System i

Bezpečnostné mapovanie podnikovej identity

Verzia 6, vydanie 1

System i

Bezpečnostné mapovanie podnikovej identity

Verzia 6, vydanie 1

Poznámka

Pred použitím týchto informácií a nimi podporovaného produktu si určite prečítajte informácie v časti “Právne vyhlásenia”, na strane 121.

Toto vydanie platí pre verziu 6, vydanie 1, modifikáciu 0 operačného systému i5/OS od spoločnosti IBM (číslo produktu 5761–SS1) a všetky ďalšie vydania a modifikácie, pokiaľ nie je v nových vydaniach uvedené inak. Táto verzia nie je určená pre všetky modely RISC (reduced instruction set computer) ani pre všetky modely CISC.

Obsah

Mapovanie podnikovej identity 1

Čo je nové vo vydaní V6R1 1
Súbor PDF pre mapovanie podnikovej identity 2
Prehľad EIM 2
Koncepty EIM 4
Radič domény EIM 5
Doména EIM 6
Identifikátor EIM 8
Definície registrov EIM 11
Definície systémového registra 13
Definície registra aplikácií 14
Definície skupinového registra 15
Asociácie EIM 16
Informácie na vyhľadanie 16
Priradenia identifikátorov 17
Priradenia politiky 21
Predvolené priradenia politiky domény . . . 21
Predvolené priradenia politiky registrov . . . 23
Priradenia politiky filtra certifikátov 24
Operácie prehľadania EIM 27
Príklady operácie vyhľadávania: Príklad 1 30
Príklady operácie vyhľadávania: Príklad 2 30
Príklady operácie vyhľadávania: Príklad 3 32
Príklady operácie vyhľadávania: Príklad 4 34
Príklady operácie vyhľadávania: Príklad 5 35
Operácie podpory a umožnenia politiky mapovaní EIM 37
Riadenie prístupu EIM 38
Skupina riadenia prístupu k EIM: Oprávnenie rozhrania API 41
Skupina riadenia prístupu EIM: Oprávnenie na úlohu EIM 43
Koncepty LDAP pre EIM 46
Charakteristický názov 46
Rodičovský rozlišovací názov 47
Schéma LDAP a ostatné úvahy o EIM 47
Základné pojmy mapovania podnikovej identity pre i5/OS 48
i5/OS faktory profilov užívateľov EIM 49
i5/OS audit pre EIM 50
Aplikácie s povoleným EIM pre i5/OS 50
Scenáre: Mapovanie podnikovej identity 50
Plánovanie EIM 51
Plánovanie mapovania podnikovej identity pre eServer 51
Požiadavky nastavenia mapovania podnikovej identity pre eServer 51
Identifikácia potrebných schopností a rolí 52
Plánovanie domény mapovania podnikovej identity 54
Plánovanie radiča domény mapovania podnikovej identity 55
Vývoj plánu pomenúvania definícií registra mapovania podnikovej identity 58
Vývoj plánu mapovania identity 59
Plánovanie priradení mapovania podnikovej identity 60
Vývoj plánu pomenúvania identifikátorov EIM 62
Pracovné listy plánovania implementácie mapovania podnikovej identity 63
Plánovanie vývoja aplikácií pre mapovanie podnikovej identity 65
Plánovanie mapovania podnikovej identity pre i5/OS 65
Nevyhnutné podmienky inštalácie EIM pre i5/OS 66
Inštalácia vyžadovaných volieb System i Navigator 66
Aspekty zálohy a obnovy pre EIM 67
Zálohovanie a obnova dát domény EIM . . . 67
Zálohovanie a obnova konfiguračných informácií EIM 67
Konfigurácia EIM 68
Vytvorenie a pripojenie k novej lokálnej doméne . . . 69
Ukončite konfiguráciu EIM pre doménu 72
Vytvorenie a pripojenie k novej vzdialenej doméne . . 73
Ukončite konfiguráciu EIM pre doménu 77
Pripojenie k existujúcej doméne 78
Ukončite konfiguráciu EIM pre doménu 82
Konfigurácia bezpečného pripojenia k radiču domény EIM 83
Riadenie mapovania podnikovej identity 84
Riadenie domén EIM (Managing Enterprise Identity) 84
Pridávanie domény EIM do zložky Domain Management 84
Pripájanie k doméne EIM 84
Povolenie priradení politiky pre doménu 85
Testovanie mapovania EIM 85
Práca s výsledkami testu a riešenie problémov 86
Odstránenie domény EIM zo zložky Domain Management 88
Vymazanie domény EIM a všetkých konfiguračných objektov 88
Riadenie definícií registrov EIM 88
Pridávanie definície systémového registra 89
Pridávanie definície registra aplikácií 89
Pridanie definície skupinového registra 90
Pridávanie aliasu do definície registra 90
Definovanie typu registra súkromného užívateľa v EIM 91
Povolenie podpory vyhľadávaní mapovania a používanie priradení politiky pre cieľový register . . 92
Vymazanie definície registra 93
Odstránenie aliasu z definície registra 94
Pridávanie člena do definície skupinového registra 94
Správa identifikátorov EIM 95
Vytváranie identifikátora EIM 95
Pridávanie aliasu do identifikátora EIM 95
Odstránenie aliasu z identifikátora EIM 96
Vymazanie identifikátora EIM 97
Prispôsobenie zobrazenia identifikátorov EIM . . 97
Mapovanie priradení EIM 97
Vytváranie priradení EIM 98
Vytváranie priradenia identifikátora EIM . . . 98
Vytváranie priradenia politiky 99
Pridávanie vyhľadávacích informácií do identity cieľového užívateľa 105

Pridanie informácií na vyhľadanie k cieľovej identite užívateľa v priradení identifikátora . . 105
Pridanie informácií na vyhľadanie k cieľovej identite užívateľa v priradení politiky 106
Odstránenie vyhľadávacích informácií z identity cieľového užívateľa 107
Odstránenie informácií na vyhľadanie pre cieľovú identitu užívateľa v priradení identifikátora 107
Zobrazenie všetkých priradení identifikátorov pre identifikátory EIM 108
Zobrazenie všetkých priradení politiky pre doménu 109
Zobrazenie všetkých priradení politiky pre definíciu registra 109
Vymazanie priradenia identifikátora 110
Vymazanie priradenia politiky 111
Riadenie prístupov užívateľov k EIM 112
Riadenie vlastností konfigurácie EIM. 112
Odstraňovanie problémov s EIM 113
Odstraňovanie problémov pripojenia k radiču domény 113
Odstraňovanie bežných problémov konfigurácie EIM a domény 115
Odstraňovanie problémov s mapovaním EIM . . . 116
Rozhrania API pre EIM 119
Súvisiace informácie pre mapovanie podnikovej identity 120

Príloha. Právne vyhlásenia 121
Ochranné známky 122
Pojmy a podmienky 123

Mapovanie podnikovej identity

EIM pre platformu System i je implementácia i5/OS infraštruktúry IBM umožňujúca administrátorom a vývojárom aplikácií riešiť problém správy viacerých registrov užívateľov v podniku.

Väčšina podnikov so sieťami čelí problému viacerých registrov užívateľov, čo vyžaduje, aby každá osoba alebo entita v podniku mala identitu užívateľa v každom registri. Potreba viacerých registrov užívateľov rýchlo prerastie do veľkého administratívneho problému, ktorý ovplyvňuje užívateľov, administrátorov a vývojárov aplikácií. EIM sprístupňuje nenáročné riešenia na jednoduchšiu správu viacerých registrov užívateľov a užívateľských identít v podniku.

EIM vám dovoľuje vytvoriť systém mapovaní identít, nazývaných priradenia, medzi rôznymi identitami užívateľa v rôznych registroch užívateľov pre osobu vo vašom podniku. EIM tiež poskytuje spoločnú množinu rozhraní API, ktoré sa dajú použiť medzi platformami na vývoj aplikácií, ktoré používajú mapovania identít, ktoré vytvoríte na vyhľadávanie vzťahov medzi identitami užívateľa. Okrem toho môžete EIM použiť v kombinácii so službou sieťovej autentifikácie a i5/OS implementáciou Kerberos na poskytnutie prostredia jednoduchého prihlásenia.

EIM môžete nakonfigurovať a riadiť prostredníctvom navigátora System i a grafického užívateľského rozhrania System i. Platforma System i používa EIM na povolenie rozhraní i5/OS na autentifikáciu užívateľov pomocou služby sieťovej autentifikácie. Aplikácie, ako aj i5/OS, môžu akceptovať vstupenky Kerberos a používať EIM na vyhľadanie užívateľského profilu, ktorý predstavuje tú istú osobu, ako predstavuje vstupenku Kerberos.

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

Čo je nové vo vydaní V6R1

Prečítajte si nové alebo zásadne zmenené informácie pre kolekciu tém o mapovaní podnikovej identity (EIM).

Nové alebo vylepšené funkcie pre EIM

- V predchádzajúcich vydaniach i5/OS EIM podporovalo len mapovanie do jednej lokálnej užívateľskej identity na jeden systém. V i5/OS V6R1 EIM podporuje výber z viacerých mapovaní lokálnej užívateľskej identity pre ten istý systém pomocou IP adresy cieľového systému na výber správneho mapovania lokálnej užívateľskej identity v danom systéme.

Ďalej je zaktualizovaná téma Jednoduché prihlásenie, ktorá poskytuje dokumentáciu o implementácii EIM ako súčasti prostredia jednoduchého prihlásenia na zníženie riadenia hesiel. Táto téma poskytuje mnoho podrobných scenárov bežných situácií jednoduchého prihlásenia s podrobnými konfiguračnými pokynmi na ich implementáciu.

Ako zistíte čo je nové alebo čo sa zmenilo

Aby ste zistili, kde boli vykonané zmeny, tieto informácie používajú:

- Značka  , ktorá označuje, kde začínajú nové alebo zmenené informácie.
- Značka  , ktorá označuje, kde nové alebo zmenené informácie končia.

Ak chcete nájsť ďalšie informácie o tom, čo je v tomto vydaní nové alebo zmenené, pozrite si Poznámky pre užívateľov.

Súbor PDF pre mapovanie podnikovej identity

Môžete zobraziť alebo vytlačiť súbor PDF týchto informácií.

Ak chcete zobraziť alebo načítať PDF verziu tohto dokumentu, zvoľte Enterprise Identity Mapping (asi 1820 KB).

Môžete zobraziť alebo stiahnuť PDF týchto súvisiacich tém:

- Téma Služby sieťovej autentifikácie (približne 1398 KB) obsahuje informácie o konfigurácii služby sieťovej autentifikácie v spojení s EIM na vytvorenie prostredia jednoduchého prihlásenia.
- Téma IBM Tivoli Directory Server for i5/OS (LDAP) (približne 1700 KB) obsahuje informácie o konfigurácii servera LDAP, ktorý môžete použiť ako radič domény EIM spolu s informáciami o rozšírenej konfigurácii LDAP.

Uloženie dokumentov PDF

Ak si chcete uložiť dokument typu PDF na svojej pracovnej stanici za účelom prezerania alebo tlače, zvoľte tento postup:

1. Kliknite pravým tlačidlom myši na odkaz na PDF vo vašom prehliadači.
2. Vyberte voľbu, ktorá ukladá súbor PDF lokálne.
3. Prejdite do adresára, do ktorého chcete tento súbor PDF uložiť.
4. Kliknite na **Save**.

Stiahnutie Adobe Reader

Ak chcete zobraziť alebo tlačiť tieto súbory PDF, musíte mať v systéme nainštalovaný Adobe Reader. Bezplatnú kópiu si môžete stiahnuť z webovej stránky Adobe (www.adobe.com/products/acrobat/readstep.html) .

Prehľad EIM

EIM vám môže pomôcť pri riešení problémov, ktoré sa objavia pri pokuse o riadenie viacerých registrov užívateľov.

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 umožňuje administrátorom a vývojárom aplikácií riešiť tento problém jednoduchšie a s menšími nákladmi než predtým.

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

Problém manažovania viacerých registrov užívateľov

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

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

Aktuálne prístupy

K dispozícii je niekoľko aktuálnych priemyselných prístupov pre riešenie problému manažovania viacerých registrov užívateľov, ale všetky poskytujú len neúplné riešenia. Napríklad LDAP (Lightweight Directory Access Protocol) poskytuje riešenie pre distribuované registre užívateľov. Použitie LDAP (alebo ďalších populárnych riešení ako Microsoft Passport) však znamená, že administrátori musia riadiť ešte ďalší register užívateľa 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 správy a pravdepodobnosť narušenia bezpečnosti. Keď viacero mechanizmov podporuje jeden prostriedok, šanca, že v jednom mechanizme sa zmení autorita a na zmenu v jednej alebo viacerých ďalších mechanizmov sa zabudne, je oveľa vyššia. Napríklad k narušeniu bezpečnosti môže dôjsť v prípade, ak má užívateľ zakázaný prístup cez jedno rozhranie, ale má povolený prístup cez jedno alebo viac iných rozhraní.

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

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

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

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

Prístup EIM

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

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

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

Schopnosť vytvárať mapovanie medzi identitami užívateľa v rôznych registroch užívateľov prináša mnoho výhod. Znamená to hlavne, že aplikácie môžu byť schopné používať jeden register užívateľov na autentifikáciu a zároveň úplne iný register užívateľov na autorizáciu. Napríklad, administrátor by mohol mapovať Windows identitu užívateľa v Kerberos registri na i5/OS užívateľský profil v inom registri užívateľa, aby sprístupnil i5/OS prostriedky, na ktoré je i5/OS užívateľský profil autorizovaný.

