400, napríklad iSeries Access for Windows, však nemôžu používať informácie na vyhľadanie na rozlišovanie medzi viacerými identitami cieľového užívateľa, vrátenými operáciou vyhľadávania. Mohli by ste preto zvážiť, že znova zadefinujete priradenia pre doménu, aby ste zabezpečili, že operácia vyhľadávania mapovania vráti jednu identitu cieľového užívateľa a tým zabezpečí, že základné aplikácie OS/400 budú môcť úspešne vykonávať operácie vyhľadávania mapovania a mapovať identity.

Ďalšie informácie o možných problémoch s mapovaním a ich riešeniach (okrem tých, ktoré sú uvedené v tejto téme) nájdete v téme “Odstraňovanie problémov s Enterprise Identity Mapping: Problémy s mapovaním” na strane 109.

Odstránenie domény Enterprise Identity Mapping zo zložky Správa domén

Doménu EIM, ktorú už nechcete ďalej manažovať, môžete odstrániť zo zložky **Správa domén**. Odstránenie domény zo zložky **Správa domén** však **nie** je to isté, ako vymazanie domény a nevymaže údaje domény z radiča domény. Pozrite si tému Vymazanie domény, ak chcete vymazať doménu a všetky údaje domény.

Na odstránenie domény nemusíte mať žiadne “Riadenie prístupu EIM” na strane 33.

Ak chcete zo zložky **Správa domén** odstrániť doménu EIM, ktorú už nechcete ďalej manažovať, vykonajte tieto kroky:

1. Rozviňte **Sieť > Enterprise Identity Mapping**.
2. Pravým tlačidlom myši kliknite na **Správa domén** a vyberte **Odstrániť doménu...**.
3. Vyberte doménu EIM, ktorú chcete odstrániť zo zložky **Správa domén**.
4. Kliknite na tlačidlo **OK**, aby sa odstránila doména.

Vymazanie domény Enterprise Identity Mapping a všetkých objektov konfigurácie

Predtým, ako budete môcť vymazať doménu EIM, musíte najprv vymazať všetky definície registra a všetky identifikátory EIM (Enterprise Identity Mapping), nachádzajúce sa v doméne. Ak nechcete vymazať doménu a všetky jej údaje, ale už nechcete doménu viac manažovať, môžete namiesto vymazania doménu odstrániť.

Ak chcete vymazať doménu EIM, musíte mať "Riadenie prístupu EIM" na strane 33 na jednej z týchto úrovní:

- Administrátor LDAP.
- Administrátor EIM.

Ak chcete vymazať doménu, vykonajte tieto kroky.

1. Rozviňte **Sieť > Enterprise Identity Mapping > Správa domén**.
2. Ak to je potrebné, vymažte všetky definície registra z domény EIM.
3. Aj je potrebné, vymažte všetky identifikátory EIM z domény EIM.
4. Pravým tlačidlom myši kliknite na doménu, ktorú chcete vymazať a vyberte **Vymazať...**.
5. V dialógovom okne **Potvrdenie vymazania** kliknite na tlačidlo **Áno**.

Manažovanie definícií registrov Enterprise Identity Mapping

Ak chcete, aby registre užívateľov a identity užívateľov, ktoré registre obsahujú, boli účastníkmi domény EIM (Enterprise Identity Mapping), musíte pre ne vytvoriť definície registrov. Potom môžete manažovať spôsob účasti registrov užívateľov a ich identít užívateľov v EIM manažovaním len týchto definícií registrov EIM.

Pri manažovaní definícií domén môžete vykonávať tieto úlohy:

- "Pridanie definície registra aplikácií"
- "Pridanie definície registra aplikácií" na strane 83
- "Pridanie aliasu k definícii registra" na strane 83
- "Definovanie súkromného typu registra užívateľov v Enterprise Identity Mapping" na strane 84
- "Aktivovanie podpory vyhľadávania mapovaní a použitia priradení politiky pre cieľový register" na strane 85
- "Zobrazenie všetkých priradení politiky pre definíciu registra" na strane 102
- "Odstránenie aliasu z definície registra" na strane 87
- "Vymazanie definície registra" na strane 86

Tieto súvisiace úlohy vám môžu pomôcť pri manažovaní alebo práci s údajmi EIM, ktoré ovplyvňujú definície registrov:

- "Vytvorenie priradenia politiky" na strane 92
- "Vymazanie priradenia politiky" na strane 103

Pridanie definície registra aplikácií

Ak chcete vytvoriť definíciu systémového registra, musíte byť pripojený k doméne EIM, v ktorej chcete pracovať a musíte mať riadenie prístupu administrátora EIM.

Ak chcete pridať definíciu systémového registra do domény EIM, vykonajte tieto kroky.

1. Rozviňte **Sieť > Enterprise Identity Mapping > Správa domén**.
2. Vyberte doménu EIM, v ktorej chcete pracovať.
   - V prípade, že doména EIM, v ktorej chcete pracovať sa nenachádza v Správe domén, pozrite si časť "Pridanie domény Enterprise Identity Mapping do zložky Správa domén" na strane 78.
   - Pokiaľ nie ste pripojený k doméne EIM, v ktorej chcete pracovať, pozrite si časť "Pripojenie k doméne Enterprise Identity Mapping" na strane 78.
3. Rozviňte doménu EIM, ku ktorej ste teraz pripojený.
4. Pravým tlačidlom myši kliknite na **Registre užívateľov**, vyberte **Pridať register**, potom vyberte **Systém...**.

5. V dialógovom okne **Pridanie systémového registera** zadajte nasledujúce informácie o definícii systémového registra:
   - Názov definície systémového registra.
   - Typ definície registra.
   - Opis definície systémového registra.
   - (Voliteľné.) URL registra užívateľov.
   - Ak to je potrebné, jeden alebo viac aliasov pre definíciu systémového registra.
6. Ak potrebujete zistiť, aké informácie treba zadať do jednotlivých polí, kliknite na tlačidlo **Pomoc**.
7. Ak chcete uložiť informácie a pridať definíciu registra do domény EIM, kliknite na tlačidlo **OK**.

Pridanie definície registra aplikácií

Ak chcete vytvoriť definíciu registra aplikácií, musíte byť pripojený k doméne EIM, v ktorej chcete pracovať a musíte mať riadenie prístupu administrátora EIM.

Ak chcete pridať definíciu registra aplikácií do domény EIM, vykonajte tieto kroky:

1. Rozviňte **Sieť > Enterprise Identity Mapping > Správa domén**.
2. Vyberte doménu EIM, v ktorej chcete pracovať.
   - V prípade, že doména EIM, v ktorej chcete pracovať sa nenachádza v Správe domén, pozrite si časť “Pridanie domény Enterprise Identity Mapping do zložky Správa domén” na strane 78.
   - Pokiaľ nie ste pripojený k doméne EIM, v ktorej chcete pracovať, pozrite si časť “Pripojenie k doméne Enterprise Identity Mapping” na strane 78.
3. Rozviňte doménu EIM, ku ktorej ste teraz pripojený.
4. Pravým tlačidlom myši kliknite na **Registre užívateľov**, vyberte **Pridať register**, potom vyberte **Aplikácia...**.
5. V dialógovom okne **Pridať register aplikácií**, zadajte nasledujúce informácie o definícii registra aplikácií:
   - Názov definície registra aplikácií.
   - Názov definície systémového registra, ktorého podmnožinou je register užívateľov aplikácie, ktorý práve definujete. Definícia systémového registra, ktorú zadávate, musí už existovať v EIM, ináč vytvorenie registra aplikácií zlyha.
   - Typ definície registra.
   - Opis definície registra aplikácií.
   - Ak to je potrebné, jeden alebo viac aliasov pre definíciu registra aplikácií.
6. Ak potrebujete zistiť aké informácie treba zadať do jednotlivých polí, kliknite na tlačidlo **Pomoc**.
7. Ak chcete uložiť informácie a pridať definíciu registra do domény EIM, kliknite na tlačidlo **OK**.

Pridanie aliasu k definícii registra

Vy alebo vývojár aplikácie môžete chcieť zadať dodatočné rozlišovacie informácie pre definíciu registra. Môžete to dosiahnuť vytvorením aliasu pre definíciu registra. Vy alebo ostatní môžete potom alias používať na lepšie rozlíšenie jedného registra užívateľov od ďalšieho.

Táto podpora aliasov umožňuje programátorom písať aplikácie bez potreby dopredu vedieť názov definície registra EIM, zvolený administrátorom, ktorý bude nasadzovať aplikáciu. Dokumentácia k aplikácii môže administrátorovi EIM oznámiť alias, ktorý používa daná aplikácia. Vďaka tejto informácii môže administrátor priradiť tento alias k definícii registra EIM, reprezentujúcej skutočný register užívateľov, ktorý chce administrátor použiť pre aplikáciu.

Ak chcete pridať alias k definícii registra, musíte byť pripojený k doméne EIM, v ktorej chcete pracovať a musíte mať oprávnenia na jednej z týchto úrovní:

- Administrátor registrov
- Administrátor pre vybraté registre (registra, ktorý upravujete)
- Administrátor EIM

Ak chcete pridať alias k definícii registra EIM, vykonajte tieto kroky:

1. Rozviňte **Sieť > Enterprise Identity Mapping > Správa domén**.
2. Vyberte doménu EIM, v ktorej chcete pracovať.
   - Ak sa doména EIM, s ktorou chcete pracovať nenachádza v zozname Správa domén, pozrite si časť “Pridanie domény Enterprise Identity Mapping do zložky Správa domén” na strane 78.
   - Ak nie ste pripojený k doméne, v ktorej chcete pracovať, pozrite si časť “Pripojenie k doméne Enterprise Identity Mapping” na strane 78.
3. Rozviňte doménu EIM, ku ktorej ste teraz pripojený.
4. Kliknite na zložku **Registre užívateľov**, aby sa zobrazil zoznam definícií registrov v doméne.

   Poznámka: Ak máte riadenie prístupu Administrátor pre vybraté registre, zoznam obsahuje len definície registrov, pre ktoré ste autorizovaný.
5. Pravým tlačidlom myši kliknite na definíciu registra, ku ktorej chcete pridať alias a vyberte položku **Vlastnosti...**.
6. Vyberte stranu **Aliasy** a zadajte názov a typ aliasu, ktorý chcete pridať.

   Poznámka: Môžete zadať typ aliasu, ktorý nie je zahrnutý v zozname typov.
7. Ak to je potrebné, kliknite na tlačidlo **Pomoc** a zistíte, aké informácie je potrebné zadať pre každé pole.
8. Kliknite na tlačidlo **Pridať**.
9. Kliknite na tlačidlo **OK**, aby sa uložili vaše zmeny v definícii registra.

Definovanie súkromného typu registra užívateľov v Enterprise Identity Mapping

Pri vytvorení definície registra EIM (Enterprise Identity Mapping) môžete zadať jeden z množstva preddefinovaných typov registra užívateľov, aby ste ním reprezentovali aktuálny register užívateľov, existujúci v systéme v rámci podniku. Aj keď preddefinované typy definície registra zahŕňajú väčšinu registrov užívateľov operačných systémov, možno budete musieť vytvoriť definíciu registra, pre ktorú EIM nezahŕňa preddefinovaný typ registra. V tejto situácii máte dve možnosti. Buď môžete použiť existujúcu definíciu registra, ktorá zodpovedá charakteristikám vášho registra užívateľov, alebo môžete definovať súkromný typ registra užívateľov.

Ak chcete definovať typ registra užívateľov, ktorý EIM nedokáže preddefinovane rozpoznať, použite identitu objektu (OID), aby ste špecifikovali typ registra v tvare **ObjectIdentifier-normalization**, kde **ObjectIdentifier** predstavuje identifikátor objektu desiatkového čísla s bodkami, napríklad 1.2.3.4.5.6.7 a **normalization** predstavuje hodnotu **caseExact** alebo hodnotu **caseIgnore**. Napríklad identifikátor objektu (OID) pre OS/400 je 1.3.18.0.2.33.2-caseIgnore.

Všetky potrebné OID by ste mali získať od legitímnych registračných autorít pre OIM, aby sa zaistilo, že vytvárate a používate jedinečné identifikátory OID. Jedinečné identifikátory OID pomáhajú predchádzať konfliktom s identifikátormi OID, vytvorenými inými organizáciami alebo aplikáciami.

Identifikátory OID je možné získať dvomi spôsobmi:

- **Zaregistrovať objekty pomocou autority**. Táto metóda je dobrou voľbou v prípade, keď na reprezentáciu informácií potrebujete malý počet pevných identifikátorov OID. Napríklad tieto identifikátory OID môžu reprezentovať politiky certifikátov pre užívateľov vo vašom podniku.
- **Získať priradenie rozsahu od registračnej autority a priraďovať svoje vlastné identifikátory OID podľa potreby**. Táto metóda, ktorá je vlastne priradenie rozsahu identifikátorov v tvare desiatkových čísiel oddelených bodkou, je dobrou voľbou, keď potrebujete veľký počet identifikátorov OID, alebo vaše priradenia OID sa menia. Priradenie rozsahu obsahuje začiatočné desiatkové čísla oddelené bodkou, od ktorých musíte odvádzať svoj **ObjectIdentifier**. Napríklad priradenie rozsahu by mohlo byť 1.2.3.4.5.. Identifikátory OID potom môžete vytvárať pridaním k tomuto základu. Napríklad môžete vytvárať identifikátory OID v tvare 1.2.3.4.5.x.x.x).

Ak sa chcete dozvedieť viac o registrácii vlastných identifikátorov OID pomocou registračnej autority, pozrite si tieto zdroje informácií v sieti Internet:

- Americký národný štandardizačný inštitút (ANSI) je registračnou entitou pre USA pre názvy organizácií pod globálnym registračným procesom vytvoreným Medzinárodnou štandardizačnou organizáciou (ISO) a

Medzinárodnou telekomunikačnou úniou (ITU). Informačný leták vo formáte Microsoft Word obsahujúci informácie o Registered Application Provider Identifier (RID) sa nachádza na webovej stránke ANSI Public Document Library http://public.ansi.org/ansionline/Documents/ . Tento dokument nájdete vybratím **Other Services > Registration Programs**. Rozsah ANSI OID pre organizácie je 2.16.840.1. ANSI účtuje za priradenie rozsahu OID poplatok. Samotné priradenie rozsahu OID od ANSI trvá približne dva týždne. ANSI priradí číslo (NEWNUM) pre vytvorenie nového rozsahu OID; napríklad: 2.16.840.1.NEWNUM.

- Vo väčšine krajín a regiónov je register OID spravovaný národnými organizáciami. Pokiaľ ide o rozsahy ANSI, sú to väčšinou rozsahy priradené pod OID 2.16. Nájdenie autority OID pre konkrétnu krajinu alebo región môže byť trochu náročnejšie. Adresy národných členov ISO je možné nájsť na adrese http://www.iso.ch/addresse/membodies.html . Tieto informácie obsahujú poštovú adresu a adresu elektronickej pošty. V niektorých prípadoch je uvedená aj webová lokalita.
- IANA (Internet Assigned Numbers Authority) priraďuje súkromné čísla podnikov (identifikátory OID) v rozsahu 1.3.6.1.4.1. IANA dodnes priradila rozsahy viac ako 7500 spoločnostiam. Stránka so žiadosťou sa nachádza na adrese http://www.iana.org/cgi-bin/enterprise.pl , pod číslami súkromných podnikov. Registrácia v IANA trvá zvyčajne jeden týždeň. OID od IANA sú k dispozícii bezplatne. IANA priradí číslo (NEWNUM), takže nový rozsah OID bude 1.3.6.1.4.1.NEWNUM.
- Federálna vláda USA spravuje Computer Security Objects Registry (CSOR). CSOR predstavuje pomenovaciu autoritu pre rozsah 2.16.840.1.101.3 a práve registruje objekty pre bezpečnostné označenia, kryptografické algoritmy a politiky certifikátov. Identifikátory OID politík certifikátov sú definované v rozsahu 2.16.840.1.101.3.2.1. CSOR poskytuje identifikátory OID agentúram federálnej vlády USA. Viac informácií o CSOR nájdete na adrese http://csrc.nist.gov/csor/ .

Viac informácií o identifikátoroch pre politiky certifikátov nájdete na adrese http://csrc.nist.gov/csor/pkireg.htm .

Aktivovanie podpory vyhľadávania mapovaní a použitia priradení politiky pre cieľový register

Podpora politiky mapovania EIM vám dovolí použiť priradenia politiky ako prostriedky na vytvorenie mapovaní typu veľa-jeden v situáciách, keď neexistujú priradenia medzi identitami užívateľa a identifikátora EIM. Priradenie politiky môžete použiť na mapovanie zdrojovej množiny viacerých identít užívateľa (namiesto jednej identity užívateľa) na jednu cieľovú identitu užívateľa v zadanom cieľovom registri užívateľov.

Skôr, ako budete môcť použiť priradenia politiky sa musíte uistiť, že ste povolili vyhľadávania mapovaní použitím priradení politiky pre doménu. Musíte tiež aktivovať jedno alebo dve nastavenia každého registra:

- **Povoliť vyhľadávanie mapovania pre register** Vyberte túto voľbu, aby sa register mohol používať v operáciách vyhľadávania mapovaní EIM, bez ohľadu na to, či sú pre tento register definované priradenia politiky.
- **Použiť priradenia politiky** Vyberte túto voľbu aby ste umožnili tomuto registru byť cieľovým registrom priradenia politiky a uistite sa, že sa môže podieľať na operáciách vyhľadávania mapovaní EIM.

Ak nepovolíte vyhľadávania mapovaní pre register, nebude sa môcť tento register vôbec zúčastniť na operáciách vyhľadávania mapovaní. Ak neurčíte, že register používa priradenia politiky, operácie vyhľadávania mapovaní EIM ignorujú všetky priradenia politiky pre register, keď sa vykonáva operácia na tomto registri.

