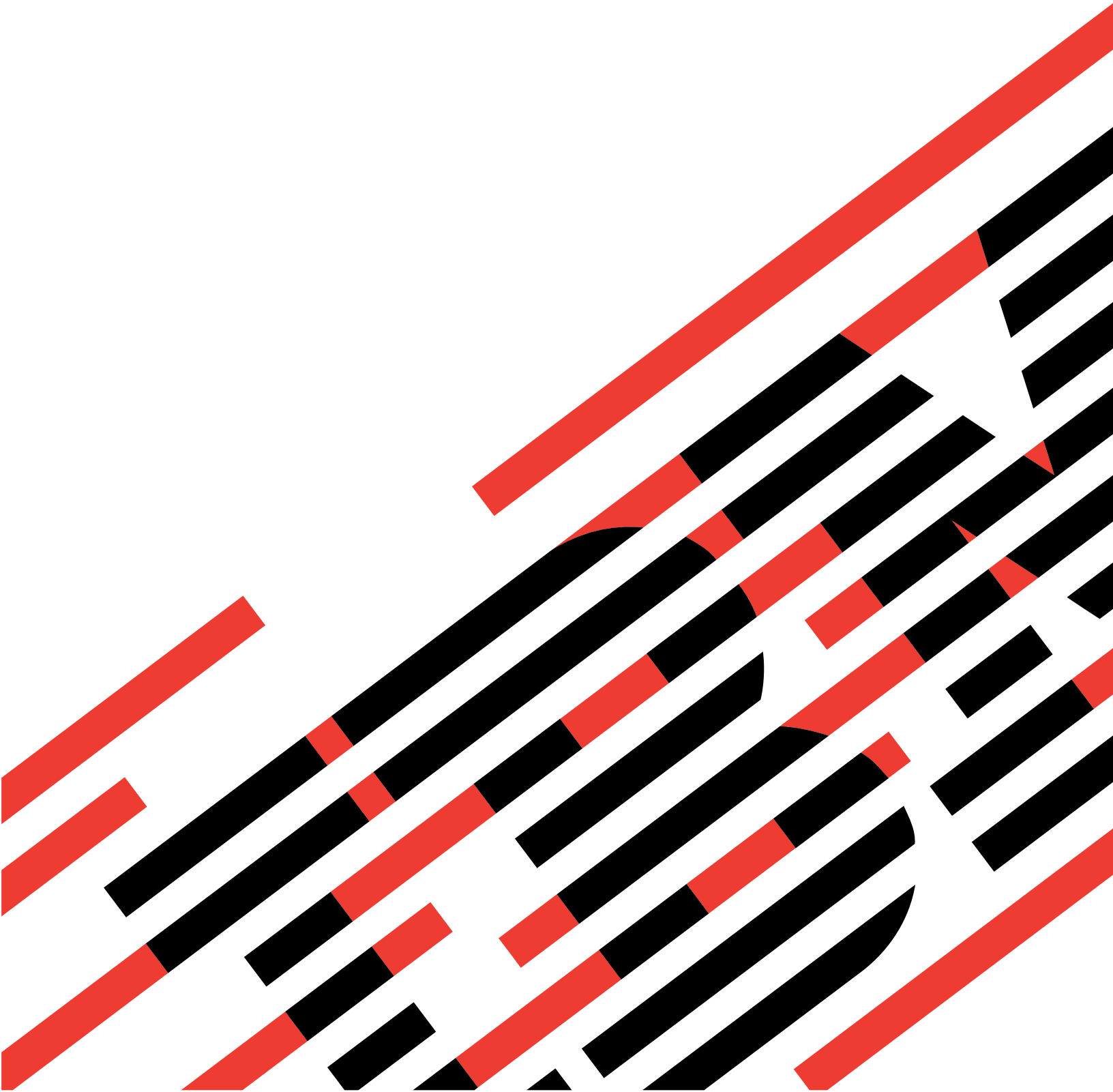
IBM

eserver

iSeries

Enterprise Identity Mapping



IBM

@server

iSeries

Enterprise Identity Mapping

Obsah

Enterprise Identity Mapping (EIM) 1
Vytlačiť túto tému 2
Prehľad technológie Enterprise Identity Mapping 2
Koncepty EIM 4
Radič domény EIM 6
Doména EIM 7
Identifikátor EIM 8
Definície registrov EIM 11
Definície systémových a aplikačných registrov 13
Priradenia EIM 14
Operácie prehľadania EIM 17
Oprávnenia EIM 18
Koncepty LDAP pre EIM 21
Rozlišovací názov LDAP 22
Rodičovský rozlišovací názov LDAP 22
Povolenie jednorazového prihlásenia cez EIM 23
Plán pre EIM 25
Inštalovať vyžadované voľby programu iSeries Navigator 25
Konfigurovať službu sieťovej autentifikácie 26
Konfigurovať EIM 26
Vytvoriť a pripojiť k novej doméne 27
Konfigurovať bezpečné pripojenie k radiču domény EIM 30
Pripojiť k existujúcej doméne 30
Manažovať EIM 33
Manažovať domény EIM 33
Pridať doménu do Manažmentu domén 33
Pripojiť k doméne 34
Vymazať doménu 34
Odstrániť doménu z Manažmentu domén 34
Manažovať priradenia 34
Vytvoriť priradenie 35
Vymazať priradenie 35
Manažovať identifikátory EIM 36
Vytvoriť identifikátor EIM 36
Pridať alias k identifikátoru EIM 36
Vymazať identifikátor EIM 37
Manažovať oprávnenia EIM pre užívateľov 37
Manažovať registre užívateľov 37
Pridať register užívateľov 38
Pridať alias do registra užívateľov 38
Definovať súkromný typ registra užívateľov v EIM 39
Odstrániť register užívateľov 40
Odstrániť alias z registra užívateľov 40
Rozhrania API pre EIM 41
Odstraňovanie problémov EIM 41
Nedá sa pripojiť k radiču domény 42
Zobrazenie zoznamu identifikátorov EIM trvá dlho 42
Sprievodca konfiguráciou EIM prestane reagovať počas dokončovania spracovania 42
Deskriptor EIM je už neplatný 43
Autentifikácia Kerberosom a diagnostické správy 43
Súvisiace informácie pre EIM 43

Enterprise Identity Mapping (EIM)

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 je mechanizmus pre mapovanie (priraďovanie) osoby alebo entity k príslušným identitám užívateľa v rôznych registroch v podniku. EIM poskytuje rozhrania API pre vytváranie a manažovanie týchto vzťahov mapovania identít, ako aj rozhrania API, ktoré používajú aplikácie na zisťovanie týchto informácií. Okrem toho, OS/400(R) používa schopnosti EIM a Kerberos na vytvorenie prostredia s jednorazovým prihlásením.

iSeries Navigator, grafické užívateľské rozhranie iSeries, poskytuje sprievodcov pre konfiguráciu a manažment EIM. Okrem toho, administrátori môžu manažovať vzťahy pre užívateľské profily cez iSeries Navigator.

Server iSeries(TM) používa EIM na to, aby rozhrania OS/400 mohli autentifikovať užívateľov pomocou služby sieťovej autentifikácie. Aplikácie, ako aj OS/400, môžu akceptovať lístky Kerberos a použiť EIM na nájdenie užívateľského profilu, ktorý reprezentuje rovnakú osobu ako reprezentuje lístok Kerberos.

Špecifické informácie o EIM nájdete v týchto témach:

Vytlačiť túto tému
Vytlačte si PDF tejto témy EIM a iných súvisiacich tém.

Prehľad technológie 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
Prečítajte si o konceptoch EIM, ktorým je potrebné porozumieť kvôli úspešnej implementácii EIM.

Koncepty LDAP pre EIM
Prečítajte si o konceptoch LDAP (Lightweight Directory Access Protocol), ktorým je potrebné porozumieť kvôli úspešnej implementácii EIM.

Povolenie jednorazového prihlásenia
Prečítajte si o výhodách, ktoré poskytuje EIM pre zjednodušenie prihlasovania užívateľov.

Plán pre EIM
Pred nakonfigurovaním EIM sa presvedčite, že máte nakonfigurované všetky vyžadované služby a aplikácie.

Konfigurovať EIM
Použite Sprievodcu konfiguráciou Enterprise Identity Mapping (ďalej len Sprievodca konfiguráciou EIM), aby ste mohli začať používať EIM.

Manažovať EIM
Manažujte vlastnosti EIM, domény EIM, registre užívateľov, oprávnenia užívateľov EIM, atď.

Rozhrania API pre EIM
Použite rozhrania API EIM vo vašich aplikáciách a sieti.

Odstraňovanie problémov s EIM
Nájdite riešenia pre bežné problémy a chyby, s ktorými sa môžete stretnúť pri používaní EIM vo vašej sieti.

Súvisiace informácie pre EIM
Obsahuje odkaz na súvisiace informácie o EIM.

Vytlačiť túto tému

Ak chcete zobraziť alebo prevziať verziu PDF, vyberte Enterprise Identity Mapping

(približne 390 KB alebo 50 strán).

Iné informácie

Môžete zobraziť alebo prevziať tieto súvisiace témy:

- Sieťové autentifikačné služby (približne 199 KB alebo 60 strán) obsahuje informácie o spôsobe konfigurácie služby sieťovej autentifikácie v spojení s EIM za účelom vytvorenia prostredia s jednorazovým prihlásením.
- Adresárové služby (LDAP) (približne 323 KB alebo 66 strán) obsahuje informácie o spôsobe konfigurácie servera LDAP, ktorý môžete použiť ako radič domény EIM, spolu s informáciami o rozšírenej konfigurácii LDAP.

Ukladanie súborov PDF

Aby ste uložili PDF na vašej pracovnej stanici kvôli prezeraniu alebo tlači:

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

Prevzatie programu Adobe Acrobat Reader

Ak potrebujete program Adobe Acrobat Reader na zobrazenie alebo tlač týchto súborov PDF, prevezmite si kópiu z webovej lokality Adobe (www.adobe.com/prodindex/acrobat/readstep.html)

.

Prehľad technológie 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 infraštruktúrna technológia od IBM

, ktorá umožňuje administrátorom a vývojárom aplikácií adresovať tento problém oveľa jednoduchšie a lacnejšie, ako bolo možné doteraz.

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. Administrátori často venujú svoj čas odstraňovaniu problémov spôsobených zlými pokusmi o prihlásenie a prestavovaniu zabudnutých hesiel, namiesto manažovania bezpečnosti podniku.

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 na 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 populárnych riešení, napríklad Microsoft Passport) však znamená, že administrátori musia manažovať ďalší register užívateľov a bezpečnostné sémantiky, alebo musia nahradiť existujúce aplikácie, ktoré sú vytvorené na používanie týchto registrov.

Pri takomto riešení musia administrátori manažovať viac bezpečnostných mechanizmov pre jednotlivé prostriedky, čo zvyšuje réžiu administrácie 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.

Iným možným riešením je používať jednorazové prihlásenie. Je k dispozícii 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 na 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 zavedenie nenákladných riešení pre jednoduché manažovanie registrov užívateľov a identít užívateľov v podniku. EIM je architektúra pre opis vzťahov medzi jednotlivcami alebo entitami (napríklad súborové servery a tlačové servery) v podniku a mnohých identít, ktoré ich reprezentujú v podniku. 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.

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. Napríklad administrátor môže namapovať identitu SAP (alebo ešte lepšie, mapovanie môže spraviť samotný SAP) na prístup k prostriedkom SAP.

Použitie mapovania identity vyžaduje, aby administrátori spravili nasledujúce:

1. Vytvorili identifikátory EIM, ktoré reprezentujú ľudí alebo entity v ich podniku.
2. Vytvorili definície registrov EIM, ktoré opisujú existujúce registre užívateľov v ich podniku.
3. Zadefinovali vzťah medzi identitami užívateľov v týchto registroch a nimi vytvorenými identifikátormi EIM.

Pre existujúce registre užívateľov nie je nutná žiadna zmena kódu. Administrátor nemusí mať mapovania pre všetky identity v registri užívateľov. EIM umožňuje mapovania typu jeden-veľa (inými slovami, jeden užívateľ s viac ako jednou identitou užívateľa v jednom registri užívateľov). EIM tiež umožňuje mapovania typu veľa-jeden (inými slovami, viacero užívateľov zdieľa jednu identitu užívateľa v jednom registri užívateľov; je to podporované, ale neodporúča sa to). Administrátor môže v EIM použiť ľubovoľný register užívateľov ľubovoľného typu.

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. Administrátori manažujú tieto údaje v adresári LDAP, ktorý poskytuje flexibilitu manažovania údajov na jednom mieste a možnosť mať repliky všade tam, kde sa používajú tieto informácie. Na záver, EIM umožňuje podnikom a vývojárom aplikácií jednoducho pracovať v širšom rozsahu prostredí s menšími nákladmi, ako by to bolo možné bez tohto prístupu.

Koncepty EIM

Konceptuálne pochopenie spôsobu fungovania EIM (Enterprise Identity Mapping) je potrebné pre úplné pochopenie spôsobu možného využitia EIM vo vašom podniku. Konfigurácia a implementácia rozhraní API EIM sa môže odlišovať pre rôzne platformy serverov, ale koncepty EIM sú spoločné pre všetky platformy IBM

.

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

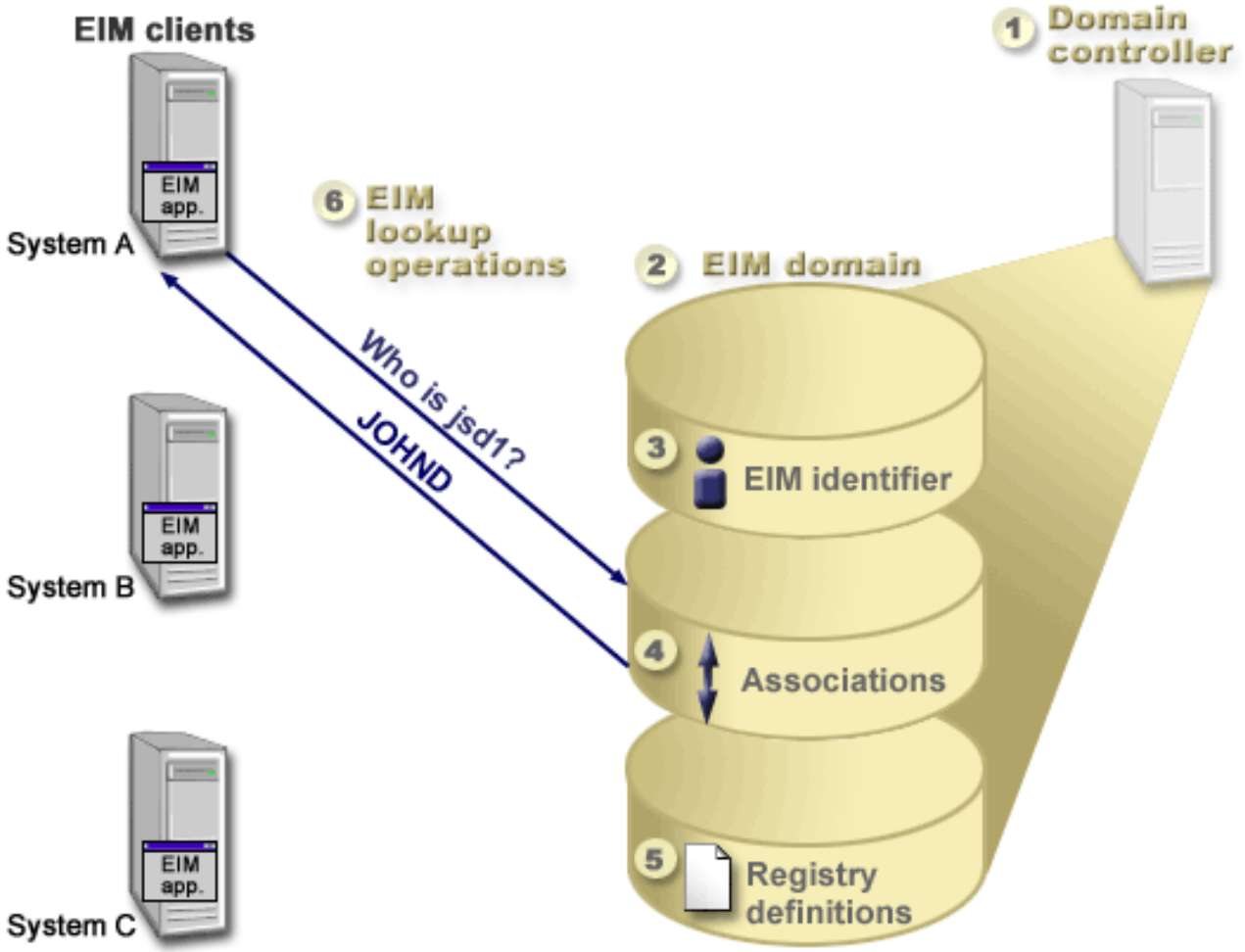
4

medzi týmito identifikátormi EIM a identitami užívateľov, a definície registrov EIM

5

.