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

EIM, použité v spojení so službou sieťovej autentifikácie, i5/OS implementácia Kerberos, poskytuje riešenie s jediným prihlásením. Je možné písať aplikácie, ktoré používajú rozhrania API GSS a EIM na akceptovanie lístkov Kerberos a na mapovanie na ďalšiu priradenú identitu užívateľa v inom registri užívateľov. Priradenie medzi identitami užívateľov, ktoré umožňuje toto mapovanie identít, možno uskutočniť vytvorením priradení identifikátora, ktoré nepriamo priraďujú jednu identitu užívateľa k inej prostredníctvom identifikátora EIM alebo vytvorením priradení politiky, ktoré priamo priraďujú jednu identitu užívateľa v skupine k jednej konkrétnej identite užívateľa.

Používanie mapovania identity vyžaduje, aby administrátori postupovali nasledovne:

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

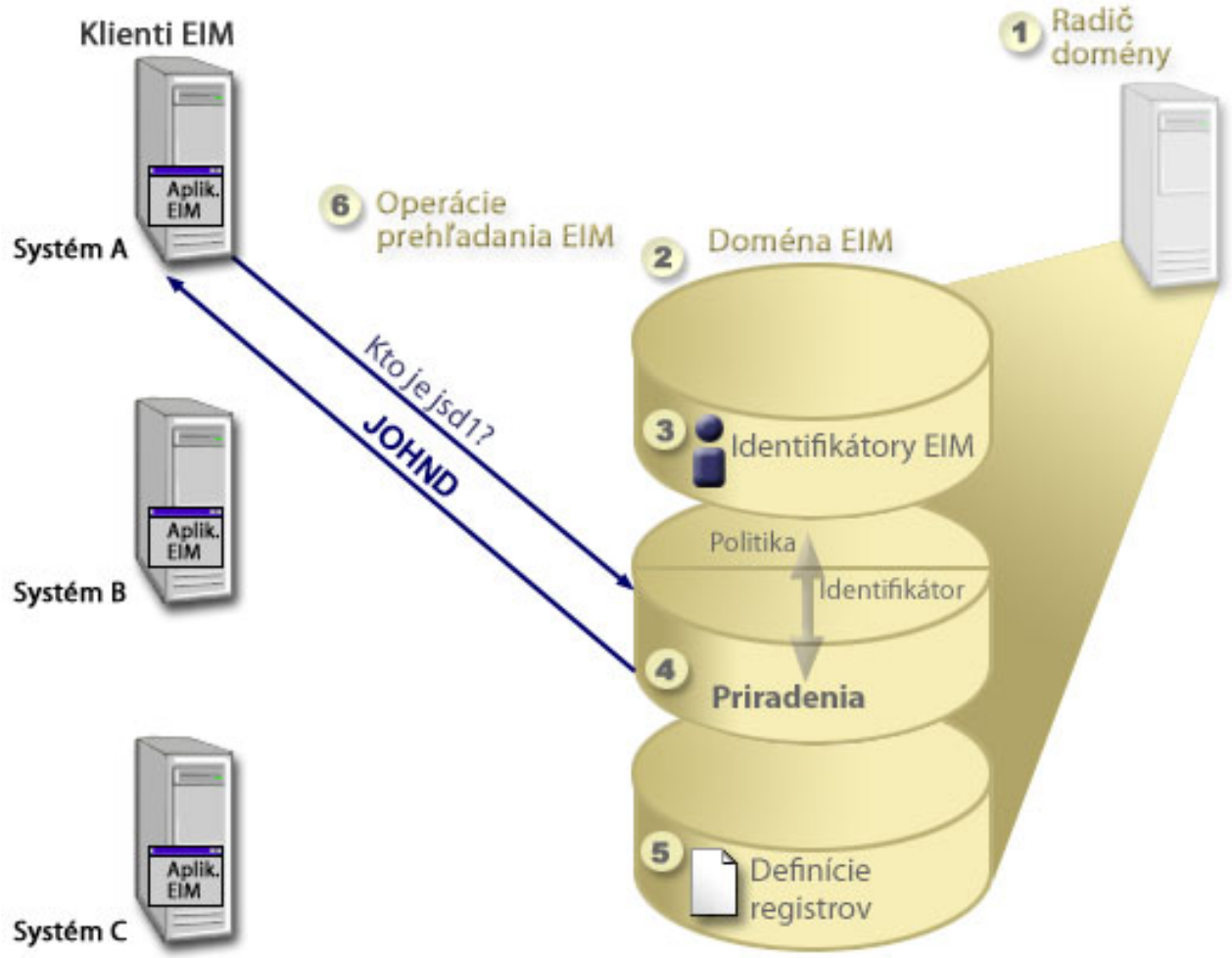
   Súvisiace informácie

   Prehľad jednoduchého prihlásenia

Koncepty EIM

Konceptuálne pochopenie spôsobu fungovania EIM je potrebné pre úplné pochopenie spôsobu možného využitia EIM vo vašom podniku. Napriek tomu, že konfigurácia a implementácia rozhraní API mapovania EIM sa môže na rôznych platformách servera líšiť, základné pojmy EIM sú spoločné pre všetky platformy IBM eServer.

Obrázok 1 poskytuje príklad implementácie EIM v podniku. Tri servery sa správajú ako klienti EIM a obsahujú aplikácie povolené EIM, ktoré vyžadujú údaje EIM pomocou vyhľadávacích operácií EIM (6). Radič domény (1) ukladá informácie o doméne EIM (2), ktoré zahŕňajú identifikátor EIM (3), priradenia (4) medzi týmito identifikátormi EIM a užívateľskými identitami a definície registrov EIM (5).



Obrázok 1. Príklad implementácie EIM

Ak chcete vedieť viac o týchto základných pojmoch EIM eServer, pozrite si nasledujúce informácie:

Súvisiace koncepty

"Koncepty LDAP pre EIM" na strane 46
EIM používa server LDAP ako radič domény na ukladanie údajov EIM. V dôsledku toho by ste mali pochopiť niektoré koncepty LDAP, ktoré sa vzťahujú na konfigurovanie a používanie EIM vo vašom podniku. Napríklad rozlišovací názov LDAP môžete použiť ako identitu užívateľa na nakonfigurovanie EIM a autentifikovanie do radiča domén EIM.

"Základné pojmy mapovania podnikovej identity pre i5/OS" na strane 48
EIM môžete implementovať na ľubovoľnú platformu IBM eServer. Keď však implementujete EIM na model System i, mali by ste byť oboznámený s niektorými informáciami špecifickými pre implementáciu System i.

Radič domény EIM

Radič domény EIM je server LDAP (Lightweight Directory Access Protocol) nakonfigurovaný na riadenie jednej alebo viacerých domén EIM. Doména EIM pozostáva zo všetkých identifikátorov EIM, priradení EIM a registrov užívateľov zadefinovaných v tejto doméne. Systémy (klienti EIM) sú spojené s doménou EIM tým, že používajú údaje domény pre operácie prehľadania EIM.

Aktuálne môžete nakonfigurovať IBM Tivoli Directory Server for i5/OS na niektorých platformách IBM eServer, aby sa správal ako radič domény EIM. Klientom domény EIM môže byť ľubovoľný klient, ktorý podporuje rozhrania API EIM. Tieto klientske systémy používajú rozhrania API mapovania EIM na kontaktovanie a spustenie radiča domény

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.

Poznámka: Adresárový server, ktorý plánujete konfigurovať vo vzdialenom systéme, musí poskytovať podporu EIM. EIM vyžaduje, aby bol radič domény hosťom adresárového servera, ktorý podporuje LDAP (Lightweight Directory Access Protocol) verziu 3. Okrem toho musí byť produkt adresárového servera nakonfigurovaný na prijatie schémy EIM. Túto podporu poskytuje IBM Tivoli Directory Server for i5/OS.

Súvisiace koncepty

"Operácie prehľadania EIM" na strane 27
Aplikácia alebo operačný systém používa rozhranie API mapovania EIM na vykonanie vyhľadávacej operácie, aby mohla aplikácia alebo operačný systém mapovať z jednej užívateľskej identity v jednom registri do inej užívateľskej identity v inom registri. Operácia prehľadania EIM je proces, prostredníctvom ktorého aplikácia alebo operačný systém vyhľadáva neznámu priradenú užívateľskú identitu v určitom cieľovom registri pomocou niektorých známych a dôveryhodných informácií.

"Schéma LDAP a ostatné úvahy o EIM" na strane 47
Tieto informácie môžete použiť, aby ste sa dozvedeli, čo sa vyžaduje, aby adresárový server fungoval s EIM.

Doména EIM

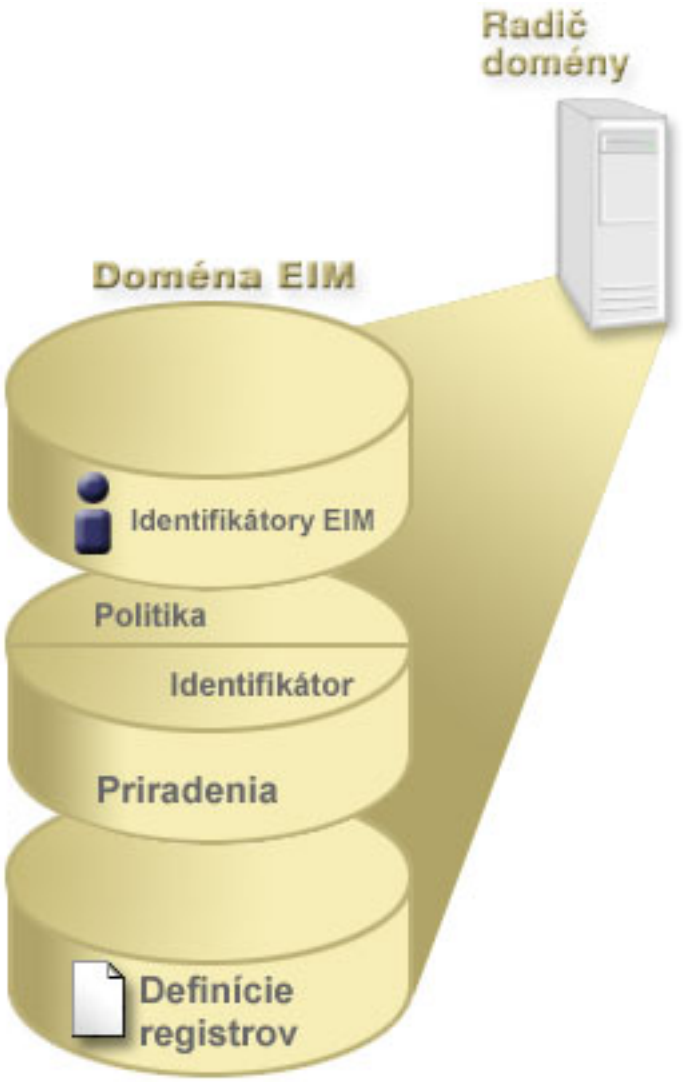
Doména EIM je adresár v serveri LDAP (Lightweight Directory Access Protocol), ktorý obsahuje údaje EIM pre podnik.

Doména EIM je kolekcia všetkých identifikátorov EIM, priradení EIM a registrov užívateľov, ktoré sú definované v tejto doméne a taktiež riadenia prístupu pre údaje. Systémy (klienti EIM) sú spojené s doménou tým, že používajú údaje domény pre operácie prehľadania EIM.

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

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

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



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

K údajom EIM patria:

Definície registrov EIM
Každá definícia registra EIM, ktorý vytvárate, predstavuje aktuálny register užívateľa (a informácie o identite užívateľa, ktoré obsahuje), ktorý existuje na systéme v rámci podniku. Keď zadefinujete špecifický register užívateľov v EIM, tento register užívateľov sa môže zaradiť do domény EIM. Môžete vytvoriť dva typy definícií registra, jeden typ sa týka systémových registrov užívateľov a druhý sa týka registrov užívateľov aplikácie.

Identifikátory EIM
Každý identifikátor EIM, ktorý vytvoríte jedinečne, predstavuje osobu alebo entitu (ako tlačový server alebo súborový server) v rámci podniku. Identifikátor EIM môžete vytvoriť, keď chcete mať mapovania typu jeden-jeden medzi identitami užívateľa, ktoré patria osobe alebo entite, s ktorou identifikátor EIM korešponduje.

Asociácie EIM
Priradenia EIM, ktoré vytvárate, predstavuje vzťahy medzi identitami užívateľa. Priradenia musíte definovať, aby klienti EIM mohli použiť rozhrania API EIM na vykonávanie operácií prehľadania EIM. Tieto operácie prehľadania EIM hľadajú v doméne EIM definované priradenia. Existujú dva rozdielne typy priradení, ktoré môžete vytvoriť:

Priradenia identifikátorov

Priradenia identifikátorov vám umožňujú definovať vzťah jeden-na-jeden medzi identitami užívateľa prostredníctvom identifikátora EIM, definovaného pre jednotlivca. Každé priradenie identifikátora EIM, ktoré vytvoríte, reprezentuje jediný, špecifický vzťah medzi identifikátorom EIM a pridruženou identitou užívateľa v rámci podniku. Priradenia identifikátorov poskytujú informácie, ktoré viažu identifikátor EIM k špecifickej identite užívateľa v špecifickom registri užívateľov a dovoľuje vám pre užívateľa vytvárať pripojenia typu jeden-jeden. Priradenia identít sú obzvlášť užitočné, keď jednotlivci majú identity užívateľa s mimoriadnymi oprávneniami a ďalšími privilégiami, ktoré chcete riadiť špecificky vytvorením mapovaní jeden-na-jeden medzi ich identitami užívateľa.