Ak chcete vyhľadávaniu mapovaní povoliť použitie priradení politiky pre cieľový register, musíte byť pripojený k doméne EIM, v ktorej chcete pracovať a musíte mať jednu z týchto úrovní: “Riadenie prístupu EIM” na strane 33

- Administrátor EIM
- Administrátor registrov
- Administrátor pre vybraté registre (pre register, ktorý chcete aktivovať).

Ak chcete povoliť podporu vyhľadávania mapovaní vo všeobecnosi a konkrétne dovoliť používať priradenia politiky, pre cieľový register vykonajte tieto kroky:

1. Rozviňte **Sieť > Enterprise Identity Mapping > Správa domén**.
2. Vyberte doménu EIM, v ktorej chcete pracovať.
   - V prípade, že doména EIM, v ktorej chcete pracovať sa nenachádza v **Správe domén**, pozrite si časť “Pridanie domény Enterprise Identity Mapping do zložky Správa domén” na strane 78.
   - Pokiaľ nie ste pripojený k doméne EIM, v ktorej chcete pracovať, pozrite si časť Pripojenie k radiču domény EIM.
3. Ak chcete zobraziť zoznam definícií registra pre doménu, vyberte **Registre užívateľov**.

   Poznámka: Ak máte riadenie prístupu Administrátor pre vybraté registre, zoznam bude obsahovať len tie definície registra, na ktoré máte oprávnenie.
4. Pravým tlačidlom myši kliknite na definíciu registra, pre ktorú chcete aktivovať podporu politiky mapovania pre priradenia politiky a vyberte **Politika mapovania...**
5. Na strane **Všeobecné**, vyberte **Aktivovať vyhľadávania mapovaní pre register**. Vybratie tejto voľby dovolí registru sa zúčastňovať na operáciách vyhľadávania mapovaní EIM. Ak túto voľbu nevyberiete, operácia vyhľadávania nemôže vrátiť údaje pre register, bez ohľadu, či je register zdrojovým alebo cieľovým registrom v operácii vyhľadávania.
6. Vyberte **Použiť priradenia politiky**. Výber tejto voľby dovoľuje operáciám vyhľadávania používať priradenia politiky ako základ pre vracanie údajov, keď register je cieľom v operácii vyhľadávania.
7. Ak chcete uložiť zmeny, kliknite na tlačidlo **OK**.

Poznámka: Skôr, ako bude môcť niektorý register použiť priradenia politiky, musíte sa tiež uistiť, že ste aktivovali priradenia politiky pre doménu.

Vymazanie definície registra

Pri vymazaní definície registra z domény EIM neovplyvníte register užívateľov, ku ktorému definícia registra prislúcha, ale takýto register užívateľov už nemôže byť ďalej účastníkom domény EIM. Pri vymazávaní definície registra však musíte však uvážiť tieto veci:

- Ak vymažete definíciu registra, stratíte všetky priradenia pre daný register užívateľov. Ak znovu definujete register pre doménu, musíte vytvoriť všetky potrebné priradenia.
- Ak vymažete definíciu registra X.509, tiež stratíte aj všetky filtre certifikátov, definované pre daný register. Ak pre doménu znovu definujete register X.509, musíte znovu vytvoriť všetky potrebné filtre certifikátov.
- Nemôžete vymazať definíciu systémového registra, ak existujú definície aplikačných registrov, špecifikujúce definíciu systémového registra ako rodičovský register.

Ak chcete vymazať definíciu registra, musíte byť pripojený k doméne EIM, v ktorej chcete pracovať a musíte mať riadenie prístupu administrátora EIM.

Ak chcete vymazať definíciu registra EIM, vykonajte tieto kroky:

1. Rozviňte **Sieť > Enterprise Identity Mapping > Správa domén**.
2. Vyberte doménu EIM, v ktorej chcete pracovať.
   - Ak sa doména EIM, s ktorou chcete pracovať nenachádza v zozname pod zložkou **Správa domén**, pozrite si časť “Pridanie domény Enterprise Identity Mapping do zložky Správa domén” na strane 78.
   - Ak nie ste pripojený k doméne EIM, v ktorej chcete pracovať, pozrite si tému Pripojiť k radiču domény EIM.
3. Rozviňte doménu EIM, ku ktorej ste pripojený.
4. Kliknite na **Registre užívateľov**, aby sa zobrazil zoznam definícií registrov pre doménu.

   Poznámka: Ak máte riadenie prístupu na úrovni Administrátor pre vybraté registre, zoznam obsahuje len tie definície registrov, na ktoré ste špecificky autorizovaný.
5. Pravým tlačidlom myši kliknite na register užívateľov, ktorý chcete vymazať a vyberte **Vymazať...**.
6. Kliknite na tlačidlo **Áno** v dialógovom okne **Potvrdenie**, aby sa vymazali definície registra.

Odstránenie aliasu z definície registra

Ak chcete odstrániť alias z definície registra EIM, musíte byť pripojený k doméne EIM, v ktorej chcete pracovať a musíte mať "Riadenie prístupu EIM" na strane 33 na jednej z týchto úrovní:

- Administrátor identifikátorov
- Administrátor pre vybraté registre (pre definíciu registra, s ktorou chcete pracovať)
- Administrátor EIM

Ak chcete odstrániť alias z definície registra EIM, vykonajte tieto kroky:

1. Rozviňte **Sieť > Enterprise Identity Mapping > Správa domén**.
2. Vyberte doménu EIM, v ktorej chcete pracovať.
   - Ak sa doména EIM, s ktorou chcete pracovať nenachádza v zozname pod zložkou Správa domén, pozrite si časť "Pridanie domény Enterprise Identity Mapping do zložky Správa domén" na strane 78.
   - Ak nie ste pripojený k doméne EIM, v ktorej chcete pracovať, pozrite si tému "Pripojenie k doméne Enterprise Identity Mapping" na strane 78.
3. Rozviňte doménu EIM, ku ktorej ste teraz pripojený.
4. Kliknite na zložku **Registre užívateľov**, aby sa zobrazil zoznam definícií registrov v doméne.

   Poznámka: Ak máte riadenie prístupu na úrovni Administrátor pre vybraté registre, zoznam obsahuje len tie definície registrov, na ktoré ste špecificky autorizovaný.
5. Pravým tlačidlom myši kliknite na definíciu registra a vyberte **Vlastnosti...**.
6. Vyberte stranu **Alias**.
7. Vyberte alias, ktorý chcete odstrániť a kliknite na tlačidlo **Odstrániť**.
8. Kliknite na tlačidlo **OK**, aby sa uložili zmeny.

Manažovanie identifikátorov Enterprise Identity Mapping

Vytvorenie a používanie identifikátorov EIM reprezentujúcich užívateľov vo vašej sieti môže byť veľmi užitočné pri sledovaní, ktorá osoba vlastní konkrétnu identitu užívateľa. Užívatelia v podniku sa takmer vždy menia, niektorí prídu, niektorí odídu, iní sa presunú medzi pracoviskami. Tieto zmeny zväčšujú pretrvávajúci problém sledovania identít užívateľov a hesiel pre systémy a aplikácie v sieti. Okrem toho manažment hesiel zaberá v podniku veľké množstvo času. Vytvorením identifikátorov EIM (Enterprise Identity Mapping) a ich priradením k identitám užívateľov pre každého užívateľa môžete realizovať proces sledovania osôb vlastniacich konkrétnu identitu užívateľa. Vykonaním tohto podstatne zjednodušíte manažment hesiel.

Implementáciou prostredia s jednoduchým prihlásením zjednodušíte proces manažovania identít užívateľov aj pre samotných užívateľov, obzvlášť v prípadoch, ak sa presúvajú do iného oddelenia alebo oblasti v rámci podniku. Povolenie jednoduchého prihlásenia odstráni potrebu užívateľov pamätať si nové mená užívateľov a heslá pre nové systémy.

Poznámka: Spôsob vytvárania a používania identifikátorov EIM závisí na potrebách vašej organizácie. Ak sa chcete dozvedieť viac, pozrite si "Vývoj plánu pomenovania identifikátorov EIM" na strane 54.

Identifikátory EIM môžete manažovať pre ktorúkoľvek doménu EIM, dostupnú pod zložkou **Správa domén**. Ak chcete manažovať identifikátory EIM v doméne EIM, môžete vykonať ktorékoľvek z týchto úloh:

- "Vytvorenie identifikátora Enterprise Identity Mapping" na strane 88
- "Pridanie aliasu k identifikátoru Enterprise Identity Mapping" na strane 88
- "Odstránenie aliasu z identifikátora Enterprise Identity Mapping" na strane 89
- "Prispôsobenie zobrazenia identifikátorov Enterprise Identity Mapping" na strane 90
- "Vymazanie identifikátora Enterprise Identity Mapping" na strane 89

Tiež môžete pri manažovaní identifikátorov EIM "Manažovanie priradení" na strane 90.

Vytvorenie identifikátora Enterprise Identity Mapping

Ak chcete vytvoriť identifikátor EIM, musíte byť pripojený k doméne EIM (Enterprise Identity Mapping), v ktorej chcete pracovať a musíte mať "Riadenie prístupu EIM" na strane 33 na jednej z týchto úrovní:

- Administrátor identifikátorov
- Administrátor EIM

Ak chcete vytvoriť identifikátor EIM pre osobu alebo entitu vo vašom podniku, vykonajte tieto kroky:

1. Rozviňte **Sieť > Enterprise Identity Mapping > Správa domén**.
2. Vyberte doménu EIM, v ktorej chcete pracovať.
   - Ak sa doména EIM, s ktorou chcete pracovať nenachádza v zozname pod zložkou **Správa domén**, pozrite si časť "Pridanie domény Enterprise Identity Mapping do zložky Správa domén" na strane 78.
   - Ak nie ste pripojený k doméne EIM, v ktorej chcete pracovať, pozrite si tému Pripojiť k radiču domény EIM.
3. Rozviňte doménu EIM, ku ktorej ste teraz pripojený.
4. Pravým tlačidlom myši kliknite na **Identifikátory** a vyberte **Nový identifikátor...**.
5. V dialógovom okne **Nový identifikátor EIM** poskytnite informácie o identifikátore EIM podľa týchto pokynov:
   - Názov pre identifikátor.
   - Či má systém generovať jedinečný názov, ak treba.
   - Opis identifikátora.
   - Jeden alebo viac aliasov pre identifikátor, ak treba.
6. Ak potrebujete zistiť, aké informácie treba zadať do jednotlivých polí, kliknite na tlačidlo **Pomoc**.
7. Po zadaní vyžadovaných informácií kliknite na tlačidlo **OK**, aby sa vytvoril identifikátor EIM.

Poznámka: Ak vytvoríte veľké množstvo identifikátorov EIM, niekedy bude trvať dlhý čas, kým sa zobrazí zoznam identifikátorov pri rozvinutí zložky **Identifikátory**. Ak chcete zvýšiť výkon v prípade veľkého počtu identifikátorov EIM, pozrite si časť "Prispôsobenie zobrazenia identifikátorov Enterprise Identity Mapping" na strane 90.

Pridanie aliasu k identifikátoru Enterprise Identity Mapping

Môžete vytvoriť alias, aby ste poskytli ďalšie rozlišovacie informácie pre "Identifikátor EIM" na strane 9. Aliasy môžu pomôcť pri hľadaní špecifického identifikátora EIM (Enterprise Identity Mapping) pri vykonávaní operácie prehľadania EIM. Napríklad aliasy môžu byť užitočné v situáciách, kedy sa niekoho skutočné meno odlišuje od mena, pod ktorým je známa daná osoba.

Názvy identifikátorov EIM musia byť jedinečné v doméne EIM. Aliasy môžu pomáhať riešiť situácie, pri ktorých môže byť použitie jedinečných názvov identifikátorov obtiažne. Napríklad odlišné osoby v podniku môžu mať rovnaké meno, čo môže spôsobiť problémy, ak ako identifikátory EIM používate mená. Napríklad, ak máte dvoch užívateľov s menom John J. Johnson, pre jedného môžete vytvoriť alias John Joseph Johnson a pre druhého John Jeffrey Johnson, čo zjednoduší rozlišovanie identity každého užívateľa. Ďalšie aliasy môžu obsahovať číslo zamestnanca, číslo oddelenia a pracovné zaradenie alebo iný rozlišovací atribút užívateľa.

Ak chcete pridať alias k identifikátoru EIM, musíte byť pripojený k doméne EIM, v ktorej chcete pracovať a musíte mať "Riadenie prístupu EIM" na strane 33 na jednej z týchto úrovní:

- Administrátor EIM
- Administrátor identifikátorov

Ak chcete pridať alias k identifikátoru EIM, vykonajte tieto kroky.

1. Rozviňte **Sieť > Enterprise Identity Mapping > Správa domén**.
2. Vyberte doménu EIM, v ktorej chcete pracovať.
   - Ak sa doména EIM, s ktorou chcete pracovať nenachádza v zozname pod zložkou Správa domén, pozrite si časť "Pridanie domény Enterprise Identity Mapping do zložky Správa domén" na strane 78.

- Ak nie ste pripojený k doméne EIM, v ktorej chcete pracovať, pozrite si tému "Pripojenie k doméne Enterprise Identity Mapping" na strane 78.

3. Rozviňte doménu EIM, ku ktorej ste pripojený.
4. Kliknite na **Identifikátory**, aby sa v pravej časti okna zobrazil zoznam identifikátorov EIM, dostupných v doméne.

   Poznámka: Zobrazenie zoznamu identifikátorov pri pokuse o rozvinutie zložky **Identifikátory** môže niekedy trvať dlho. Ak chcete zvýšiť výkon pri veľkom počte identifikátorov EIM v doméne, pozrite si časť "Prispôsobenie zobrazenia identifikátorov Enterprise Identity Mapping" na strane 90.

5. Pravým tlačidlom myši kliknite na identifikátor EIM, ku ktorému chcete pridať alias a vyberte **Vlastnosti**.
6. V poli **Alias** zadajte názov aliasu, ktorý chcete pridať k tomuto identifikátoru EIM a kliknite na tlačidlo **Pridať**.
7. Kliknite na tlačidlo **OK**, aby sa uložili zmeny pre identifikátor EIM.

Odstránenie aliasu z identifikátora Enterprise Identity Mapping

Ak chcete odstrániť alias z identifikátora EIM (Enterprise Identity Mapping), musíte byť pripojený k doméne EIM, v ktorej chcete pracovať a musíte mať "Riadenie prístupu EIM" na strane 33 na jednej z týchto úrovní:

- Administrátor identifikátorov
- Administrátor EIM

Ak chcete odstrániť alias z identifikátora EIM, vykonajte tieto kroky:

1. Rozviňte **Sieť > Enterprise Identity Mapping > Správa domén**.
2. Vyberte doménu EIM, v ktorej chcete pracovať.
   - Ak sa doména EIM, s ktorou chcete pracovať nenachádza v zozname pod zložkou Správa domén, pozrite si časť "Pridanie domény Enterprise Identity Mapping do zložky Správa domén" na strane 78.
   - Ak nie ste pripojený k doméne EIM, v ktorej chcete pracovať, pozrite si tému "Pripojenie k doméne Enterprise Identity Mapping" na strane 78.
3. Rozviňte doménu EIM, ku ktorej ste pripojený.
4. Kliknite na **Identifikátory**, aby sa v pravej časti okna zobrazil zoznam identifikátorov EIM, dostupných v doméne.

   Poznámka: Zobrazenie zoznamu identifikátorov pri pokuse o rozvinutie zložky **Identifikátory** môže niekedy trvať dlho. Ak chcete zvýšiť výkon pri veľkom počte identifikátorov EIM v doméne, pozrite si časť "Prispôsobenie zobrazenia identifikátorov Enterprise Identity Mapping" na strane 90.

5. Pravým tlačidlom myši kliknite na identifikátor EIM, ku ktorému chcete pridať alias a vyberte **Vlastnosti**.
6. Vyberte alias, ktorý chcete odstrániť a kliknite na tlačidlo **Odstrániť**.
7. Kliknite na tlačidlo **OK**, aby sa uložili vaše zmeny.

Vymazanie identifikátora Enterprise Identity Mapping

Ak chcete vymazať identifikátor EIM, musíte byť pripojený k doméne EIM (Enterprise Identity Mapping), v ktorej chcete pracovať a musíte mať riadenie prístupu administrátora EIM.

Ak chcete vymazať identifikátor EIM, vykonajte tieto kroky:

1. Rozviňte **Sieť > Enterprise Identity Mapping > Správa domén**.
2. Vyberte doménu EIM, v ktorej chcete pracovať.
   - Ak sa doména EIM, s ktorou chcete pracovať nenachádza v zozname pod zložkou **Správa domén**, pozrite si časť "Pridanie domény Enterprise Identity Mapping do zložky Správa domén" na strane 78.
   - Ak nie ste pripojený k doméne EIM, v ktorej chcete pracovať, pozrite si tému Pripojiť k radiču domény EIM.
3. Rozviňte doménu EIM, ku ktorej ste teraz pripojený.
4. Kliknite na **Identifikátory**.

   Poznámka: Zobrazenie zoznamu identifikátorov pri pokuse o rozvinutie zložky **Identifikátory** môže niekedy trvať dlho. Ak chcete zvýšiť výkon pri veľkom počte identifikátorov EIM v doméne, pozrite si časť "Prispôsobenie zobrazenia identifikátorov Enterprise Identity Mapping" na strane 90.