Obrázok 1: Príklad implementácie EIM



Viac informácií o týchto konceptoch EIM nájdete v týchto témach:

- Radič domény EIM
- Doména EIM
- Identifikátor EIM
- Definície registrov EIM
- Priradenia EIM
- Operácie prehľadania EIM
- Oprávnenia EIM

Radič domény EIM

Radič domény EIM je server LDAP (Lightweight Directory Access Protocol), ktorý je nakonfigurovaný na manažovanie aspoň jednej domény 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. V podniku musí existovať minimálne jeden radič domény EIM.

V súčasnosti môžete nakonfigurovať niektoré platformy IBM

ako radiče 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 za účelom vykonania operácií prehľadania EIM.

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.

Doména EIM

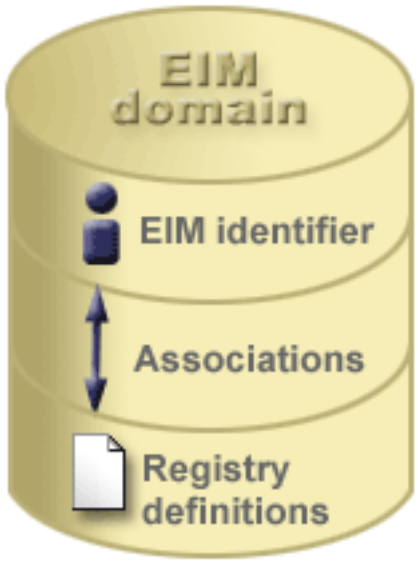
Doména EIM je adresár na serveri LDAP (Lightweight Directory Access Protocol), ktorý obsahuje údaje EIM pre podnik. Doména EIM je kolekcia všetkých identifikátorov EIM, priradení EIM a registrov užívateľov, ktoré sú zadefinované v danej doméne. Systémy (klienti EIM) sú spojené s doménou tým, že používajú 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. EIM sleduje len informácie o vzťahoch, preto nie je potrebná synchronizácia medzi registrami užívateľov a EIM.

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 uložené v tejto doméne



K údajom EIM patria:

- **Identifikátory EIM.**Každý vami vytvorený identifikátor EIM reprezentuje osobu alebo entitu (napríklad tlačový server alebo súborový server) v podniku. Pozrite si tému Identifikátor EIM, kde nájdete viac informácií.
- **Definície registrov EIM.**Každá vami vytvorená definícia registra EIM reprezentuje skutočný register užívateľov (a informácie o obsiahnutých identitách užívateľov), ktorý existuje na niektorom systéme v podniku. Keď zadefinujete špecifický register užívateľov v EIM, tento register užívateľov sa môže zaradiť do domény EIM. Pozrite si tému Definície registrov EIM, kde nájdete viac informácií.
- **Priradenia EIM.**Každé vami vytvorené priradenie EIM reprezentuje vzťah medzi identifikátorom EIM a priradenou identitou v podniku. Priradenia vytvárate pre identity v registroch užívateľov, ktoré tvoria doménu EIM. Priradenia poskytujú informácie, ktoré viažu identifikátor EIM k špecifickej identite užívateľa v špecifickom registri užívateľov. Priradenia sa musia zadefinovať aj na to, aby klienti EIM mohli používať rozhrania API EIM na vykonávanie úspešných operácií prehľadania EIM. Tieto operácie prehľadania EIM hľadajú v doméne EIM definované priradenia medzi identifikátormi EIM a identitami užívateľov v známych registroch užívateľov. Pozrite si tému Operácie prehľadania EIM, kde nájdete viac informácií.

Po vytvorení vašich identifikátorov EIM, definícií registrov a priradení môžete začať používať EIM na oveľa jednoduchšiu organizáciu a prácu s identitami užívateľov vo vašom podniku.

Identifikátor EIM

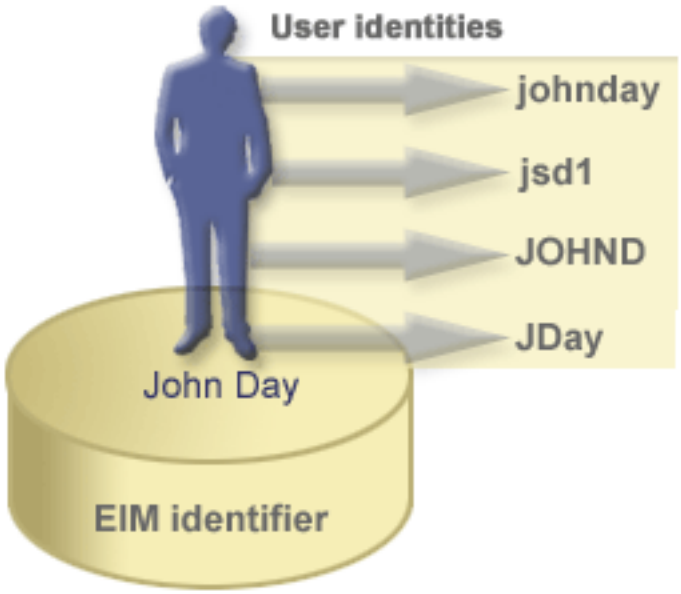
Identifikátor EIM reprezentuje osobu alebo entitu v podniku. Typická sieť obsahuje rôzne hardvérové platformy a aplikácie a k nim priradené registre užívateľov. Väčšina platforiem a veľa aplikácií používa registre užívateľov špecifické pre platformu alebo aplikáciu. Tieto registre užívateľov obsahujú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

Keď vytvoríte identifikátor EIM a priradíte ho k rôznym identitám užívateľov pre osobu alebo entitu, zjednoduší sa vytváranie heterogénnych, viacvrstvových aplikácií, napríklad prostredie s jednorazovým prihlásením. Keď vytvoríte identifikátor EIM a jeho priradenia, zjednoduší sa vytvorenie a používanie nástrojov zjednodušujúcich administráciu, ktorá zahŕňa manažovanie všetkých identít užívateľov niektorej osoby alebo entity v 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* štyri identity v štyroch rôznych registroch užívateľov: johnday, jsd1, JOHND a JDay.

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

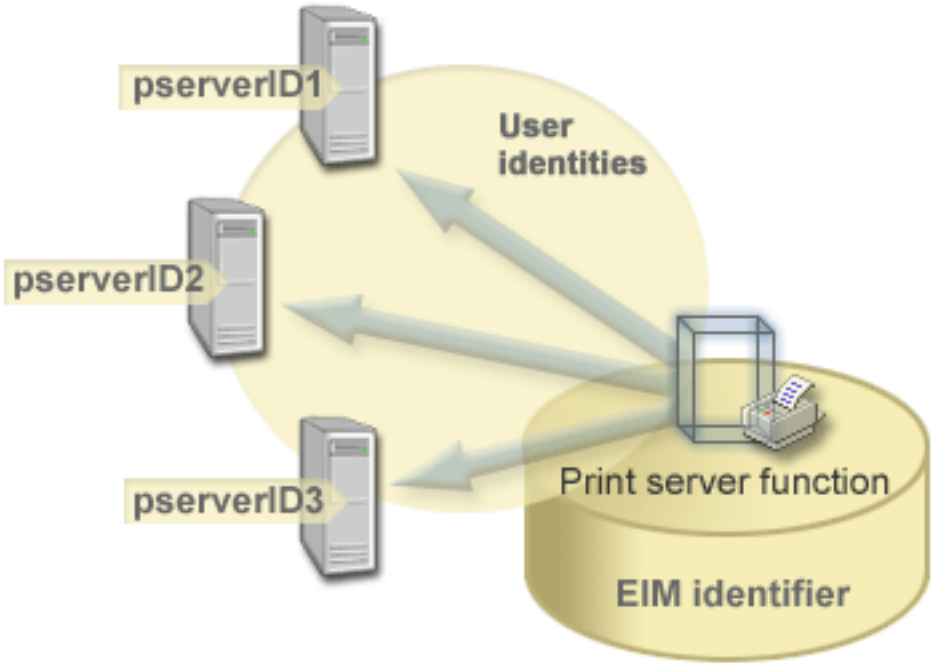


V EIM môžete vytvoriť priradenia, ktoré definujú vzťahy medzi identifikátorom John Day a každou z rôznych identít užívateľa pre *John Day*. Vytvorením týchto priradení na zadefinovanie týchto vzťahov môžete vy a ostatní písať aplikácie, ktoré používajú rozhrania API EIM na vyhľadanie potrebnej, ale neznámej 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 na viacerých systémoch. Na Obrázku 4 funkcia tlačového servera v podniku prebieha na 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. V tomto príklade identifikátor EIM funkcie tlačového servera reprezentuje skutočnú entitu funkcie tlačového servera v podniku. Priradenia sú vytvorené kvôli zadefinovaniu vzťahov medzi identifikátorom EIM (funkcia tlačového servera) a každou z identít užívateľa pre túto funkciu (pserverID1, pserverID2 a pserverID3). 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.

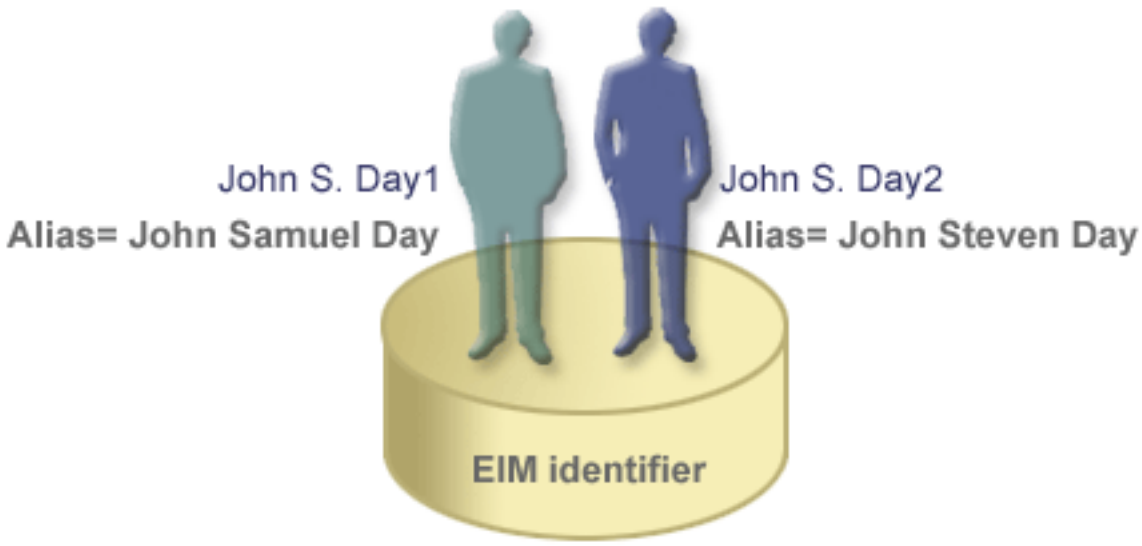
Identifikátory EIM a používanie aliasov

Pre identifikátory EIM tiež môžete vytvoriť aliasy. Aliasy môžu pomôcť pri hľadaní špecifického identifikátora EIM 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.

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, založené na rovnakom mene *John S. Day*



Pomocou aliasov môže administrátor EIM poskytnúť dodatočné informácie o osobe pre každý identifikátor EIM. Tieto informácie sa tiež môžu použiť v operácii prehľadania EIM na rozlíšenie medzi užívateľmi, ktorých reprezentuje daný identifikátor. Napríklad alias pre John S. Day1 môže byť John Samuel Day a alias pre John S. Day2 môže byť John Steven Day.

Každý identifikátor EIM môže mať viac aliasov na určenie, ktorého *John S. Day* reprezentuje daný identifikátor EIM. Administrátor EIM môže pridať ďalší alias ku každému z identifikátorov EIM pre tieto dve osoby, aby ich rozlíšil ešte viac. Napríklad dodatočné aliasy môžu obsahovať číslo zamestnanca, číslo oddelenia, pracovný titul alebo iný rozlišovací atribút.

Definície registrov EIM

Definícia registra EIM reprezentuje skutočný 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. Príkladom registra užívateľov je register z/OS Security Server Resource Access Control Facility (RACF(R)). 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 bežného registra užívateľov je distribučné centrum kľúčov (KDC) Kerberos a register užívateľských profilov OS/400.

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

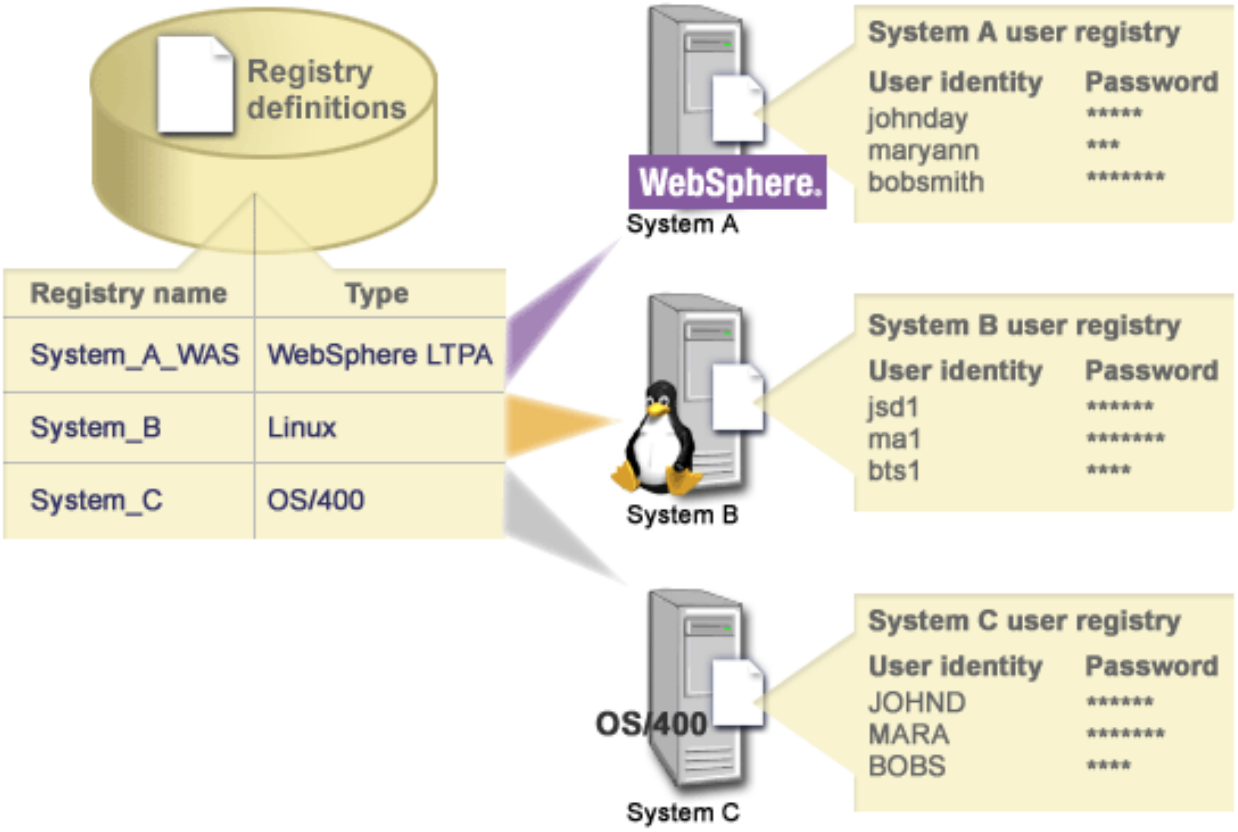
- Jedinečný, ľubovoľný názov registra EIM
- Typ registra užívateľov

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 aplikačný register užívateľov. Pri vytváraní jedinečných názvov definícií registrov EIM môžete použiť ľubovoľnú kombináciu alfanumerických znakov, písmená rôznej veľkosti a medzery.

Na Obrázku 6 administrátor vytvoril definície registra EIM pre registre užívateľov reprezentujúce System A, System B a System C. Napríklad System A obsahuje register užívateľov pre WebSphere LTPA (Lightweight Third-Party Authentication). Názov definície registra, ktorý použije administrátor, pomáha identifikovať špecifický výskyt daného typu registra užívateľov. Napríklad adresa IP alebo názov hostiteľa je často

dostatočný pre veľa typov registrov užívateľov. V tomto príklade administrátor identifikuje špecifickú inštanciu registra užívateľov pomocou názvu definície registra System_A_WAS. Okrem názvu administrátor tiež určí typ registra ako WebSphere LTPA.

Obrázok 6: Definície registra EIM pre tri registre užívateľov v podniku



Môžete tiež zadefinovať registre užívateľov, ktoré existujú v iných registroch užívateľov. Napríklad register z/OS Security Server (RACF) môže obsahovať špecifické registre užívateľov, ktoré sú podmnožinou užívateľov v úplnom registri užívateľov RACF. Viac informácií o tejto problematike nájdete v téme Definície systémových a aplikačných registrov.