Priradenia politiky

Priradenia politiky vám umožňujú definovať vzťah medzi skupinou identít užívateľa v jednom alebo viacerých registroch užívateľa a jednotlivou identitou užívateľa v ďalšom registri užívateľa. Každé vytvorenie priradenia politiky EIM vedie k mapovaniu typu veľa-jeden medzi zdrojovou skupinou identít užívateľa v jednom registri užívateľov a jednou cieľovou identitou užívateľa. Typicky vytvárate priradenia politiky, aby ste mapovali skupinu užívateľov, ktorí všetci vyžadujú rovnakú úroveň autorizácie, na jedinú identitu užívateľa s takouto úrovňou autorizácie.

Súvisiace koncepty

"Definície registrov EIM" na strane 11
Definícia registra EIM je položka v EIM, ktorú vytvoríte na reprezentovanie aktuálneho registra užívateľov existujúceho v systéme v rámci podniku. Register užívateľov slúži ako adresár a obsahuje zoznam platných identít užívateľov pre konkrétny systém alebo aplikáciu.

"Identifikátor EIM"
Identifikátor EIM predstavuje 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.

"Operácie prehľadania EIM" na strane 27
Aplikácia alebo operačný systém používa rozhranie API mapovania EIM na vykonanie vyhľadávacej operácie, aby mohla aplikácia alebo operačný systém mapovať z jednej užívateľskej identity v jednom registri do inej užívateľskej identity v inom registri. Operácia prehľadania EIM je proces, prostredníctvom ktorého aplikácia alebo operačný systém vyhľadáva neznámu priradenú užívateľskú identitu v určitom cieľovom registri pomocou niektorých známych a dôveryhodných informácií.

Identifikátor EIM

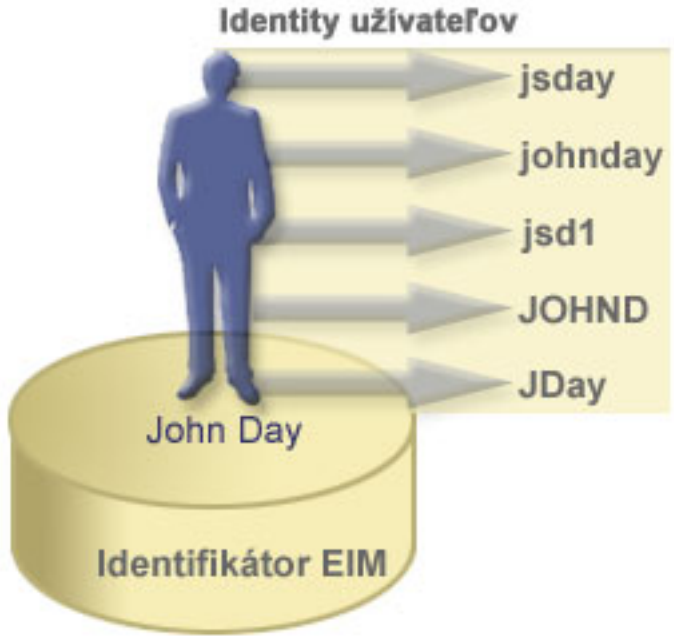
Identifikátor EIM predstavuje osobu alebo entitu v podniku. Typická sieť obsahuje rôzne hardvérové platformy a aplikácie a k nim priradené registre užívateľov. Väčšina platforiem a veľa aplikácií používa registre užívateľov, špecifické pre platformu alebo aplikáciu. Tieto registre užívateľov obsahujú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

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

Identifikátor EIM, reprezentujúci osobu

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

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

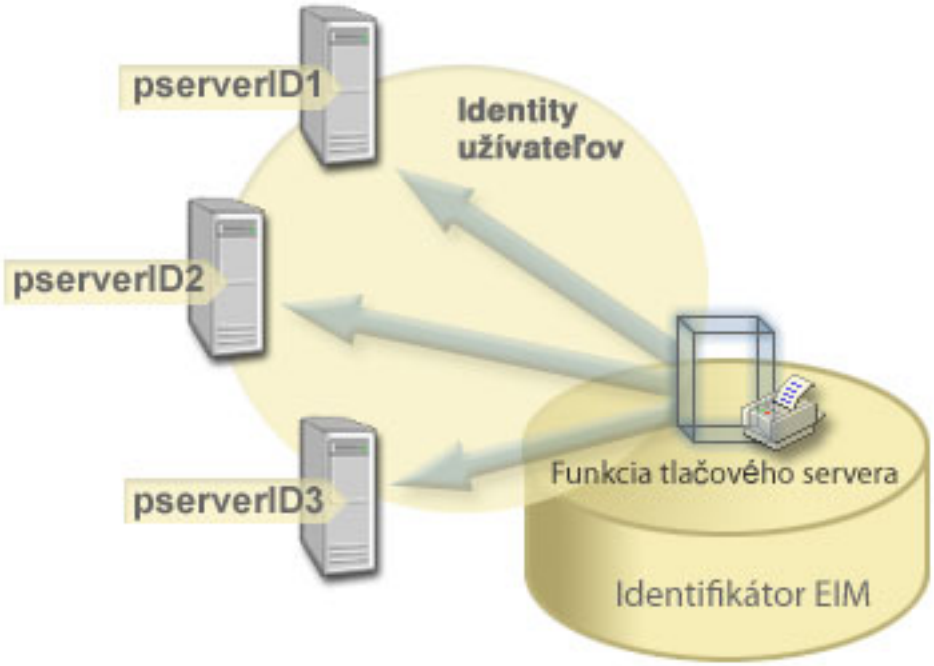


V EIM môžete vytvoriť priradenia, ktoré definujú vzťahy medzi identifikátorom John Day a každou z rôznych identít užívateľa pre *John Day*. Vytvorením týchto priradení na zadefinovanie týchto vzťahov môžete vy a ostatní písať aplikácie, ktoré používajú rozhrania API EIM na vyhľadanie potrebnej, ale neznámej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

Identifikátor EIM, reprezentujúci entitu

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

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



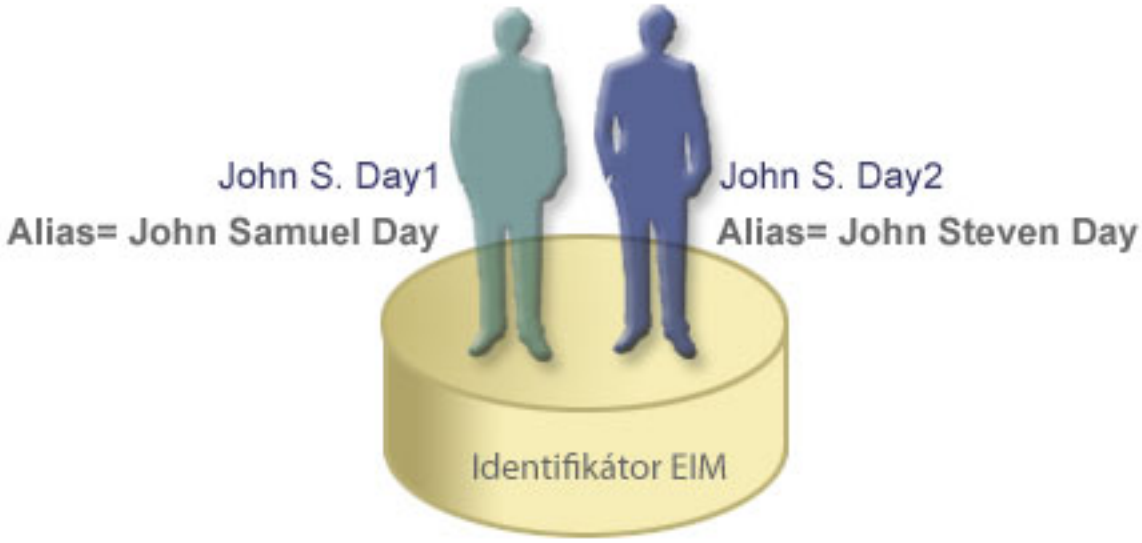
Pomocou EIM môžete vytvoriť jeden identifikátor, ktorý reprezentuje funkciu tlačového servera v celom podniku. Ako ukazuje príklad, identifikátor EIM Funkcia tlačového servera reprezentuje aktuálnu entitu funkcie tlačového servera v podniku. Na zadefinovanie vzťahu medzi identifikátorom EIM (Funkcia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

Identifikátory EIM a používanie aliasov

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

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

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



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

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

Súvisiace koncepty

"Doména EIM" na strane 6
Doména EIM je adresár v serveri LDAP (Lightweight Directory Access Protocol), ktorý obsahuje údaje EIM pre podnik.

Definície registrov EIM

Definícia registra EIM je položka v EIM, ktorú vytvoríte na reprezentovanie aktuálneho registra užívateľov existujúceho v systéme v rámci podniku. Register užívateľov slúži ako adresár a obsahuje zoznam platných identít užívateľov pre konkrétny systém alebo aplikáciu.

Základný register užívateľov obsahuje identity užívateľov a ich heslá. Jedným z príkladov registra užívateľov je register z/OS Security Server Resource Access Control Facility (RACF). Registre užívateľov tiež môžu obsahovať aj iné informácie. Napríklad adresár LDAP (Lightweight Directory Access Protocol) obsahuje prihlasovacie rozlišovacie názvy, heslá a riadenie prístupu k údajom, ktoré sú uložené v LDAP. Ďalšie príklady spoločných registrov užívateľov sú principáli v Kerberos sfére alebo identity užívateľov vo Windows doméne aktívneho adresára a i5/OS register užívateľských profilov.

Môžete tiež zadefinovať registre užívateľov, ktoré existujú v iných registroch užívateľov. Niektoré aplikácie používajú podmnožinu identít užívateľov z jednej inštancie registra užívateľov. Napríklad, register z/OS bezpečnostného servera (RACF) môže obsahovať špecifické registre užívateľov, ktoré sú podmnožinou užívateľov v rámci celkového RACF registra užívateľov.

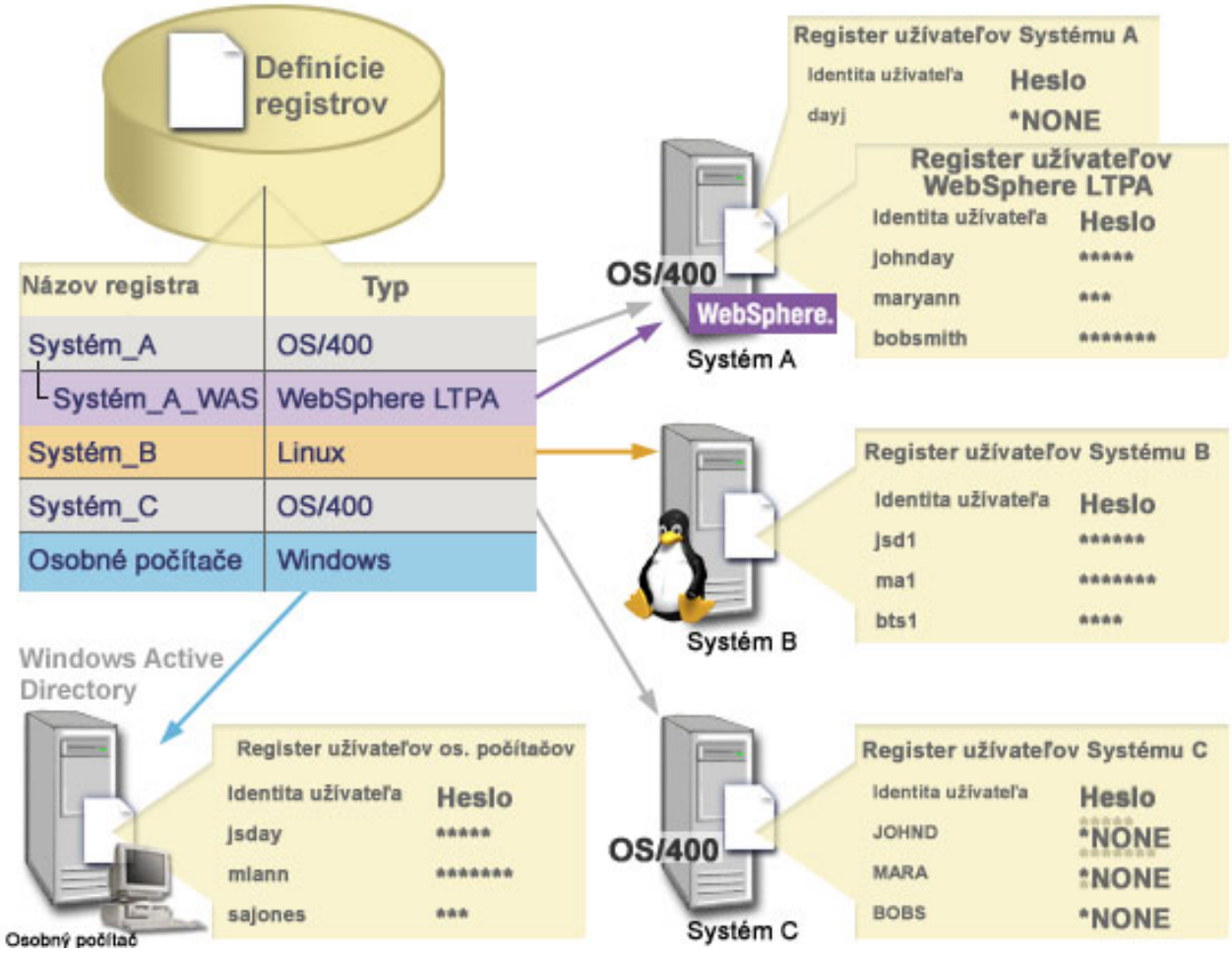
Definície registrov EIM poskytujú informácie o registroch užívateľov v podniku. Administrátor zadefinuje tieto registre v EIM zadaním týchto informácií:

- Jedinečný ľubovoľný názov registra EIM. Každá definícia registra reprezentuje špecifickú inštanciu registra užívateľov. Môžete vybrať taký názov definície registra EIM, ktorý vám pomôže identifikovať konkrétnu inštanciu registra užívateľov. Napríklad pre systémový register užívateľov môžete vybrať názov hostiteľa TCP/IP alebo názov hostiteľa skombinovaný s názvom aplikácie pre register užívateľov aplikácie. Môžete použiť ľubovoľnú kombináciu alfanumerických znakov, veľké i malé písmená a medzery na vytvorenie jedinečných názvov definícií registrov EIM.
- Typ registra užívateľov. Existuje viacero preddefinovaných typov registrov užívateľov, ktoré EIM poskytuje na pokrytie väčšiny registrov užívateľov operačného systému. Sú to:
  - AIX
  - Domino - dlhý názov
  - Domino - krátky názov
  - Kerberos
  - Kerberos - rozlišujúci veľkosť písmen
  - LDAP
  - - LDAP - Skratka
  - Linux
  - Adresárový server Novell
  - - Ostatné
  - - Ostatné - rozlišujúce malé a veľké písmená
  - i5/OS (alebo OS/400)
  - Tivoli Access Manager
  - RACF
  - Windows - lokálny
  - Windows doména (Kerberos) (Tento typ zohľadňuje veľkosť písmen.)
  - X.509

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

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

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



Poznámka: Aby sa ďalej znížila potreba riadiť heslá užívateľov, administrátor na obrázku 6 nastavuje heslá užívateľských profilov i5/OS v systéme A a systéme C na *NONE. Administrátor v tomto prípade nakonfiguruje prostredie jednoduchého prihlásenia a jediné aplikácie, s ktorými jeho užívatelia pracujú sú aplikácie povolené EIM, ako napríklad System i Navigator. Následne administrátor chce odstrániť heslá z ich užívateľských profilov i5/OS, takže ako užívatelia, tak aj administrátor, majú menej hesiel na riadenie.

Súvisiace koncepty

"Doména EIM" na strane 6
Doména EIM je adresár v serveri LDAP (Lightweight Directory Access Protocol), ktorý obsahuje údaje EIM pre podnik.

"Definovanie typu registra súkromného užívateľa v EIM" na strane 91
Keď vytvárate definíciu registra EIM, môžete zadať jedno číslo z preddefinovaných typov registra užívateľov na reprezentáciu aktuálneho registra užívateľov, ktorý sa nachádza v systéme v rámci podniku.

Definície systémového registra

Definícia systémového registra je záznam, ktorý vytvárate v EIM na reprezentovanie a popis jedinečného registra užívateľa v rámci pracovnej stanice alebo servera.

Definíciu systémového registra EIM pre register užívateľov môžete vytvoriť, ak má register v podniku jednu z nasledujúcich čŕt:

- Register je poskytovaný operačným systémom, ako AIX, i5/OS, alebo produktom riadenia bezpečnosti, ako z/OS Security Server Resource Access Control Facility (RACF).
- Register obsahuje identity užívateľov, ktoré sú jedinečné pre špecifickú aplikáciu, napríklad Lotus Notes.

- Tento register obsahuje distribuované identity užívateľov, napríklad principály Kerberos alebo rozlišovacie názvy LDAP (Lightweight Directory Access Protocol).

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

Súvisiace úlohy

"Pridávanie definície registra aplikácií" na strane 89
Ak chcete vytvoriť definíciu registra aplikácií, musíte byť pripojený do domény EIM, v ktorej chcete pracovať a musíte mať riadenie prístupov administrátora EIM.

Definície registra aplikácií

Definícia registra aplikácií je záznam v EIM, ktorý ste vytvorili pre popis a reprezentáciu podmnožiny identít užívateľa, ktoré sú definované v systémovom registri. Tieto identity užívateľov zdieľajú spoločnú množinu atribútov alebo charakteristík, ktoré im umožňujú použiť konkrétnu aplikáciu alebo množinu aplikácií.

Definície registra aplikácií reprezentujú registre užívateľov, ktoré existujú v rámci iných registrov užívateľov. Napríklad, register z/OS bezpečnostného servera (RACF) môže obsahovať špecifické registre užívateľov, ktoré sú podmnožinou užívateľov v rámci celkového RACF registra užívateľov. Kvôli tomuto vzťahu, musíte zadať pre každú definíciu registra aplikácií, ktorú vytvoríte, názov registra rodičovského systému.

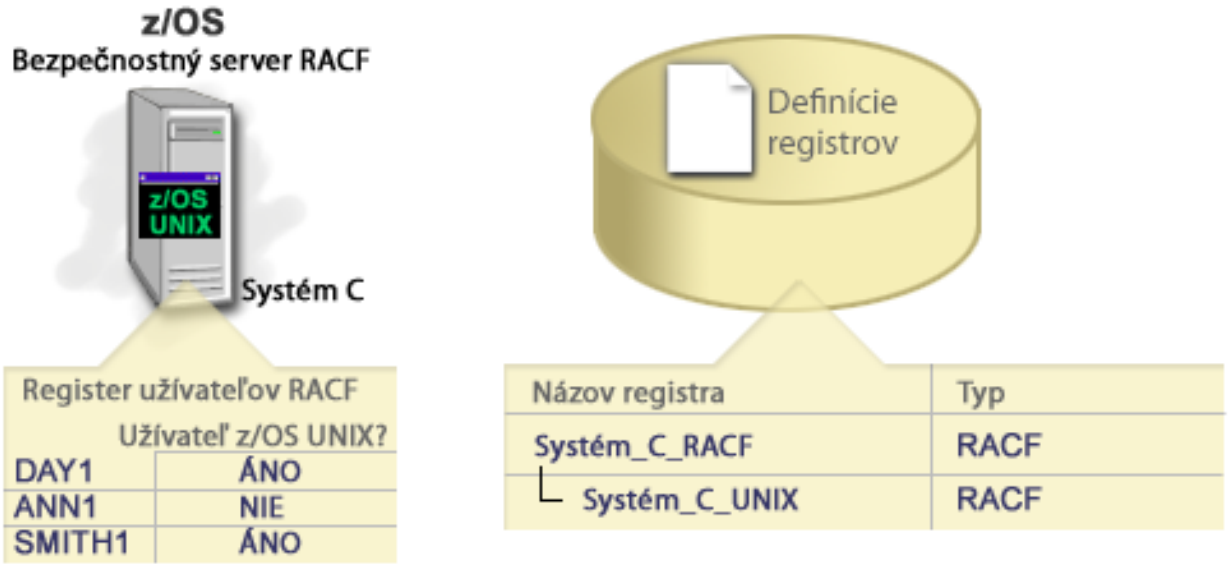
Pokiaľ majú identity užívateľa v registri nasledujúce črty, môžete vytvoriť definíciu aplikačného registra EIM pre register užívateľov:

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

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

Napríklad obrázok 7 ukazuje, ako vytvoril administrátor EIM definíciu systémového registra na reprezentovanie registra z/OS Security Server RACF. Administrátor tiež vytvoril definíciu registra aplikácií na reprezentovanie identít užívateľa v rámci RACF registra, ktorý používa z/OS(TM) UNIX systémové služby (z/OS UNIX). Systém C obsahuje register užívateľov RACF, ktorý obsahuje informácie pre tri identity užívateľov, DAY1, ANN1 a SMITH1. Dve z týchto identít užívateľov (DAY1 a SMITH1) sprístupňujú z/OS UNIX na systéme C. Tieto identity užívateľov sú v skutočnosti RACF užívatelia s jedinečnými atribútmi, ktoré ich identifikujú ako užívateľov z/OS UNIX. V rámci definícii registrov EIM definoval administrátor EIM System_C_RACF na reprezentovanie celkového registra užívateľov RACF. Administrátor tiež definoval System_C_UNIX na preprezentovanie identít, ktoré majú atribúty z/OS UNIX.

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



Definície skupinového registra

Logické zoskupovanie definícií registrov vám umožňuje redukovať množstvo práce, ktorú musíte vykonať, aby ste nakonfigurovali mapovanie EIM. Definíciu skupinového registra môžete riadiť podobným spôsobom, ako riadite definíciu individuálneho registra.

Všetci členovia definície skupinového registra typicky obsahujú minimálne jednu spoločnú identitu užívateľa, ku ktorej chcete vytvoriť cieľové alebo zdrojové priradenie. Vzájomným zoskupením členov ste schopní vytvoriť iba jediné priradenie, namiesto viacerých priradení do definície skupinového registra a identity užívateľa.

Napríklad, John Day sa prihlasuje do jeho primárneho systému s identitou užívateľa jday a používa tú istú identitu užívateľa, JOHND, na viacerých systémoch. Z tohto dôvodu register užívateľa pre každý systém obsahuje identitu užívateľa JOHND. Typicky John Day vytvára samostatné cieľové priradenie z identifikátora EIM John Day EIM ku každému z individuálnych registrov užívateľov, ktoré obsahujú identitu užívateľa JOHND. Ak chce znížiť množstvo práce, ktorú musí vykonať pri konfigurovaní mapovania EIM, môže vytvoriť jednu definíciu skupinového registra so všetkými registrami užívateľov, ktoré uchovávajú identitu užívateľa JOHND ako člena skupiny. Potom bude môcť vytvoriť jednotlivé cieľové priradenie z John Day identifikátora EIM k definícii skupinového registra namiesto viacerých cieľových priradení z identifikátora EIM John Day ku každej z definícií individuálneho registra. Toto jednotlivé cieľové priradenie k definícii skupinového registra umožňuje identite užívateľa John Day jday mapovať na identitu užívateľa JOHND.

Prečítajte si nasledujúce informácie o definíciách skupinových registrov:

- Všetci členovia (definície individuálnych registrov) definície skupinového registra musia mať rovnaké rozlišovanie veľkých a malých písmen.
- Všetci členovia (definície individuálnych registrov) definície skupinového registra musia byť definovaní v doméne EIM predtým, ako ich môžete pridať do definície skupinového registra.
- Definícia registra môže byť členom viacerých skupín, ale nemali by ste zadávať individuálny register užívateľov ako člena viacerých definícií skupinových registrov, pretože vyhľadávacie operácie môžu vrátiť nejednoznačné výsledky. Definícia skupinového registra nemôže byť členom ďalšej definície skupinového registra.

Súvisiace koncepty

"Príklady operácie vyhľadávania: Príklad 5" na strane 35
Použite tento príklad, ak sa chcete dozvedieť viac o operáciách vyhľadávania, ktoré produkujú nejednoznačné výsledky, ktorých súčasťou sú definície skupinových registrov.

Asociácie EIM

Priradenie EIM je položka, ktorú vytvoríte v doméne EIM na definovanie vzťahu medzi užívateľskými identitami v rôznych registroch užívateľov. Typ priradenia ktoré vytvárate závisí od toho, či je definovaný vzťah priamy alebo nepriamy.

V EIM môžete vytvoriť dva typy priradení: priradenia identifikátora a priradenia politiky. Priradenia politiky môžete použiť namiesto alebo v kombinácií s priradeniami identifikátora. Spôsob, akým použijete priradenia závisí na vašom úplnom pláne implementácie EIM.

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

Informácie na vyhľadanie

Pomocou EIM môžete poskytnúť voliteľné údaje, ktoré sa nazývajú vyhľadávacie informácie, na ďalšiu identifikáciu cieľovej užívateľskej identity. Táto cieľová identita užívateľa môže byť špecifikovaná buď v priradení identifikátora alebo v priradení politiky.

Informácie na vyhľadanie sú jedinečným znakovým reťazcom, ktorý môže buď API eimGetTargetFromSource EIM, alebo API eimGetTargetFromIdentifier EIM používať pri operácii vyhľadávania mapovaní na ďalšie zjemnenie hľadania cieľovej identity užívateľa, ktorá je objektom operácie. Údaje, ktoré špecifikujete pre informácie na vyhľadanie korešpondujú s parametrom dodatočných informácií užívateľov z registra pre tieto rozhrania API EIM.

Informácie na vyhľadanie sú potrebné, len keď operácia vyhľadávania mapovaní môže vrátiť viac ako jednu cieľovú identitu užívateľa. Operácia vyhľadávania mapovania môže vrátiť viacero identít cieľového užívateľa v prípade jednej alebo viacerých nasledujúcich situácií:

- Identifikátor EIM má viaceré individuálne cieľové priradenia k rovnakému cieľovému registru.
- Viac ako jeden identifikátor EIM má v zdrojovom priradení zadanú tú istú identitu užívateľa a každý z nich má cieľové priradenie k tomu istému cieľovému registru, aj keď identita užívateľa zadaná pre každé cieľové priradenie môže byť rôzna.
- Viac ako jedno predvolené priradenie politiky domény určuje ten istý cieľový register.
- Viac ako jedno predvolené priradenie politiky registra určuje ten istý zdrojový register a ten istý cieľový register.
- Viac ako jedno priradenie politiky filtra certifikátov určuje ten istý zdrojový register X.509, filter certifikátov a cieľový register.