5. Vyberte identifikátor EIM, ktorý chcete vymazať. Ak chcete vymazať viacero identifikátorov, pri výbere identifikátorov EIM stlačte kláves **Ctrl**.
6. Pravým tlačidlom myši kliknite na vybraté identifikátory EIM a vyberte **Vymazať**.
7. V dialógovom okne **Potvrdenie vymazania** kliknite na tlačidlo **Áno**, aby sa vymazali vybraté identifikátory EIM.

Prispôsobenie zobrazenia identifikátorov Enterprise Identity Mapping

Zobrazenie zoznamu identifikátorov pri pokuse o rozvinutie zložky **Identifikátory** môže niekedy trvať dlho. Ak chcete zvýšiť výkon v prípade veľkého počtu identifikátorov EIM (Enterprise Identity Mapping) v doméne, môžete prispôsobiť zobrazenie zložky **Identifikátory**.

Ak chcete prispôsobiť zobrazenie zložky **Identifikátory**, vykonajte tieto kroky:

1. Rozviňte **Network —> Enterprise Identity Mapping —> Domain Management**.
2. Vyberte doménu EIM, v ktorej chcete pracovať.
   - Ak sa doména EIM, s ktorou chcete pracovať nenachádza v zozname pod zložkou **Správa domén**, pozrite si časť “Pridanie domény Enterprise Identity Mapping do zložky Správa domén” na strane 78.
   - Ak nie ste pripojený k doméne EIM, v ktorej chcete pracovať, pozrite si tému Pripojiť k radiču domény EIM.
3. Pravým tlačidlom myši kliknite na zložku **Identifikátory** a vyberte **Prispôsobiť toto zobrazenie**.
4. Zadajte kritériá, ktoré chcete použiť pre zobrazenie identifikátorov EIM v doméne. Ak chcete znížiť počet zobrazených identifikátorov EIM, zadajte znaky, ktoré chcete použiť pre triedenie identifikátorov. V názve identifikátora môžete zadať jeden alebo viac zástupných znakov (*). Napríklad môžete ako vaše kritérium triedenia v poli **Identifikátory** zadať *JOHNSON*. Výsledky budú zahŕňať všetky identifikátory EIM, kde je znakový reťazec JOHNSON definovaný ako časť názvu identifikátora EIM a tiež budú zahŕňať identifikátory EIM, kde je znakový reťazec JOHNSON definovaný ako časť aliasu pre identifikátor EIM.
5. Kliknite na tlačidlo **OK**, aby sa uložili vaše zmeny.

Manažovanie priradení

EIM vám dovoľuje vytvárať a manažovať dva typy priradení, ktoré definujú priame alebo nepriame vzťahy medzi identitami užívateľa: priradenia identifikátorov a priradenia politiky. EIM vám dovoľuje vytvárať a manažovať priradenia identifikátorov medzi identifikátormi EIM a ich identitami užívateľa, ktoré vám dovoľujú definovať nepriame, ale špecifické, individuálne vzťahy medzi identitami užívateľa. EIM vám tiež dovoľuje vytvoriť priradenia politiky na opísanie vzťahu medzi viacerými identitami užívateľa v jednom alebo viacerých registroch a individuálnej cieľovej identity užívateľa v inom registri. Priradenia politiky používajú podporu politiky mapovania EIM na vytvorenie mapovaní typu veľa-jeden medzi identitami užívateľov bez toho, aby vyžadovali identifikátor EIM. Oba typy priradení definujú vzťahy medzi identitami užívateľov v podniku, manažovanie priradení je dôležitým prvkom pri manažovaní EIM.

Údržba priradení v doméne je kľúč k zjednodušeniu administratívnych úloh vyžadovaných na vedenie záznamov o užívateľoch, ktorý majú kontá v rôznych systémoch v sieti. Ak implementujete bezpečnú sieť s jednoduchým prihlásením, potrebujte udržiavať priradenia identifikátorov a priradenia politiky aktuálne.

S priradeniami môžete vykonávať nasledujúce riadiace úlohy:

- “Vytvorenie priradení” na strane 91
- Pridať informácie na vyhľadanie do cieľovej identity užívateľa.
- Odstrániť informácie na vyhľadanie z cieľovej identity užívateľa.
- Zobraziť priradenia pre identifikátor EIM.
- Zobraziť všetky priradenia politiky pre doménu.
- Zobraziť všetky priradenia politiky pre register.
- “Vymazanie priradenia identifikátora” na strane 102
- “Vymazanie priradenia politiky” na strane 103

Vytvorenie priradení

Priradenia môžete vytvoriť nasledujúcimi dvoma spôsobmi:

- Môžete vytvoriť priradenie identifikátora na nepriame definovanie vzťahu medzi identitami užívateľov, ktoré používa jedna osoba. Priradenie identifikátora opisuje vzťah medzi identifikátorom EIM a identitou užívateľa v registri užívateľov. Priradenia identifikátorov vám dovoľujú vytvoriť mapovania typu jeden-jeden medzi identifikátormi EIM a jednotlivými, rôznymi identitami užívateľa, ktoré súvisia s užívateľom, ktorý je reprezentovaný identifikátorom EIM.
- Môžete vytvoriť priradenie politiky na priame definovanie vzťahu medzi viacerými identitami užívateľov v jednom alebo viacerých registroch a individuálnou cieľovou identitou užívateľa v inom registri. Priradenia politiky používajú podporu politiky mapovania EIM na vytvorenie mapovaní typu veľa-jeden medzi identitami užívateľa bez zahrnutia identifikátora EIM. Priradenia politiky vám umožnia rýchlo vytvoriť veľké množstvo mapovaní medzi identitami užívateľa v rôznych registroch užívateľov.

Rozhodnutie či vytvoriť priradenia identifikátorov, priradenia politiky, alebo použiť obidve tieto metódy závisí na vašich potrebách implementácie EIM. Ak sa chcete dozvedieť viac, pozrite si časť Vytvorenie celkového plánu mapovania identity.

Vytvorenie priradenia identifikátora: Priradenia identifikátorov definujú vzťah medzi identifikátormi EIM a identitou užívateľa vo vašom podniku pre osobu alebo entitu, ktorej sa týka identifikátor EIM. Môžete vytvoriť tri typy priradení identifikátorov: cieľové, zdrojové a administratívne. Ak sa chcete vyhnúť možným problémom s priradeniami a spôsobom mapovania identít, musíte skôr ako začnete definovať priradenia, vytvoriť celkový plán mapovania identít pre váš podnik.

Ak chcete vytvoriť priradenie identifikátora, musíte byť pripojený k doméne EIM, v ktorej chcete pracovať a musíte mať priradenia vyžadované podľa typu priradenia, ktoré chcete vytvoriť.

Ak chcete vytvoriť zdrojové alebo administratívne priradenie, musíte mať riadenie prístupu k EIM na jednej z týchto úrovní:

- Administrátor identifikátorov
- Administrátor EIM

Ak chcete vytvoriť cieľové priradenie, musíte mať riadenie prístupu k EIM na jednej z týchto úrovní:

- Administrátor registrov
- Administrátor pre vybraté registre (definície registra, ktorá odkazuje na register užívateľov, obsahujúci cieľovú identitu užívateľa)
- Administrátor EIM

Ak chcete vytvoriť priradenie identifikátora, vykonajte tieto kroky:

1. Rozviňte **Sieť > Enterprise Identity Mapping > Správa domén**.
2. Vyberte doménu EIM, v ktorej chcete pracovať.
   - V prípade, že doména EIM, v ktorej chcete pracovať sa nenachádza v **Správe domén**, pozrite si časť "Pridanie domény Enterprise Identity Mapping do zložky Správa domén" na strane 78.
   - Pokiaľ nie ste pripojený k doméne EIM, v ktorej chcete pracovať, pozrite si časť Pripojenie k radiču domény EIM.
3. Rozviňte doménu EIM, ku ktorej ste teraz pripojený.
4. Ak chcete zobraziť zoznam identifikátorov EIM, kliknite na **Identifikátory**.

   Poznámka: Zobrazenie zoznamu identifikátorov pri pokuse o rozvinutie zložky **Identifikátory** môže niekedy trvať dlho. Ak chcete zvýšiť výkon pri veľkom počte identifikátorov EIM v doméne, pozrite si časť "Prispôsobenie zobrazenia identifikátorov Enterprise Identity Mapping" na strane 90.
5. Pravým tlačidlom myši kliknite na identifikátor EIM, pre ktorý chcete vytvoriť priradenie a vyberte **Vlastnosti...**
6. Vyberte stranu **Priradenia** a kliknite na tlačidlo **Pridať...**.

7. V dialógovom okne **Priedanie priradenia** zadajte nasledujúce informácie na definovanie priradenia:
   - Názov registra, ktorý obsahuje identitu užívateľa, ktorú chcete priradiť identifikátoru EIM. Zadajte presný názov existujúcej definície registra alebo ho vyhľadajte.
   - Názov identity užívateľa, ktorú chcete priradiť identifikátoru EIM.
   - Typ priradenia. Priradenie môže mať jeden z týchto troch typov:
     – Administratívne
     – Zdrojové
     – Cieľové
8. Ak potrebujete zistiť, aké informácie treba zadať do jednotlivých polí, kliknite na tlačidlo **Pomoc**.
9. Voliteľné. Ak chcete zobraziť pre cieľové priradenie dialógové okno **Pridanie priradenia - Rozšírené**, kliknite na tlačidlo **Rozšírené...**. Ak sa chcete vrátiť do dialógového okna **Pridanie priradenia**, zadajte informácie na vyhľadanie pre cieľovú identitu užívateľa a kliknite na tlačidlo **OK**.
10. Ak chcete vytvoriť priradenie, kliknite po zadaní vyžadovaných informácií na tlačidlo **OK**.

Vytvorenie priradenia politiky: Priradenie politiky poskytuje prostriedky na priame definovanie vzťahu medzi viacerými identitami užívateľa v jednom alebo viacerých registroch a individuálnou cieľovou identitou užívateľa v inom registri. Priradenia politiky používajú podporu politiky mapovania EIM na vytvorenie mapovaní typu veľa-jeden medzi identitami užívateľa bez zahrnutia identifikátora EIM. Priradenia politiky môžete používať rôznymi spôsobmi prekrývania, preto musíte sa dôkladne oboznámiť s podporou politiky mapovania EIM skôr, než priradenia politiky vytvoríte a začnete používať. Ak sa chcete vyhnúť možným problémom s priradeniami a spôsobom mapovania identít, musíte skôr ako začnete definovať priradenia, vytvoriť celkový plán mapovania identít pre váš podnik.

Rozhodnutie či vytvoriť priradenia identifikátorov, priradenia politiky, alebo použiť obidve tieto metódy závisí na vašich potrebách implementácie EIM.

Spôsob, akým vytvoríte priradenia politiky sa líši v závislosti na type priradenia politiky. Ak sa chcete dozvedieť viac o vytváraní priradenia politiky, pozrite si časť:

- Vytvorenie predvoleného priradenia politiky domény.
- Vytvorenie predvoleného priradenia politiky registra.
- Vytvorenie priradenia politiky filtra certifikátov.

Vytvorenie predvoleného priradenia politiky domény: Ak chcete vytvoriť predvolené priradenie politiky domény, musíte byť pripojený k doméne EIM, v ktorej chcete pracovať a musíte mať “Riadenie prístupu EIM” na strane 33 na jednej z týchto úrovní:

- Administrátor EIM
- Administrátor registrov

Poznámka: Priradenie politiky opisuje vzťah medzi viacerými identitami užívateľa a jednou identitou užívateľa v cieľovom registri užívateľov. Priradenie politiky môžete použiť na opísanie vzťahu medzi zdrojovou množinou viacerých identít užívateľa a jednou identitou cieľového užívateľa v určenom cieľovom registri užívateľov. Priradenia politiky používajú podporu politiky mapovania EIM na vytvorenie mapovaní typu veľa-jeden medzi identitami užívateľov bez toho, aby vyžadovali identifikátor EIM.

Priradenia politiky môžete používať rôznymi spôsobmi prekrývania, preto musíte sa dôkladne oboznámiť s podporou politiky mapovania EIM skôr, než priradenia politiky vytvoríte a začnete používať. Podobne, aby ste predišli možným problémom s priradeniami a spôsobom, akým mapujú identity, musíte predtým, než začnete definovať priradenia, vytvoriť celkový plán mapovania identít pre váš podnik.

V predvolenom priradení politiky domény sú všetci užívatelia v doméne zdrojom priradenia politiky a sú mapovaní na jeden cieľový register a cieľového užívateľa. Pre každý register v doméne môžete zadefinovať predvolené priradenie politiky domény. Ak sa dve alebo viac priradení politiky domény týka rovnakého cieľového registra, pre každé z týchto priradení politiky môžete zadefinovať jedinečné informácie na vyhľadanie, aby ste zabezpečili, že operácie vyhľadávania mapovaní môžu medzi nimi rozlíšiť. V opačnom prípade môžu operácie vyhľadávania mapovaní vrátiť

viaceré identity cieľového užívateľa. V dôsledku týchto nejednoznačných výsledkov nebudú aplikácie, ktoré sa spoliehajú na EIM, pravdepodobne schopné určiť konkrétnu cieľovú identitu, ktorá sa má použiť.

Ak chcete vytvoriť predvolené priradenie politiky domény, vykonajte nasledujúce kroky:

1. Rozviňte **Sieť > Enterprise Identity Mapping > Správa domén**.
2. Pravým tlačidlom myši kliknite na doménu EIM, v ktorej chcete pracovať a vyberte **Politika mapovania...**
   - Ak doména EIM, s ktorou chcete pracovať nie je uvedená pod **Správa domén**, pozrite si časť "Pridanie domény Enterprise Identity Mapping do zložky Správa domén" na strane 78.
   - Ak momentálne nie ste pripojený k doméne EIM, v ktorej chcete pracovať, pozrite si Pripojenie k radiču domény EIM.
3. Na strane Všeobecné vyberte **Povoliť vyhľadávanie mapovaní pomocou priradení politiky pre doménu**.
4. Vyberte stranu **Doména** a kliknite na **Pridať...**.
5. V dialógovom okne **Pridanie predvoleného priradenia politiky domény** uveďte nasledujúce požadované informácie:
   - Názov definície **Cieľového registra** pre priradenie politiky.
   - Názov identity **Cieľového užívateľa** pre priradenie politiky.
6. Ak potrebujete viac detailov o dokončení tohto a následných dialógových okien, kliknite na **Pomoc**.
7. Voliteľné. Kliknite na **Rozšírené...**, aby sa zobrazilo dialógové okno **Pridanie priradenia - Rozšírené**. Zadajte **Informácie na vyhľadanie** pre priradenie politiky a kliknite na **OK**, aby ste sa vrátili do dialógového okna **Pridanie predvoleného priradenia politiky domény**.

   Poznámka: Ak sa dve alebo viaceré predvolené priradenia politiky domény týkajú rovnakého cieľového registra, musíte pre každú z identít cieľového užívateľa v týchto priradeniach politiky definovať jedinečné informácie na vyhľadanie. Zadefinovaním informácií na vyhľadanie pre každú identitu cieľového užívateľa v tejto situácii zabezpečte, aby operácie vyhľadávania mapovaní mohli medzi nimi rozlišovať. V opačnom prípade môžu operácie vyhľadávania mapovaní vrátiť viaceré identity cieľového užívateľa. V dôsledku týchto nejednoznačných výsledkov nebudú aplikácie, ktoré sa spoliehajú na EIM, pravdepodobne schopné určiť konkrétnu cieľovú identitu, ktorá sa má použiť.
8. Ak chcete vytvoriť nové priradenie politiky, kliknite na **OK** a vráťte sa na stranu **Doména**. Nové priradenie politiky sa teraz zobrazí v tabuľke **Predvolené priradenia politiky**.
9. Skontrolujte, či je nové priradenie politiky pre cieľový register aktivované.
10. Kliknite na **OK**, aby ste uložili vaše zmeny a zatvorili dialógové okno **Politika mapovania**.

Poznámka: Skontrolujte, či sú podpora politiky mapovania a používanie priradení politiky pre cieľový register užívateľov správne aktivované. Ak nie sú aktivované, priradenie politiky nenadobudne účinnosť.

Vytvorenie predvoleného priradenia politiky registra: Ak chcete vytvoriť predvolené priradenie politiky registra, musíte byť pripojený k doméne EIM, v ktorej chcete pracovať a musíte mať "Riadenie prístupu EIM" na strane 33 na jednej z týchto úrovní:

- Administrátor EIM
- Administrátor registrov

Poznámka: Priradenie politiky opisuje vzťah medzi viacerými identitami užívateľa a jednou identitou užívateľa v cieľovom registri užívateľov. Priradenie politiky môžete použiť na opísanie vzťahu medzi zdrojovou množinou viacerých identít užívateľa a jednou identitou cieľového užívateľa v určenom cieľovom registri užívateľov. Priradenia politiky používajú podporu politiky mapovania EIM na vytvorenie mapovania typu veľa-jeden medzi identitami užívateľa bez toho, aby vyžadovali identifikátor EIM.

Priradenia politiky môžete používať rôznymi spôsobmi prekrývania, preto musíte sa dôkladne oboznámiť s podporou politiky mapovania EIM skôr, než priradenia politiky vytvoríte a začnete používať. Podobne, aby ste predišli možným problémom s priradeniami a spôsobom, akým mapujú identity, musíte predtým, než začnete definovať priradenia, vytvoriť celkový plán mapovania identít pre váš podnik.

V predvolenom priradení politiky registra sú všetci užívatelia v jednom registri zdrojom priradenia politiky a sú mapovaní na jeden cieľový register a cieľového užívateľa. Keď aktivujete predvolené priradenie politiky registra pre cieľový register, priradenie politiky zabezpečí, že tieto identity zdrojového užívateľa môžu byť všetky mapované na jeden určený cieľový register a cieľového užívateľa.