Definície registrov EIM a používanie aliasov

Pre definície registrov EIM tiež môžete vytvoriť aliasy. 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 DNS LDAP

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 pri inicializácii skontrolovať alias a nájsť 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.

Definície systémových a aplikačných registrov

Niektoré aplikácie používajú podmnožinu identít užívateľov z jednej inštancie registra užívateľov. EIM umožňuje administrátorom vymodelovať tento scenár prostredníctvom dvoch druhov definícií registrov EIM: systémový a aplikačný.

Definícia systémového registra reprezentuje rozdielny register na pracovnej stanici alebo serveri. Definíciu systémového registra môžete vytvoriť v prípade, ak register v podniku má jednu z týchto charakteristík:

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

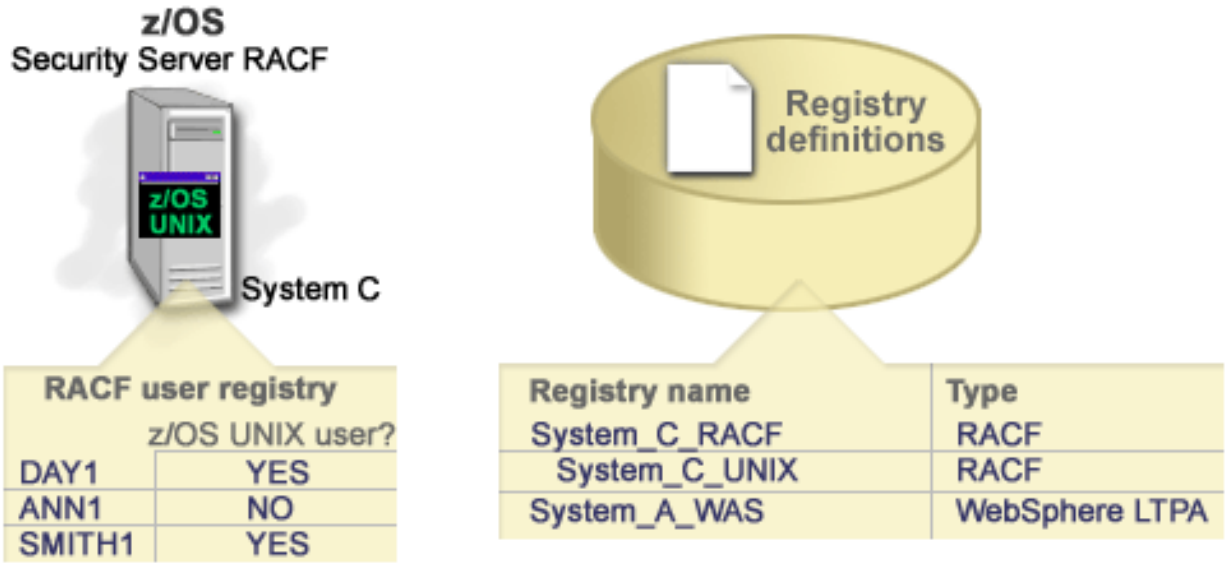
Definícia aplikačného registra reprezentuje podmnožinu identít užívateľov, ktoré sú definované v systémovom registri. Tieto identity užívateľov zdieľajú spoločnú množinu atribútov alebo charakteristík, ktoré im umožňujú použiť konkrétnu aplikáciu alebo množinu aplikácií. Definíciu aplikačného registra môžete vytvoriť v prípade, ak identity užívateľov majú tieto charakteristiky:

- Identity užívateľov pre aplikáciu alebo množinu aplikácií nie sú uložené v registri užívateľov, špecifickom pre danú aplikáciu alebo množinu aplikácií.
- Identity užívateľov pre aplikáciu alebo množinu aplikácií sú uložené v systémovom registri, ktorý obsahuje identity užívateľov pre iné aplikácie.

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.

Napríklad Obrázok 7 znázorňuje definíciu systémového registra, vytvorenú administrátorom na reprezentovanie registra z/OS Security Server RACF. Administrátor tiež vytvoril definíciu aplikačného registra na reprezentovanie identít užívateľov v registri RACF, ktoré používajú z/OS UNIX System Services (z/OS UNIX). System 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 k z/OS UNIX na System C. Tieto identity užívateľov sú skutoční užívatelia RACF s jedinečnými atribútmi, ktoré ich identifikujú ako užívateľov z/OS UNIX. Pokiaľ ide o definície registrov EIM, administrátor EIM zadefinoval System_C_RACF na reprezentovanie celého registra užívateľov RACF. Administrátor tiež zadefinoval System_C_UNIX na reprezentovanie identít užívateľov, 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 vzťah medzi identifikátorom EIM, ktorý reprezentuje špecifickú osobu a jednou identitou užívateľa v registri užívateľov, ktorá tiež reprezentuje danú 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. 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*.

Aby ste mohli vytvoriť priradenie, musíte najprv vytvoriť príslušný identifikátor EIM a príslušnú definíciu registra EIM pre register užívateľov, ktorý obsahuje 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

Administrátor môže vytvoriť rôzne typy priradení medzi identifikátorom EIM a identitou užívateľa podľa spôsobu použitia danej identity užívateľa. 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 takmer všetky aplikácie museli používať identity užívateľov z jedného registra užívateľov pre autentifikáciu aj autorizáciu. Pomocou operácií prehľadania EIM môžu aplikácie používať identity užívateľov z jedného registra užívateľov na autentifikáciu a zároveň iný register užívateľov na autorizáciu.

V EIM existujú tri typy priradení, ktoré môže administrátor zadefinovať medzi identifikátorom EIM a identitou užívateľa. Tieto typy sú: zdrojové, cieľové a administratívne priradenie.

Zdrojové priradenie

Keď sa identita užívateľa použije na *autentifikáciu*, táto identita užívateľa by mala mať zdrojové priradenie k identifikátoru EIM. Zdrojové priradenie umožňuje použiť identitu užívateľa ako zdroj v operácii vyhľadania EIM na nájdenie inej identity užívateľa, ktorá je priradená k rovnakému identifikátoru EIM. Ak sa identita užívateľa, ktorá má len zdrojové priradenie použije ako cieľová identita v operácii prehľadania EIM, nevrátia sa žiadne priradené identity užívateľov.

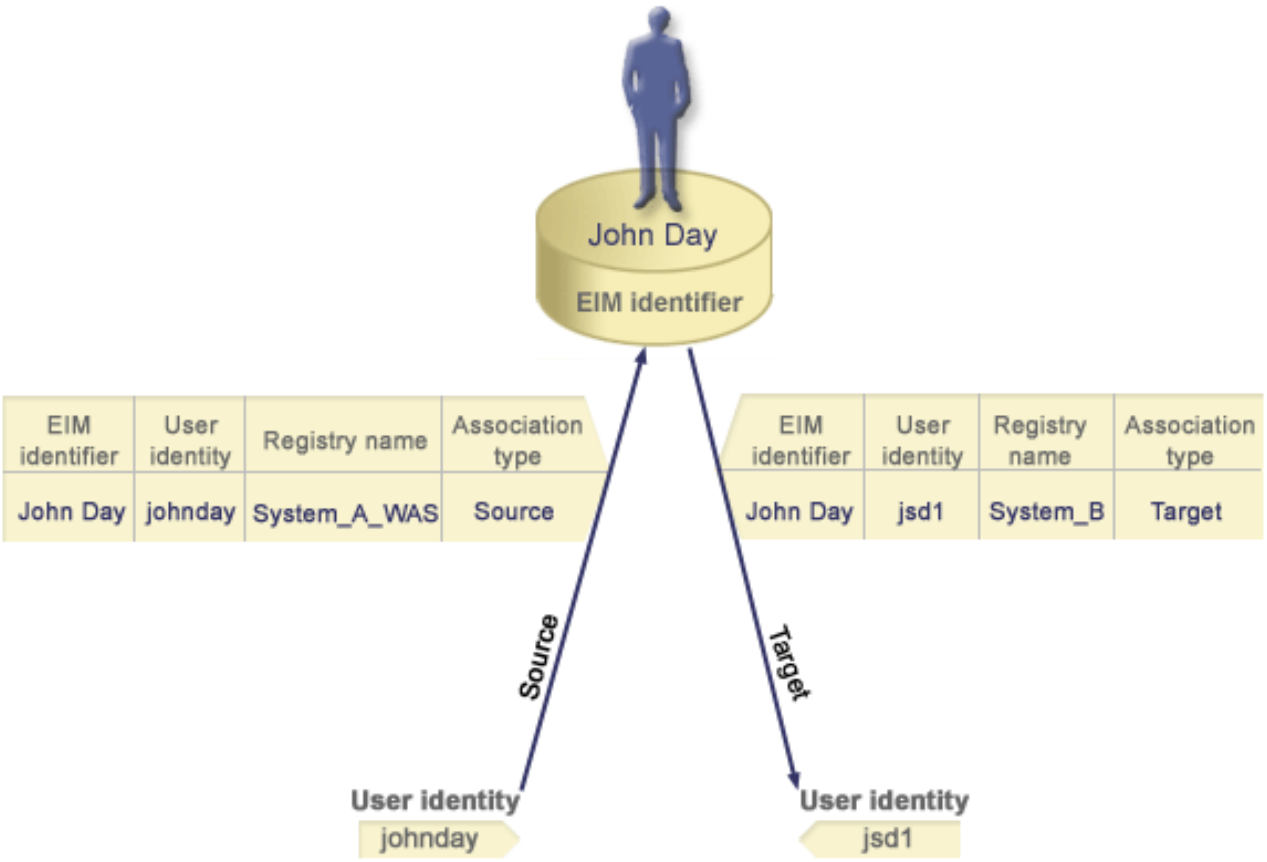
Cieľové priradenie

Keď sa identita užívateľa použije na *autorizáciu* namiesto autentifikácie, daná identita užívateľa by mala mať cieľové priradenie k identifikátoru EIM. Cieľové priradenie umožňuje vrátenie identity užívateľa ako výsledok operácie prehľadania EIM. Ak sa identita užívateľa, ktorá má len cieľové priradenie použije ako zdrojová identita v operácii prehľadania EIM, nevrátia sa žiadne priradené identity užívateľov.

Môže byť potrebné vytvoriť cieľové aj zdrojové priradenie pre jednu identitu užívateľa. Je to potrebné, ak niekto používa jeden systém ako klienta aj server, alebo ak dotyčný vystupuje ako administrátor. Napríklad užívateľ sa normálne autentifikuje pre platformu Windows a spúšťa aplikácie pristupujúce k serveru AIX. Kvôli pracovnej náplni sa tento užívateľ musí občas prihlásiť priamo na server AIX. V tejto situácii by ste vytvorili zdrojové aj cieľové priradenie medzi identitou užívateľa AIX a identifikátorom EIM tejto osoby. Identity užívateľov, reprezentujúce koncových užívateľov sú zvyčajne len cieľové priradenia.

Obrázok 6 znázorňuje príklad zdrojového a cieľového priradenia. V tomto príklade administrátor vytvoril dve priradenia pre identifikátor EIM John Day, aby zadefinoval vzťah medzi týmto identifikátorom a dvomi priradenými identitami užívateľov. Administrátor vytvoril zdrojové priradenie pre johnday, identitu užívateľa WebSphere LTPA (Lightweight Third-Party Authentication) v registri užívateľov System_A_WAS. Administrátor tiež vytvoril cieľové priradenie pre jsd1, užívateľský profil OS/400 v registri užívateľov System B. Tieto priradenia umožňujú aplikáciám získať neznámu identitu užívateľa (cieľ, jsd1) na základe známej identity užívateľa (zdroj, johnday) pomocou operácie prehľadania EIM.

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



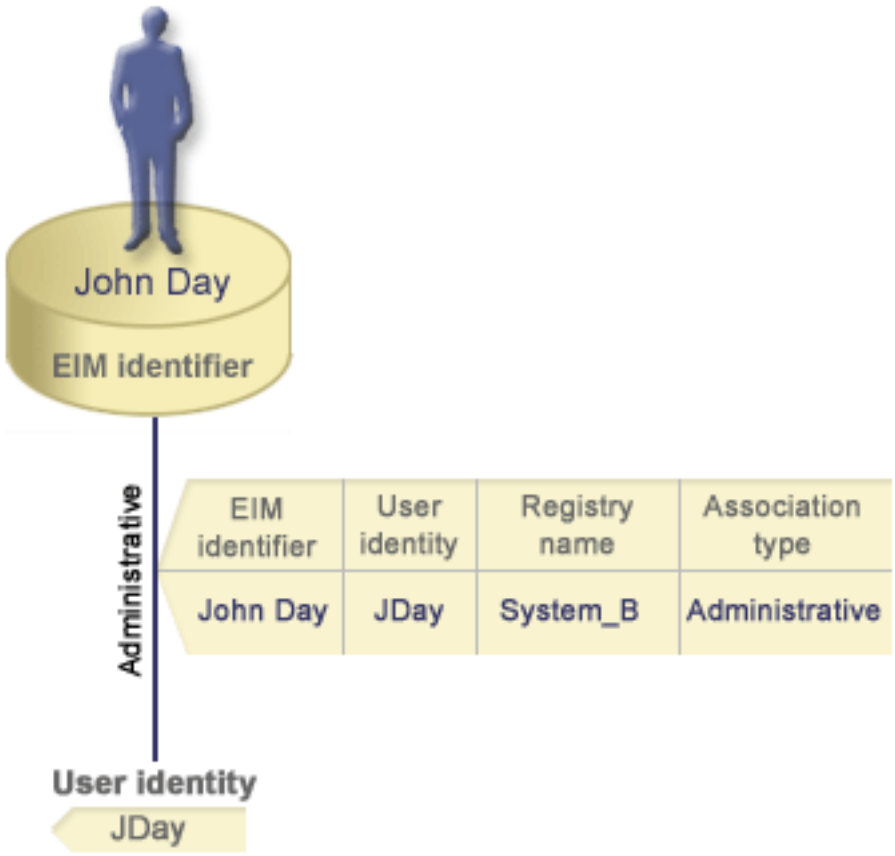
Administratívne priradenie

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

Kvôli podstate reprezentovanej administratívnymi priradeniami, operácia prehľadania EIM, ktorá by poskytla zdrojovej identite užívateľa administratívne priradenie, nevráti 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 John Day jednu identitu užívateľa v System A a inú identitu užívateľa v System B, ktorý je 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 užívateľa John Day pre tento systém pomocou cudzieho autentifikačného mechanizmu. Použitím administratívneho priradenia pre identitu užívateľa JDay na System B môže administrátor EIM zistiť, že John Day vlastní konto na 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 na tomto systéme.

Obrázok 7: Administratívne priradenie EIM pre identifikátor EIM John Day



Operácie prehľadania EIM

Operácia prehľadania EIM je proces, ktorým aplikácia alebo operačný systém nájde neznámu priradenú identitu užívateľa v špecifickom cieľovom registri tým, že poskytne niektoré známe a dôveryhodné informácie. Aplikácie používajúce rozhrania API EIM môžu vykonávať tieto operácie vyhľadávania informácií EIM 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 aplikácia poskytne *ako zdroj identitu užívateľa*, aplikácia tiež musí poskytnúť názov definície registra EIM pre zdroj identity užívateľa a názov definície registra EIM, ktorý je cieľom operácie prehľadania EIM. Aby sa identita užívateľa dala v operácii vyhľadania EIM použiť ako zdroj, musí byť pre ňu definované zdrojové priradenie.