Poznámka: Operácia vyhľadávania mapovaní, ktorá vracia viac ako jednu cieľovú identitu užívateľa, môže spôsobovať problémy pre aplikácie dovolené od EIM, vrátane i5/OS aplikácií a produktov, ktoré nie sú navrhnuté pre ošetrenie takýchto nejednoznačných výsledkov. Základné aplikácie i5/OS ako napríklad System i Access for Windows však nemôžu používať vyhľadávacie informácie na rozlíšenie medzi viacerými cieľovými užívateľskými identitami vrátenými operáciou vyhľadávania. Následne by ste mohli zvážiť predefinovanie priradení pre doménu, aby ste zabezpečili, že operácia vyhľadávania mapovania dokáže vrátiť jedinú cieľovú identitu užívateľa pre zaistenie, aby základné i5/OS aplikácie mohli úspešne vykonať operácie vyhľadávania a mapovať identity.

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

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

oprávnením užívateľa pre JDUSER. Druhé cieľové priradenie je pre identitu užívateľa JDSECADM v cieľovom registri systému A a má zadané informácie na vyhľadanie správcu bezpečnosti pre JDSECADM.

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

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

Vzhľadom na to, že priradenia politiky certifikátov a iné priradenia môžete použiť viacerými súbežnými spôsobmi, mali by ste pred vytvorením a použitím priradení politiky certifikátov dôkladne porozumieť podpore politiky mapovania EIM a spôsobu fungovania vyhľadávacích operácií.

Súvisiace koncepty

"Operácie podpory a umožnenia politiky mapovaní EIM" na strane 37
Podpora politiky mapovania podnikovej identity (EIM) umožňuje používať v doméne EIM priradenia politiky a tiež špecifické priradenia identifikátorov. Priradenia politiky môžete používať namiesto alebo v kombinácii s priradeniami identifikátorov.

"Operácie prehľadania EIM" na strane 27
Aplikácia alebo operačný systém používa rozhranie API mapovania EIM na vykonanie vyhľadávacej operácie, aby mohla aplikácia alebo operačný systém mapovať z jednej užívateľskej identity v jednom registri do inej užívateľskej identity v inom registri. Operácia prehľadania EIM je proces, prostredníctvom ktorého aplikácia alebo operačný systém vyhľadáva neznámu priradenú užívateľskú identitu v určitom cieľovom registri pomocou niektorých známych a dôveryhodných informácií.

"Predvolené priradenia politiky domény" na strane 21
Predvolené priradenie politiky domény predstavuje jeden typ priradenia politiky, ktorý môžete použiť na vytvorenie mapovaní typu veľa-jeden medzi identitami užívateľov.

"Predvolené priradenia politiky registrov" na strane 23
Predvolené priradenie politiky registra predstavuje jeden typ priradenia politiky, ktorý môžete použiť na vytvorenie mapovaní typu veľa-jeden medzi identitami užívateľov.

Priradenia identifikátorov

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

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

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

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

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

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

Zdrojové priradenie

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

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

Cieľové priradenie

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

Keď sa identita užívateľa použije na *autorizáciu* namiesto autentifikácie, daná identita užívateľa by mala mať cieľové priradenie k identifikátoru EIM. Môžete napríklad vytvoriť cieľové priradenie pre užívateľský profil i5/OS, pretože táto forma užívateľskej identity určuje, ktoré prostriedky a privilégiá užívateľ na danej platforme System i má. Ak chcete zabezpečiť úspešné operácie vyhľadávania mapovaní pre identifikátory EIM, zdrojové a cieľové priradenia sa musia použiť pre jeden identifikátor EIM spoločne.

Vzťah zdrojového a cieľového priradenia

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

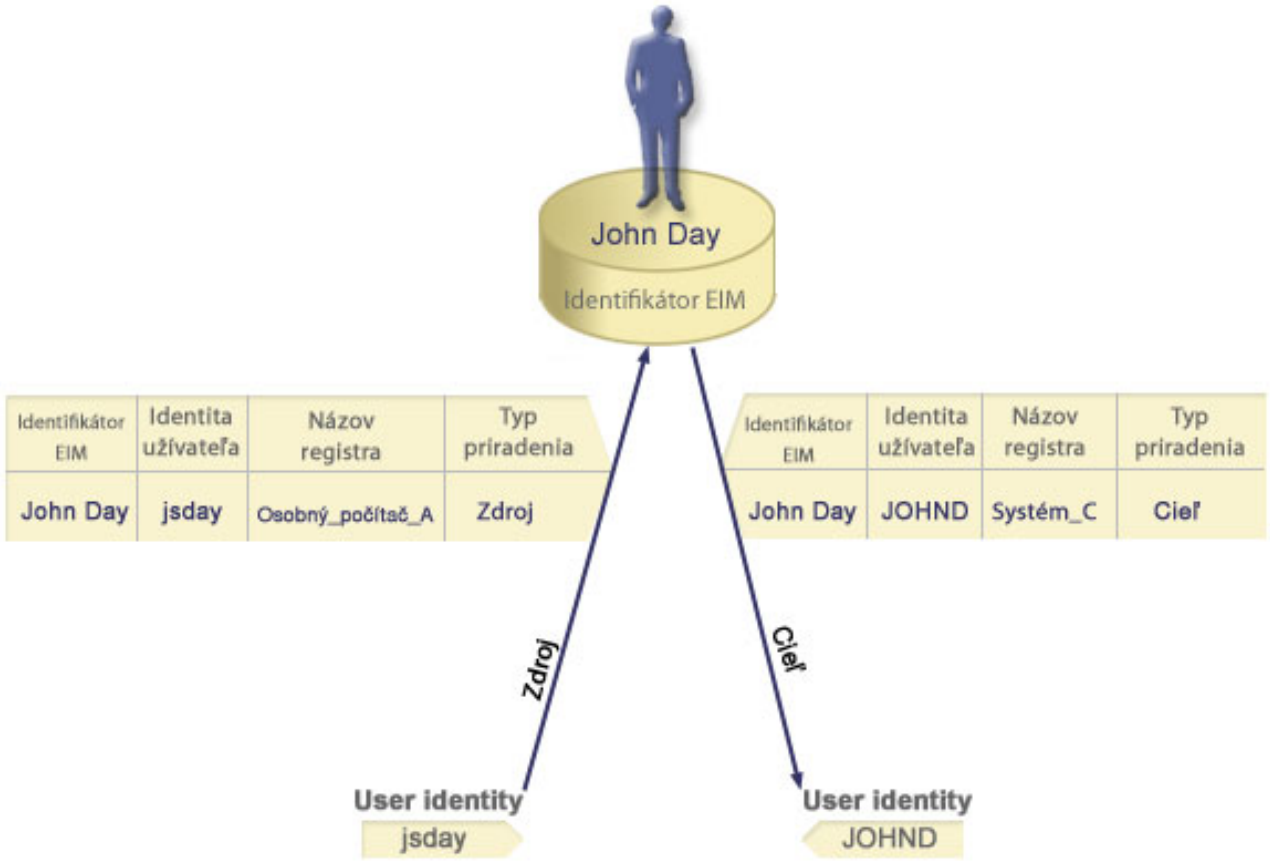
Užívatelia vo vašom podniku sa napríklad normálne prihlásia a autentifikujú na pracovné plochy Windows a získajú prístup na platformu System i na vykonanie mnohých úloh. Užívatelia sa prihlásia na svoje pracovné plochy pomocou principálu Kerberos a na platformu System i pomocou užívateľského profilu i5/OS. Chcete vytvoriť prostredie jednoduchého prihlásenia, v ktorom sa užívatelia autentifikujú na svoje pracovné plochy pomocou principálu Kerberos a už sa nemusia manuálne autentifikovať na platformu System i.

Na splnenie tohto cieľa stačí vytvoriť zdrojové priradenie pre principál Kerberos pre každého užívateľa k identifikátoru EIM užívateľa. Potom vytvoríte cieľové priradenie pre profil užívateľa i5/OS pre každého užívateľa, a to bude identifikátor EIM tohto užívateľa. Táto konfigurácia zabezpečí, že i5/OS môže vykonať vyhľadávaciu operáciu mapovania s cieľom určiť správny užívateľský profil potrebný pre užívateľa, ktorý vstupuje na platformu System i po

autentifikácii na svoju pracovnú plochu. i5/OS potom užívateľovi umožní prístup k zdrojom na serveri na základe príslušného profilu užívateľa bez toho, aby sa užívateľ musel na server autentifikovať manuálne.

Obrázok 6 znázorňuje ďalší príklad, kde administrátor EIM vytvoril dve priradenia, zdrojové a cieľové, pre identifikátor EIM John Day na definovanie vzťahu medzi týmto identifikátorom a dvoma priradenými identitami užívateľov. Administrátor vytvoril zdrojové priradenie pre princípál Kerberos jsday v registri užívateľov Desktops. Administrátor taktiež vytvorí cieľové priradenie pre JOHND, užívateľský profil i5/OS v registri užívateľov v System_C. Tieto priradenia poskytujú aplikáciám prostriedky na získanie neznámej identity užívateľa (cieľ JOHND) na základe známej identity užívateľa (zdroj jsday) ako časti operácie prehľadania EIM.

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



Aby sme uviedli rozšírený príklad, predpokladajme, že administrátor EIM si uvedomí, že John Day používa rovnaký užívateľský profil i5/OS, jsd1, na piatich rozličných systémoch. V tejto situácii musí administrátor vytvoriť šesť priradení pre identifikátor EIM John Day, aby zadefinoval vzťah medzi týmto identifikátorom a priradenou užívateľskou identitou v piatich registroch užívateľov: zdrojové priradenie pre johnday, princípála Kerberos v registri užívateľov Desktop_A a päť cieľových priradení pre jsd1, užívateľský profil i5/OS v piatich registroch užívateľov: System_B, System_C, System_D, System_E, a System_F. Na zmenu rozsahu prác, ktoré je potrebné vykonať na konfiguráciu mapovania EIM, musí administrátor EIM vytvoriť definíciu skupinového registra. Súčasťou definície skupinového registra sú definované názvy registra System_B, System_C, System_D, System_E, a System_F. To, že sú členy v skupine, umožňuje administrátorovi vytvoriť jediné cieľové priradenie definícii skupinového registra a identity užívateľov, namiesto viacerých priradení k jednotlivým názvom registrov. Zdrojové a cieľové priradenia poskytujú aplikáciám prostriedky na získanie neznámej identity užívateľa (cieľ jsd1) v piatich registroch užívateľov, ktoré sú zastúpené ako skupinová definícia na základe známej identity užívateľa (zdroj johnday) ako časti operácie prehľadania EIM.

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

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

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

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

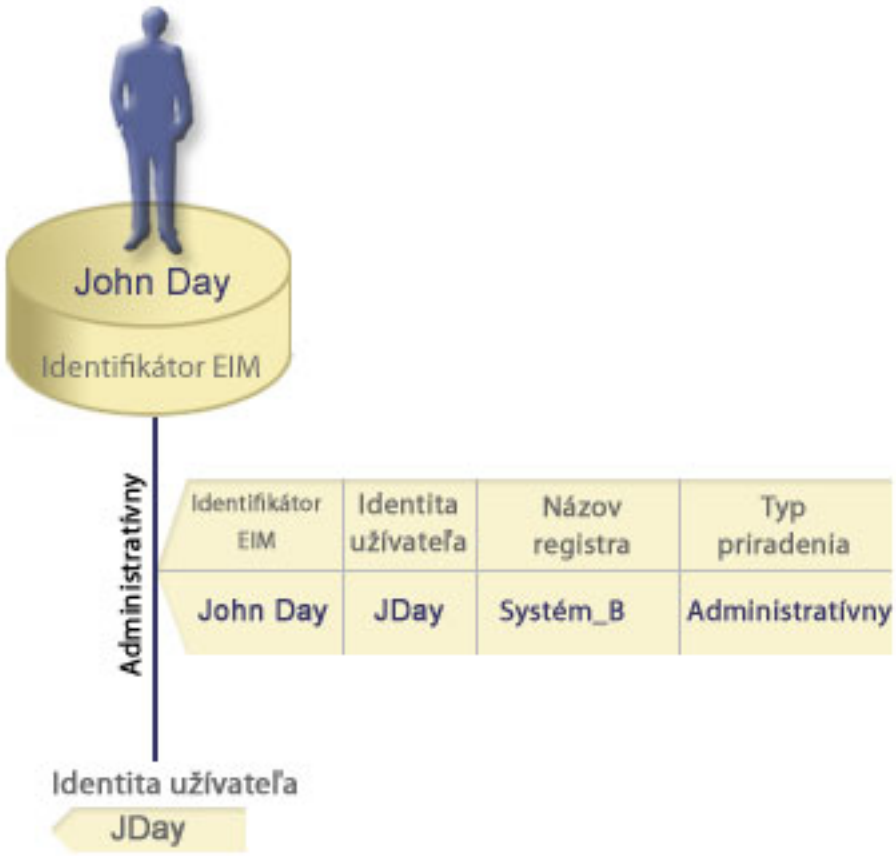
Administratívne priradenie

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

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

Obrázok 7 znázorňuje príklad administratívneho priradenia. V tomto príklade má zamestnanec John Day identitu užívateľa John_Day v systéme A a identitu užívateľa JDay v systéme B, ktorý predstavuje vysoko bezpečný systém. Administrátor systému chce zaistiť, aby sa užívatelia autentifikovali pre System B len pomocou lokálneho registra užívateľov tohto systému. Administrátor nechce povoliť aplikácii autentifikovať zamestnanca s menom John Day do systému pomocou iného autentifikačného mechanizmu. Použitím administratívneho priradenia pre identitu užívateľa JDay v System B môže administrátor EIM zistiť, že John Day vlastní konto v System B, ale EIM v operáciách prehľadania EIM nevráti žiadne informácie o identite JDay. Aplikácie nenájdu pomocou operácií prehľadania EIM identity užívateľov s administratívnymi priradeniami ani v prípade, ak existujú v tomto systéme.