Ak chcete vytvoriť predvolené priradenie politiky registra, vykonajte nasledujúce kroky:

1. Rozviňte **Sieť > Enterprise Identity Mapping > Správa domén**.
2. Pravým tlačidlom myši kliknite na doménu EIM, v ktorej chcete pracovať a vyberte **Politika mapovania...**
   - Ak doména EIM, s ktorou chcete pracovať nie je uvedená pod **Správa domén**, pozrite si časť "Pridanie domény Enterprise Identity Mapping do zložky Správa domén" na strane 78.
   - Ak momentálne nie ste pripojený k doméne EIM, v ktorej chcete pracovať, pozrite si Pripojenie k radiču domény EIM.
3. Na strane Všeobecné vyberte **Povoliť vyhľadávanie mapovaní pomocou priradení politiky pre doménu**.
4. Vyberte stranu **Register** a kliknite na **Pridať...**.
5. V dialógovom okne **Pridanie predvoleného priradenia politiky registra** uveďte nasledujúce požadované informácie:
   - Názov definície **Zdrojového registra** pre priradenie politiky.
   - Názov definície **Cieľového registra** pre priradenie politiky.
   - Názov identity **Cieľového užívateľa** pre priradenie politiky.
6. Ak potrebujete viac detailov o dokončení tohto a následných dialógových okien, kliknite na **Pomoc**.
7. Voliteľné. Kliknite na **Rozšírené...**, aby sa zobrazilo dialógové okno **Pridanie priradenia - Rozšírené**. Zadajte **Informácie na vyhľadanie** pre priradenie politiky a kliknite na **OK**, aby ste sa vrátili do dialógového okna **Pridanie predvoleného priradenia politiky registra**.

   Poznámka: Ak sa dve alebo viac priradení politiky s rovnakým zdrojovým registrom týka rovnakého cieľového registra, musíte pre každú z identít cieľového užívateľa v týchto priradeniach politiky definovať jedinečné informácie na vyhľadanie. Zadefinovaním informácií na vyhľadanie pre každú identitu cieľového užívateľa v tejto situácii zabezpečte, aby operácie vyhľadávania mapovaní mohli medzi nimi rozlišovať. V opačnom prípade môžu operácie vyhľadávania mapovaní vrátiť viaceré identity cieľového užívateľa. V dôsledku týchto nejednoznačných výsledkov nebudú aplikácie, ktoré sa spoliehajú na EIM, pravdepodobne schopné určiť konkrétnu cieľovú identitu, ktorá sa má použiť.
8. Ak chcete vytvoriť nové priradenie politiky, kliknite na **OK** a vráťte sa na stránku **Registry**. Nové predvolené priradenie politiky registra sa teraz zobrazí v tabuľke **Predvolené priradenia politiky**.
9. Skontrolujte, či je nové priradenie politiky pre cieľový register aktivované.
10. Kliknite na **OK**, aby ste uložili vaše zmeny a zatvorili dialógové okno **Politika mapovania**.

Poznámka: Skontrolujte, či sú podpora politiky mapovania a používanie priradení politiky pre cieľový register užívateľov správne aktivované. Ak nie sú aktivované, priradenie politiky nenadobudne účinnosť.

Vytvorenie priradenia politiky filtra certifikátov: Ak chcete vytvoriť priradenie politiky filtra certifikátov, musíte byť pripojený k doméne EIM, v ktorej chcete pracovať a musíte mať "Riadenie prístupu EIM" na strane 33 na jednej z týchto úrovní:

- Administrátor EIM
- Administrátor registrov

Poznámka: Priradenie politiky opisuje vzťah medzi zdrojo množinou viacerých identít užívateľa a jednou identitou cieľového užívateľa v určenom cieľovom registri užívateľov. Priradenia politiky používajú podporu politiky mapovania EIM na vytvorenie mapovaní typu veľa-jeden medzi identitami užívateľov bez toho, aby vyžadovali identifikátor EIM.

Priradenia politiky môžete používať rôznymi spôsobmi prekrývania, preto musíte sa dôkladne oboznámiť s podporou politiky mapovania EIM skôr, než priradenia politiky vytvoríte a začnete používať. Podobne,

aby ste predišli možným problémom s priradeniami a spôsobom, akým mapujú identity, musíte predtým, než začnete definovať priradenia, vytvoriť celkový plán mapovania identít pre váš podnik.

V priradení politiky filtra certifikátov uveďte ako zdroj priradenia politiky množinu certifikátov v jednom registri X.509. Tieto certifikáty sa mapujú na jeden cieľový register a cieľového užívateľa, ktorého určíte. Na rozdiel od predvoleného priradenia politiky registra, v ktorom sú všetci užívatelia v jednom registri zdrojom priradenia politiky, oblasť priradenia politiky filtra certifikátov je pružnejšia. Ako zdroj môžete uviesť podskupinu certifikátov v tomto registri. Filter certifikátov, ktorý uvediete pre priradenie politiky, určuje jeho oblasť.

Poznámka: Keď chcete mapovať všetky certifikáty v registri užívateľov X.509 na jednu identitu cieľového užívateľa, vytvorte a použite predvolené priradenie politiky registra.

Filter certifikátov určuje, ako priradenie politiky filtra certifikátov mapuje jednu zdrojovú sadu identít užívateľa, v tomto prípade digitálnych certifikátov, na identitu určeného cieľového užívateľa. Filter certifikátov, ktorý chcete použiť, musí preto existovať predtým, než vytvoríte priradenie politiky filtra certifikátov.

Predtým, než vytvoríte priradenie politiky filtra certifikátov, musíte najprv vytvoriť filter certifikátov, ktorý sa použije ako základ pre priradenie politiky.

Ak chcete vytvoriť priradenie politiky filtra certifikátov, vykonajte nasledujúce kroky:

1. Rozviňte **Sieť > Enterprise Identity Mapping > Správa domén**.
2. Pravým tlačidlom myši kliknite na doménu EIM, v ktorej chcete pracovať a vyberte **Politika mapovania...**
   - Ak doména EIM, s ktorou chcete pracovať nie je uvedená pod **Správa domén**, pozrite si časť “Pridanie domény Enterprise Identity Mapping do zložky Správa domén” na strane 78.
   - Ak momentálne nie ste pripojený k doméne EIM, v ktorej chcete pracovať, pozrite si Pripojenie k radiču domény EIM.
3. Na strane Všeobecné vyberte **Povoliť vyhľadávanie mapovaní pomocou priradení politiky pre doménu**.
4. Vyberte stranu **Filter certifikátov** a kliknite na **Pridať...**, aby sa zobrazilo dialógové okno **Pridanie priradenia politiky filtra certifikátov**.
5. Ak potrebujete viac detailov o dokončení tohto a následných dialógových okien, kliknite na **Pomoc**.
6. Na zadefinovanie priradenia politiky uveďte nasledujúce požadované informácie:
   - Zadajte názov definície registra užívateľov X.509, ktorý sa bude používať ako **Zdrojový register X.509** pre priradenie politiky. Prípadne kliknite na **Prehľaadať...** a definíciu vyberte zo zoznamu definícií registrov pre túto doménu.
   - Kliknite na **Vybrať**, aby sa zobrazilo dialógové okno **Výber filtra certifikátov** a vyberte existujúci filter certifikátov, ktorý sa použije ako základ pre nové priradenie politiky filtra certifikátov.

     Poznámka: **Musíte** použiť existujúci filter certifikátov. Ak filter certifikátov, ktorý chcete použiť nie je uvedený, kliknite na **Pridať...** a vytvorte nový filter certifikátov.
   - Zadajte názov definície **Cieľového registra** alebo kliknite na **Prehľadať...** a vyberte definíciu zo zoznamu existujúcich definícií registrov pre túto doménu.
   - Zadajte názov **Cieľového užívateľa** na ktorého sa majú mapovať všetky certifikáty v **Zdrojovom registri X.509**, ktoré sa zhodujú s filtrom certifikátov. Prípadne kliknite na **Prehľadať...** a užívateľa vyberte zo zoznamu užívateľov, ktorých pozná táto doména.
   - Voliteľné. Kliknite na **Rozšírené...**, aby sa zobrazilo dialógové okno **Pridanie priradenia - Rozšírené**. Zadajte **Informácie na vyhľadanie** pre identitu cieľového užívateľa a kliknite na **OK**, aby ste sa vrátili do dialógového okna **Pridanie priradenia politiky filtra certifikátov**.

     Poznámka: Ak sa dve alebo viac priradení politiky s kritériami rovnakého zdrojového registra X.509 a kritériami rovnakého filtra certifikátov týkajú rovnakého cieľového registra, musíte v každom z týchto priradení politiky definovať jedinečné informácie na vyhľadanie pre identity cieľového užívateľa. Zadefinovaním informácií na vyhľadanie pre každú identitu cieľového užívateľa v tejto situácii zabezpečte, aby operácie vyhľadávania mapovaní mohli medzi nimi rozlišovať. V opačnom

prípade môžu operácie vyhľadávania mapovaní vrátiť viaceré identity cieľového užívateľa. V dôsledku týchto nejednoznačných výsledkov nebudú aplikácie, ktoré sa spoliehajú na EIM, pravdepodobne schopné určiť konkrétnu cieľovú identitu, ktorá sa má použiť.

7. Ak chcete vytvoriť priradenie politiky filtra certifikátov, kliknite na **OK** a vráťte sa na stranu **Filter certifikátov**. Nové priradenie politiky sa zobrazí v zozname.
8. Skontrolujte, či je nové priradenie politiky pre cieľový register aktivované.
9. Kliknite na **OK**, aby ste uložili vaše zmeny a zatvorili dialógové okno **Politika mapovania**.

Poznámka: Skontrolujte, či sú podpora politiky mapovania a používanie priradení politiky pre cieľový register užívateľov správne aktivované. Ak nie sú aktivované, priradenie politiky nenadobudne účinnosť.

Vytvorenie filtra certifikátov: Filter certifikátov definuje sadu podobných atribútov certifikátu rozlišovacieho názvu pre skupinu užívateľských certifikátov v zdrojovom registri užívateľov X.509. Filter certifikátov môžete použiť ako základ priradenia politiky filtra certifikátov. Filter certifikátov v priradení politiky určuje, ktoré certifikáty v určenom zdrojovom registri X.509 treba mapovať na určeného cieľového užívateľa. Certifikáty obsahujúce informácie o DN subjektu a DN vydavateľa, ktoré spĺňajú kritériá filtra, sa mapujú na určeného cieľového užívateľa počas operácií vyhľadávania mapovaní EIM.

Ak chcete vytvoriť filter certifikátov, musíte byť pripojený k doméne EIM, v ktorej chcete pracovať a musíte mať "Riadenie prístupu EIM" na strane 33 na jednej z týchto úrovní:

- Administrátor EIM
- Administrátor registrov
- Administrátor pre vybraté registre (pre definíciu registra, týkajúcu sa registra užívateľov X.509, pre ktorých chcete vytvoriť filter certifikátov)

Na základe informácií z digitálneho certifikátu o konkrétnom rozlišovacom názve (DN) vytvorte filter certifikátov. Informácie o DN, ktoré uviediete, môžu byť buď rozlišovacím názvom subjektu, ktorý označuje vlastníka certifikátu, alebo rozlišovacím názvom vydavateľa, ktorý označuje vydavateľa certifikátu. Vo filtri certifikátov môžete uviesť informácie o úplnom alebo čiastočnom DN.

Keď filter certifikátov pridáte do priradenia politiky filtra certifikátov, filter certifikátov určí, ktoré certifikáty v registri X.509 sa mapujú na identitu cieľového užívateľa, určenú priradením politiky. Keď je digitálny certifikát identitou zdrojového užívateľa v operácii vyhľadávania mapovaní EIM (po tom, ako žiadajúca aplikácia použije na naformátovanie názvu identity užívateľa API EIM eimFormatUserIdentity()) a platí priradenie politiky filtra certifikátov, EIM porovná informácie o DN v certifikáte s informáciami o DN alebo čiastočnom DN, uvedenými vo filtri. Ak sa informácie o DN v certifikáte zhodujú s informáciami vo filtri, EIM vráti identitu cieľového užívateľa, ktorú špecifikovalo priradenie politiky filtra certifikátov.

Pri vytváraní filtra certifikátov môžete požadované informácie o rozlišovacom názve poskytnúť jedným z troch spôsobov:

- Pre **DN subjektu**, pre **DN vydavateľa** alebo pre obe môžete zadať úplné alebo čiastočné DN konkrétneho certifikátu.
- Informácie môžete skopírovať z konkrétneho certifikátu do vašej odkladacej schránky a použiť ich na vytvorenie zoznamu kandidátov filtra certifikátov podľa informácií o rozlišovacom názve v certifikáte. Potom sa môžete rozhodnúť, ktoré DN sa majú použiť pre filter certifikátov.

  Poznámka: Ak chcete vytvoriť požadované informácie o rozlišovacom názve a vytvoriť filter certifikátov, musíte pred vykonaním tejto úlohy skopírovať informácie z certifikátu do odkladacej schránky. Formát kódovania certifikátu musí byť base64. Detailnejšie informácie týkajúce sa metód získavania certifikátu v správnom formáte nájdete v časti Filter certifikátov.
- Zoznam kandidátov filtra certifikátov môžete vytvoriť podľa informácií o rozlišovacom názve z digitálneho certifikátu, v prípade ktorého existuje zdrojové priradenie s identifikátorom EIM. Potom sa môžete rozhodnúť, ktoré DN sa majú použiť pre filter certifikátov.

Ak chcete vytvoriť filter certifikátov, ktorý sa má používať ako základ pre priradenie politiky filtra certifikátov, vykonajte nasledujúce kroky:

1. Rozviňte **Sieť > Enterprise Identity Mapping > Správa domén**.
2. Pravým tlačidlom myši kliknite na doménu EIM, v ktorej chcete pracovať a vyberte **Politika mapovania...**
   - Ak doména EIM, s ktorou chcete pracovať nie je uvedená pod **Správa domén**, pozrite si časť "Pridanie domény Enterprise Identity Mapping do zložky Správa domén" na strane 78.
   - Ak momentálne nie ste pripojený k doméne EIM, v ktorej chcete pracovať, pozrite si Pripojenie k radiču domény EIM.
3. Vyberte stranu **Filter certifikátov** a kliknite na **Filtre certifikátov...**, aby sa zobrazilo dialógové okno **Filtre certifikátov**.

   Poznámka: Ak kliknete na **Filtre certifikátov...** a nevyberiete priradenie politiky, zobrazí sa dialógové okno **Výber registrov EIM**. Toto dialógové okno vám umožní vybrať register X.509 zo zoznamu definícií registra X.509 v doméne, pre ktorú chcete zobraziť filtre certifikátov. Obsah zoznamu je rôzny v závislosti od typu vášho riadenia prístupu k EIM.
4. Kliknite na **Pridať...**, aby sa zobrazilo dialógové okno **Pridanie filtra certifikátov**.
5. V dialógovom okne **Pridanie filtra certifikátov** sa musíte rozhodnúť, či chcete pridať jeden filter certifikátov alebo vytvoriť filter certifikátov na základe konkrétneho digitálneho certifikátu. Ak potrebujete viac detailov o dokončení tohto a následných dialógových okien, kliknite na **Pomoc**.
   a. Ak vyberiete **Pridať jeden filter certifikátov**, môžete zadať informácie o konkrétnom úplnom alebo čiastočnom **DN subjektu**, o úplnom alebo čiastočnom **DN vydavateľa** alebo o oboch. Ak chcete vytvoriť filter certifikátov, kliknite na **OK** a vráťte sa do dialógového okna **Filtre certifikátov**. Filter sa teraz zobrazí v zozname.
   b. Ak sa rozhodnete **Vytvoriť filter certifikátov z digitálneho certifikátu**, kliknite na **OK**, aby sa zobrazilo dialógové okno **Generovanie filtrov certifikátov**.
      1) Zakódovanú verziu informácií certifikátu vo formáte base64, ktorú ste predtým skopírovali do odkladacej schránky, vložte do poľa **Informácie o certifikáte**.
      2) Kliknite na **OK**, aby sa vytvoril zoznam možných filtrov certifikátov podľa **DN subjektu** a **DN vydavateľa** certifikátu.
      3) Z dialógového okna **Výber filtrov certifikátov** vyberte jeden alebo viacero týchto filtrov certifikátov. Kliknite na **OK**, aby ste sa vrátili do dialógového okna **Výber filtrov certifikátov**, kde sú teraz zobrazené vybraté filtre certifikátov.
   c. Ak sa rozhodnete **Vytvoriť filter certifikátov zo zdrojového priradenia pre užívateľa X.509**, kliknite na **OK**, aby sa zobrazilo dialógové okno **Generovanie filtrov certifikátov**. Toto dialógové okno zobrazuje zoznam identít užívateľov X.509, ktorí majú v doméne zdrojové priradenie s identifikátorom EIM.
      1) Vyberte identitu užívateľa X.509, ktorého digitálny certifikát chcete použiť na vytvorenie jedného alebo viacerých kandidátov filtra certifikátov a kliknite na **OK**.
      2) Kliknite na **OK**, aby sa vytvoril zoznam možných filtrov certifikátov podľa **DN subjektu** a **DN vydavateľa** certifikátu.
      3) Z dialógového okna **Výber filtrov certifikátov** vyberte jeden alebo viacero týchto možných filtrov certifikátov. Kliknite na **OK**, aby ste sa vrátili do dialógového okna **Výber filtrov certifikátov**, kde sú teraz zobrazené vybraté filtre certifikátov.

Nový filter certifikátov môžete teraz použiť ako základ pre vytvorenie priradenia politiky filtra certifikátov.