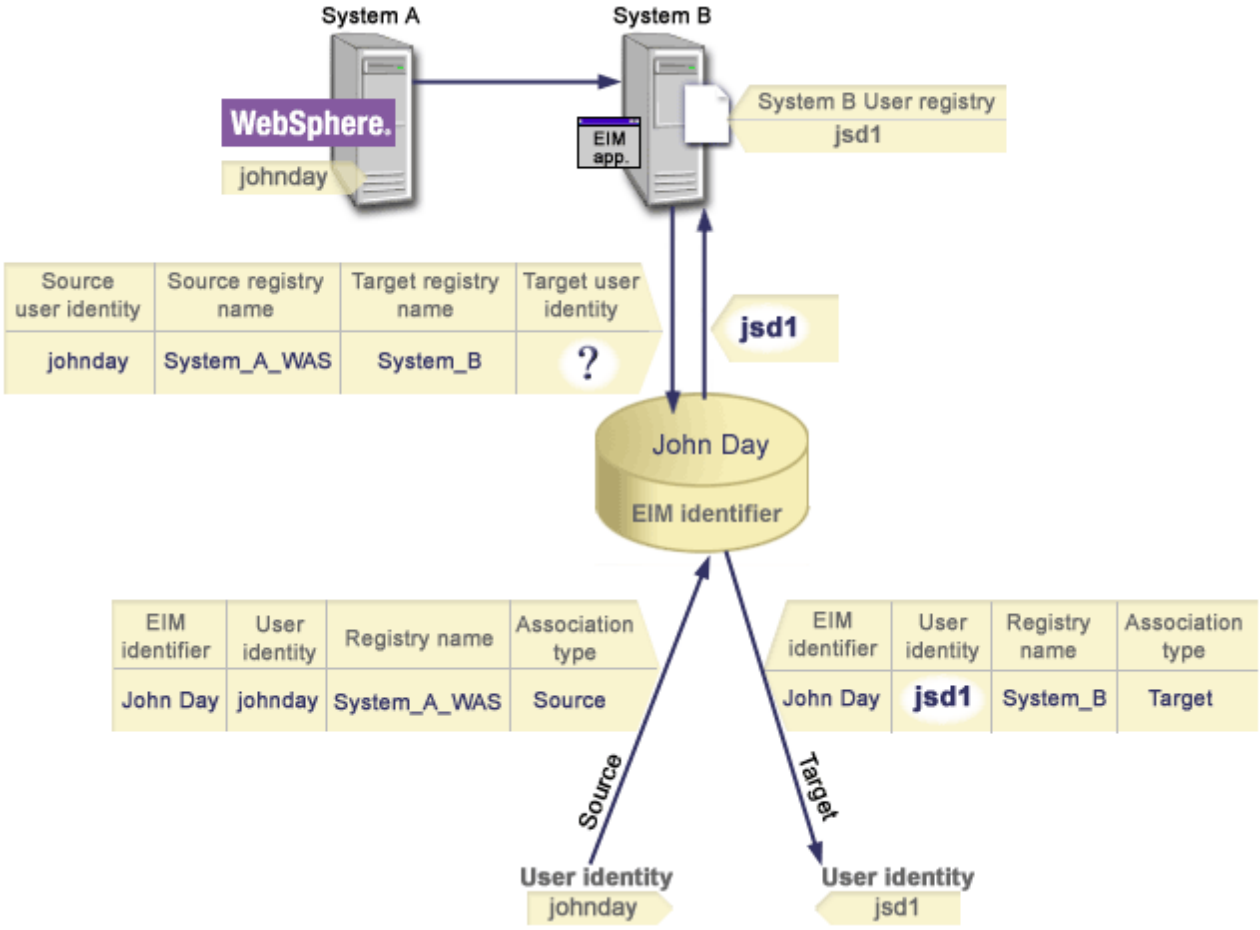
Keď aplikácia poskytne *identifikátor EIM ako zdroj* operácie prehľadania EIM, aplikácia tiež musí poskytnúť názov definície registra EIM, ktorý je cieľom operácie prehľadania EIM. Aby sa dala identita užívateľa vrátiť ako cieľ ľubovoľného typu operácie prehľadania EIM, pre danú identitu užívateľa musí byť definované cieľové priradenie.

Poskytnuté informácie sa odovzdajú do radiča domény EIM, kde sú uložené všetky informácie EIM a operácia prehľadania EIM nájde zdrojové priradenie, ktoré vyhovuje poskytnutým informáciám. Na základe identifikátora EIM (poskytnutého do API, alebo určeného z informácií zdrojového priradenia) operácia prehľadania EIM potom pohľadá cieľové priradenie pre daný identifikátor, ktorý vyhovuje cieľovému názvu definície registra EIM.

Na Obrázku 10 sa identita užívateľa johnday autentifikuje aplikačnému serveru Websphere pomocou LPTA (Lightweight Third-Party Authentication) na System A. Aplikačný server Websphere na System A zavolá

natívny program na System B, aby pristúpil k údajom na System B. Tento natívny program použije API EIM na vykonanie operácie prehľadania EIM, založenej na identite užívateľa na System A ako zdroji 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 sa odovzdajú do radiča domény EIM a operácia prehľadania EIM pohľadá zdrojové priradenie, ktoré vyhovuje týmto informáciám. Pomocou názvu identifikátora EIM operácia prehľadania EIM pohľadá cieľové priradenie pre identifikátor John Day, ktorý vyhovuje cieľovému názvu definície registra EIM pre System_B. Keď sa nájde vyhovujúce cieľové priradenie, operácia prehľadania EIM vráti aplikácii identitu užívateľa jsd1.

Obrázok 10: Operácia prehľadania EIM, založená na známej identite užívateľa johnday



Oprávnenia EIM

Oprávnenia EIM umožňujú užívateľovi vykonávať špecifické administratívne úlohy alebo operácie prehľadania EIM. Udeľovať alebo odoberať oprávnenia pre iných užívateľov môžu len užívatelia s oprávnením administrátora EIM. Oprávnenia EIM sa udeľujú len identitám užívateľov, ktoré sú známe radiču domény EIM.

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

- **Administrátor LDAP (Lightweight Directory Access Protocol).** Toto oprávnenie umožňuje užívateľovi nakonfigurovať novú doménu EIM. Užívateľ s týmto oprávnením môže vykonať tieto funkcie:
  - Vytvoriť doménu

  - Vymazať doménu
  - Vytvoriť a odstrániť identifikátory EIM
  - Vytvoriť a odstrániť definíciu registra EIM
  - Vytvoriť a odstrániť zdrojové, cieľové a administratívne priradenia
  - Vykonať operácie prehľadania EIM
  - Opakovane získať priradenia, identifikátory EIM a definície registrov EIM
  - Pridať, odstrániť a zobraziť informácie o oprávnení EIM
- **Administrátor EIM.** Toto oprávnenie umožňuje užívateľovi manažovať všetky údaje EIM v tejto doméne EIM. Užívateľ s týmto oprávnením môže vykonať tieto funkcie:
  - Vymazať doménu
  - Vytvoriť a odstrániť identifikátory EIM
  - Vytvoriť a odstrániť definíciu registra EIM
  - Vytvoriť a odstrániť zdrojové, cieľové a administratívne priradenia
  - Vykonať operácie prehľadania EIM
  - Opakovane získať priradenia, identifikátory EIM a definície registrov EIM
  - Pridať, odstrániť a zobraziť informácie o oprávnení EIM
- **Administrátor identifikátorov EIM.** Toto oprávnenie umožňuje užívateľovi pridávať a meniť identifikátory EIM a manažovať zdrojové a administratívne priradenia. Užívateľ s týmto oprávnením môže vykonať tieto funkcie:
  - Vytvoriť identifikátor EIM
  - Pridať a odstrániť zdrojové priradenia
  - Pridať a odstrániť administratívne priradenia
  - Vykonať operácie prehľadania EIM
  - Opakovane získať priradenia, identifikátory EIM a definície registrov EIM
- **Vyhľadávanie mapovaní EIM.** Toto oprávnenie umožňuje užívateľovi vykonávať operácie prehľadania EIM. Užívateľ s týmto oprávnením môže vykonať tieto funkcie:
  - Vykonať operácie prehľadania EIM
  - Opakovane získať priradenia, identifikátory EIM a definície registrov EIM
- **Administrátor registrov EIM.** Toto oprávnenie umožňuje užívateľovi manažovať všetky definície registrov EIM. Užívateľ s týmto oprávnením môže vykonať tieto funkcie:
  - Pridať a odstrániť cieľové priradenia
  - Vykonať operácie prehľadania EIM
  - Opakovane získať priradenia, identifikátory EIM a definície registrov EIM
- **X administrátor registra EIM.** Toto oprávnenie umožňuje užívateľovi manažovať špecifickú definíciu registra EIM. Toto oprávnenie umožňuje užívateľovi:
  - Pridať a odstrániť cieľové priradenia pre definíciu registra EIM
  - Vykonať operácie prehľadania EIM
  - Opakovane získať priradenia, identifikátory EIM a definície registrov EIM

Každá z nasledujúcich tabuliek je zorganizovaná podľa úlohy EIM, ktorú vykonáva dané API. Každá tabuľka zobrazuje každé API EIM, rôzne oprávnenia EIM a prístup, aký má každé z týchto oprávnení k určitým funkciám EIM.

Tabuľka 1: Práca s doménami

API EIM	Administrátor LDAP	Administrátor EIM	Administrátor identifikátorov EIM	Vyhľadávanie mapovania EIM	Administrátor registrov EIM	X administrátor registrov EIM
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	Vyhľadávanie mapovania 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	-	-	-	-

Tabuľka 3: Práca s registrami

API EIM	Administrátor LDAP	Administrátor EIM	Administrátor identifikátorov EIM	Vyhľadávanie mapovania EIM	Administrátor registrov EIM	X administrátor registrov EIM
eimAddApplicationRegistry	X	X	-	-	-	-
eimAddSystemRegistry	X	X	-	-	-	-
eimChangeRegistry	X	X	-	-	X	X
eimChangeRegistryUser	X	X	-	-	X	X
eimChgRegistryAlias	X	X	-	-	X	X
eimGetRegistryFromAlias	X	X	X	X	X	X
eimListRegistries	X	X	X	X	X	X
eimListRegistryAliases	X	X	X	X	X	X
eimListRegistryUsers	X	X	X	X	X	X
eimRemoveRegistry	X	X	-	-	-	-

Tabuľka 4: Práca s priradeniami

Pre API eimAddAssociation() a eimRemoveAssociation() existujú štyri parametre určujúce 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	Vyhľadávanie mapovania EIM	Administrátor registrov EIM	X administrátor registrov EIM
eimAddAssociation (administratívne)	X	X	X	-	-	-
eimAddAssociation (zdrojové)	X	X	X	-	-	-
eimAddAssociation (zdrojové a cieľové)	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 (zdrojové a cieľové)	X	X	X	-	X	X
eimRemoveAssociation (cieľové)	X	X	-	-	X	X

Tabuľka 5: Práca s mapovaniami

API EIM	Administrátor LDAP	Administrátor EIM	Administrátor identifikátorov EIM	Vyhľadávanie mapovania 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 6: Práca s prístupom

API EIM	Administrátor LDAP	Administrátor EIM	Administrátor identifikátorov EIM	Vyhľadávanie mapovania EIM	Administrátor registrov EIM	X administrátor registrov EIM
eimAddAccess	X	X	-	-	-	-
eimListAccess	X	X	-	-	-	-
eimListUserAccess	X	X	-	-	-	-
eimQueryAccess	X	X	-	-	-	-
eimRemoveAccess	X	X	-	-	-	-

Koncepty LDAP pre EIM

Enterprise Identity Mapping (EIM) používa server LDAP (Lightweight Directory Access Protocol) ako radič domény EIM na ukladanie údajov EIM. Rozlišovacie názvy LDAP môžete použiť pri konfigurácii EIM pre váš server iSeries a ako prostriedok na autentifikáciu pre radič domény EIM.

Ak chcete použiť rozlišovacie názvy EIM pri konfigurácii a administrácii EIM, mali by ste byť oboznámený s týmito konceptmi LDAP:

- Rozlišovací názov LDAP
- Rodičovský rozlišovací názov LDAP

Rozlišovací názov LDAP

Rozlišovací názov (DN) LDAP je položka LDAP (Lightweight Directory Access Protocol), ktorá identifikuje a opisuje autorizovaného užívateľa pre server LDAP. Pomocou Sprievodcu konfiguráciou EIM môžete nakonfigurovať server LDAP na ukladanie informácií o doméne EIM. Rozlišovacie názvy LDAP môžete použiť ako spôsob pre prístup a získavanie týchto údajov EIM, aby váš server iSeries mohol byť súčasťou prostredia s jednorazovým prihlásením.

Rozlišovacie názvy obsahujú názov samotnej entity a názvy objektov nad ňou v adresári LDAP (v poradí odspodu nahor). Príkladom úplného rozlišovacieho názvu LDAP by mohlo byť 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 LDAP. V tomto príklade cn=Tim Jones pomenúva položku, preto je RDN. o=IBM, c=US je rodičovské DN pre cn=Tim Jones. Pozrite si tému Rodičovský rozlišovací názov LDAP, kde nájdete informácie o použití v EIM.

Pretože EIM používa server LDAP na ukladanie údajov EIM, rozlišovacie názvy LDAP môžete použiť ako prostriedok na autentifikáciu pre radič domény EIM. Rozlišovacie názvy LDAP tiež môžete použiť pri konfigurácii EIM pre váš server iSeries. Rozlišovacie názvy môžete použiť napríklad vtedy, keď:

- Konfigurujete server LDAP ako radič domény EIM. Spravíte to vytvorením a použitím rozlišovacieho názvu LDAP, ktorý identifikuje administrátora LDAP pre daný server LDAP. Ak server LDAP ešte nebol nakonfigurovaný, môžete ho nakonfigurovať pomocou Sprievodcu konfiguráciou EIM, ak ho používate na vytvorenie a pripojenie k novej doméne.
- 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 LDAP musí reprezentovať užívateľa, ktorý je autorizovaný vytvárať objekty v lokálnom názvovom priestore servera LDAP.
- Používate Sprievodcu konfiguráciou EIM na výber typu užívateľa na vykonávanie operácií EIM v mene funkcií operačného systému. K takýmto operáciám patrí vyhľadávanie mapovania a vymazávanie priradení pri vymazávaní lokálneho užívateľského profilu OS/400. Rozlišovací názov je jeden z typov užívateľov, ktorý môžete vybrať.
- Pripájate sa k radiču domény kvôli administrácii EIM, napríklad kvôli manažovaniu registrov a identifikátorov a vykonaniu operácií vyhľadávania mapovaní.

Ak sa chcete dozvedieť viac o rozlišovacích názvoch a spôsobe, akým ich používa LDAP, pozrite si dokument Základy LDAP.

Rodičovský rozlišovací názov LDAP

Rodičovský rozlišovací názov (DN) LDAP 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 v prípade, ak to je DN na najvyššej úrovni názvového priestoru servera LDAP.

Príkladom úplného rozlišovacieho názvu LDAP by mohlo byť 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.

Pretože EIM používa server LDAP na ukladanie údajov EIM, rozlišovacie názvy LDAP môžete použiť ako prostriedok na autentifikáciu pre radič domény EIM. Rozlišovacie názvy LDAP a rodičovské rozlišovacie

názvy môžete použiť pri konfigurácii EIM pre váš server iSeries. Napríklad, keď používate Sprievodcu konfiguráciou EIM na vytvorenie a pripojenie k novej doméne, môžete zadať rodičovské DN pre vami vytváranú doménu. Pomocou rodičovského DN môžete zadať miesto v lokálnom názvovom priestore LDAP, kam sa majú uložiť údaje EIM pre danú doménu. Ak nezadáte rodičovské DN, údaje EIM sa uložia do vlastnej prípony v názvovom priestore.

Ak sa chcete dozvedieť viac o rozlišovacích názvoch a spôsobe ich použitia, pozrite si dokument Základy LDAP.

Povolenie jednorazového prihlásenia cez EIM

EIM poskytuje nenákladný mechanizmus pre povolenie jednorazového prihlásenia v podniku. Implementácia OS/400 pre EIM a Kerberos poskytuje skutočné viacvrstvové, heterogénne prostredie s jednorazovým prihlásením. Keď je v podniku dostupné jednorazové prihlásenie, pre užívateľov, administrátorov a vývojárov aplikácií to má tieto výhody:

Výhody pre užívateľov
V prostredí s jednorazovým prihlásením sa autentifikácia vykonáva pri každom pokuse užívateľa o prístup k novému systému; užívatelia však nebudú požiadaní o zadanie hesla. EIM odstraňuje potrebu, aby si užívatelia museli pamätať a manažovať viac mien užívateľov a hesiel pre prístup k iným systémom v sieti. Keď je užívateľ raz autentifikovaný pre sieť, môže pristupovať k službám a aplikáciám v podniku bez potreby viacerých hesiel pre tieto iné systémy.

Výhody pre administrátorov
Pre administrátora jednorazové prihlásenie zjednodušuje celý manažment bezpečnosti podniku. Bez jednorazového prihlásenia mohli užívatelia a aplikácie ukladať heslá na rôzne systémy, ktoré mohli kompromitovať bezpečnosť celej siete. Administrátori spotrebovali veľa času a peňazí hľadaním riešení odstraňujúcich tieto bezpečnostné riziká. Jednorazové prihlásenie znižuje réžiu administrátora pri manažovaní autentifikácie a robí celú sieť bezpečnou. Okrem toho, jednorazové prihlásenie redukuje administratívne náklady na prestavovanie zabudnutých hesiel.

Výhody pre vývojárov aplikácií
Pre vývojárov aplikácií, ktoré sa musia používať v heterogénnych sieťach, EIM poskytuje infraštruktúru pre vývoj aplikácií fungujúcich na rôznych platformách. Použitím rozhraní API EIM môžu programátori písať aplikácie, ktoré používajú najvhodnejší existujúci register užívateľov pre autentifikáciu a zároveň používajú iný register užívateľov pre autorizáciu. Vývojári aplikácií nemusia vo svojich aplikáciách podporovať registre užívateľov, špecifické pre platformu, pretože EIM poskytuje infraštruktúru na vytváranie aplikácií, ktoré mapujú identity užívateľov z týchto registrov užívateľov na jeden identifikátor EIM. Okrem toho, EIM umožňuje programátorom udržiavať tieto aplikácie bez zmeny súvisiacich bezpečnostných sémantík a bezpečnosť na úrovni aplikácií výrazne znižuje cenu implementácie viacvrstvových, multiplatformových aplikácií.