Obrázok 7: Administratívne priradenie EIM pre identifikátor EIM John Day



Priradenia politiky

Politika mapovania podnikovej identity (EIM) umožňuje administrátorovi EIM vytvárať a používať priradenia politiky na definovanie vzťahu medzi viacerými identitami užívateľa v jednom alebo viacerých registroch užívateľa, a jednotlivou identitou užívateľa v inom registri užívateľa.

Priradenia politiky používajú podporu politík mapovania EIM na vytvorenie mapovaní typu veľa-jeden medzi identitami užívateľov bez použitia identifikátora EIM. Priradenia politiky môžete používať namiesto alebo v kombinácii s priradeniami identifikátorov, ktoré poskytujú mapovania typu veľa-jeden medzi identifikátorom EIM a jednou identitou užívateľa.

Priradenie politiky ovplyvňuje len identity užívateľov, pre ktoré neexistujú konkrétne samostatné priradenia EIM. Ak existujú konkrétne priradenia identifikátorov medzi identifikátorom EIM a identitami užívateľov, aplikácii vykonávajúcej operáciu vyhľadávania sa vráti cieľová identita užívateľa z priradenia identifikátora, aj keď existuje priradenie politiky a priradenia politiky sú povolené.

Môžete vytvoriť tri rôzne typy priradení politiky:

Súvisiace koncepty

"Operácie prehľadania EIM" na strane 27
Aplikácia alebo operačný systém používa rozhranie API mapovania EIM na vykonanie vyhľadávacej operácie, aby mohla aplikácia alebo operačný systém mapovať z jednej užívateľskej identity v jednom registri do inej užívateľskej identity v inom registri. Operácia prehľadania EIM je proces, prostredníctvom ktorého aplikácia alebo operačný systém vyhľadáva neznámu priradenú užívateľskú identitu v určitom cieľovom registri pomocou niektorých známych a dôveryhodných informácií.

Predvolené priradenia politiky domény:

Predvolené priradenie politiky domény predstavuje jeden typ priradenia politiky, ktorý môžete použiť na vytvorenie mapovaní typu veľa-jeden medzi identitami užívateľov.

Predvolené priradenie politiky domény môžete použiť na namapovanie zdrojovej množiny viacerých identít užívateľov (v tomto prípade všetkých užívateľov v doméne) k jednej cieľovej identite užívateľa v konkrétnom cieľovom registri užívateľov. Pri predvolenom priradení politiky domény predstavujú všetci užívatelia v doméne zdroj priradenia politiky a sú namapovaní k jednému cieľovému registru a jednej cieľovej identite užívateľa.

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

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

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

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

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

Predvolené priradenie politiky domény môžete definovať pre každý register v doméne. Ak dve alebo viacero priradení politiky domény odkazuje na rovnaký cieľový register, musíte pre každé z týchto priradení politiky zadefinovať jedinečné vyhľadávacie informácie a zabezpečiť tak, aby ich vyhľadávacie operácie mapovania rozlišovali. V opačnom prípade môžu operácie vyhľadávania mapovaní vrátiť viacero cieľových identít užívateľov. Následkom týchto nejednoznačných výsledkov môže byť neschopnosť aplikácií spoliehajúcich sa na EIM určiť presnú cieľovú identitu užívateľa, ktorá sa má použiť.

Vzhľadom na to, že priradenia politiky môžete použiť viacerými súbežnými spôsobmi, mali by ste najprv dôkladne porozumieť podpore politiky mapovania EIM a spôsobu fungovania vyhľadávacích operácií a potom vytvárať a používať priradenia politiky.

Poznámka: Mohli by ste chcieť vytvoriť priradenie predvolenej politiky domény s cieľovou identitou užívateľa, ktorá existuje v rámci definície skupinového registra. Všetci užívatelia v doméne sú zdrojom priradenia politiky a sú namapovaní k cieľovej užívateľskej identite v cieľovej definícii skupinového registra. Užívateľská identita, ktorú definujete v predvolenom priradení politiky domény, existuje v rámci členov definície skupinového registra.

Napríklad John Day používa rovnaký užívateľský profil i5/OS, John_Day, na piatich rôznych systémoch: Systém B, Systém C, Systém D, Systém E a Systém F. Na zníženie množstva práce , ktoré musí vykonať na konfiguráciu mapovania EIM, administrátor EIM vytvorí definíciu skupinového registra s názvom Group_1. Členovia definície skupinového registra zahŕňajú názvy definícií registra System_B, System_C, System_D, System_E a System_F. Zoskupovanie členov umožňuje administrátorovi vytvoriť jedno cieľové priradenie k definícii skupinového registra a užívateľskú identitu, a nie viaceré priradenia k individuálnym definíciám registra.

Administrátor EIM vytvorí predvolené priradenie politiky domény s cieľovou identitou užívateľa John_Day v cieľovom registri Group_1. V takom prípade sa nepoužije žiadne iné priradenie špecifického identifikátora alebo priradenie politiky. Preto, keď je špecifikovaná Group_1 ako cieľový register v operáciách vyhľadávania, predvolená politika domény zaručí, že cieľová identita užívateľa John_Day sa vráti pre všetky užívateľské identity v doméne, ktorá nemá pre nich definované žiadne špecifické priradenia identifikátora.

Súvisiace koncepty

"Informácie na vyhľadanie" na strane 16
Pomocou EIM môžete poskytnúť voliteľné údaje, ktoré sa nazývajú vyhľadávacie informácie, na ďalšiu identifikáciu cieľovej užívateľskej identity. Táto cieľová identita užívateľa môže byť špecifikovaná buď v priradení identifikátora alebo v priradení politiky.

"Operácie podpory a umožnenia politiky mapovaní EIM" na strane 37
Podpora politiky mapovania podnikovej identity (EIM) umožňuje používať v doméne EIM priradenia politiky a tiež špecifické priradenia identifikátorov. Priradenia politiky môžete používať namiesto alebo v kombinácii s priradeniami identifikátorov.

Predvolené priradenia politiky registrov:

Predvolené priradenie politiky registra predstavuje jeden typ priradenia politiky, ktorý môžete použiť na vytvorenie mapovaní typu veľa-jeden medzi identitami užívateľov.

Predvolené priradenie politiky registra môžete použiť na namapovanie zdrojovej množiny viacerých identít užívateľov (v tomto prípade sa nachádzajú v jednom registri) k jednej cieľovej identite užívateľa v konkrétnom cieľovom registri užívateľov. Pri predvolenom priradení politiky registra predstavujú všetci užívatelia v jednom registri zdroj priradenia politiky a sú namapovaní k jednému cieľovému registru a cieľovému užívateľovi.

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

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

Napríklad vytvoríte predvolené priradenie politiky registra so zdrojovým registrom my_realm.com, ktorý predstavuje principály v konkrétnom realme Kerberos. Pre toto priradenie politiky musíte tiež zadať cieľovú užívateľskú identitu general_user1 v cieľovom registri i5/OS_system_reg, ktorý je konkrétny profil užívateľa v užívateľskom registri i5/OS. V tomto prípade ste nevytvorili žiadne priradenia identifikátorov ani priradenia politiky, týkajúce sa identít užívateľov v zdrojovom registri. Preto keď zadáte i5/OS_system_reg ako cieľový register a my_realm.com ako zdrojový register vyhľadávacích operácií, politika priradenia štandardného registra zaručí, že cieľová identita užívateľa general_user1 sa vráti pre všetky užívateľské identity v my_realm.com, ktoré nemajú definované žiadne konkrétne priradené identifikátory alebo politiky filtrovania certifikátov.

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

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

Môžete definovať viac ako jedno predvolené priradenie politiky registra. Ak dve alebo viacero priradení politiky s rovnakým zdrojovým registrom odkazuje na rovnaký cieľový register, musíte pre každé z týchto priradení politiky zadefinovať jedinečné vyhľadávacie informácie a zabezpečiť tak, aby ich vyhľadávacie operácie mapovania rozlišovali. V opačnom prípade môžu operácie vyhľadávania mapovaní vrátiť viacero cieľových identít užívateľov. Následkom týchto nejednoznačných výsledkov môže byť neschopnosť aplikácií spoliehajúcich sa na EIM určiť presnú cieľovú identitu, ktorá sa má použiť.

Vzhľadom na to, že priradenia politiky môžete použiť viacerými súbežnými spôsobmi, mali by ste pred vytvorením a použitím priradení politiky dôkladne porozumieť podpore politiky mapovania EIM a spôsobu fungovania vyhľadávacích operácií.

Poznámka: Môžete vytvoriť politiku priradenia predvoleného registra s cieľovou identitou užívateľa, ktorá existuje v rámci skupinovej definície registra. Všetci užívatelia v zdrojovom registri užívateľov sú zdrojom priradenia politiky a sú mapovaní na jednu cieľovú identitu užívateľa v cieľovej definícii skupinového registra. Užívateľská definícia, ktorú zadefinujete v predvolenom registri politiky priradenia, existuje v rámci členov skupinovej definície registra.

Napríklad John Day používa rovnaký profil užívateľa i5/OS, John_Day, na piatich rozličných systémoch: System_B, System_C, System_D, System_E, a System_F. Aby sa zredukovalo množstvo práce, ktorú musí vykonať na konfiguráciu mapovania EIM, administrátor EIM vytvorí skupinovú definíciu registra s názvom Group_1. Súčasťou definície skupinového registra sú definované názvy registra System_B, System_C, System_D, System_E, a System_F. To, že sú členy v skupine, umožňuje administrátorovi vytvoriť jediné cieľové priradenie definícii skupinového registra a identity užívateľov, namiesto viacerých priradení k jednotlivým definíciám registrov.

Administrátor EIM vytvorí predvolené priradenie politiky registra so zdrojovým registrom my_realm.com, ktorý predstavuje princípály v konkrétnom prostredí Kerberos. Pre toto priradenie politiky taktiež zadá cieľovú užívateľskú identitu John_Day v cieľovom registri Group_1. V tomto prípade neplatia žiadne iné priradenia identifikátorov alebo politiky. Preto keď zadáte Group_1 ako cieľový register a my_realm.com ako zdrojový register vyhľadávacích operácií, politika priradenia štandardného registra zaručí, že cieľová identita užívateľa John_Day sa vráti pre všetky užívateľské identity v my_realm.com, ktoré nemajú definované žiadne konkrétne priradené identifikátory.

Súvisiace koncepty

"Informácie na vyhľadanie" na strane 16
Pomocou EIM môžete poskytnúť voliteľné údaje, ktoré sa nazývajú vyhľadávacie informácie, na ďalšiu identifikáciu cieľovej užívateľskej identity. Táto cieľová identita užívateľa môže byť špecifikovaná buď v priradení identifikátora alebo v priradení politiky.

"Operácie podpory a umožnenia politiky mapovaní EIM" na strane 37
Podpora politiky mapovania podnikovej identity (EIM) umožňuje používať v doméne EIM priradenia politiky a tiež špecifické priradenia identifikátorov. Priradenia politiky môžete používať namiesto alebo v kombinácii s priradeniami identifikátorov.

Priradenia politiky filtra certifikátov:

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

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

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

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

Keď digitálny certifikát je identitou zdrojového užívateľa vo vyhľadávacej operácii mapovania podnikovej identity (EIM) (potom keď požadujúca aplikácia použije eimFormatUserIdentity() EIM API na formátovanie mena identity užívateľa), EIM najprv skontroluje, či existuje spojenie identifikátora medzi identifikátorom EIM a špecifikovanou identitou užívateľa. Ak neexistuje, EIM porovná informácií o DN v certifikáte s hodnotou DN alebo s čiastočnými informáciami zadanými vo filtri pre priradenie politiky. Ak informácie DN v certifikáte spĺňajú kritérium filtra, EIM vráti cieľovú identitu užívateľa, zadanú priradením politiky. Výsledkom je namapovanie tých certifikátov v zdrojovom registri X.509, ktoré spĺňajú kritérium filtra certifikátov, k jednej cieľovej identite užívateľa podľa priradenia politiky filtra certifikátov.

Napríklad vytvoríte priradenie politiky filtra certifikátov so zdrojovým registrom certificates.x509. Tento register obsahuje certifikáty pre všetkých zamestnancov spoločnosti vrátane tých, ktoré používajú všetci manažéri v oddelení ľudských zdrojov na prístup k určitým súkromným interným webových stránkam ako aj ostatné prostriedky, do ktorých majú prístup prostredníctvom modelu System i. Pre toto spojenie politiky tiež špecifikujete identitu cieľového užívateľa hr_managers v cieľovom registri system_abc, ktorý je špecifickým užívateľským profilom v registri užívateľov i5/OS. Ak chcete skontrolovať, že toto priradenie politiky pokrýva len certifikáty patriace manažérom ľudských zdrojov, zadajte filter certifikátov s rozlišovacím názvom subjektu (SDN) ou=hrmgr,o=myco.com,c=us.