Pridanie informácií na vyhľadanie k cieľovej identite užívateľa

Informácie na vyhľadanie predstavujú voliteľné jedinečné identifikačné údaje cieľovej identity užívateľa, definované v priradení. Toto priradenie môže byť cieľové priradenie identifikátora alebo priradenie politiky. Informácie na vyhľadanie sú potrebné, len ak operácia vyhľadávania mapovaní môže vrátiť viac ako jednu cieľovú identitu užívateľa. Táto situácia môže vytvoriť problémy pre aplikácie podporujúce EIM, vrátane aplikácií systému OS/400 a produktov, ktoré neboli navrhnuté na obslúženie týchto nejednoznačných výsledkov.

Keď je to potrebné, môžete pridať informácie na vyhľadanie pre každú cieľovú identitu užívateľa, čím poskytnete detailnejšie identifikačné informácie, ktoré viac opisujú každú cieľovú identitu užívateľa. Ak definujete informácie na vyhľadanie pre cieľovú identitu užívateľa, musia sa poskytnúť operácii vyhľadávania mapovaní, aby táto operácia vrátila jedinečnú cieľovú identitu užívateľa. V opačnom prípade nemusia byť aplikácie spoliehajúce sa na EIM schopné určiť presnú cieľovú identitu, ktorá sa má použiť.

Poznámka: Ak nechcete, aby boli operácie prehľadania EIM schopné vracať viac ako jednu cieľovú identitu užívateľa, mali by ste namiesto používania informácií na vyhľadanie opraviť konfiguráciu vašich priradení. Pozrite si časť “Odstraňovanie problémov s Enterprise Identity Mapping: Problémy s mapovaním” na strane 109, kde nájdete detailné informácie.

Spôsob pridania informácií na vyhľadanie na ďalšie definovanie cieľovej identity užívateľa závisí od toho, či cieľová identita užívateľa je definovaná v priradení identifikátora alebo v cieľovom priradení. Bez ohľadu na metódu, ktorú použijete na pridanie informácií na vyhľadanie, zadané informácie sa naviažu k cieľovej identite užívateľa, a nie k priradeniam identifikátorov alebo priradeniam politiky, v ktorých sa identita užívateľa nachádza.

Pridanie informácií na vyhľadanie k cieľovej identite užívateľa v priradení identifikátora

Ak chcete pridať informácie na vyhľadanie k cieľovej identite užívateľa v priradení identifikátora, musíte byť pripojený k doméne EIM, v ktorej chcete pracovať a musíte mať oprávnenia na jednej z týchto úrovní:

- Administrátor registrov
- Administrátor pre vybraté registre (definície registra, ktorá odkazuje na register užívateľov, obsahujúci cieľovú identitu užívateľa)
- Administrátor EIM

Ak chcete pridať informácie na vyhľadanie k cieľovej identite užívateľa v priradení identifikátora, vykonajte tieto kroky:

1. Rozviňte **Sieť > Enterprise Identity Mapping > Správa domén**.
2. Vyberte doménu EIM, v ktorej chcete pracovať.
   - Ak sa doména EIM, s ktorou chcete pracovať nenachádza v zozname **Správa domén**, pozrite si časť “Pridanie domény Enterprise Identity Mapping do zložky Správa domén” na strane 78.
   - Ak nie ste pripojený k doméne, v ktorej chcete pracovať, pozrite si časť Pripojenie k radiču domény EIM.
3. Rozviňte doménu EIM, ku ktorej ste pripojený.
4. Zobrazte zoznam identifikátorov EIM pre doménu kliknutím na zložku **Identifikátory**.

   Poznámka: Zobrazenie zoznamu identifikátorov po rozvinutí zložky **Identifikátory** môže niekedy trvať dlho. Ak chcete zvýšiť výkon pri veľkom počte identifikátorov EIM v doméne, môžete prispôsobiť zobrazenie zložky **Identifikátory** pomocou obmedzenia vyhľadávacieho kritéria, ktoré sa používa na zobrazenie identifikátorov. Pravým tlačidlom myši kliknite na zložku **Identifikátory**, vyberte položku **Prispôsobiť zobrazenie... > Zahrnúť** a zadajte kritérium zobrazenia, ktoré sa má použiť na generovanie zoznamu identifikátorov EIM, ktoré sa majú zahrnúť do tohto zobrazenia.
5. Pravým tlačidlom myši kliknite na identifikátor EIM a vyberte položku **Vlastnosti...**.
6. Vyberte stranu **Priradenia**, potom vyberte zdrojové priradenie, ku ktorému chcete pridať informácie na vyhľadanie a kliknite na tlačidlo **Detaily...**. Ak to je potrebné, kliknite na tlačidlo **Pomoc** a zistíte, aké informácie je potrebné zadať pre každé pole.
7. V dialógovom okne **Priradenie - Detaily** zadajte **Informácie na vyhľadanie**, ktoré chcete používať na ďalšiu identifikáciu cieľovej identity užívateľa v tomto priradení a kliknite na tlačidlo **Pridať**.
8. Opakujte tento krok pre každú položku informácií na vyhľadanie, ktorú chcete pridať k priradeniu.
9. Kliknite na tlačidlo **OK**, aby sa uložili vaše zmeny a aby ste sa vrátili do dialógového okna **Priradenie - Detaily**.
10. Kliknite na tlačidlo **OK**, aby ste zatvorili okno.

Pridanie informácií na vyhľadanie k cieľovej identite užívateľa v priradení politiky

Ak chcete pridať informácie na vyhľadanie k cieľovej identite užívateľa v priradení politiky, musíte byť pripojený k doméne EIM, v ktorej chcete pracovať a musíte mať oprávnenia na jednej z týchto úrovní:

- Administrátor registrov
- Administrátor pre vybraté registre (definície registra, ktorá odkazuje na register užívateľov, obsahujúci cieľovú identitu užívateľa (ID))
- Administrátor EIM

Ak chcete pridať informácie na vyhľadanie k cieľovej identite užívateľa v priradení politiky, vykonajte tieto kroky:

1. Rozviňte **Sieť > Enterprise Identity Mapping > Správa domén**.
2. Pravým tlačidlom myši kliknite na doménu EIM, v ktorej chcete pracovať a vyberte položku **Politika mapovania...**.
   - Ak sa doména EIM, s ktorou chcete pracovať nenachádza v zozname **Správa domén**, pozrite si časť "Pridanie domény Enterprise Identity Mapping do zložky Správa domén" na strane 78.
   - Ak nie ste pripojený k doméne, v ktorej chcete pracovať, pozrite si časť Pripojenie k radiču domény EIM.
3. V dialógovom okne **Politika mapovania** môžete použiť strany na zobrazenie priradení politiky pre doménu.
4. Nájdite a vyberte priradenie politiky pre cieľový register obsahujúci cieľovú identitu užívateľa, ku ktorej chcete pridať informácie na vyhľadanie.
5. Kliknite na tlačidlo **Detaily...** na zobrazenie vhodného dialógového okna **Priradenie politiky - Detaily** pre vybratý typ priradenia politiky. Ak to je potrebné, kliknite na tlačidlo **Pomoc** a zistíte, aké informácie je potrebné zadať pre každé pole.
6. Zadajte **Informácie na vyhľadanie**, ktoré chcete používať na ďalšiu identifikáciu cieľovej identity užívateľa v tomto priradení politiky a kliknite na tlačidlo **Pridať**. Opakujte tento krok pre každú položku informácií na vyhľadanie, ktorú chcete pridať k priradeniu.
7. Kliknite na **OK**, aby sa uložili vykonané zmeny a aby ste sa vrátili do pôvodného okna **Priradenie politiky - Detaily**.
8. Kliknite na tlačidlo **OK**, aby ste zatvorili okno.

Odstránenie informácií na vyhľadanie pre cieľovú identitu užívateľa

Informácie na vyhľadanie sú voliteľné jedinečné identifikujúce údaje pre cieľovú identitu užívateľa, definovanú v priradení. Toto priradenie môže byť buď cieľovým priradením identifikátora alebo priradením politiky. Informácie na vyhľadanie sú potrebné, len keď operácia vyhľadávania mapovaní môže vrátiť viac ako jednu cieľovú identitu užívateľa. Táto situácia môže vytvoriť problémy pre aplikácie podporujúce EIM, vrátane aplikácií a produktov OS/400, ktoré nie sú navrhnuté na spracovanie týchto nejednoznačných výsledkov.

Tieto informácie na vyhľadanie musia byť poskytnuté operácii vyhľadávania mapovaní na zaistenie, že operácia môže vrátiť jedinečnú cieľovú identitu užívateľa. Ak však už skôr definované informácie na vyhľadanie nie sú potrebné, tieto informácie môžete odstrániť, takže už nebudú musieť byť poskytované pre operácie vyhľadávania.

Ako odstránite informácie na vyhľadanie z cieľovej identity užívateľa, záleží od toho, či je cieľová identita užívateľa definovaná v priradení identifikátora alebo cieľovom priradení. Informácie na vyhľadanie sú zviazané s cieľovou identitou užívateľa, nie s priradením identifikátora alebo priradeniami politiky, v ktorých sa táto identita užívateľa nájde. Keď vymažete posledné priradenie identifikátora alebo priradenie politiky, ktoré definuje túto cieľovú identitu užívateľa, z domény EIM sa vymaže identita užívateľa aj informácie na vyhľadanie.

Odstránenie informácií na vyhľadanie pre cieľovú identitu užívateľa v priradení identifikátora

Keď chcete odstrániť informácie na vyhľadanie pre cieľovú identitu užívateľa v priradení identifikátora, musíte byť pripojený k doméne EIM, v ktorej chcete pracovať a musíte mať "Riadenie prístupu EIM" na strane 33 na jednej z týchto úrovní:

- Administrátor registrov
- Administrátor pre vybraté registre (pre definíciu registra, ktorá odkazuje do registra užívateľov, ktorý obsahuje cieľovú identitu užívateľa)
- Administrátor EIM

Keď chcete odstrániť informácie na vyhľadanie pre cieľovú identitu užívateľa v priradení identifikátora, vykonajte tieto kroky:

1. Rozviňte **Sieť > Enterprise Identity Mapping > Správa domén**.
2. Vyberte doménu EIM, v ktorej chcete pracovať.
   - Ak doména EIM, s ktorou chcete pracovať nie je uvedená pod **Správa domén**, pozrite si časť “Pridanie domény Enterprise Identity Mapping do zložky Správa domén” na strane 78.
   - Ak nie ste práve pripojený k doméne EIM, v ktorej chcete pracovať, pozrite si tému Pripojenie k radiču domény EIM.
3. Rozviňte doménu EIM, ku ktorej ste pripojený.
4. Kliknite na **Identifikátory**, aby sa zobrazil zoznam identifikátorov EIM pre túto doménu.

   Poznámka: Zobrazenie zoznamu identifikátorov pri pokuse o rozvinutie zložky **Identifikátory** môže niekedy trvať dlho. Ak chcete zlepšiť výkon, keď máte v doméne veľký počet identifikátorov EIM, môžete upraviť pohľad na zložku **Identifikátory** obmedzením vyhľadávacieho kritéria používaného na zobrazovanie identifikátorov. Kliknite pravým tlačidlom na **Identifikátory**, vyberte **Prispôsobiť toto zobrazenie... > Zahrnúť** a zadajte kritérium zobrazenia, ktoré sa použije na generovanie zoznamu identifikátorov EIM, ktoré sa zahrnú do zoznamu.
5. Kliknite pravým tlačidlom myši na identifikátor EIM a vyberte **Vlastnosti...**.
6. Vyberte stranu **Priradenia**, vyberte cieľové priradenie pre identitu užívateľa, pre ktorú chcete odstrániť informácie na vyhľadanie a kliknite na **Detaily...**.
7. V dialógovom okne **Priradenie - Detaily** vyberte informácie na vyhľadanie, ktoré chcete odstrániť z cieľovej identity užívateľa a kliknite na **Odstrániť**.

   Poznámka: Keď kliknete na **Odstrániť**, nezobrazí sa žiadna výzva na potvrdenie.
8. Kliknite na **OK**, aby sa uložili vaše zmeny a aby ste sa vrátili do dialógového okna **Priradenie - Detaily**.
9. Kliknite na tlačidlo **OK**, aby ste zatvorili okno.

Odstránenie informácií na vyhľadanie pre cieľovú identitu užívateľa v priradení politiky

Keď chcete odstrániť informácie na vyhľadanie pre cieľovú identitu užívateľa v priradení politiky, musíte byť pripojený k doméne EIM, v ktorej chcete pracovať a musíte mať “Riadenie prístupu EIM” na strane 33 na niektorej z týchto úrovní:

- Administrátor registrov
- Administrátor pre vybraté registre (pre definíciu registra, ktorý odkazuje do registra užívateľov, ktorý obsahuje cieľovú identitu (ID) užívateľa)
- Administrátor EIM

Keď chcete odstrániť informácie na vyhľadanie pre cieľovú identitu užívateľa v priradení politiky, vykonajte tieto kroky:

1. Rozviňte **Sieť > Enterprise Identity Mapping > Správa domén**.
2. Pravým tlačidlom myši kliknite na doménu EIM, v ktorej chcete pracovať a vyberte **Politika mapovania...**
   - Ak doména EIM, s ktorou chcete pracovať nie je uvedená pod **Správa domén**, pozrite si časť “Pridanie domény Enterprise Identity Mapping do zložky Správa domén” na strane 78.
   - Ak nie ste práve pripojený k doméne EIM, v ktorej chcete pracovať, pozrite si tému Pripojenie k radiču domény EIM.
3. V dialógovom okne **Politika mapovania** môžete použiť strany na zobrazenie priradení politiky pre doménu.

4. Nájdite a vyberte priradenie politiky pre cieľový register, ktorý obsahuje cieľovú identitu užívateľa, pre ktorú chcete odstrániť informácie na vyhľadanie.
5. Kliknite na **Detaily...**, aby sa zobrazilo príslušné dialógové okno **Priradenie politiky - Detaily** pre vami vybratý typ priradenia politiky.
6. Vyberte informácie na vyhľadanie, ktoré chcete odstrániť z cieľovej identity užívateľa a kliknite na **Odstrániť**.

   Poznámka: Keď kliknete na **Odstrániť**, nezobrazí sa žiadna výzva na potvrdenie.
7. Kliknite na **OK**, aby sa uložili vykonané zmeny a aby ste sa vrátili do pôvodného okna **Priradenie politiky - Detaily**.
8. Kliknite na tlačidlo **OK**, aby ste zatvorili okno.

Zobrazenie všetkých priradení identifikátorov pre identifikátor EIM

Ak chcete zobraziť všetky priradenia pre identifikátor EIM, musíte byť pripojený k doméne EIM, v ktorej chcete pracovať a na vykonanie tejto úlohy, musíte mať niektorú úroveň "Riadenie prístupu EIM" na strane 33. Na zobrazenie všetkých priradení potrebujete ľubovoľnú úroveň riadenia prístupu, okrem riadenia prístupu Administrátor pre vybraté registre. Táto úroveň riadenia prístupu vám dovoľuje zobraziť a filtrovať len tie priradenia pre registre, na ktoré máte explicitné oprávnenie, ak tiež nemáte oprávnenie na riadenie prístupu operácií vyhľadávania mapovaní EIM.

Ak chcete zobraziť všetky priradenia medzi identifikátorom EIM a identitami užívateľa (ID), ktorých priradenia boli definované pre identifikátor EIM, vykonajte tieto kroky:

Ak chcete zobraziť priradenia identifikátora, vykonajte tieto kroky:

1. Rozviňte **Sieť > Enterprise Identity Mapping > Správa domén**.
2. Vyberte doménu EIM, v ktorej chcete pracovať.
   - V prípade, že doména EIM, v ktorej chcete pracovať sa nenachádza v **Správe domén**, pozrite si časť "Pridanie domény Enterprise Identity Mapping do zložky Správa domén" na strane 78.
   - Pokiaľ nie ste pripojený k doméne EIM, v ktorej chcete pracovať, pozrite si časť Pripojenie k radiču domény EIM.
3. Rozviňte doménu EIM, ku ktorej ste pripojený.
4. Kliknite na **Identifikátory**.

   Poznámka: Zobrazenie zoznamu identifikátorov pri pokuse o rozvinutie zložky **Identifikátory** môže niekedy trvať dlho. Ak chcete zvýšiť výkon pri veľkom počte identifikátorov EIM v doméne, môžete prispôsobiť zobrazenie zložky **Identifikátory** pomocou obmedzenia vyhľadávacieho kritéria, ktoré sa používa na zobrazenie identifikátorov. Pravým tlačidlom myši kliknite na **Identifikátory**, zvoľte **Prispôsobiť tento pohľad... > Zahrnúť**, a zadajte kritérium zobrazenia, ktoré sa má použiť na generovanie zoznamu identifikátorov EIM, ktoré budú zahrnuté do pohľadu.
5. Vyberte identifikátor EIM, pravým tlačidlom myši kliknite na identifikátor EIM a vyberte **Vlastnosti**.
6. Ak chcete zobraziť zoznam identít užívateľa, priradených vybratému identifikátoru EIM vyberte stranu **Priradenia**.
7. Kliknite na tlačidlo **OK**, aby ste zatvorili okno.

Zobrazenie všetkých priradení politiky pre doménu

Ak chcete zobraziť všetky priradenia politiky pre doménu, musíte byť pripojený k doméne EIM, v ktorej chcete pracovať a musíte mať na vykonanie tejto úlohy miektorú úroveň "Riadenie prístupu EIM" na strane 33. Na zobrazenie všetkých priradení politiky potrebujete ľubovoľnú úroveň riadenia prístupu, okrem riadenie prístupu Administrátor pre vybraté registre. Táto úroveň riadenia prístupu vám dovoľuje zobraziť a filtrovať len tie priradenia pre registre, na ktoré máte explicitné oprávnenie. Následne, s týmto riadením prístupu nemôžete zobraziť žiadne predvolené priradenia politiky domény, ak tiež nemáte oprávnenie na riadenie prístupu operácií vyhľadávania mapovaní EIM.