Povolenie jednorazového prihlásenia v iSeries
Na povolenie prostredia s jednorazovým prihlásením používa IBM dve navzájom sa dopĺňajúce technológie: EIM a službu sieťovej autentifikácie, ktorá je implementáciou Kerberosu a rozhraní API GSS od IBM. Nakonfigurovaním týchto dvoch technológií môže administrátor povoliť prostredie s jednorazovým prihlásením. Windows 2000, XP, AIX a zSeries používajú na autentifikáciu užívateľov do siete protokol Kerberos. Kerberos zahŕňa použitie sieťového, bezpečného distribučného centra kľúčov, ktoré autentifikuje principálov (užívatelia Kerberosu) do siete. Užívateľ prijme lístok Kerberosu od centralizovaného distribučného centra kľúčov. Tento lístok autentifikuje užívateľa na prístup k iným službám v podniku. Lístok môže prejsť od užívateľa do služby, ktorá akceptuje lístky. Služba akceptujúca lístky ich používa na určenie za koho sa prehlasuje užívateľ (v registri užívateľov Kerberos a realme), a že je naozaj ten, za koho sa prehlasuje.

Kým služba sieťovej autentifikácie umožňuje serveru iSeries byť súčasťou realmu Kerberos, EIM poskytuje mechanizmus pre priradenie týchto principálov Kerberos k jednému identifikátoru EIM, ktorý reprezentuje

užívateľa v celom podniku. Iné identity užívateľov, napríklad meno užívateľa OS/400, sa tiež môžu priradiť k tomuto identifikátoru EIM. Na základe týchto priradení poskytuje EIM mechanizmus pre OS/400 a aplikácie na určenie, či užívateľský profil OS/400 reprezentuje osobu alebo entitu reprezentovanú princípálom Kerberos. Informácie v EIM môžete považovať za strom, ktorého koreň je identifikátor EIM a listy sú identity užívateľov, priradené k identifikátoru EIM ako vetvy.

Pomocou obrázka dole si predstavte, že užívateľ (napríklad John Smith) sa prihlási do siete cez jeho PC s Windows a použije inštanciu OS/400, aby mal prístup k aplikáciám podporujúcim Kerberos. John nie je požiadaný o zadanie jeho mena užívateľa OS/400. Tieto aplikácie môžu vyhľadať priradenie k Johnovmu identifikátoru EIM a nájsť tak meno užívateľa OS/400. John Smith vo svojom užívateľskom profile OS/400 nepotrebuje heslo, pretože tento užívateľský profil sa už nepoužíva na autentifikáciu; používa sa len na autorizáciu.

Obrázok 1. Prostredie s jednorazovým prihlásením

Téma Scenár: Povolenie jednorazového prihlásenia poskytuje príklad, ako administrátor nakonfiguruje službu sieťovej autentifikácie a EIM, aby povolil prostredie s jednorazovým prihlásením.

Pomocou jednorazového prihlásenia je možné pristúpiť k týmto aplikáciám:

- iSeries Navigator
- PC5250 Emulator

- Distributed Relational Database Architecture (TM)(DRDA)(R)
- NetServer
- QFileSvr.400

Plán pre EIM

EIM na serveri iSeries zahŕňa viacero technológií a služieb. Pred nakonfigurovaním EIM na vašom serveri by ste mali vybrať funkčnosť, ktorú chcete implementovať pomocou EIM a jednorazového 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 použití služby sieťovej autentifikácie poskytuje EIM pre váš podnik možnosť jednorazového prihlásenia.

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

Plánovací pracovný list	Odpovede
Je váš OS/400 V5R2 (5722-SS1) alebo novší?	
Je na vašich serveroch iSeries nainštalovaný produkt Cryptographic Access Provider (5722-AC3)?	
Je na príslušných osobných počítačoch vo vašej sieti (počítače používané na prácu so servermi iSeries) a na vašich serveroch iSeries nainštalovaný produkt iSeries Access for Windows (5722-XE1)?	
Je na všetkých osobných počítačoch vo vašej sieti a na vašich systémoch iSeries nainštalovaný podkomponent Sieť?	
Ak je aktuálne nakonfigurovaný server LDAP a chcete ho použiť ako radič domény EIM, poznáte rozlišovací názov (DN) a heslo administrátora LDAP?	
Ak je aktuálne nakonfigurovaný server LDAP, môže sa dočasne zastaviť? (Bude to potrebné kvôli dokončeniu procesu konfigurácie EIM.)	
Máte špeciálne oprávnenia *SECADM, *ALLOBJ a *IOSYSCFG?	
Aplikovali ste najnovšie dočasné opravy programu (PTF)?	

Ak plánujete používať Kerberos na autentifikáciu užívateľov, mali by ste tiež nakonfigurovať službu sieťovej autentifikácie. Pozrite si dokument Plánovanie služby sieťovej autentifikácie, kde nájdete pracovný list pre plánovanie služby sieťovej autentifikácie.

Ak konfigurujete službu sieťovej autentifikácie a EIM, aby ste povolili jednorazové prihlásenie, pozrite si dokument Scenár: Povolenie jednorazového prihlásenia, ktorý vysvetľuje, ako nakonfigurovať podnik na použitie oboch týchto produktov.

Inštalovať vyžadované voľby programu iSeries Navigator

Aby ste povolili prostredie s jednorazovým prihlásením s EIM a službou sieťovej autentifikácie, musíte najprv nainštalovať obe potrebné voľby programu iSeries Navigator, Sieť a Bezpečnosť. EIM sa nachádza vo voľbe Sieť a služba sieťovej autentifikácie vo voľbe Bezpečnosť. Ak vo vašej sieti neplánujete používať službu sieťovej autentifikácie, nemusíte inštalovať voľbu Bezpečnosť programu iSeries Navigator.

Aby ste nainštalovali voľbu Sieť programu iSeries Navigator, alebo aby ste skontrolovali, či je aktuálne nainštalovaná, skontrolujte, že na PC, ktoré používate na prácu so serverom iSeries je nainštalovaný produkt iSeries Access for Windows.

Aby ste nainštalovali voľbu Sieť:

1. Kliknite na **Start —> Programs —> IBM iSeries Access for Windows —> Selektívne nastavenie**.

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 zvyškom Selektívneho nastavenia.

Konfigurovať službu sieťovej autentifikácie

Služba sieťovej autentifikácie vám umožňuje používať autentifikáciu Kerberosom na vašom serveri iSeries. Táto služba nie je nutná pre používanie EIM na vašom serveri; autentifikácia Kerberosom však poskytuje mnohé výhody pre bezpečnosť vo vašej sieti.

Služba sieťovej autentifikácie, ak sa používa v spojení s EIM, vám poskytuje prostriedky na povolenie prostredia s jednorazovým prihlásením. Prostredie s jednorazovým prihlásením je výhodné pre užívateľov aj administrátorov. Užívatelia musia manažovať menej mien užívateľov a hesiel, administrátori musia uchovávať menej informácií pre každého užívateľa. Povolenie prostredia s jednorazovým prihlásením tiež pomáha premostiť medzeru medzi viacerými platformami a odlišnými systémami, ktoré môžu byť vo vašej sieti, preto sa môžu zredukovať náklady na vývoj aplikácií a všeobecnú administráciu.

Ak aktuálne nemáte nakonfigurovanú službu sieťovej autentifikácie na vašom serveri iSeries alebo na všetkých serveroch vo vašej sieti, pozrite si dokument Plán pre službu sieťovej autentifikácie, kde nájdete informácie o plánovaní, ktoré vám pomôžu začať s konfiguráciou. Ak ste oboznámený so službou sieťovej autentifikácie, pozrite si dokument Konfigurovať službu sieťovej autentifikácie, ktorý vám pomôže začať proces konfigurácie.

Konfigurovať EIM

Aby ste povolili prostredie s jednorazovým prihlásením vo viacerých platformách bez potreby meniť nižšie bezpečnostné politiky, musíte nakonfigurovať EIM a zároveň aj službu sieťovej autentifikácie. Konfigurácia a používanie služby sieťovej autentifikácie však nie je nevyhnutné a povinné pre konfiguráciu a používanie EIM.

Aby ste spustili proces konfigurácie EIM pre server iSeries, aby sa stal súčasťou prostredia s jednorazovým prihlásením, použite Sprievodcu konfiguráciou EIM. Podľa vašich požiadaviek na konfiguráciu môžete použiť sprievodcu na pripojenie k existujúcej doméne, alebo na vytvorenie a pripojenie novej domény.

Sprievodca konfiguráciou EIM vám umožňuje jednoducho vykonať základnú konfiguráciu EIM. Napríklad, ak ešte nemáte nakonfigurovaný server LDAP, alebo ste ešte nenakonfigurovali službu sieťovej autentifikácie, Sprievodca konfiguráciou EIM vám pomôže vykonať tieto úlohy.

Po použití sprievodcu na vykonanie základnej konfigurácie EIM musíte vykonať niekoľko dodatočných konfiguračných krokov, aby ste mohli používať prostredie s jednorazovým prihlasovaním. Pozrite si dokument Scenár: Povolenie jednorazového prihlásenia, kde nájdete príklad, ako fiktívna spoločnosť nakonfigurovala prostredie s jednorazovým prihlásením, využívajúce službu sieťovej autentifikácie a EIM.

Pred použitím Sprievodcu konfiguráciou EIM by ste mali dokončiť všetky kroky plánovania na určenie presného spôsobu, akým použijete EIM a službu sieťovej autentifikácie pri povoľovaní prostredia s jednorazovým prihlásením. Po dokončení plánovania môžete použiť sprievodcu na nakonfigurovanie EIM pre váš server iSeries jedným z dvoch spôsobov: vytvoriť nové domény, alebo sa pripojiť k existujúcim doménam. Informácie ku konfigurácii EIM sú v nasledujúcich témach:

Vytvoriť a pripojiť k novej doméne
Vyberte túto úlohu, ak chcete vytvoriť doménu EIM pre vašu sieť a nakonfigurovať server iSeries tak, aby bol jej súčasťou. Sprievodca vytvorí novú doménu a nakonfiguruje lokálny server LDAP tak, aby bol radičom domény EIM pre túto novú doménu. Ak na serveri iSeries aktuálne nie je povolený Kerberos, sprievodca vás vyzve na spustenie Sprievodcu konfiguráciou služby sieťovej autentifikácie. Po dokončení tejto úlohy môžete nakonfigurovať ďalšie servery iSeries, aby boli súčasťou domény. Aby

ste nakonfigurovali ďalšie servery iSeries ako súčasť domény, pripojte sa ku každému z nich a pomocou Sprievodcu konfiguráciou EIM nakonfigurujte server na pripojenie sa k existujúcej doméne.

Pripojiť k existujúcej doméne
Keď použijete Sprievodcu konfiguráciou EIM na nakonfigurovanie radiča domény a domény EIM, vyberte túto úlohu, aby ste nakonfigurovali ďalšie servery iSeries ako súčasť domény. Túto úlohu musíte vykonať pre každý server iSeries v sieti, ktorý bude používať EIM. Po dokončení sprievodcu musíte zadať informácie o doméne, ku ktorej sa pripája, vrátane informácií o pripojení (ako je číslo portu a či sa má použiť TLS (Transport Layer Security)/SSL (Secure Sockets Layer)) k radiču domény EIM). Ak na serveri iSeries aktuálne nie je povolený Kerberos, sprievodca vás vyzve na spustenie Sprievodcu konfiguráciou služby sieťovej autentifikácie.

Ako spustiť Sprievodcu konfiguráciou EIM

Aby ste spustili Sprievodcu konfiguráciou EIM, vykonajte tieto kroky:

1. Spustite iSeries Navigator.
2. Prihláste sa do servera iSeries, pre ktorý chcete nakonfigurovať EIM.
   Ak konfigurujete EIM pre viac ako jeden server iSeries, začnite s tým, na 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 voľbu **Pripojiť k existujúcej doméne** alebo **Vytvoriť a pripojiť k novej doméne**.

Po dokončení Sprievodcu konfiguráciou EIM a vytvorení radiča domény a nakonfigurovaní vašich serverov iSeries ako súčasť domény musíte vykonať tieto kroky, aby ste dokončili konfiguráciu EIM:

1. Pridať registre EIM do domény EIM pre servery iné ako iSeries a aplikácie, ktoré majú byť súčasťou domény EIM.
2. Vytvoriť identifikátory EIM v doméne pre každého jedinečného užívateľa alebo entitu pre systémy, ktoré sú súčasťou domény EIM.
3. Vytvoriť priradenia medzi rôznymi identitami užívateľov pre osobu alebo entitu a týmito identifikátormi EIM.

Vytvoriť a pripojiť k novej doméne

Sprievodcu konfiguráciou EIM môžete použiť na konfiguráciu servera LDAP na serveri iSeries, aby bol radičom domény EIM pre novú doménu. Ak to je potrebné, Sprievodca konfiguráciou EIM zaistí, aby ste zadali základné konfiguračné informácie pre server LDAP.

Ak na serveri iSeries aktuálne nie je povolený Kerberos, sprievodca vás vyzve na spustenie Sprievodcu konfiguráciou služby sieťovej autentifikácie. Po dokončení tohto sprievodcu bude nová doména EIM nakonfigurovaná, váš systém iSeries bude nakonfigurovaný na pripojenie k tejto novej doméne a vami zadané registre užívateľov budú pridané do domény.

Aby ste mohli použiť sprievodcu na vykonanie tejto úlohy, musíte mať špeciálne oprávnenia *SECADM (Security Administrator), *ALLOBJ (All Object) a *IOSYSCFG (System Configuration).

Aby ste spustili a použili Sprievodcu konfiguráciou EIM na vytvorenie a pripojenie k novej doméne EIM, vykonajte tieto kroky pomocou programu iSeries Navigator:

Poznámka: Tento sprievodca tiež nakonfiguruje lokálny server LDAP ako nový radič domény EIM.

1. Rozviňte **Sieť** —> **Enterprise Identity Mapping**.

2. Pravým tlačidlom myši kliknite na **Konfigurácia** a vyberte **Konfigurovať...**, aby sa spustil Sprievodca konfiguráciou EIM.
3. Na strane sprievodcu **Vitajte** vyberte **Vytvoriť a pripojiť k novej doméne** a kliknite na tlačidlo **Ďalej**.
4. Ak na serveri iSeries aktuálne nie je nakonfigurovaná služba sieťovej autentifikácie, zobrazí sa dialógové okno **Konfigurácia služby sieťovej autentifikácie**. Toto dialógové okno vám umožňuje vybrať, či chcete nakonfigurovať službu sieťovej autentifikácie. Ak vyberiete **Áno**, spustí sa Sprievodca konfiguráciou služby sieťovej autentifikácie. Po dokončení konfigurácie služby sieťovej autentifikácie pokračujete ďalej v Sprievodcovi konfiguráciou EIM.
5. Ak lokálny server LDAP nie je aktuálne nakonfigurovaný, zobrazí sa dialógové okno **Konfigurácia adresárového servera**. Aby ste nakonfigurovali lokálny server LDAP, v dialógovom okne zadajte tieto informácie:
   - V poli **Port** akceptujte predvolené číslo portu **389**, alebo zadajte iné číslo portu, ktorý sa použije pre nezabezpečenú komunikáciu EIM s adresárovým serverom.
   - V poli **Rozlišovací názov** zadajte rozlišovací názov (DN) LDAP, ktorý identifikuje administrátora LDAP pre server LDAP. Sprievodca konfiguráciou EIM vytvorí toto DN administrátora LDAP a použije ho pri konfigurácii servera LDAP ako radiča domény pre vami vytváranú doménu.
   - V poli **Heslo** zadajte heslo pre administrátora LDAP.
   - V poli **Potvrdenie hesla** znovu zadajte heslo.
   - Kliknite na tlačidlo **Ďalej**.
6. V dialógovom okne **Zadanie radiča 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 použiť špeciálne znaky ako sú = + < > , # ; \ a *.
   - V poli **Opis** zadajte opisný text domény.
   - Kliknite na tlačidlo **Ďalej**.
7. V dialógovom okne **Zadanie rodičovského DN domény** vyberte, či chcete zadať rodičovské DN pre vami vytváranú doménu. 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.
8. V dialógovom okne **Zadanie užívateľa pre pripojenie** vyberte **typ užívateľa** pre pripojenie. Môžete vybrať jeden z týchto typov užívateľov: Rozlišovací názov a heslo, Súbor kľúčov Kerberos a principál alebo Principál Kerberos a heslo. Dva typy užívateľov Kerberos sú k dispozícii len v prípade, ak je pre lokálny systém iSeries nakonfigurovaná služba sieťovej autentifikácie. Vami vybratý typ užívateľa určuje ostatné informácie, ktoré musíte poskytnúť v tomto dialógovom okne:
   - Ak vyberiete **Rozlišovací názov a heslo**, zadajte tieto informácie:
     - V poli **Rozlišovací názov** zadajte rozlišovací názov (DN) LDAP, ktorý identifikuje užívateľa oprávneného vytvárať objekty v lokálnom názvovom priestore servera LDAP. Ak ste použili tohto sprievodcu na nakonfigurovanie servera LDAP v predchádzajúcom kroku, mali by ste zadať rozlišovací názov administrátora LDAP, ktorý ste vytvorili v danom kroku.
     - V poli **Heslo** zadajte heslo pre daného užívateľa.
     - V poli **Potvrdenie hesla** znovu zadajte heslo.
   - Ak vyberiete **Súbor kľúčov Kerberos a principál**, zadajte tieto informácie:
     - V poli **Súbor kľúčov** zadajte názov súboru kľúčov na serveri iSeries, ktorý identifikuje užívateľa oprávneného vytvárať objekty v lokálnom názvovom priestore servera LDAP. Môžete tiež kliknúť na tlačidlo **Prehľadať** a vybrať súbor kľúčov.
     - V poli **Principál** zadajte názov principálu Kerberos, ktorý sa použije na identifikáciu užívateľa.