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

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

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

Keďže priradenia politiky certifikátov a ostatné priradenia môžete používať rôznymi súbežnými spôsobmi, mali by ste dôkladne porozumieť podpore politiky mapovania EIM a tiež tomu, ako fungujú operácie vyhľadávania ešte predtým, než začnete vytvárať a používať priradenia politiky certifikátov.

Poznámka: Mohli by ste chcieť vytvoriť priradenie politiky filtrovania certifikátov s cieľovou identitou užívateľa, ktorá existuje v rámci definície skupinového registra. Užívatelia v zdrojovom registri, ktorí spĺňajú kritériá špecifikované filtrom certifikátov, sú zdrojom priradenia politiky a sú mapované k cieľovej identite užívateľa v cieľovej definícii skupinového registra. Identita užívateľa, ktorú definujete v priradení politiky filtrovania certifikátov, existuje v rámci členov definície skupinového registra.

Napríklad John Day používa rovnaký i5/OS užívateľský profil, John_Day, na piatich rôznych systémoch: Systém B, Systém C, Systém D, Systém E a Systém F. Na zníženie množstva práce, ktoré musí vykonať na konfiguráciu mapovania EIM, administrátor EIM vytvorí definíciu skupinového registra. Členovia definície skupinového registra zahŕňajú názvy definícií registra System_B, System_C, System_D, System_E a System_F. Zoskupovanie členov umožňuje administrátorom vytvoriť jedno cieľové priradenie k definícii skupinového registra a identite užívateľa, a nie viaceré priradenia k individuálnym definíciám registra.

Administrátor EIM vytvorí priradenie politiky filtrovania certifikátov, kde definuje podmnožinu certifikátov v rámci jedného X.509 registra, ako zdroja priradenia politiky. Špecifikuje cieľovú identitu užívateľa John_Day v cieľovom registri Group_1. V tomto prípade sa nepoužije žiadne iné priradenie špecifického identifikátora alebo iné priradenie politiky filtrovania certifikátov. Takže keď je Group_1 špecifikovaná ako cieľový register v operácii vyhľadávania, všetky certifikáty v zdrojovom X.509 registri, ktoré sa zhodujú s kritériom filtra certifikátu, sú namapované k špecifikovanej cieľovej identite užívateľa.

Filtre certifikátov:

Filter certifikátov definuje sadu podobných atribútov certifikátov s charakteristickým názvom pre skupinu užívateľských certifikátov v zdrojovom registri užívateľov X.509. Filter certifikátov môžete použiť ako základ priradenia politiky filtra certifikátov.

Filter certifikátov v priradení politiky určuje, ktoré certifikáty v zadanom zdrojovom registri X.509 sa majú namapovať k zadanému cieľovému užívateľovi. Tie certifikáty, ktoré majú informáciu Subject DN a Issuer DN, ktoré vyhovujú kritériam filtra, sú namapované do špecifikovaného cieľového užívateľa počas operácií vyhľadávania mapovania podnikovej identity (EIM).

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

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

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

Existuje niekoľko metód, ktoré môžete použiť pri vytváraní filtra certifikátov vrátane použitia Format EIM Policy Filter API na vygenerovanie filtrov certifikátov pomocou certifikátu ako šablóny na vytvorenie potrebných DN v príslušnom poradí a formáte pre SDN a IDN.

Súvisiace koncepty

“Charakteristický názov” na strane 46
Rozlišovací názov (DN) je LDAP záznam, ktorý jednoznačne identifikuje a popisuje záznam v adresárovom (LDAP) serveri. Použite konfiguračného sprievodcu EIM na konfigurovanie adresárového servera pre ukladanie informácií domény EIM. EIM používa adresárový server na ukladanie údajov EIM, preto môžete použiť rozlišovacie názvy ako prostriedky autentifikácie do radiča doemény EIM.

Súvisiace informácie

API filtra politiky formátu EIM (eimFormatPolicyFilter)

Operácie prehľadania EIM

Aplikácia alebo operačný systém používa rozhranie API mapovania EIM na vykonanie vyhľadávacej operácie, aby mohla aplikácia alebo operačný systém mapovať z jednej užívateľskej identity v jednom registri do inej užívateľskej identity v inom registri. Operácia prehľadania EIM je proces, prostredníctvom ktorého aplikácia alebo operačný systém vyhľadáva neznámu priradenú užívateľskú identitu v určitom cieľovom registri pomocou niektorých známych a dôveryhodných informácií.

Aplikácie používajúce rozhrania API EIM môžu vykonávať tieto operácie prehľadania EIM na informáciách len vtedy, ak sú tieto informácie uložené v doméne EIM. Aplikácia môže vykonať jeden z dvoch typov operácií prehľadania EIM podľa typu informácií, ktoré aplikácia poskytne ako zdroj operácie prehľadania EIM: identita užívateľa alebo identifikátor EIM.

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

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

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

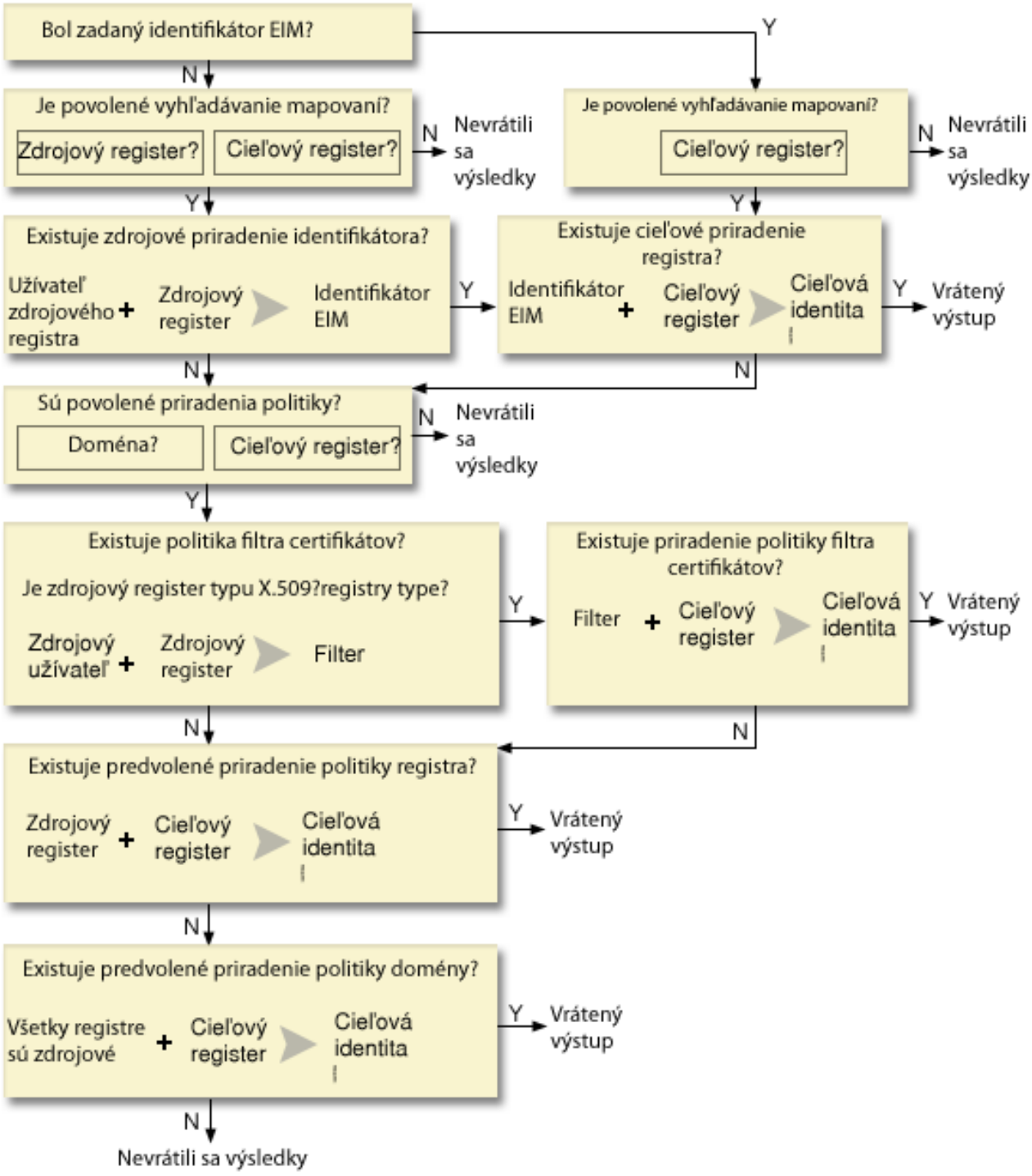
- Identifikátor EIM ako zdroj alebo štartovací bod operácie.
- Názov definície registra EIM, ktorá je cieľom operácie prehľadania EIM. Táto definícia registra opisuje register užívateľov, ktorý obsahuje identitu užívateľa, ktorú aplikácia hľadá.

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

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

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

Obrázok 10: Základný diagram postupu operácie prehľadania EIM



Poznámka: V nasledujúcom toku operácie vyhľadávania najskôr kontrolujú definíciu jednotlivého registra, ako zadaný zdrojový register alebo cieľový register. Ak operácie vyhľadávania nedokážu nájsť mapovanie použitím definície jednotlivého registra, zisťuje sa, či definícia jednotlivého registra je členom definície skupinového registra. Ak je členom definície skupinového registra, operácie vyhľadávania kontrolujú, či definícia skupinového registra vyhovuje požiadavke vyhľadávania mapovania.

Operácia vyhľadávania prebieha týmto spôsobom:

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

Ak sa chcete viac dozvedieť o operáciách vyhľadávania EIM, pozrite si nasledujúce príklady:

Súvisiace koncepty

“Doména EIM” na strane 6
Doména EIM je adresár v serveri LDAP (Lightweight Directory Access Protocol), ktorý obsahuje údaje EIM pre podnik.

“Priradenia politiky” na strane 21
Politika mapovania podnikovej identity (EIM) umožňuje administrátorovi EIM vytvárať a používať priradenia politiky na definovanie vzťahu medzi viacerými identitami užívateľa v jednom alebo viacerých registroch užívateľa, a jednotlivou identitou užívateľa v inom registri užívateľa.

“Radič domény EIM” na strane 5
Radič domény EIM je server LDAP (Lightweight Directory Access Protocol) nakonfigurovaný na riadenie jednej alebo viacerých domén EIM. Doména EIM pozostáva zo všetkých identifikátorov EIM, priradení EIM a registrov užívateľov zadefinovaných v tejto doméne. Systémy (klienti EIM) sú spojené s doménou EIM tým, že používajú údaje domény pre operácie prehľadania EIM.

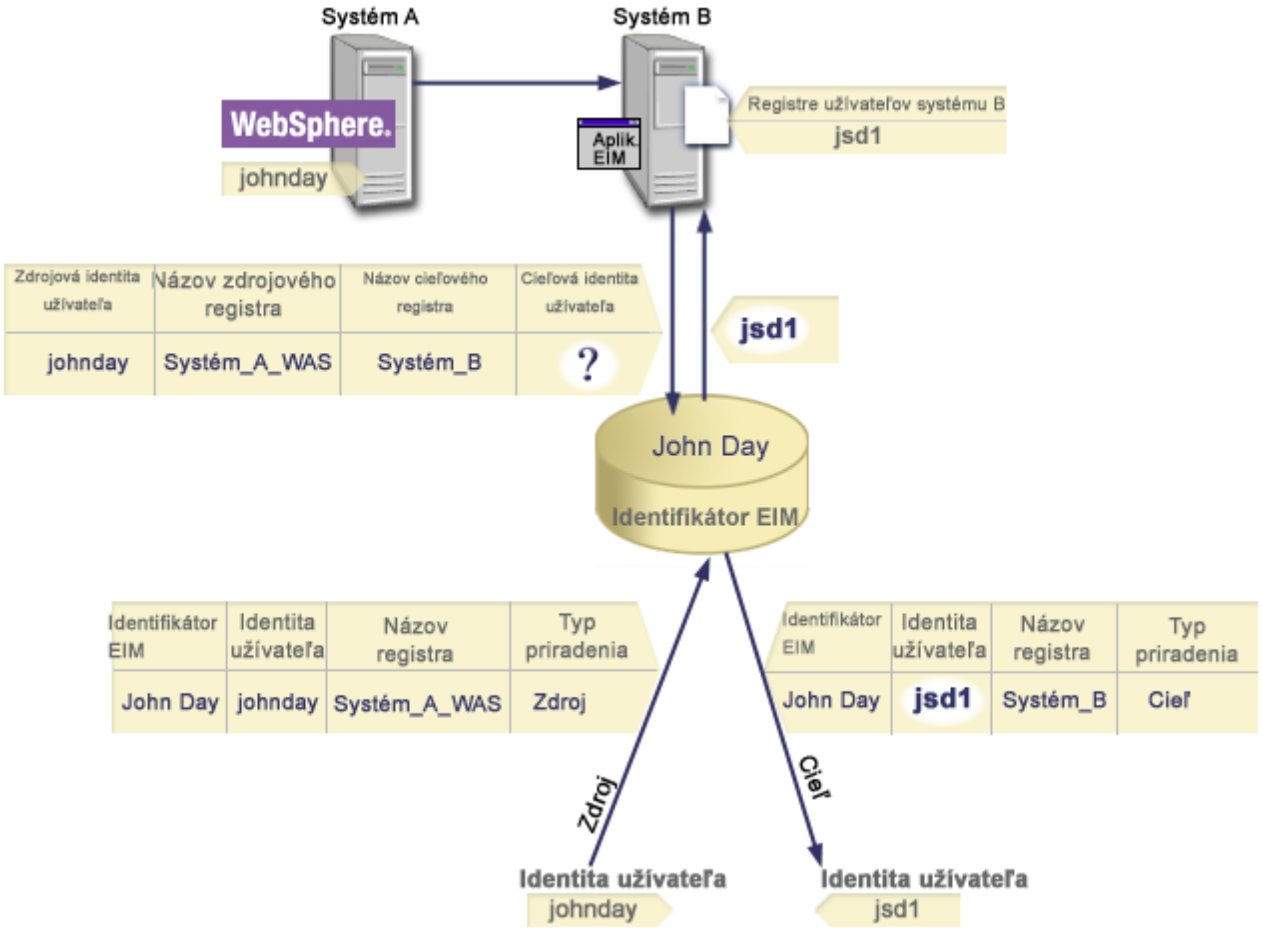
“Informácie na vyhľadanie” na strane 16
Pomocou EIM môžete poskytnúť voliteľné údaje, ktoré sa nazývajú vyhľadávacie informácie, na ďalšiu identifikáciu cieľovej užívateľskej identity. Táto cieľová identita užívateľa môže byť špecifikovaná buď v priradení identifikátora alebo v priradení politiky.