Ak chcete zobraziť všetky priradenia politiky pre doménu, vykonajte tieto kroky:

1. Rozviňte **Sieť > Enterprise Identity Mapping > Správa domén**.

2. Pravým tlačidlom myši kliknite na doménu EIM, v ktorej chcete pracovať a vyberte **Politika mapovania...**
   - V prípade, že doména EIM, v ktorej chcete pracovať sa nenachádza v **Správe domén**, pozrite si časť "Pridanie domény Enterprise Identity Mapping do zložky Správa domén" na strane 78.
   - Pokiaľ nie ste pripojený k doméne EIM, v ktorej chcete pracovať, pozrite si časť Pripojenie k radiču domény EIM.
3. Podľa nasledujúcich krokov vyberte stranu na zobrazenie priradení politiky definovaných pre doménu:
   - Ak chcete zobraziť predvolené priradenia politiky domény, definované pre doménu a zistiť, či je priradenie politiky povolené na úrovni registra, vyberte stranu **Doména**.
   - Ak chcete zobraziť predvolené priradenia politiky domény, definované pre doménu, vyberte stranu **Register**. Môžete tiež zobraziť, ktoré zdrojové a cieľové registre ovplyvňujú priradenia politiky.
   - Ak chcete zobraziť priradenia politiky filtra certifikátov, definované a povolené na úrovni registra, vyberte stranu **Filter certifikátov**.
4. Kliknite na tlačidlo **OK**, aby ste zatvorili okno.

Zobrazenie všetkých priradení politiky pre definíciu registra

Ak chcete zobraziť všetky priradenia politiky definované pre špecifický register, musíte byť pripojený k doméne EIM, v ktorej chcete pracovať a musíte mať na vykonanie tejto úlohy niektorú úroveň "Riadenie prístupu EIM" na strane 33. Na zobrazenie všetkých priradení politiky potrebujete ľubovoľnú úroveň riadenia prístupu, okrem riadenia prístupu Administrátor pre vybraté registre. Táto úroveň riadenia prístupu vám dovoľuje zobraziť a filtrovať len tie priradenia pre registre, na ktoré máte explicitné oprávnenie. Následne, s týmto riadením prístupu nemôžete zobraziť žiadne predvolené priradenia politiky domény, ak tiež nemáte oprávnenie na riadenie prístupu operácií vyhľadávania mapovaní EIM.

Ak chcete zobraziť všetky priradenia politiky pre definíciu registra, vykonajte tieto kroky:

1. Rozviňte **Sieť > Enterprise Identity Mapping > Správa domén**.
2. Ak chcete zobraziť zoznam definícií registra pre doménu, rozviňte doménu EIM, v ktorej chcete pracovať a vyberte **Registre užívateľov**.
   - V prípade, že doména EIM, v ktorej chcete pracovať sa nenachádza v **Správe domén**, pozrite si časť "Pridanie domény Enterprise Identity Mapping do zložky Správa domén" na strane 78.
   - Pokiaľ nie ste pripojený k doméne EIM, v ktorej chcete pracovať, pozrite si časť Pripojenie k radiču domény EIM.
3. Pravým tlačidlom myši kliknite na definíciu registra s ktorou chcete pracovať a vyberte **Politika mapovania...**
4. Podľa nasledujúcich krokov vyberte stranu na zobrazenie priradení politiky definovaných pre zadanú definíciu registra:
   - Ak chcete zobraziť predvolené priradenia politiky domény definované pre register, vyberte stranu **Doména**.
   - Ak chcete zobraziť predvolené priradenia politiky registra definované a povolené pre register, vyberte stranu **Register**.
   - Ak chcete zobraziť priradenia politiky certifikátu filtrov, definované a povolené pre register, vyberte stranu **Filter certifikátov**.
5. Kliknite na tlačidlo **OK**, aby ste zatvorili okno.

Vymazanie priradenia identifikátora

Ak chcete vymazať priradenie identifikátora, musíte byť pripojený k doméne EIM, v ktorej chcete pracovať a musíte mať oprávnenie vyžadované typom pripojenia, ktoré chcete vymazať.

Ak chcete vymazať zdrojové alebo administratívne priradenie, musíte mať riadenie prístupu k EIM na jednej z týchto úrovní:

- Administrátor identifikátorov
- Administrátor EIM

Ak chcete vymazať cieľové priradenie, musíte mať riadenie prístupu k EIM na jednej z týchto úrovní:

- Administrátor registrov
- Administrátor pre vybraté registre (definície registra, ktorá odkazuje na register užívateľov, obsahujúci cieľovú identitu užívateľa)
- Administrátor EIM

Ak chcete vymazať priradenie identifikátora, vykonajte tieto kroky.

1. Rozviňte **Sieť > Enterprise Identity Mapping > Správa domén**.
2. Vyberte doménu EIM, v ktorej chcete pracovať.
   - V prípade, že doména EIM, v ktorej chcete pracovať sa nenachádza v **Správe domén**, pozrite si časť "Pridanie domény Enterprise Identity Mapping do zložky Správa domén" na strane 78.
   - Pokiaľ nie ste pripojený k doméne EIM, v ktorej chcete pracovať, pozrite si časť Pripojenie k radiču domény EIM.
3. Rozviňte doménu EIM, ku ktorej ste teraz pripojený.
4. Kliknite na **Identifikátory**.

   Poznámka: Zobrazenie zoznamu identifikátorov pri pokuse o rozvinutie zložky **Identifikátory** môže niekedy trvať dlho. Ak chcete zvýšiť výkon pri veľkom počte identifikátorov EIM v doméne, pozrite si časť "Prispôsobenie zobrazenia identifikátorov Enterprise Identity Mapping" na strane 90.
5. Pravým tlačidlom myši kliknite na identifikátor EIM, pre ktorý chcete vymazať priradenie a vyberte **Vlastnosti...**
6. Ak chcete zobraziť aktuálne priradenia pre identifikátor EIM, vyberte stranu **Priradenia**.
7. Ak chcete vymazať priradenie, vyberte ho a kliknite na tlačidlo **Odstrániť**.

   Poznámka: Po kliknutí na tlačidlo **Odstrániť** sa nezobrazí žiadna výzva na potvrdenie odstránenia.
8. Ak chcete uložiť zmeny, kliknite na tlačidlo **OK**.

Poznámka: Keď odstránite cieľové priradenie, všetky operácie vyhľadávania mapovaní pre cieľový register, ktoré sa spoliehajú na použitie vymazaného priradenia môžu zlyhať, ak pre ovplyvnený cieľový register neexistujú ďalšie priradenia (buď priradenia politiky, alebo priradenia identifikátorov).

Jediný spôsob definovania identity užívateľa v EIM je zadanie identity užívateľa ako súčasti priradenia, buď priradenia identifikátora, alebo priradenia politiky. Následne, keď vymažete posledné cieľové priradenie pre identitu užívateľa (odstránením samotného cieľového priradenia alebo odstránením priradenia politiky), daná identita užívateľa už nie je definovaná v EIM. Následne, názov identity užívateľa a všetky informácie na vyhľadanie pre danú identitu užívateľa sa stratia.

Vymazanie priradenia politiky

Ak chcete vymazať priradenie politiky, musíte byť pripojený k doméne EIM, v ktorej chcete pracovať a musíte mať "Riadenie prístupu EIM" na strane 33 na jednej z týchto úrovni:

- Administrátor registrov
- Administrátor EIM

Ak chcete vymazať priradenie politiky, vykonajte tieto kroky:

1. Rozviňte **Sieť > Enterprise Identity Mapping > Správa domén**.
2. Pravým tlačidlom myši kliknite na doménu EIM, v ktorej chcete pracovať a vyberte **Politika mapovania...**
   - V prípade, že doména EIM, v ktorej chcete pracovať sa nenachádza v **Správe domén**, pozrite si časť "Pridanie domény Enterprise Identity Mapping do zložky Správa domén" na strane 78.
   - Pokiaľ nie ste pripojený k doméne EIM, v ktorej chcete pracovať, pozrite si časť Pripojenie k radiču domény EIM.
3. Vyberte vhodnú stranu pre typ priradenia politiky, ktorú chcete vymazať.
4. Na danej strane vyberte vhodné priradenie politiky a kliknite na tlačidlo **Odstrániť**.

Poznámka: Po kliknutí na tlačidlo **Odstrániť** sa nezobrazí žiadna výzva na potvrdenie odstránenia.

5. Kliknite na tlačidlo **OK**, aby sa zatvorilo dialógové okno **Politika mapovania** a uložili vaše zmeny.

Poznámka: Keď odstránite cieľové priradenie politiky, všetky operácie vyhľadávania mapovaní pre cieľový register, ktoré využívajú vymazané priradenie politiky môžu zlyhať, ak ostatné priradenia (priradenia politiky alebo priradenia identifikátorov) neexistujú pre ovplyvnený cieľový register.

Jediný spôsob definovania identity užívateľa v EIM je zadanie identity užívateľa ako súčasti priradenia, buď priradenia identifikátora, alebo priradenia politiky. Následne, keď vymažete posledné cieľové priradenie pre identitu užívateľa (odstránením samotného cieľového priradenia alebo odstránením priradenia politiky), daná identita užívateľa už nie je definovaná v EIM. Následne, názov identity užívateľa a všetky informácie na vyhľadanie pre danú identitu užívateľa sa stratia.

Manažovanie riadenia prístupu užívateľa EIM

Užívateľ EIM je užívateľ vlastniaci "Riadenie prístupu EIM" na strane 33 na základe jeho členstva v preddefinovanej skupine užívateľov LDAP (Lightweight Directory Access Protocol). Špecifikovanie riadenia prístupu k EIM pre daného užívateľa pridá tohto užívateľa do špecifickej skupiny užívateľov LDAP. Každá skupina LDAP má oprávnenie na vykonávanie rôznych administratívnych úloh EIM v doméne. Jednotlivé administratívne úlohy a ich typy, vrátane operácií vyhľadávania, ktoré môže užívateľ EIM vykonať, sú určené skupinou riadenia prístupu, do ktorej patrí užívateľ EIM.

Pridávať ďalších užívateľov do skupiny riadenia prístupu k EIM alebo meniť nastavenia riadenia prístupu pre iných užívateľov môžu len užívatelia s riadením prístupu Administrátor LDAP alebo EIM. Predtým, než sa užívateľ môže stať členom skupiny riadenia prístupu k EIM, musí mať tento užívateľ položku v adresárovom serveri, ktorý funguje ako radič domény EIM. Taktiež členmi skupiny riadenia prístupu k EIM sa môžu stať len špecifické typy užívateľov: principály Kerberos, rozlišovacie názvy a užívateľské profily OS/400.

Poznámka: Ak chcete mať typ užívateľa principál Kerberos dostupný v EIM, musíte nakonfigurovať v systéme službu sieťovej autentifikácie. Ak chcete mať v EIM dostupný typ užívateľský profil OS/400, musíte nakonfigurovať príponu systémového objektu v adresárovom serveri. Toto umožní adresárovému serveru referencovať systémové objekty OS/400, akými sú napríklad užívateľské profily OS/400.

Ak chcete manažovať riadenie prístupu pre existujúceho užívateľa adresárového servera alebo chcete pridať existujúceho užívateľa adresára do skupiny riadenia prístupu k EIM, vykonajte tieto kroky:

1. Rozviňte **Sieť > Enterprise Identity Mapping > Správa domén**.
2. Vyberte doménu EIM, v ktorej chcete pracovať.
   - Ak sa doména EIM, s ktorou chcete pracovať nenachádza v zozname pod zložkou **Správa domén**, pozrite si časť "Pridanie domény Enterprise Identity Mapping do zložky Správa domén" na strane 78.
   - Ak nie ste pripojený k doméne EIM, v ktorej chcete pracovať, pozrite si tému Pripojiť k radiču domény EIM.

   Poznámka: K doméne sa musíte pripojiť pomocou užívateľského oprávnenia, ktoré má oprávnenie administrátora EIM.
3. Pravým tlačidlom myši kliknite na doménu EIM, do ktorej ste pripojený a vyberte **Riadenie prístupu...**
4. V dialógovom okne **Úprava riadenia prístupu k EIM** vyberte **Typ užívateľa**, aby sa zobrazili polia potrebné pre poskytnutie informácií identifikujúcich užívateľa.
5. Zadajte vyžadované informácie o užívateľovi pre identifikáciu užívateľa, ktorému chcete manažovať riadenie prístupu k EIM a kliknite na tlačidlo **OK**, aby sa zobrazil panel **Úprava riadenia prístupu k EIM**. Ak potrebujete zistiť, aké informácie treba zadať do jednotlivých polí, kliknite na tlačidlo **Pomoc**.
6. Vyberte jednu alebo viac skupín **riadenia prístupu** pre užívateľa a kliknite na tlačidlo **OK**, aby ste pridali tohto užívateľa do vybratej skupiny. Kliknite na tlačidlo **Pomoc**, kde nájdete detailnejšie informácie o oprávneniach každej skupiny a nájdete informácie o akýchkoľvek špeciálnych požiadavkách.
7. Po poskytnutí vyžadovaných informácií kliknite na tlačidlo **OK**, aby sa uložili vaše zmeny.

Manažovanie vlastností konfigurácie EIM

Manažovať môžete niekoľko rôznych vlastností konfigurácie EIM vášho servera. Zvyčajne to nepotrebujete často. Avšak, občas sa vyskytne situácia, kedy potrebujete urobiť zmeny do vlastností konfigurácie. Napríklad, ak bude váš systém vypnutý a potrebuje znovu vytvoriť vlastnosti vašej konfigurácie EIM, môžete znovu spustiť Sprievodcu konfiguráciou EIM alebo zmeniť vlastnosti priamo tu. Iný príklad je, že ak ste nevybrali vytvorenie definícií registra pre lokálne registre v Sprievodcovi konfiguráciou EIM, definičné informácie registra môžete zaktualizovať tu.

Vlastnosti, ktoré môžete meniť sú:

- Doménu EIM, ktorej účastníkom je server.
- Informácie o pripojení pre radič domény EIM.
- Identita užívateľa, ktorú systém používa na vykonávanie operácií EIM v mene funkcií operačného systému.
- Názvy definícií registrov, ktoré sa týkajú aktuálnych registrov užívateľov, ktoré môže systém používať, keď vykonáva operácie EIM v mene funkcií operačného systému. Tieto názvy definícií registrov sa týkajú lokálnych registrov užívateľov, ktoré môžete vytvoriť počas behu sprievodcu konfiguráciou EIM.

  Poznámka: Ak ste vybrali nevytvorenie názvov definícií lokálneho registra v sprievodcovi konfiguráciou EIM, pretože registre už boli definované pre doménu EIM alebo preto, lebo ich chcete zadefinovať pre doménu neskôr, musíte zaktualizovať vlastnosti konfigurácie systému týmito názvami definícií registrov na tomto mieste. Systém potrebuje tieto informácie o definíci registra na vykonávanie operácií EIM v mene funkcií operačného systému.

Ak chcete zmeniť konfiguračné vlastnosti EIM, musíte mať tieto špeciálne oprávnenia:

- Administrátor bezpečnosti (*SECADM)
- Všetky objekty (*ALLOBJ)

Ak chcete zmeniť konfiguračné vlastnosti pre server iSeries, vykonajte tieto kroky:

1. Rozviňte **Sieť > Enterprise Identity Mapping**.
2. Pravým tlačidlom myši kliknite na **Konfigurácia** a vyberte **Vlastnosti**.
3. Vykonajte zmeny v konfiguračných informáciách EIM.
4. Ak chcete zistiť, aké informácie treba zadať do jednotlivých polí dialógového okna, kliknite na tlačidlo **Pomoc**.
5. Ak sa chcete uistiť, že všetky zadané informácie umožnia systému úspešne vytvoriť pripojenie k radiču domény EIM, kliknite na tlačidlo **Skontrolovať konfiguráciu**.
6. Ak chcete uložiť zmeny, kliknite na tlačidlo **OK**.

Poznámka: Ak ste nepoužili sprievodcu konfiguráciou EIM na vytvorenie alebo pripojenie domény, nepokúšajte sa vytvoriť konfiguráciu EIM ručným zadaním vlastností konfigurácie. Použitím sprievodcu na vytvorenie základnej konfigurácie EIM sa môžete vyhnúť potencionálnym konfiguračným problémom, pretože sprievodca spraví viac, ako len nakonfigurovanie vlastností.

Rozhrania API Enterprise Identity Mapping

| EIM (Enterprise Identity Mapping) poskytuje techniky pre manažment identít užívateľov medzi platformami. EIM má
| niekoľko aplikačných programových rozhraní (API), ktoré môžu aplikácie používať na vykonávanie operácií EIM v
| mene aplikácie alebo užívateľa aplikácie. Tieto rozhrania API môžete použiť na vykonávanie operácií vyhľadávania
| mapovaní identity, rôznych funkcií manažmentu a konfigurácie EIM, ako aj na zmenu informácií a vytváranie dotazov.
| Všetky tieto rozhrania API sú podporované v platformách IBM.