- V poli **Realm** zadajte názov realmu Kerberos pre daný principál. Názov principálu a realmu jedinečne identifikujú užívateľov Kerberosu v súbore kľúčov. Napríklad principál jsmith v realme ordept.myco.com je v súbore kľúčov reprezentovaný ako jsmith@ordept.myco.com.

- Ak vyberiete **Principál Kerberos a heslo**, zadajte tieto informácie:
  - V poli **Principál** zadajte názov principálu Kerberos, ktorý identifikuje užívateľa oprávneného vytvárať objekty v lokálnom názvovom priestore servera LDAP.
  - V poli **Realm** zadajte názov realmu Kerberos pre daný principál.
  - V poli **Heslo** zadajte heslo pre daného užívateľa.
  - V poli **Potvrdenie hesla** znovu zadajte heslo. Názov principálu a realmu jedinečne identifikujú užívateľov Kerberosu v súbore kľúčov. Napríklad principál jsmith v realme ordept.myco.com je v súbore kľúčov reprezentovaný ako jsmith@ordept.myco.com.
- Kliknite na tlačidlo **Skontrolovať pripojenie**, aby ste otestovali konfiguračné informácie vášho užívateľa pre pripojenie k radiču domény.
- Kliknite na tlačidlo **Ďalej**.

9. V dialógovom okne **Informácie o registri** vyberte typ registrov užívateľov, ktoré chcete pridať do domény EIM. Vyberte jeden alebo oba tieto typy registrov užívateľov:
   - Vyberte **OS400**, ak chcete do domény EIM pridať register užívateľov reprezentujúci lokálny register. V poskytnutom poli zadajte názov registra na vytvorenie v doméne. Názov registra EIM je ľubovoľný reťazec reprezentujúci typ registra a špecifickú inštanciu tohto registra.
   - Vyberte **Kerberos**, ak chcete do domény EIM pridať register užívateľov Kerberos. V poskytnutom poli zadajte názov registra na vytvorenie v doméne a podľa potreby začiarknite **Identity užívateľov Kerberos zohľadňujú veľkosť písmen**.
   - Kliknite na tlačidlo **Ďalej**.
10. V dialógovom okne **Zadanie systémového užívateľa EIM** vyberte typ užívateľa, ktorý má použiť systém pri vykonávaní operácií EIM v mene funkcií operačného systému. K takýmto operáciám patrí vyhľadávanie mapovania a vymazávanie priradení pri vymazávaní lokálneho užívateľského profilu OS/400. Môžete vybrať jeden z týchto typov užívateľov: Rozlišovací názov a heslo, Súbor kľúčov Kerberos a principál alebo Principál Kerberos a heslo. Vami vybratý typ užívateľa určuje ostatné informácie, ktoré musíte poskytnúť v tomto dialógovom okne:

Poznámka: Vami zadaný užívateľ musí mať privilégiá minimálne na vykonanie vyhľadania mapovania a administráciu registra pre lokálny register užívateľov. Ak vami zadaný užívateľ nemá tieto privilégiá, niektoré funkcie operačného systému, súvisiace s jednorazovým prihlásením a vymazávaním užívateľských profilov môžu zlyhať.

11. Ak vyberiete **Rozlišovací názov a heslo**, zadajte tieto informácie:
    - V poli **Rozlišovací názov** zadajte rozlišovací názov LDAP, identifikujúci užívateľa, ktorého má OS/400 použiť pri kontaktovaní radiča domény EIM.
    - V poli **Heslo** zadajte heslo pre daného užívateľa.
    - V poli **Potvrdenie hesla** znovu zadajte heslo.
12. Ak vyberiete **Principál Kerberos a heslo**, zadajte tieto informácie:
    - V poli **Principál** zadajte názov principálu Kerberos, identifikujúci užívateľa, ktorého má OS/4OO použiť pri kontaktovaní radiča domény EIM.
    - V poli **Realm** zadajte názov realmu Kerberos pre daný principál.
    - V poli **Heslo** zadajte heslo pre daného užívateľa.
    - V poli **Potvrdenie hesla** znovu zadajte heslo. Názov principálu a realmu jedinečne identifikujú užívateľov Kerberosu v súbore kľúčov. Napríklad principál jsmith v realme ordept.myco.com je v súbore kľúčov reprezentovaný ako jsmith@ordept.myco.com.
13. Ak vyberiete **Súbor kľúčov Kerberos a principál**, zadajte tieto informácie:

- V poli **Súbor kľúčov** zadajte názov súboru kľúčov na serveri iSeries, identifikujúci užívateľa, ktorého má OS/400 použiť pri kontaktovaní radiča domény EIM. Môžete tiež kliknúť na tlačidlo **Prehľadať** a vybrať súbor kľúčov.
- V poli **Principál** zadajte názov principálu Kerberos, ktorý sa použije na identifikáciu užívateľa.
- V poli **Realm** zadajte názov realmu Kerberos pre daný principál. Názov principálu a realmu jedinečne identifikujú užívateľov Kerberosu v súbore kľúčov. Napríklad principál jsmith v realme ordept.myco.com je v súbore kľúčov reprezentovaný ako jsmith@ordept.myco.com.

14. Kliknite na tlačidlo **Skontrolovať pripojenie**, aby ste otestovali pripojenie k radiču domény pre systémového užívateľa, ktorého ste práve vytvorili.
15. Kliknite na tlačidlo **Ďalej**.
16. Na paneli **Sumár** skontrolujte vami zadané konfiguračné informácie. Ak sú všetky informácie správne, kliknite na tlačidlo **Dokončiť**.

Po dokončení sprievodcu ste dokončili vašu základnú konfiguráciu EIM. Aby ste dokončili vašu konfiguráciu EIM pre tento server, musíte vykonať tieto úlohy:

1. Pridať doménu, ktorú ste vytvorili, do zložky Manažment domén EIM.
2. Pridať registre EIM do domény EIM pre iné servery a aplikácie, ktoré majú byť súčasťou domény EIM.
3. Vytvoriť identifikátory EIM v doméne pre každého jedinečného užívateľa alebo entitu pre systémy, ktoré sú súčasťou domény EIM.
4. Vytvoriť priradenia medzi rôznymi identitami užívateľov pre osobu alebo entitu a týmito identifikátormi EIM.

Okrem toho môžete použiť SSL (Secure Sockets Layer) alebo TLS (Transport Layer Security) na nakonfigurovanie bezpečného pripojenia k radiču domény.

Konfigurovať bezpečné pripojenie k radiču domény EIM

Keď použijete sprievodcu na vytvorenie a pripojenie k novej doméne, môžete použiť SSL (Secure Sockets Layer) alebo TLS (Transport Layer Security) na vytvorenie bezpečného pripojenia k radiču domény EIM. Aby ste nakonfigurovali SSL alebo TLS pre EIM, musíte vykonať tieto úlohy:

1. Povoliť SSL pre radič domény servera LDAP.
2. Použiť Správcu digitálnych certifikátov (DCM) na vytvorenie certifikátu, ktorý potrebuje server LDAP na používanie SSL.
3. Použiť DCM na priradenie certifikátu k serveru LDAP.
4. Zaktualizovať vlastnosti konfigurácie EIM, aby špecifikovali, že server iSeries používa bezpečné pripojenie SSL.
5. Zaktualizovať vlastnosti domény EIM pre každú doménu EIM, aby špecifikovali, že EIM používa pri manažovaní domény cez program iSeries Navigator pripojenie SSL.

Pripojiť k existujúcej doméne

Sprievodcu konfiguráciou EIM môžete použiť na pripojenie k existujúcej doméne EIM. Túto voľbu Sprievodcu konfiguráciou EIM použite v prípade, ak je už v sieti nakonfigurovaná doména EIM a radič domény. Pri prechode sprievodcom musíte zadávať informácie o doméne, vrátane informácií o pripojení k radiču domény EIM. Sprievodca uloží tieto informácie na server iSeries a potom ich použije na pripojenie k radiču domény EIM. Sprievodca tiež vytvorí register užívateľov EIM, reprezentujúci register užívateľských profilov OS/400 na tomto serveri iSeries.

Aby ste mohli použiť sprievodcu na vykonanie tejto úlohy, musíte mať špeciálne oprávnenia *SECADM (Security Administrator) a *ALLOBJ (All Object).

Aby ste spustili a použili Sprievodcu konfiguráciou EIM na pripojenie k existujúcej doméne, vykonajte tieto kroky pomocou programu iSeries Navigator:

1. Rozviňte **Sieť —> Enterprise Identity Mapping**.

2. Pravým tlačidlom myši kliknite na **Konfigurácia** a vyberte **Konfigurovať...**, aby sa spustil Sprievodca konfiguráciou EIM. Po spustení sprievodcu pri prechádzaní dialógovými oknami zadajte nasledujúce informácie.
3. V dialógovom okne **Vitajte** vyberte **Pripojiť k existujúcej doméne** a kliknite na tlačidlo **Ďalej**.
4. Ak na serveri iSeries aktuálne nie je nakonfigurovaná služba sieťovej autentifikácie, zobrazí sa dialógové okno **Konfigurácia služby sieťovej autentifikácie**. Toto dialógové okno vám umožňuje vybrať, či chcete nakonfigurovať službu sieťovej autentifikácie. Ak vyberiete **Áno**, spustí sa Sprievodca konfiguráciou služby sieťovej autentifikácie. Po dokončení konfigurácie služby sieťovej autentifikácie pokračujete ďalej v Sprievodcovi konfiguráciou EIM.
5. Keď sa zobrazí dialógové okno **Zadanie radiča domény**, poskytnite tieto informácie:
   - V poli **Názov radiča domény** zadajte názov systému, ktorý slúži ako radič domény pre doménu EIM, ku ktorej chcete pripojiť server iSeries.
   - Kliknite na **Použiť SSL (Secure Sockets Layer)**, ak chcete pri získavaní informácií EIM z radiča domény používať SSL na ochranu prenosu údajov EIM.
   - Kliknite na **Skontrolovať pripojenie**, aby ste otestovali konfiguračné informácie vášho radiča domény.

Poznámka: Ak ste vybrali použitie SSL a zobrazila sa chybová správa, môže to znamenať, že daný server LDAP nie je nakonfigurovaný na použitie SSL.

   - Kliknite na tlačidlo **Ďalej**.
6. V dialógovom okne **Zadanie užívateľa pre pripojenie** vyberte **typ užívateľa** pre pripojenie. Môžete vybrať jeden z týchto typov užívateľov: Rozlišovací názov a heslo, Súbor kľúčov Kerberos a principál alebo Principál Kerberos a heslo. Dva typy užívateľov Kerberos sú k dispozícii len v prípade, ak je pre lokálny systém iSeries nakonfigurovaná služba sieťovej autentifikácie. Vami vybratý typ užívateľa určuje ostatné informácie, ktoré musíte poskytnúť v tomto dialógovom okne:
   - Ak vyberiete **Rozlišovací názov a heslo**, zadajte tieto informácie:
     - V poli **Rozlišovací názov** zadajte rozlišovací názov (DN) LDAP, ktorý identifikuje užívateľa oprávneného vytvárať objekty v lokálnom názvovom priestore servera LDAP.
     - V poli **Heslo** zadajte heslo pre daného užívateľa.
     - V poli **Potvrdenie hesla** znovu zadajte heslo.
   - Ak vyberiete **Súbor kľúčov Kerberos a principál**, zadajte tieto informácie:
     - V poli **Súbor kľúčov** zadajte názov súboru kľúčov na serveri iSeries, ktorý identifikuje užívateľa oprávneného vytvárať objekty v lokálnom názvovom priestore servera LDAP. Môžete tiež kliknúť na tlačidlo **Prehľadať** a vybrať súbor kľúčov.
     - V poli **Principál** zadajte názov principálu Kerberos, ktorý sa použije na identifikáciu užívateľa.
     - V poli **Realm** zadajte názov realmu Kerberos pre daný principál. Názov principálu a realmu jedinečne identifikujú užívateľov Kerberosu v súbore kľúčov. Napríklad principál jsmith v realme ordept.myco.com je v súbore kľúčov reprezentovaný ako jsmith@ordept.myco.com.
   - Ak vyberiete **Principál Kerberos a heslo**, zadajte tieto informácie:
     - V poli **Principál** zadajte názov principálu Kerberos, ktorý identifikuje užívateľa oprávneného vytvárať objekty v lokálnom názvovom priestore servera LDAP.
     - V poli **Realm** zadajte názov realmu Kerberos pre daný principál.
     - V poli **Heslo** zadajte heslo pre daného užívateľa.
     - V poli **Potvrdenie hesla** znovu zadajte heslo. Názov principálu a realmu jedinečne identifikujú užívateľov Kerberosu v súbore kľúčov. Napríklad principál jsmith v realme ordept.myco.com je v súbore kľúčov reprezentovaný ako jsmith@ordept.myco.com.
   - Kliknite na tlačidlo **Skontrolovať pripojenie**, aby ste otestovali konfiguračné informácie vášho užívateľa pre pripojenie k radiču domény.
   - Kliknite na tlačidlo **Ďalej**.

7. Na strane **Zadanie domény** vyberte názov domény, do ktorej sa chcete pripojiť a kliknite na tlačidlo **Ďalej**.
8. Na strane **Informácie o registri** vyberte typ registrov užívateľov, ktoré chcete pridať do domény EIM. Vyberte jeden alebo oba tieto typy registrov užívateľov:
   - Vyberte **OS400**, ak chcete do domény EIM pridať register užívateľov reprezentujúci lokálny register. V poskytnutom poli zadajte názov registra na vytvorenie v doméne. Názov registra EIM je ľubovoľný reťazec reprezentujúci typ registra a špecifickú inštanciu tohto registra.
   - Vyberte **Kerberos**, ak chcete do domény EIM pridať register užívateľov Kerberos. V poskytnutom poli zadajte názov registra na vytvorenie v doméne a podľa potreby začiarknite **Identity užívateľov Kerberos zohľadňujú veľkosť písmen**. Môžete použiť predvolenú hodnotu; názov registra Kerberos je rovnaký ako názov realmu. Ak použijete rovnaký názov registra Kerberos ako názov realmu, môžete zvýšiť výkon pri získavaní informácií z registra. Viac informácií o spôsobe definovania registrov užívateľov v EIM nájdete v téme Definície registrov EIM.
   - Kliknite na tlačidlo **Ďalej**.
9. V dialógovom okne **Zadanie systémového užívateľa EIM** vyberte typ užívateľa, ktorý má použiť systém pri vykonávaní operácií EIM v mene funkcií operačného systému. K takýmto operáciám patrí vyhľadávanie mapovania a vymazávanie priradení pri vymazávaní lokálneho užívateľského profilu OS/400. Môžete vybrať jeden z týchto typov užívateľov: Rozlišovací názov a heslo, Súbor kľúčov Kerberos a principál alebo Principál Kerberos a heslo. Vami vybratý typ užívateľa určuje ostatné informácie, ktoré musíte poskytnúť v tomto dialógovom okne:
   - Ak vyberiete **Rozlišovací názov a heslo**, zadajte tieto informácie:
     - V poli **Rozlišovací názov** zadajte rozlišovací názov LDAP, identifikujúci užívateľa, ktorého má OS/400 použiť pri kontaktovaní radiča domény EIM.
     - V poli **Heslo** zadajte heslo pre daného užívateľa.
     - V poli **Potvrdenie hesla** znovu zadajte heslo.
   - Ak vyberiete **Principál Kerberos a heslo**, zadajte tieto informácie:
     - V poli **Principál** zadajte názov principálu Kerberos, identifikujúci užívateľa, ktorého má OS/4OO použiť pri kontaktovaní radiča domény EIM.
     - V poli **Realm** zadajte názov realmu Kerberos pre daný principál.
     - V poli **Heslo** zadajte heslo pre daného užívateľa.
     - V poli **Potvrdenie hesla** znovu zadajte heslo. Názov principálu a realmu jedinečne identifikujú užívateľov Kerberosu v súbore kľúčov. Napríklad principál jsmith v realme ordept.myco.com je v súbore kľúčov reprezentovaný ako jsmith@ordept.myco.com.
   - Ak vyberiete **Súbor kľúčov Kerberos a principál**, zadajte tieto informácie:
     - V poli **Súbor kľúčov** zadajte názov súboru kľúčov na serveri iSeries, identifikujúci užívateľa, ktorého má OS/400 použiť pri kontaktovaní radiča domény EIM. Môžete tiež kliknúť na tlačidlo **Prehľadať** a vybrať súbor kľúčov.
     - V poli **Principál** zadajte názov principálu Kerberos, ktorý sa použije na identifikáciu užívateľa.
     - V poli **Realm** zadajte názov realmu Kerberos pre daný principál.
   - Kliknite na tlačidlo **Skontrolovať pripojenie**, aby ste otestovali pripojenie pre systémového užívateľa, ktorého ste práve vytvorili.
   - Kliknite na tlačidlo **Ďalej**.
10. Na paneli **Sumár** skontrolujte vami zadané konfiguračné informácie. Ak sú všetky informácie správne, kliknite na tlačidlo **Dokončiť**.