Rozhrania API EIM sa delia do týchto kategórií:

- Operácie s deskriptormi a pripojeniami EIM
- Administrácia domény EIM
- Operácie s registrom

- Operácie s identifikátormi EIM
- Manažovanie priradení EIM
- Operácie vyhľadávania mapovaní EIM
- Manažovanie autorizácie EIM

Aplikácie, ktoré používajú tieto rozhrania API na manažovanie alebo používajú informácie EIM v doméne EIM sa zvyčajne držia tohto programovacieho modelu:

1. Získanie deskriptora EIM
2. Pripojenie k doméne EIM
3. Normálne aplikačné spracovanie
4. Použitie API pre správu EIM alebo operácie vyhľadávania mapovania identity EIM
5. Normálne aplikačné spracovanie
6. Zrušenie deskriptora EIM pred ukončením

Pozrite si tému Rozhrania API EIM (Enterprise Identity Mapping), kde nájdete detailnejšie informácie a úplný zoznam rozhraní API EIM dostupných pre server iSeries.

Odstraňovanie problémov s Enterprise Identity Mapping

EIM (Enterprise Identity Mapping) je zostavené z viacerých technológií a z veľa aplikácií a funkcií. Problém sa preto môže vyskytnúť vo viacerých oblastiach. Nasledujúce informácie opisujú niekoľko bežných problémov a chýb, ku ktorým môže dôjsť pri používaní EIM a niekoľko návrhov na opravenie chýb a problémov.

- "Odstraňovanie problémov s pripojením radiča domény"
- "Odstraňovanie všeobecných problémov s konfiguráciou a doménou EIM" na strane 108
- "Odstraňovanie problémov s Enterprise Identity Mapping: Problémy s mapovaním" na strane 109

Ak používate EIM na aktivovanie prostredia s jednoduchým prihlásením a chcete sa dozvedieť viac o odstraňovaní problémov, pozrite si časť Odstraňovanie problémov s nastavením jednoduchého prihlásenia v téme Jednoduché prihlásenie.

Odstraňovanie problémov s pripojením radiča domény

Pri pripájaní k radiču domény môže k problémom prispieť množstvo faktorov. Nasledujúcu tabuľku použite na určenie, ako riešiť možné problémy s pripojením radiča domény.

Tabuľka 27. Bežné problémy s pripojením radiča domény EIM a ich riešenia

Možný problém	Možné riešenie
Nemôžete sa pripojiť k radiču domény, keď používate na riadenie EIM iSeries Navigator.	Informácie o pripojení radiča domény pre doménu, ktorú chcete riadiť sú možno zadané nesprávne. Vykonajte tieto kroky na overenie informácií o pripojení domény: • Rozviňte **Sieť > Enterprise Identity Mapping > Správa domén**. Kliknite pravým tlačidlom na doménu, ktorú chcete riadiť a vyberte **Vlastnosti**. • Skontrolujte správnosť názvu pre **Radič domény** a pre **Rodičovské DN**, ak je zadané. • Overte, či sú informácie pre **Pripojenie** pre radič domény správne. Presvedčte sa, či je číslo pre **Port** správne. Ak je vybraté **Use secure connection (SSL or TLS)**, adresárový server musí byť nakonfigurovaný na použitie SSL. Kliknite na **Skontrolovať pripojenie**, aby ste overili, že môžete používať zadané informácie na úspešné vytvorenie pripojenia k radiču domény. • Overte, či sú informácie o užívateľovi v paneli **Pripojenie k radiču domény** správne.
Operačný systém alebo aplikácie sa nemôžu pripojiť k radiču domény a pristupovať k údajom EIM. Napríklad operácie vyhľadávania mapovaní EIM vykonávané pre systém zlyhávajú. Môže k tomu dôjsť, pretože konfigurácia EIM v systéme alebo systémoch je nesprávna.	Overte svoju konfiguráciu EIM. Rozviňte **Sieť > Enterprise Identity Mapping > Konfigurácia** v systéme, s ktorým sa pokúšate autentifikovať. Kliknite pravým tlačidlom myši na zložku **Konfigurácia**, vyberte **Vlastnosti** a overte nasledujúce: • Stránka **Doména**: – Názov radiča domény a čísla portov sú správne. – Kliknite na **Skontrolovať konfiguráciu**, aby ste overili, či je radič domény aktívny. – Názov lokálneho registra je špecifikovaný správne – Názov registra Kerberos je špecifikovaný správne. – Overte, či je vybraté **Povoliť operácie EIM pre tento systém**. • Strana **Užívateľ systému**: – Špecifikovaný užívateľ má dostatočné riadenie prístupu k EIM na vykonanie vyhľadávania mapovaní a heslo pre užívateľa je platné. Pozrite si online pomoc, aby ste sa dozvedeli viac o rôznych typoch oprávnení užívateľa. **Poznámka:** Ak ste zmenili heslo pre špecifikovaného systémového užívateľa v adresárovom serveri, musíte zmeniť heslo aj tu. Ak sa tieto heslá nezhodujú, systémový užívateľ nemôže vykonávať funkcie EIM pre operačný systém a operácie vyhľadávania mapovaní zlyhajú. – Kliknite na **Skontrolovať pripojenie**, aby ste potvrdili, že informácie o zadanom užívateľovi sú správne.
Konfiguračné informácie sa zdajú správne, ale nemôžete sa pripojiť k radiču domény.	• Presvedčte sa, či je adresárový server, ktorý vystupuje ako radič domény EIM, aktívny. Ak je radič domény server iSeries, môžete použiť iSeries Navigator a vykonať tieto kroky: 1. Rozviňte **Sieť > Servery > TCP/IP**. 2. Skontrolujte, že adresárový server má stav **Spustený**. Ak je tento server zastavený, pravým tlačidlom myši kliknite na **Adresárový server** a vyberte **Spustiť...**

Po overení informácií o pripojení a aktivity adresárového servera sa pokúste pripojiť k radiču domény vykonaním týchto krokov:

1. Rozviňte **Sieť > Enterprise Identity Mapping > Správa domén**.
2. Pravým tlačidlom myši kliknite na doménu EIM, ku ktorej sa chcete pripojiť a vyberte **Pripojiť...**.
3. Zadajte typ užívateľa a vyžadované informácie o užívateľovi, ktoré sa majú použiť pre pripojenie k radiču domény EIM.
4. Kliknite na tlačidlo **OK**.

Odstraňovanie všeobecných problémov s konfiguráciou a doménou EIM

Existuje veľa všeobecných problémov, ku ktorým môže dôjsť pri konfigurácii EIM pre váš systém, ako aj problémov, ktoré sa môžu vyskytnúť počas prístupu k doméne EIM. Nasledujúcu tabuľku použite, aby ste sa dozvedeli viac o niektorých bežných problémoch a možných riešeniach, ktoré môžete použiť na odstránenie týchto problémov.

Tabuľka 28. Bežné problémy s konfiguráciou EIM a doménou a ich riešenia

Možný problém	Možné riešenie
Sprievodca konfiguráciou EIM sa javí ako zaseknutý počas spracovania kroku **Dokončiť**.	Sprievodca môže čakať na spustenie radiča domény. Overte, či sa počas štartovania adresárového servera nevyskytli žiadne chyby. Pre servery iSeries skontrolujte protokol úlohy QDIRSRV v subsystéme QSYSWRK. Ak chcete skontrolovať protokol úloh, vykonajte tieto kroky: 1. V iSeries Navigator rozviňte **Riadenie prevádzky > Podsystémy > Qsyswrk**. 2. Pravým tlačidlom myši kliknite na **Qdirsrv** a vyberte **Protokol úlohy**.
Keď používate Sprievodcu konfiguráciou EIM na vytvorenie domény vo vzdialenom systéme, dostali ste túto chybovú správu: ″The parent distinguished name (DN) you entered is not valid. The DN must exist on the remote directory server. Specify or select a new or existing parent DN.’	Rodičovské DN uvedené pre vzdialenú doménu, neexistuje. Keď sa chcete dozvedieť viac o používaní sprievodcu konfiguráciou EIM, pozrite si “Vytvorenie a pripojenie k novej vzdialenej doméne” na strane 66. Môžete si tiež pozrieť online pomoc, kde nájdete detailné informácie o špecifikovaní rodičovského DN, keď vytvárate doménu.
Dostanete správu oznamujúcu, že doména EIM neexistuje.	Ak ste nevytvorili doménu EIM, použite sprievodcu konfiguráciou EIM. Tento sprievodca pre vás vytvorí doménu EIM alebo vám umožní nakonfigurovať existujúcu doménu EIM. Ak ste vytvorili doménu EIM, presvedčte sa, že uvedený užívateľ je členom skupiny “Riadenie prístupu EIM” na strane 33 s dostatočným oprávnením na prístup k nej.
Dostanete správu oznamujúcu, že objekt EIM (identifikátor, register, priradenie, priradenie politiky alebo filter certifikátov), sa nenašiel alebo že nemáte oprávnenie na údaje EIM.	Overte, či objekt EIM existuje a či je špecifikovaný užívateľ členom skupiny “Riadenie prístupu EIM” na strane 33 s dostatočným oprávnením na tento objekt.

Tabuľka 28. Bežné problémy s konfiguráciou EIM a doménou a ich riešenia (pokračovanie)

Možný problém	Možné riešenie
Zobrazenie zoznamu identifikátorov pri pokuse o rozvinutie zložky **Identifikátory** môže niekedy trvať dlho.	Toto sa môže stať, ak existuje veľké množstvo identifikátorov EIM v doméne. Keď to chcete vyriešiť, môžete upraviť zobrazenie zložky **Identifikátory** obmedzením vyhľadávacieho kritéria použitého na zobrazenie identifikátorov. Ak chcete prispôsobiť zobrazenie pre identifikátory EIM, vykonajte tieto kroky: 1. V iSeries Navigator rozviňte **Sieť > Enterprise Identity Mapping > Správa domén**. 2. Rozviňte doménu, ktorej identifikátory chcete zobraziť. 3. Kliknite pravým tlačidlom myši na **Identifikátory** a vyberte **Prispôsobiť toto zobrazenie > Zahrnúť...**. 4. Zadajte zobrazovacie kritérium, ktoré sa použije pre generovanie zoznamu identifikátorov EIM, ktoré sa zahrnú do zobrazenia. **Poznámka:** Môžete použiť hviezdičku (*) ako zástupný znak. 5. Kliknite na tlačidlo **OK**. Najbližšie, keď kliknete na **Identifikátory**, zobrazia sa len tie identifikátory EIM, ktoré vyhovujú vami zadanému kritériu.
Počas manažovania EIM cez iSeries Navigator sa zobrazí chybová správa, oznamujúca, že identifikátor EIM už nie je platný.	Pripojenie k radiču domény bolo prerušené. Ak chcete obnoviť pripojenie k radiču domény, vykonajte tieto kroky: 1. V iSeries Navigator rozviňte **Sieť > Enterprise Identity Mapping > Správa domén**. 2. Pravým tlačidlom myši kliknite na doménu, v ktorej chcete pracovať a vyberte **Znovu pripojiť...**. 3. Zadajte informácie pre pripojenie. 4. Kliknite na tlačidlo **OK**.
Keď používate protokol Kerberos pre autentifikáciu s EIM, do protokolu úlohy sa zapíše diagnostická správa CPD3E3F.	Táto správa sa vygeneruje vždy, keď zlyhá autentifikácia alebo operácia mapovania identity. Táto diagnostická správa obsahuje hlavné aj vedľajšie stavové kódy označujúce miesto vzniku problému. Väčšina bežných problémov je zdokumentovaná v správe spolu s informáciami o obnove. Odstraňovanie problému začnite prečítaním pomocných informácií z diagnostickej správy. Mohlo by vám pomôcť aj prečítanie témy Odstraňovanie problémov s jednoduchým prihlásením.

Odstraňovanie problémov s Enterprise Identity Mapping: Problémy s mapovaním

Existuje množstvo bežných problémov, ktoré môžu spôsobiť úplné zlyhanie alebo neočakávané fungovanie mapovaní EIM (Enterprise Identity Mapping). Použite nasledujúcu tabuľku na nájdenie informácií o probléme, ktorý môže spôsobovať zlyhanie mapovania EIM a na nájdenie jeho možných riešení. Ak mapovania EIM zlyhávajú, budete asi musieť prejsť každým riešením a vyriešiť problém alebo problémy spôsobujúce zlyhania mapovaní.

Tabuľka 29. Bežné problémy s mapovaním EIM a ich riešenia

Možný problém	Možné riešenia
Informácie o pripojení pre radič domény nemusia byť správne alebo radič domény nemusí byť aktívny.	Pozrite si časť Problémy s pripojením radiča domény, kde sa dozviete, ako skontrolovať informácie o pripojení pre radič domény a ako skontrolovať, či je radič domény aktívny.

Tabuľka 29. Bežné problémy s mapovaním EIM a ich riešenia (pokračovanie)

Možný problém	Možné riešenia
Operácie vyhľadávania mapovaní EIM, vykonávané systémom zlyhávajú. Môže k tomu dôjsť, pretože konfigurácia EIM v systéme alebo systémoch je nesprávna.	Skontrolujte vašu konfiguráciu EIM. Rozviňte **Sieť-->Enterprise Identity Mapping-->Konfigurácia** v systéme, v ktorom sa chcete autentifikovať. Pravým tlačidlom myši kliknite na zložku **Konfigurácia**, vyberte **Vlastnosti** a skontrolujte nasledujúce: • Strana **Doména**: – Názov radiča domény a čísla portov sú správne. – Kliknite na tlačidlo **Skontrolovať konfiguráciu** a skontrolujte, či je radič domény aktívny. – Názov lokálneho registra je zadaný správne. – Názov registra Kerberos je zadaný správne. – Skontrolujte, či je vybraté **Povoliť operácie EIM pre tento systém**. • Strana **Užívateľ systému**: – Zadaný užívateľ má dostatočné riadenie prístupu k EIM na vykonanie vyhľadávania mapovaní a heslo užívateľa je platné. Pozrite si online pomoc, kde sa dozviete o rozdielnych typoch oprávnení užívateľov. **Poznámka:** Ak ste zmenili heslo užívateľa systému v adresárovom serveri, musíte to zmeniť aj tu. Ak sa tieto heslá nezhodujú, užívateľ systému nemôže vykonávať funkcie EIM operačného systému a operácie vyhľadávania mapovaní zlyhajú. – Kliknite na tlačidlo **Skontrolovať pripojenie** a skontrolujte správnosť zadaných informácií o užívateľovi.

Tabuľka 29. Bežné problémy s mapovaním EIM a ich riešenia (pokračovanie)

Možný problém	Možné riešenia
Operácia vyhľadávania mapovaní môže vracať viaceré cieľové identity užívateľov. Toto môže nastať pri jednej alebo viacerých z nasledujúcich situácií: • Identifikátor EIM má viaceré samostatné cieľové priradenia k jednému cieľovému registru. • Viac ako jeden identifikátor EIM má v zdrojovom priradení zadanú tú istú identitu užívateľa a každý z nich má cieľové priradenie k tomu istému cieľovému registru, aj keď identita užívateľa zadaná pre každé cieľové priradenie môže byť rôzna. • Viac ako jedno predvolené priradenie politiky domény určuje ten istý cieľový register. • Viac ako jedno predvolené priradenie politiky registra určuje ten istý zdrojový register a ten istý cieľový register. • Viac ako jedno priradenie politiky filtra certifikátov určuje ten istý zdrojový register X.509, filter certifikátov a cieľový register.	Použite funkciu "Testovanie mapovaní EIM" na strane 79 na kontrolu správnosti mapovania konkrétnej zdrojovej identity užívateľa k vhodnej cieľovej identite užívateľa. Riešenie problému závisí od výsledkov testu podľa týchto pokynov: • Test vracia viaceré nežiaduce cieľové identity. Znamená to, že konfigurácia priradenia pre doménu nie je správna, dôvod je jeden z nasledujúcich: – Cieľové alebo zdrojové priradenie pre identifikátor EIM nie je správne nakonfigurované. Napríklad neexistuje zdrojové priradenie pre principál Kerberos (alebo užívateľa systému Windows) alebo je nesprávne. Alebo cieľové priradenie určuje nesprávnu identitu užívateľa. Zobrazte všetky priradenia identifikátorov pre identifikátor EIM a skontrolujte priradenia pre konkrétny identifikátor. – Priradenie politiky nie je správne nakonfigurované. Zobrazte všetky priradenia politiky pre doménu a skontrolujte informácie o zdroji a cieli pre všetky priradenia politiky definovaných v doméne. • Test vracia viaceré cieľové identity a tieto výsledky sú vhodné vzhľadom na spôsob konfigurácie priradení. V tejto situácii potrebujete zadať informácie na vyhľadanie pre každú cieľovú identitu užívateľa na zabezpečenie vrátenia jednej cieľovej identity užívateľa operáciou vyhľadávania, a nie všetkých možných cieľových identít užívateľov. Pozrite si časť Pridanie informácií na vyhľadanie k cieľovej identite užívateľa. **Poznámka:** Tento prístup funguje, len keď má aplikácia povolené používať informácie na vyhľadanie. Avšak, základné aplikácie systému OS/400, ako napríklad iSeries Access for Windows, nemôžu používať informácie na vyhľadanie na rozlíšenie medzi viacerými cieľovými identitami užívateľov, ktoré vráti operácia vyhľadávania. Mali by ste preto zvážiť predefinovanie priradení domény, aby ste zabezpečili vrátenie jednej cieľovej identity užívateľa operáciou vyhľadávania mapovaní, úspešné vykonanie operácií vyhľadávania mapovaní základnými aplikáciami systému OS/400 a úspešné mapovania identít.