Po dokončení sprievodcu ste dokončili vašu základnú konfiguráciu EIM. Aby ste dokončili vašu konfiguráciu EIM pre tento server, musíte vykonať tieto úlohy:

1. Pridať doménu, ku ktorej ste sa pripojili, do zložky Manažment domén EIM.
2. Pridať registre EIM do domény EIM pre servery iné ako iSeries a aplikácie, ktoré majú byť súčasťou domény EIM.

3. Vytvoriť identifikátory EIM v doméne pre každého jedinečného užívateľa alebo entitu pre systémy, ktoré sú súčasťou domény EIM.
4. Vytvoriť priradenia medzi rôznymi identitami užívateľov pre osobu alebo entitu a týmito identifikátormi EIM.

Aby ste povolili prostredie s jednorazovým prihlásením, musíte tiež nakonfigurovať službu sieťovej autentifikácie pre server iSeries.

Manažovať EIM

Po nakonfigurovaní EIM na vašom serveri iSeries môžete manažovať vašu doménu EIM a informácie pomocou množstva úloh. Nasledujúce témy opisujú špecifické úlohy použité na manažovanie EIM na vašom serveri iSeries a vo vašej podnikovej sieti.

Manažovať domény EIM
Umožňuje vám pracovať s informáciami EIM, obsiahnutými vo vašej doméne EIM a s vlastnosťami vašej domény EIM.

Manažovať priradenia
Umožňuje vám pracovať s priradeniami identít užívateľov k identifikátorom EIM pre všetkých užívateľov v podniku.

Manažovať identifikátory EIM
Umožňuje vám pracovať s identifikátormi EIM, priradenými k užívateľom v podniku.

Manažovať oprávnenia EIM pre užívateľov
Umožňuje vám riadiť bezpečnosť vašich informácií EIM pomocou oprávnení EIM na riadenie funkcií a operácií EIM, ktoré môžu vykonávať užívatelia.

Manažovať registre užívateľov
Umožňuje vám pracovať s registrami, ktoré ste pridali do vašej domény EIM.

Manažovať domény EIM

Na manažovanie všetkých vašich domén EIM môžete použiť program iSeries Navigator. Aby ste mohli manažovať ľubovoľnú doménu EIM, táto doména musí byť uvedená, alebo ju musíte pridať do zložky Manažment domén pod zložkou Sieť v programe iSeries Navigator. Po vytvorení a nakonfigurovaní novej domény EIM ju musíte pridať do zložky Manažment domén, aby ste mohli manažovať informácie v danej doméne.

Aby ste mohli manažovať doménu EIM, umiestnenú kdekoľvek v rovnakej sieti, môžete použiť ľubovoľné pripojenie iSeries. iSeries, ktorý je pripojený k programu iSeries Navigator nemusí byť súčasťou domény, aby ste ju mohli manažovať.

Vaše domény EIM môžete manažovať pomocou týchto úloh:

- Pridať doménu do Manažmentu domén
- Pripojiť k doméne
- Vymazať doménu
- Odstrániť doménu z Manažmentu domén

Pridať doménu do Manažmentu domén

Aby ste mohli pridať doménu, musíte mať špeciálne oprávnenie *SECADM. Aby ste pridali existujúcu doménu EIM do manažmentu domén, vykonajte tieto kroky.

1. Rozviňte **Sieť —> Enterprise Identity Mapping**.
2. Pravým tlačidlom myši kliknite na **Manažment domén** a vyberte **Pridať doménu...**.

3. Zadajte vyžadované informácie o doméne a pripojení.
4. Kliknite na tlačidlo **OK**, aby sa pridala doména.

Pripojiť k doméne
Ak aktuálne nie ste pripojený k doméne EIM, v ktorej chcete pracovať, musíte sa k nej najprv pripojiť. K doméne EIM sa môžete pripojiť aj v prípade, ak váš server iSeries nie je aktuálne nakonfigurovaný ako súčasť tejto domény.

Aby ste sa pripojili k doméne EIM, vykonajte tieto kroky:
1. Rozviňte **Sieť —> Enterprise Identity Mapping —> Manažment domén**.
2. Vyberte doménu, ku ktorej sa chcete pripojiť. Ak tu vami požadovaná doména nie je uvedená, musíte Pridať doménu do Manažmentu domén.
3. Pravým tlačidlom myši kliknite na doménu EIM, ku ktorej sa chcete pripojiť a vyberte **Pripojiť...**.
4. Zadajte typ užívateľa a vyžadované informácie o užívateľovi, ktoré sa majú použiť pre pripojenie k radiču domény EIM.
5. Kliknite na tlačidlo **OK**.

Vymazať doménu
Aby ste mohli vykonať túto úlohu, musíte mať oprávnenie administrátora LDAP alebo oprávnenie administrátora EIM. Aby ste mohli vymazať doménu EIM, najprv musíte odstrániť všetky registre a informácie o identifikátoroch EIM z danej domény.

Aby ste vymazali doménu, vykonajte tieto kroky.
1. Rozviňte **Sieť —> Enterprise Identity Mapping —> Manažment domén**.
2. Odstráňte všetky registre užívateľov z domény EIM.
3. Vymažte všetky identifikátory EIM z domény EIM.
4. Pravým tlačidlom myši kliknite na doménu, ktorú chcete vymazať a kliknite na tlačidlo **Vymazať...**.
5. V dialógovom okne **Potvrdenie vymazania** kliknite na tlačidlo **Áno**.

Odstrániť doménu z Manažmentu domén
Po vykonaní zmien v doméne ju môžete odstrániť zo zložky Manažment domén, ale nie je to nutné.

Aby ste odstránili doménu, vykonajte tieto kroky:
1. Rozviňte **Sieť —> Enterprise Identity Mapping**.
2. Pravým tlačidlom myši kliknite na **Manažment domén** a vyberte **Odstrániť doménu...**.
3. Vyberte doménu EIM, ktorú chcete odstrániť z manažmentu domén.
4. Kliknite na tlačidlo **OK**, aby sa odstránila doména.

Manažovať priradenia
Priradenie definuje vzťah medzi identifikátorom EIM a identitou užívateľa v registri. Napríklad môžete vytvoriť priradenie medzi užívateľským profilom OS/400 alebo princípálom Kerberosu a identifikátorom EIM. Toto priradenie sa neskôr môže použiť na určenie identifikátorov EIM, ktoré patria do lokálneho užívateľského profilu iSeries alebo princípálu Kerberosu.

Vytvorenie priradení identít užívateľov k príslušným identifikátorom EIM je kľúčom k zjednodušeniu administratívnych úloh potrebných na sledovanie užívateľov s kontami na rôznych systémov v sieti.

Manažovanie týchto priradení vám tiež umožňuje vo vašej sieti využívať jednorazové prihlásenie. Pri implementácii bezpečnej siete s jednorazovým prihlásením musíte priradenia udržiavať aktuálnymi.

Môžete vytvoriť tri typy priradení: zdrojové, cieľové a administratívne. Aby ste mohli vytvoriť alebo upraviť priradenia medzi identitami užívateľov a príslušnými identifikátormi EIM, môžete vykonať jednu z týchto úloh:

- Vytvoriť priradenie
- Vymazať priradenie

Vytvoriť priradenie

Aby ste povolili prostredie s jednorazovým prihlásením, musíte vytvoriť priradenia medzi rôznymi identitami užívateľa niektorej osoby alebo entity a jedným identifikátorom EIM pre danú osobu alebo entitu. Môžete vytvoriť tri typy priradení: cieľové, zdrojové a administratívne.

Aby ste mohli vytvoriť zdrojové alebo administratívne priradenie, musíte mať oprávnenie administrátora identifikátorov alebo oprávnenie administrátora EIM. Aby ste mohli vytvoriť cieľové priradenie, musíte mať oprávnenie administrátora registra na všetky registre, oprávnenie administrátora registra na špecifický register alebo oprávnenie administrátora EIM.

Aby ste vytvorili priradenie pre identifikátor EIM, vykonajte tieto kroky:

1. Rozviňte **Sieť —> Enterprise Identity Mapping —> Manažment domén**.
2. Musíte byť pripojený k doméne EIM, v ktorej chcete pracovať.
   - Ak doména EIM, v ktorej chcete pracovať nie je uvedená v zložke Manažment domén, pozrite si tému Pridanie domény EIM do Manažmentu domén.
   - Ak aktuálne nie ste pripojený k doméne EIM, v ktorej chcete pracovať, pozrite si tému Pripojenie k radiču domény EIM.
3. Rozviňte doménu EIM, ku ktorej ste teraz pripojený.
4. Kliknite na **Identifikátory**, aby sa zobrazil zoznam identifikátorov EIM.
5. Pravým tlačidlom myši kliknite na požadovaný identifikátor EIM a vyberte **Vlastnosti...**.
6. Kliknite na záložku **Priradenia**.
7. Kliknite na tlačidlo **Pridať...**, aby sa zobrazilo dialógové okno **Pridanie priradenia**.
8. Ak potrebujete viac informácií k vyplneniu polí, kliknite na tlačidlo **Pomoc**.
9. Po zadaní vyžadovaných informácií kliknite na tlačidlo **OK**.

Vymazať priradenie

Aby ste mohli vymazať administratívne alebo zdrojové priradenie, musíte mať oprávnenie administrátora identifikátorov alebo oprávnenie administrátora EIM. Aby ste mohli vymazať cieľové priradenie, musíte mať oprávnenie administrátora na vybraté registre (vrátane registra, s ktorým chcete pracovať), oprávnenie administrátora registra alebo oprávnenie administrátora EIM.

Aby ste vymazali priradenie, vykonajte tieto kroky.

1. Rozviňte **Sieť —> Enterprise Identity Mapping —> Manažment domén**.
2. Musíte byť pripojený k doméne EIM, v ktorej chcete pracovať:
   - Ak doména EIM, v ktorej chcete pracovať nie je uvedená v Manažmente domén, pozrite si tému Pridanie domény EIM do manažmentu domén.
   - Ak aktuálne nie ste pripojený k doméne EIM, v ktorej chcete pracovať, pozrite si tému Pripojenie k doméne EIM.
3. Rozviňte doménu EIM, ku ktorej ste teraz pripojený.
4. Kliknite na tlačidlo **Identifikátory**.
5. Pravým tlačidlom myši kliknite na vami požadovaný identifikátor EIM a vyberte **Vlastnosti...**.
6. Kliknite na záložku **Priradenia**, aby sa zobrazili aktuálne priradenia pre daný identifikátor EIM.
7. Vyberte priradenie, ktoré chcete odstrániť.
8. Kliknite na tlačidlo **Odstrániť**, aby sa odstránili priradenia.
9. Kliknite na tlačidlo **OK**.

Manažovať identifikátory EIM

Aktualizácia identifikátorov EIM, ktoré reprezentujú užívateľov vo vašej sieti je veľmi dôležitá z hľadiska bezpečnosti. Užívatelia v podniku sa takmer vždy menia, niektorí prídu, niektorí odídu, iní sa presunú medzi pracoviskami. S týmito zmenami vzniká potreba sledovať kontá užívateľov a ich prístup k systémom v sieti. Vytvorenie identifikátorov EIM a ich priradenie k identitám užívateľov pre každého užívateľa toto sledovanie zjednodušuje.

Povolenie jednorazového prihlásenia zjednodušuje prácu užívateľov aj pri ich presune do iného oddelenia alebo oblasti v podniku. Možno je potrebné zmeniť ich zabezpečenie a prístup k systému. Povolením jednorazového prihlásenia odpadá pre týchto užívateľov potreba pamätať si nové mená užívateľov a heslá pre nové systémy.

Manažovanie identifikátorov EIM pre vašich užívateľov v podniku zahŕňa mnoho úloh, ktoré môžu byť rutinné. Na manažment identifikátorov EIM vo vašej sieti a doménach môžete použiť tieto úlohy:

- Vytvoriť identifikátor EIM
- Pridať alias k identifikátoru EIM
- Vymazať identifikátor EIM

Viac informácií o manažovaní priradení nájdete v téme Manažovať priradenia.

Vytvoriť identifikátor EIM

Aby ste mohli vytvoriť identifikátor EIM, musíte mať buď oprávnenie administrátora identifikátorov, alebo oprávnenie administrátora EIM.

Aby ste vytvorili identifikátor EIM pre osobu alebo entitu, vykonajte tieto kroky:

1. Rozviňte **Sieť —> Enterprise Identity Mapping —> Manažment domén**.
2. Musíte byť pripojený k doméne EIM, v ktorej chcete pracovať:
   - Ak doména EIM, v ktorej chcete pracovať nie je uvedená v **Manažmente domén**, pozrite si tému Pridať doménu do Manažmentu domén.
   - Ak aktuálne nie ste pripojený k doméne EIM, v ktorej chcete pracovať, pozrite si tému Pripojiť k doméne.
3. Rozviňte doménu EIM, ku ktorej ste teraz pripojený.
4. Pravým tlačidlom kliknite na **Identifikátory** a vyberte **Nový identifikátor...**.
5. Ak potrebujete viac informácií k niektorému z polí, kliknite na tlačidlo **Pomoc**.
6. Po zadaní vyžadovaných informácií kliknite na tlačidlo **OK**.

Pridať alias k identifikátoru EIM

Môžete chcieť vytvoriť alias, ktorý poskytne dodatočné rozlišovacie informácie pre identifikátor EIM. Vy alebo ostatní potom môžu použiť tento alias na rozlíšenie jedného identifikátora EIM od druhého. 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.

Aby ste mohli pridať alias k identifikátoru, musíte mať oprávnenie administrátora identifikátorov alebo oprávnenie administrátora EIM.

Aby ste pridali alias k identifikátoru EIM, vykonajte tieto kroky.

1. Rozviňte **Sieť —> Enterprise Identity Mapping —> Manažment domén**.
2. Musíte byť pripojený k doméne EIM, v ktorej chcete pracovať:
   - Ak doména EIM, v ktorej chcete pracovať nie je uvedená v Manažmente domén, pozrite si tému Pridanie domény EIM do Manažmentu domén.
   - Ak aktuálne nie ste 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. Pravým tlačidlom myši kliknite na vami požadovaný identifikátor EIM a vyberte **Vlastnosti**. Ak neexistujú žiadne identifikátory EIM, pozrite si tému Vytvoriť identifikátor EIM.
5. Zadajte názov aliasu, ktorý chcete pridať k tomuto identifikátoru EIM a kliknite na tlačidlo **Pridať**.
6. Kliknite na tlačidlo **OK**, aby sa uložili zmeny.

Vymazať identifikátor EIM

Aby ste mohli vymazať identifikátor EIM, musíte mať oprávnenie administrátora EIM.

Aby ste vymazali identifikátor EIM, vykonajte tieto kroky:

1. Rozviňte **Sieť —> Enterprise Identity Mapping —> Manažment domén**.
2. Musíte byť pripojený k doméne EIM, v ktorej chcete pracovať:
   - Ak doména EIM, v ktorej chcete pracovať nie je uvedená v Manažmente domén, pozrite si tému Pridanie domény EIM do Manažmentu domén.
   - Ak aktuálne nie ste pripojený k doméne EIM, v ktorej chcete pracovať, pozrite si tému Pripojenie k radiču domény EIM.
3. Rozviňte doménu EIM, ku ktorej ste teraz pripojený.
4. Kliknite na tlačidlo **Identifikátory**.
5. Vyberte jeden alebo viac identifikátorov EIM na vymazanie.
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.

Manažovať oprávnenia EIM pre užívateľov

EIM definuje rôzne oprávnenia EIM, ktoré sú potrebné pre vykonávanie rôznych operácií v doméne. Patria sem funkcie manažmentu domény, napríklad vytváranie identifikátorov, výpis registrov a vykonávanie operácie vyhľadávania mapovaní. Udeľovať alebo odoberať oprávnenia pre iných užívateľov môžu len užívatelia s oprávnením administrátora EIM.

Pozrite si tému Oprávnenia EIM, kde nájdete krátky opis každej skupiny oprávnení a detaily o prístupe, ktorý má každé z týchto oprávnení k určitým funkciám EIM.

Aby ste zmenili oprávnenia EIM pre užívateľa, vykonajte tieto kroky:

1. V programe iSeries Navigator rozviňte **Sieť —> Enterprise Identity Mapping —> Manažment domén**.
2. Rozviňte doménu EIM, v ktorej chcete pracovať. Ak nie ste aktuálne pripojený k tejto doméne, budete požiadaný o pripojenie. K doméne sa musíte pripojiť pomocou užívateľského oprávnenia, ktoré má oprávnenie administrátora EIM.
3. Pravým tlačidlom myši kliknite na danú doménu EIM a vyberte **Oprávnenie...**.
4. V dialógovom okne **Úprava oprávnenia EIM** zadajte užívateľa, ktorého oprávnenia EIM chcete zmeniť.
5. Kliknite na tlačidlo **OK**.
6. V dialógovom okne **Úprava oprávnenia EIM** spravte potrebné zmeny v oprávneniach pre daného užívateľa.
7. Po dokončení kliknite na tlačidlo **OK**, aby sa uložili zmeny v oprávneniach.

Manažovať registre užívateľov

Aby ste mohli vytvoriť priradenia medzi identitami obsiahnutými v registroch užívateľov a príslušnými identifikátormi EIM, najprv musíte zadefinovať register užívateľov v doméne EIM:

Súčasťou manažovania registrov užívateľov v doméne EIM sú tieto úlohy.

- Pridať register užívateľov

- Pridať alias do registra užívateľov
- Definovať súkromný typ registra užívateľov v EIM
- Odstrániť register užívateľov
- Odstrániť alias z registra užívateľov

Pridať register užívateľov

Aby ste mohli pridať register užívateľov, musíte mať oprávnenie administrátora EIM. Detaily o tomto oprávnení a jeho právomociach nájdete v téme Oprávnenia EIM.

Aby ste pridali register užívateľov do domény EIM, vykonajte tieto kroky.

1. Rozviňte **Sieť —> Enterprise Identity Mapping —> Manažment domén**.
2. Pripojte sa k doméne EIM pomocou užívateľa s oprávnením administrátora EIM.
   - Ak doména EIM, v ktorej chcete pracovať nie je uvedená v zložke Manažment domén, pozrite si tému Pridanie domény EIM do manažmentu domén.
   - Ak aktuálne nie ste pripojený k doméne EIM, v ktorej chcete pracovať, pozrite si tému Pripojenie k radiču domény EIM.
3. Rozviňte doménu EIM, ku ktorej ste teraz pripojený.
4. Pravým tlačidlom myši kliknite na **Registre užívateľov** a vyberte **Pridať register...**.
5. Zadajte vyžadované informácie o registri užívateľov. Pre register užívateľov tiež môžete zadať informácie o aliase.
6. Kliknite na tlačidlo **OK**, aby sa uložili informácie a register užívateľov pridal do domény EIM.

Pridať alias do registra užívateľov

Vy alebo vývojár aplikácie môže chcieť vytvoriť alias, ktorý poskytne dodatočné rozlišovacie informácie pre register užívateľov. Vy alebo ostatní potom môžu použiť tento alias na rozlíšenie jedného registra užívateľov od druhého. Napríklad vývojári aplikácie a administrátori používajú alias pre register užívateľov na dohodnutie sa, ktoré registre EIM by mala používať aplikácia. Viac informácií o používaní aliasov s registrami užívateľov nájdete v téme Definície registrov EIM.

Ak chcete pridať alias do registra užívateľov, musíte použiť jedno z týchto oprávnení: administrátor EIM, administrátor registra na všetky registre alebo administrátor registra na špecifický register, pre ktorý vykonávate túto úlohu.

Aby ste pridali alias do registra užívateľov v doméne EIM, vykonajte tieto kroky:

1. Rozviňte **Sieť —> Enterprise Identity Mapping —> Manažment domén**.
2. Musíte byť pripojený k doméne EIM, v ktorej chcete pracovať:
   - Ak doména EIM, v ktorej chcete pracovať nie je uvedená v zložke Manažment domén, pozrite si tému Pridanie domény EIM do manažmentu domén.
   - Ak aktuálne nie ste pripojený k doméne EIM, v ktorej chcete pracovať, pozrite si tému Pripojenie k radiču domény EIM.
3. Rozviňte doménu EIM, ku ktorej ste teraz pripojený.
4. Kliknite na **Registre užívateľov**, aby sa zobrazil zoznam registrov v danej doméne.
5. Pravým tlačidlom myši kliknite register užívateľov, do ktorého pridávate alias a vyberte **Vlastnosti...**.
6. Kliknite na záložku **Alias** z dialógového okna **Vlastnosti**.
7. Zadajte názov a typ aliasu, ktorý chcete pridať. Môžete zadať typ aliasu, ktorý nie je uvedený v zozname typov.
8. Kliknite na tlačidlo **Pridať**.
9. Kliknite na tlačidlo **OK**, aby sa uložili zmeny.

Definovať súkromný typ registra užívateľov v EIM

Aby ste zadefinovali typ registra užívateľov, ktorý EIM štandardne nepozná, typ registra musíte zadať v tvare **identifikátor_objektu-normalizácia**, kde **identifikátor_objektu** je identifikátor objektu, tvorený desiatkovými číslami oddelenými bodkou, napríklad 1.2.3.4.5.6.7, a **normalizácia** je buď hodnota **caseExact**, alebo hodnota **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 **identifikátor_objektu**. 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 dokument s odkazmi na prihlasovacie formuláre sa nachádza na webovej lokalite ANSI na adrese http://web.ansi.org/public/services/reg_org.html

  . Rozsah OID od ANSI 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), ktoré tvorí nový rozsah OID: 2.16.840.1.NEWNUM.
- Vo väčšine krajín a regiónov je register OID spravovaný národnými organizáciami. Podobne ako pri rozsahu od ANSI, takéto rozsahy sa zvyčajne priraďujú pod OID 2.16. Nájdenie autority OID pre konkrétnu krajinu alebo región môže byť trochu náročnejšie. Adresy hlavných národných členov ISO nájdete 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.
- Iným možným začiatočným bodom je Medzinárodný register schém ISO DCC NSAP. NSAP je skratka od Network Service Access Point a používa sa v rôznych medzinárodných štandardoch. Register pre schémy sa dá získať na adrese http://www.fei.org.uk v časti ISO DCC NSAP

  . Táto webová lokalita aktuálne uvádza kontaktné informácie pre 13 pomenovacích autorít, z ktorých niektoré tiež priraďujú identifikátory OID.

- Internet Assigned Numbers Authority (IANA) prirađuje súkromné čísla podnikom; sú to identifikátory OID z rozsahu 1.3.6.1.4.1. IANA dodnes priradila rozsahy viac ako 7500 spoločnostiam. Stránka so žiadosťou je umiestnená na adrese http://www.iana.org/cgi-bin/enterprise.pl

  v časti Private Enterprise Numbers. Registrácia v IANA trvá zvyčajne jeden týždeň. OID od IANA sú k dispozícii bezplatne. IANA priradí číslo (NEWNUM) a nový rozsah OID bude 1.3.6.1.4.1.NEWNUM.
- Federálna vláda USA spravuje Computer Security Objects Registry (CSOR). CSOR je pomenovacia autorita pre rozsah 2.16.840.1.101.3 a aktuálne 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

.

Odstrániť register užívateľov

Odstránenie registra užívateľov z domény EIM spôsobí stratu všetkých priradení identifikátorov EIM k identitám užívateľov v registri užívateľov. Pridaním registra užívateľov do domény EIM po jeho odstránení sa neobnovia vzťahy priradenia.

Aby ste mohli odstrániť register užívateľov, musíte mať oprávnenie administrátora EIM.

Aby ste odstránili register užívateľov, vykonajte tieto kroky:

1. Rozviňte **Sieť —> Enterprise Identity Mapping —> Manažment domén**.
2. Musíte byť pripojený k doméne EIM, v ktorej chcete pracovať.
   - Ak doména EIM, v ktorej chcete pracovať nie je uvedená v zložke Manažment domén, pozrite si tému Pridanie domény EIM do manažmentu domén.
   - Ak aktuálne nie ste pripojený k doméne EIM, v ktorej chcete pracovať, pozrite si tému Pripojenie k radiču domény EIM.
3. Rozviňte doménu EIM, ku ktorej ste teraz pripojený.
4. Kliknite na **Registre užívateľov**, aby sa zobrazil zoznam registrov užívateľov v danej doméne.
5. Pravým tlačidlom myši kliknite na register užívateľov, ktorý chcete odstrániť a kliknite na tlačidlo **Vymazať...**.
6. V dialógovom okne **Potvrdenie** kliknite na tlačidlo **Áno**, aby sa vymazal register užívateľov.

Odstrániť alias z registra užívateľov

Aby ste mohli odstrániť alias z registra užívateľov, musíte mať oprávnenie administrátora registra a oprávnenie administrátora pre vybraté položky (vrátane registra, s ktorým chcete pracovať) alebo oprávnenie administrátora EIM.

Aby ste odstránili alias z registra užívateľov v doméne EIM, vykonajte tieto kroky:

1. Rozviňte **Sieť —> Enterprise Identity Mapping —> Manažment domén**.
2. Musíte byť pripojený k doméne EIM, v ktorej chcete pracovať:
   - Ak doména EIM, v ktorej chcete pracovať nie je uvedená v zložke Manažment domén, pozrite si tému Pridanie domény EIM do manažmentu domén.

- Ak aktuálne nie ste pripojený k doméne EIM, v ktorej chcete pracovať, pozrite si tému Pripojenie k radiču domény EIM.

3. Rozviňte doménu EIM, ku ktorej ste teraz pripojený.
4. Kliknite na **Registre užívateľov**, aby sa zobrazil zoznam registrov v danej doméne.
5. Pravým tlačidlom myši kliknite register užívateľov, ktorého alias chcete odstrániť a vyberte **Vlastnosti**.
6. Kliknite na záložku **Alias** z dialógového okna **Vlastnosti**.
7. Vyberte alias, ktorý chcete odstrániť a kliknite na tlačidlo **Odstrániť**.
8. Kliknite na tlačidlo **OK**, aby sa uložili zmeny.

Rozhrania API pre EIM

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 vykonanie operácií vyhľadania mapovania identity, rôznych funkcií manažmentu a konfigurácie EIM, ako aj na zmenu informácií a vytváranie dotazov.

Rozhrania API EIM sa delia do týchto kategórií:

- Operácie s deskriptormi a pripojeniami EIM
- Administrácia domény EIM
- Operácie s registrom
- Operácie s identifikátormi EIM
- Manažment priradení EIM
- Operácie vyhľadávania mapovaní EIM
- Manažment 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 administráciu EIM alebo operácie vyhľadávania mapovania identity EIM
5. Normálne aplikačné spracovanie
6. Zrušenie deskriptora EIM pred ukončením

Detailné informácie a úplný zoznam rozhraní API EIM, ktoré sú dostupné pre server iSeries nájdete v téme Rozhrania API pre EIM (Enterprise Identity Mapping).

Odstraňovanie problémov EIM

EIM je tvorené viacerými technológiami a množstvom aplikácií a funkcií. Kvôli veľkému množstvu ciest, ktoré môžu viesť k odstráneniu problémov sme pripravili nasledujúce témy obsahujúce detailné inštrukcie ako odstrániť problémy alebo opraviť niektoré bežné chyby, s ktorými sa môžete stretnúť:

- Nedá sa pripojiť k radiču domény
- Zobrazenie zoznamu identifikátorov EIM trvá dlho
- Sprievodca konfiguráciou EIM prestane reagovať počas dokončovania spracovania
- Deskriptor EIM je už neplatný
- Autentifikácia Kerberosom a diagnostické správy

Nedá sa pripojiť k radiču domény

Pri pripájaní k radiču domény môže k problémom prispieť množstvo faktorov. Pozrite si tieto položky, ktoré vám môžu pomôcť nájsť príčinu problému:

- Skontrolujte správnosť zadaných informácií pre tieto položky:
  - Názov radiča domény
  - Zadaný port
  - ID užívateľa a heslo
- Skontrolujte, že radič domény je aktívny. Ak je radič domény na serveri iSeries, môžete použiť program iSeries Navigator a vykonajte 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...**

Keď bude radič domény aktívny, znovu sa skúste pripojiť k doméne.

1. Rozviňte **Sieť —> Enterprise Identity Mapping —> Manažment domén**.
2. Vyberte doménu, ku ktorej sa chcete pripojiť. Ak nie sú uvedené žiadne domény alebo doména, v ktorej chcete pracovať nie je uvedená v zložke Manažment domén, musíte pridať doménu EIM do manažmentu domén.
3. Pravým tlačidlom myši kliknite na doménu EIM, ku ktorej sa chcete pripojiť a vyberte **Pripojiť...**.
4. Zadajte typ užívateľa a vyžadované informácie o užívateľovi, ktoré sa majú použiť pre pripojenie k radiču domény EIM.
5. Kliknite na tlačidlo **OK**.

Zobrazenie zoznamu identifikátorov EIM trvá dlho

Pri otváraní zložky Identifikátory v programe iSeries Navigator môže vygenerovanie zoznamu identifikátorov trvať dlhšie. Ak je vo vašej doméne veľký počet identifikátorov EIM, môžete zúžiť vyhľadávacie kritérium pre zobrazenie zoznamu.

Aby ste prispôsobili zobrazenie pre identifikátory EIM, vykonajte tieto kroky:

1. V programe iSeries Navigator rozviňte **Sieť —> Enterprise Identity Mapping —> Manažment domén**.
2. Rozviňte doménu, ktorej identifikátory chcete zobraziť.
3. Pravým tlačidlom myši kliknite na **Identifikátory** a vyberte **Prispôsobiť toto zobrazenie —> Zahrnúť...**.
4. Zadajte vami požadované kritérium zobrazovania. Môžete použiť aj zástupný znak hviezdička (*).
5. Kliknite na tlačidlo OK.

Pri najbližšom kliknutí na **Identifikátory** sa zobrazia len tie identifikátory, ktoré vyhovujú vami zadanému kritériu. Ak chcete zobraziť všetky identifikátory EIM, použite kroky opísané hore a ako voľbu prispôsobenia zobrazenia vyberte **Všetky identifikátory**.

Sprievodca konfiguráciou EIM prestane reagovať počas dokončovania spracovania

Ak sprievodca prestane reagovať počas dokončovania spracovania, je možné, že sprievodca čaká na spustenie radiča domény. Skontrolujte, že počas spúšťania servera LDAP nedošlo k žiadnym chybám. Pri serveroch iSeries skontrolujte úlohu QDIRSRV v podsystéme QSYSWRK.

Aby ste skontrolovali protokol úloh, vykonajte tieto kroky:

1. V programe iSeries Navigator rozviňte **Riadenie prevádzky —> Podsystémy —> Qsyswrk**.
2. Pravým tlačidlom myši kliknite na **Qdirsrv** a vyberte **Protokol úlohy**.

Deskriptor EIM je už neplatný

Ak sa užívateľ počas manažovania EIM cez program iSeries Navigator stretne s chybou označujúcou, že deskriptor EIM je už neplatný, došlo k strate pripojenia k radiču domény.

Aby ste obnovili pripojenie k radiču domény, vykonajte tieto kroky:

1. V programe iSeries Navigator rozviňte **Sieť —> Enterprise Identity Mapping —> Manažment 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**.

Autentifikácia Kerberosom a diagnostické správy

Keď na autentifikáciu s EIM používate protokol Kerberos, pri každom zlyhaní autentifikácie alebo operácií mapovania identity sa do protokolu úloh zapíše diagnostická správa CPD3E3F. 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.

Súvisiace informácie pre EIM

Môžete požadovať viac informácií o iných technológiách súvisiacich s EIM. Nasledujúce témy Informačného centra vám pomôžu porozumieť týmto technológiám:

- **Služba sieťovej autentifikácie**
  Táto téma poskytuje informácie o konfigurácii služby sieťovej autentifikácie na iSeries. Služba sieťovej autentifikácie umožňuje serveru iSeries tvoriť súčasť existujúcej siete Kerberos. Keď sa používa s EIM, služba sieťovej autentifikácie poskytuje jednorazové prihlásenie pre sieť.
- **Adresárové služby (LDAP)**
  Táto téma poskytuje informácie o konfigurácii a konceptoch pre Adresárové služby (LDAP). EIM používa server LDAP na ukladanie údajov EIM a priradení mapovaní.

Vytlačené v USA