Tabuľka 29. Bežné problémy s mapovaním EIM a ich riešenia (pokračovanie)

Možný problém	Možné riešenia
Operácie prehľadania EIM nevracajú žiadne výsledky a priradenia pre doménu sú nakonfigurované.	Použite funkciu "Testovanie mapovaní EIM" na strane 79 na kontrolu správnosti mapovania konkrétnej zdrojovej identity užívateľa k vhodnej cieľovej identite užívateľa. Skontrolujte, že ste pre test poskytli správne informácie. Ak sú správne a test nevracia žiadne výsledky, problém môže byť spôsobený jedným z nasledujúcich dôvodov: • Konfigurácia priradenia je nesprávna. Skontrolujte vašu konfiguráciu priradenia pomocou informácií o riešení problému poskytnutých v predchádzajúcej položke. • Podpora priradenia politiky na úrovni domény nie je povolená. Budete musieť povoliť priradenia politiky pre doménu. • Podpora vyhľadávania mapovaní alebo priradenia politiky na úrovni registra nie je povolená. Budete musieť povoliť podporu vyhľadávania mapovaní a používania priradení politiky pre cieľový register. • Definícia registra a identity užívateľov sa nezhodujú z dôvodu rozlišovania veľkosti písmen. Môžete vymazať a znovu vytvoriť register alebo priradenie so správnou veľkosťou písma.

Súvisiace informácie pre Enterprise Identity Mapping

Možno sa budete chcieť dozvedieť viac o technológiách súvisiacich s EIM (Enterprise Identity Mapping). Nasledujúce témy Informačného centra vám pomôžu porozumieť týmto technológiám:

- **Jednoduché prihlásenie** Táto téma poskytuje informácie o konfigurovaní a manažovaní prostredia s jednoduchým prihlásením pre váš podnik a zahrňuje niekoľko scenárov, pomocou ktorých môžete zistiť, ako môže byť prostredie s jednoduchým prihlásením pre váš podnik prospešné.
- **Služba sieťovej autentifikácie** Táto téma poskytuje informácie o konfigurácii a iné informácie o používaní služby sieťovej autentifikácie, implementácie protokolu Kerberos v iSeries. Počas konfigurovania služby sieťovej autentifikácie v spojení s EIM môžete pre váš podnik vytvoriť prostredie s jednoduchým prihlásením.
- **IBM Directory Server pre iSeries (LDAP)** Táto téma poskytuje konfiguračné a konceptuálne informácie o IBM Directory Server pre iSeries (LDAP). EIM môže použiť adresárový server aby vystupoval ako hostiteľ radiča domény EIM a ukladal údaje domény EIM.

Podmienky sťahovania a tlače informácií

Povolenie na používanie vybratých informácií, ktoré si chcete stiahnuť, je podmienené vaším súhlasom s nasledujúcimi podmienkami.

Osobné použitie: Tieto informácie môžete kopírovať len na svoje osobné nekomerčné použitie pod podmienkou, že dodržíte všetky oznámenia o vlastníckych právach. V žiadnom prípade nemôžete tieto informácie ani žiadnu ich časť distribuovať, prezentovať alebo z nich vytvárať odvodené práce, bez výslovného súhlasu spoločnosti IBM.

Komerčné použitie: V rámci vášho podniku môžete kopírovať, distribuovať a prezentovať tieto informácie len za predpokladu, že dodržíte všetky oznámenia o vlastníckych právach. V žiadnom prípade nemôžete tieto informácie ani žiadnu ich časť distribuovať, prezentovať alebo z nich vytvárať odvodené práce mimo vášho podniku bez výslovného súhlasu spoločnosti IBM.

Okrem povolení výslovne vyjadrených v tomto dokumente, nie sú pre uvedené informácie, údaje, softvér alebo iné duševné vlastníctvo v nich obsiahnuté, udelené žiadne iné výslovné alebo mlčky predpokladané povolenia, oprávnenia alebo práva.

| IBM si vyhradzuje právo vypovedať oprávnenia uvádzané v tomto dokumente kedykoľvek, ak usúdi, že používanie
| týchto informácií poškodzuje jej záujmy alebo ak spoločnosť IBM zistí, že vyššie uvedené inštrukcie nie sú náležite
| dodržiavané.

| Stiahnuť, exportovať a re-exportovať môžete tieto informácie len v tom prípade, ak vyhovujú všetkým platným
| zákonom a predpisom, vrátane zákonov a predpisov USA týkajúcich sa exportu. IBM NEPOSKYTUJE ŽIADNU
| ZÁRUKU NA OBSAH TÝCHTO INFORMÁCIÍ. TIETO INFORMÁCIE SA POSKYTUJÚ ″TAK AKO SÚ″ BEZ
| AKÝCHKOĽVEK VÝSLOVNÝCH ALEBO MLČKY PREDPOKLADANÝCH ZÁRUK, VRÁTANE, ALE BEZ
| OBMEDZENIA NA ZÁRUKY NEPORUŠENIA PRÁV, PREDAJNOSTI ALEBO VHODNOSTI NA KONKRÉTNY
| ÚČEL

Všetky materiály sú chránené autorským právom IBM Corporation.

| Stiahnutím alebo vytlačením informácií z týchto stránok vyjadrujete svoj súhlas s týmito podmienkami.

Príloha. Právne vyhlásenia

Tieto informácie boli vyvinuté pre produkty a služby ponúkané v USA.

IBM nemusí ponúkať produkty, služby alebo vlastnosti opisované v tomto dokumente v iných krajinách. Informácie o aktuálne dostupných produktoch a službách vo vašej krajine získate od predstaviteľa lokálnej pobočky IBM. Žiadny odkaz na produkt, program alebo službu IBM nie je myslený tak a ani neimplikuje, že sa môže používať len tento produkt, program alebo služba od IBM. Namiesto nich sa môže použiť ľubovoľný funkčne ekvivalentný produkt, program alebo služba, ktorá neporušuje intelektuálne vlastnícke právo IBM. Vyhodnotenie a kontrola činnosti produktu, programu alebo služby inej ako od IBM je však na zodpovednosti užívateľa.

IBM môže vlastniť patenty alebo nevybavené prihlášky patentov, týkajúce sa predmetu opísaného v tomto dokumente. Získanie tohto dokumentu vám nedáva žiadnu licenciu na tieto patenty. Žiadosti o licencie môžete zasielať písomne na:

| IBM Director of Licensing
| IBM Corporation
| North Castle Drive
| Armonk, NY 10504-1785
| U.S.A.

Žiadosti o licencie týkajúce sa dvojbajtových (DBCS) informácií smerujte na oddelenie intelektuálneho vlastníctva IBM vo vašej krajine alebo ich pošlite písomne na:

| IBM World Trade Asia Corporation
| Licensing
| 2-31 Roppongi 3-chome, Minato-ku
| Tokyo 106-0032, Japan

Nasledujúci odsek sa netýka Veľkej Británie ani žiadnej inej krajiny, kde sú takéto vyhlásenia nezlučiteľné s lokálnym zákonom: SPOLOČNOSŤ INTERNATIONAL BUSINESS MACHINES POSKYTUJE TÚTO PUBLIKÁCIU "TAK AKO JE" BEZ ZÁRUKY AKÉHOKOĽVEK DRUHU, VYJADRENEJ ALEBO IMPLIKOVANEJ, VRÁTANE (ALE NEOBMEDZENE) IMPLIKOVANÝCH ZÁRUK NEPOŠKODENIA, PREDAJNOSTI ALEBO VHODNOSTI NA KONKRÉTNY ÚČEL. Niektoré štáty nedovoľujú zrieknutie sa vyjadrených alebo mlčky predpokladaných záruk v určitých transakciách, preto sa vás toto vyhlásenie nemusí týkať.

Tieto informácie môžu obsahovať technické nepresnosti alebo typografické chyby. Tieto informácie sa periodicky menia; tieto zmeny budú začlenené do nových vydaní publikácie. IBM môže kedykoľvek bez ohlásenia spraviť zmeny a/alebo vylepšenia v produkte(och) a/alebo programe(och) opísanom v tejto publikácii.

Všetky odkazy v týchto informáciách na webové lokality iné ako od IBM sú poskytnuté len pre pohodlie a v žiadnom prípade neslúžia ako potvrdenie obsahu týchto webových lokalít. Materiály na týchto webových lokalitách nie sú časťou produktov IBM a použitie týchto webových lokalít je na vaše vlastné riziko.

| IBM môže použiť alebo distribuovať všetky vami poskytnuté informácie ľubovoľným spôsobom bez toho, aby voči vám
| vznikli akékoľvek záväzky.

Vlastníci licencií na tento program, ktorí chcú o ňom získať informácie za účelom povolenia: (i) výmeny informácií medzi nezávisle vytvorenými programami a inými programami (vrátane tohto) a (ii) vzájomného použitia vymieňaných informácií by mali kontaktovať:

| IBM Corporation
| Software Interoperability Coordinator, Department 49XA
| 3605 Highway 52 N
| Rochester, MN 55901
| U.S.A.

Takéto informácie môžu byť dostupné, môžu byť predmetom príslušných pojmov a podmienok a v niektorých prípadoch sú dostupné za poplatok.

Licenčný program spomínaný v týchto informáciách a všetky pre neho dostupné licenčné materiály, poskytuje spoločnosť IBM na základe podmienok zmlúv IBM Customer Agreement, IBM International Program License Agreement, IBM License Agreement for Machine Code alebo na základe inej rovnocennej zmluvy.

Všetky údaje o výkone, uvádzané v tomto dokumente boli získané v riadenom prostredí. Výsledky získané v iných prevádzkových prostrediach sa môžu podstatne odlišovať. Niektoré merania boli vykonané v systémoch vývojovej úrovne a nie je žiadna záruka, že tieto merania budú rovnaké vo všeobecne dostupných systémoch. Okrem toho, niektoré výsledky boli odhadnuté extrapoláciou. Skutočné výsledky sa môžu odlišovať. Užívatelia tohto dokumentu by si mali overiť použiteľnosť týchto údajov pre svoje špecifické prostredie.

Informácie o produktoch iných ako od IBM boli získané od poskytovateľov týchto produktov, z ich uverejnených oznámení alebo z iných, verejne dostupných zdrojov. IBM netestovala tieto produkty a nemôže potvrdiť presnosť ich výkonu, kompatibilitu ani žiadne iné tvrdenie týkajúce sa produktov iných ako od IBM. Otázky k schopnostiam produktov iných ako od IBM by ste mali adresovať poskytovateľom týchto produktov.

Všetky vyhlásenia týkajúce sa budúceho smerovania alebo úmyslov IBM sú predmetom zmeny alebo zrušenia bez ohlásenia a vyjadrujú len zámery a ciele.

Všetky ceny IBM sú navrhované predajné ceny stanovené spoločnosťou IBM, sú aktuálne a sú predmetom zmeny bez ohlásenia. Ceny dílerov môžu byť odlišné.

Tieto informácie slúžia len na plánovacie účely. Tu uvedené informácie sú predmetom zmeny pred sprístupnením opisovaných produktov.

Tieto informácie obsahujú príklady údajov a hlásení používaných v každodenných firemných operáciách. Kvôli ich čo najlepšej ilustrácii obsahujú tieto príklady mená osôb, názvy spoločností, pobočiek a produktov. Všetky tieto mená a názvy sú vymyslené a akákoľvek podobnosť s menami, názvami a adresami používanými skutočnými osobami a spoločnosťami je čisto náhodná.

LICENCIA NA AUTORSKÉ PRÁVA:

Tieto informácie obsahujú vzorové aplikačné programy v zdrojovom kóde, ktoré ilustrujú programovacie techniky v rôznych platformách. Tieto vzorové programy môžete kopírovať, upravovať a distribuovať v ľubovoľnej forme bez platenia poplatku spoločnosti IBM, za účelom vývoja, použitia, marketingu alebo distribúcie aplikačných programov vyhovujúcich aplikačnému programovému rozhraniu pre prevádzkovú platformu, pre ktorú sú napísané tieto vzorové programy. Tieto príklady neboli dôkladne otestované pri všetkých podmienkach. IBM preto nemôže garantovať alebo predpokladať spoľahlivosť, použiteľnosť ani funkciu týchto programov.

VZHĽADOM NA VŠETKY ZÁKONNÉ ZÁRUKY, KTORÉ NIE JE MOŽNÉ VYLÚČIŤ, IBM, JEJ VÝVOJOVÍ PRACOVNÍCI A DODÁVATELIA, NEDÁVAJÚ ŽIADNE ZÁRUKY, ČI UŽ VYJADRENÉ ALEBO MLČKY PREDPOKLADANÉ, VRÁTANE ALE BEZ OBMEDZENIA NA MLČKY PREDPOKLADANÉ ZÁRUKY NEPORUŠENIA PRÁV, PREDAJNOSTI ALEBO VHODNOSTI NA KONKRÉTNY ÚČEL OHĽADOM PROGRAMU ALEBO TECHNICKEJ PODPORY (AK NEJAKÁ EXISTUJE).

ZA ŽIADNYCH OKOLNOSTÍ NIE SÚ IBM A ANI JEJ VÝVOJOVÍ PRACOVNÍCI A DODÁVATELIA ZODPOVEDNÍ ZA ČOKOĽVEK Z NASLEDUJÚCEHO, ANI V PRÍPADE UPOZORNENIA NA MOŽNOSŤ VYSKYTU TEJTO SITUÁCIE:

1. STRATA ALEBO POŠKODENIE ÚDAJOV;
2. ŠPECIÁLNE, NÁHODNÉ ALEBO NEPRIAME ŠKODY ALEBO ZA ŽIADNE NEPRIAME EKONOMICKÉ ŠKODY, ALEBO
3. UŠLÝ ZISK, STRATA OBCHODOV, PRÍJMOV, POVESTI ALEBO OČAKÁVANÝCH ÚSPOR.

| NIEKTORÉ PRÁVNE SYSTÉMY NEUMOŽŇUJÚ VYLÚČENIE ALEBO OBMEDZENIE NÁHODNÝCH ČI
| NÁSLEDNÝCH ŠKÔD, TAKŽE VYŠŠIE UVEDENÉ VYLÚČENIE ALEBO OBMEDZENIE SA NA VÁS
| NEMUSÍ VZŤAHOVAŤ.

Každá kópia alebo časť týchto vzorových programov alebo odvodená práca musí obsahovať túto poznámku o autorských právach:

© (IBM) (2004). Časti tohto kódu sú odvodené od vzorových programov spoločnosti IBM. © Copyright IBM Corp. 2004. Všetky práva vyhradené.

Ak si prezeráte elektronickú kópiu týchto informácií, nemusia byť zobrazené fotografie ani farebné ilustrácie.

Ochranné známky

Nasledujúce pojmy sú ochranné známky spoločnosti International Business Machines v USA, v iných krajinách alebo v oboch:

AIX
Distributed Relational Database Architecture
Domino
DRDA
e(logo)server
eServer
IBM
iSeries
OS/400
pSeries
RACF
RDN
Tivoli
WebSphere
xSeries
z/OS
zSeries

| Lotus, Lotus Notes, Freelance a WordPro sú ochrannými známkami spoločnosti International Business Machines
| Corporation a Lotus Development Corporation v USA alebo iných krajinách.

Microsoft, Windows, Windows NT a logo Windows sú ochranné známky spoločnosti Microsoft v USA alebo iných krajinách.

UNIX je registrovaná ochranná známka spoločnosti The Open Group v USA a iných krajinách.

Ostatné názvy spoločnosti, produktov alebo služieb môžu byť ochrannými alebo servisnými známkami iných subjektov.

Podmienky sťahovania a tlače informácií

| Povolenie na používanie vybratých informácií, ktoré si chcete stiahnuť, je podmienené vaším súhlasom s nasledujúcimi
| podmienkami.

| **Osobné použitie:** Tieto informácie môžete kopírovať len na svoje osobné nekomerčné použitie pod podmienkou, že
| dodržíte všetky oznámenia o vlastníckych právach. V žiadnom prípade nemôžete tieto informácie ani žiadnu ich časť
| distribuovať, prezentovať alebo z nich vytvárať odvodené práce, bez výslovného súhlasu spoločnosti IBM.

Komerčné použitie: V rámci vášho podniku môžete kopírovať, distribuovať a prezentovať tieto informácie len za predpokladu, že dodržíte všetky oznámenia o vlastníckych právach. V žiadnom prípade nemôžete tieto informácie ani žiadnu ich časť distribuovať, prezentovať alebo z nich vytvárať odvodené práce mimo vášho podniku bez výslovného súhlasu spoločnosti IBM.

Okrem povolení výslovne vyjadrených v tomto dokumente, nie sú pre uvedené informácie, údaje, softvér alebo iné duševné vlastníctvo v nich obsiahnuté, udelené žiadne iné výslovné alebo mlčky predpokladané povolenia, oprávnenia alebo práva.

IBM si vyhradzuje právo vypovedať oprávnenia uvádzané v tomto dokumente kedykoľvek, ak usúdi, že používanie týchto informácií poškodzuje jej záujmy alebo ak spoločnosť IBM zistí, že vyššie uvedené inštrukcie nie sú náležite dodržiavané.

Stiahnuť, exportovať a re-exportovať môžete tieto informácie len v tom prípade, ak vyhovujú všetkým platným zákonom a predpisom, vrátane zákonov a predpisov USA týkajúcich sa exportu. IBM NEPOSKYTUJE ŽIADNU ZÁRUKU NA OBSAH TÝCHTO INFORMÁCIÍ. TIETO INFORMÁCIE SA POSKYTUJÚ ″TAK AKO SÚ″ BEZ AKÝCHKOĽVEK VÝSLOVNÝCH ALEBO MLČKY PREDPOKLADANÝCH ZÁRUK, VRÁTANE, ALE BEZ OBMEDZENIA NA ZÁRUKY NEPORUŠENIA PRÁV, PREDAJNOSTI ALEBO VHODNOSTI NA KONKRÉTNY ÚČEL

Všetky materiály sú chránené autorským právom IBM Corporation.

Stiahnutím alebo vytlačením informácií z týchto stránok vyjadrujete svoj súhlas s týmito podmienkami.

Vytlačené v USA