Príklady operácie vyhľadávania: Príklad 1

Použite tento príklad, aby ste zistili, ako pracuje proces hľadania pre operáciu vyhľadávania, ktorá vracia cieľovú identitu užívateľa zo špecifických priradení identifikátora na základe známej identity užívateľa.

Na obrázku 11 sa identita užívateľa johnday autentifikuje do WebSphere Application Server pomocou Lightweight Third-Party Authentication (LPTA) v systéme A. WebSphere aplikačný server na systéme A volá integrovaný program na systéme B, aby sprístupnil údaje na systéme B. Integrovaný program používa EIM API pre vykonanie operácie vyhľadávania EIM na základe identity užívateľa na systéme A, ako zdroji tejto operácie. Aplikácia poskytne tieto informácie na vykonanie operácie: johnday ako zdrojová identita užívateľa, System_A_WAS ako zdrojový názov definície registra EIM a System_B ako cieľový názov definície registra EIM. Tieto zdrojové informácie sú postúpené do EIM a operácia prehľadania EIM nájde zdrojové priradenie identifikátora, ktoré vyhovuje týmto informáciám. Pomocou názvu identifikátora EIM John Day operácia prehľadania EIM vyhľadá cieľové priradenie identifikátora pre identifikátor, ktorý sa zhoduje s cieľovým názvom definície registra EIM pre System_B. Keď sa nájde vyhovujúce cieľové priradenie, operácia prehľadania EIM vráti aplikácii identitu užívateľa jsd1.

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



Príklady operácie vyhľadávania: Príklad 2

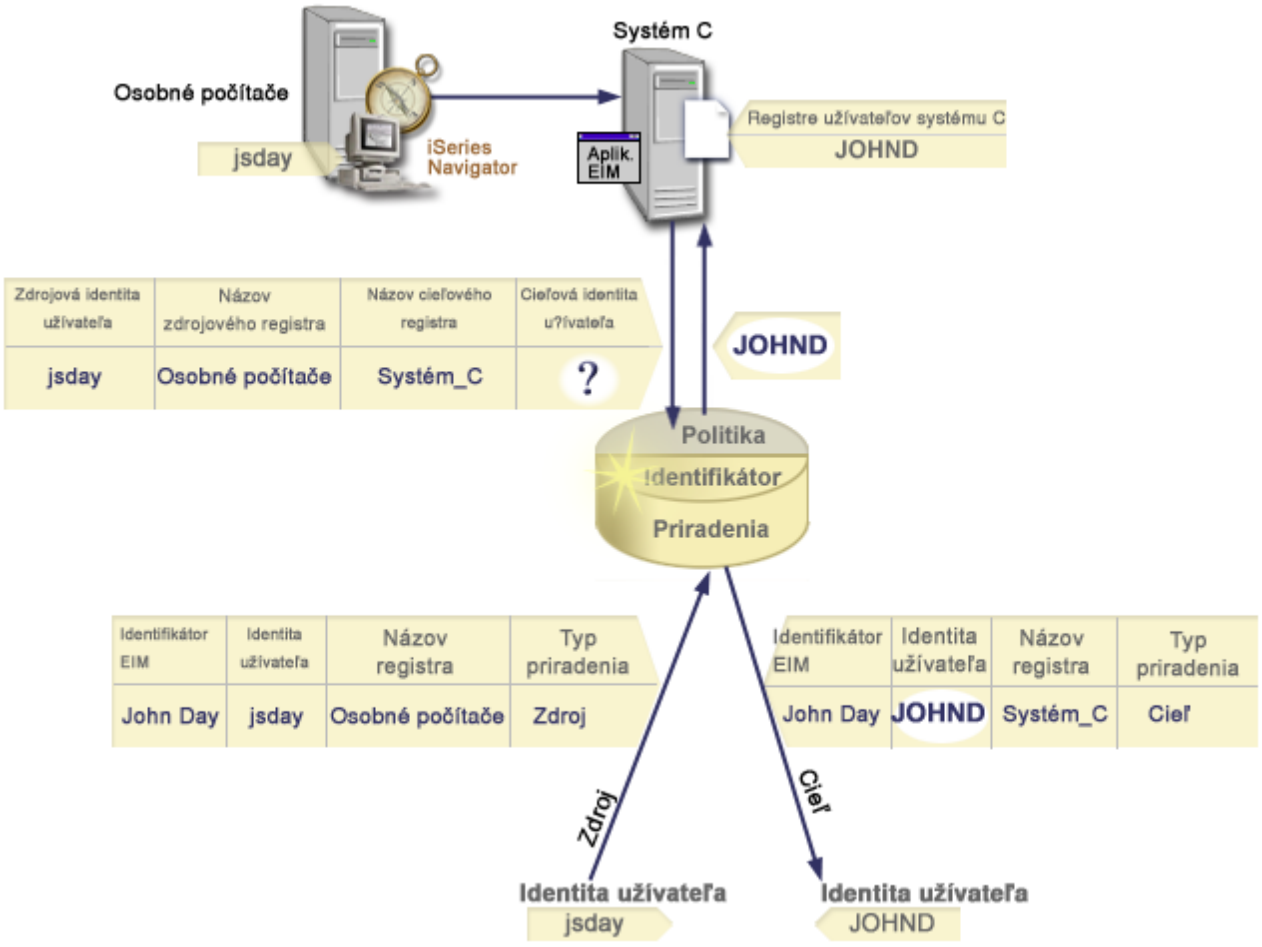
Použite tento príklad, aby ste zistili, ako pracuje proces hľadania pre operáciu vyhľadávania, ktorá vracia cieľovú identitu užívateľa zo špecifických priradení identifikátora na základe známeho principálu Kerberos.

Na obrázku 12 chce administrátor mapovať užívateľa Windows v registri Windows Active Directory na užívateľský profil i5/OS. Autentifikačnou metódou, ktorú používa Windows je Kerberos a názov registra Windows Active Directory, ako ho definoval administrátor v EIM je Desktops. Identita užívateľa, z ktorej chce administrátor namapovať, je princípál Kerbera s názvom jsday. Názov registra, i5/OS ako ho administrátor definoval v EIM, je System_C a identita užívateľa, ku ktorej chce administrátor vytvoriť mapovanie, je užívateľský profil s názvom JOHND.

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

- Zdrojové priradenie pre princípál Kerberos s názvom jsday v registri Desktops.
- Cieľové priradenie pre i5/OS užívateľský profil s názvom JOHND v registri System_C.

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



Táto konfigurácia umožňuje operáciu vyhľadávania mapovaní pre mapovanie z princípálu Kerberos na i5/OS užívateľský profil nasledovne:

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

Operácia vyhľadávania prebieha týmto spôsobom:

1. Užívateľ jsday sa prihlasuje a autentifikuje do Windows pomocou svojho principálu Kerberos v registri Windows Active Directory Desktops.
2. Užívateľ otvorí System i Navigator na prístup k údajom na System_C.
3. i5/OS používa EIM API na vykonanie operácie vyhľadávania EIM použitím zdrojovej identity užívateľa jsday, zdrojového registra Desktops a cieľového registra System_C.
4. Operácia prehľadania EIM kontroluje, či je vyhľadávanie mapovaní povolené pre zdrojový register Desktops a cieľový register System_C. Sú povolené.
5. Operácia vyhľadávania kontroluje zdrojové priradenie špecifického identifikátora, ktoré sa zhoduje s dodanou zdrojovou identitou užívateľa jsday v zdrojovom registri Desktops.
6. Operácia vyhľadávania používa porovnanie zdrojového priradenia identifikátora na určenie príslušného názvu identifikátora EIM, ktorý je John Day.
7. Operácia vyhľadávania používa tento názov identifikátora EIM na hľadanie cieľového priradenia identifikátora pre identifikátor EIM, ktorý sa zhoduje so špecifikovaným cieľovým názvom definície registra EIM systému System_C.
8. Také cieľové priradenie identifikátora existuje a operácia vyhľadávania vráti cieľovú identitu užívateľa JOHND ako je definovaná v cieľovom priradení.
9. Keď je vyhľadávacia operácia mapovania ukončená, System i Navigator začne pracovať pod užívateľským profilom JOHND. Oprávnenie užívateľa na prístup k prostriedkom a vykonávanie úkonov v System i Navigator je určené oprávnením zadefinovaným pre užívateľský profil JOHND, a nie oprávnením zadefinovaným pre užívateľskú identitu jsday.

Príklady operácie vyhľadávania: Príklad 3

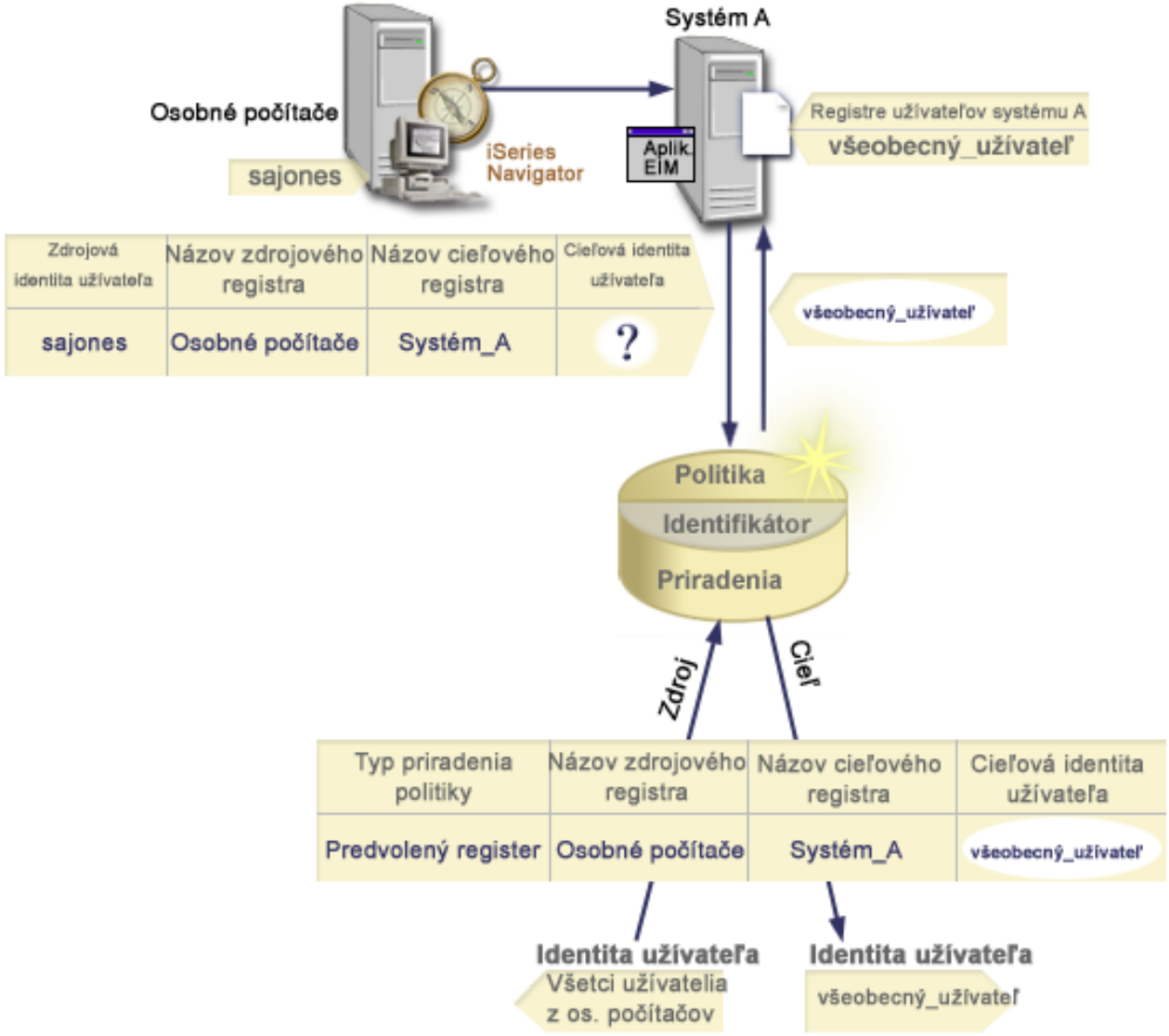
Použite tento príklad, aby ste zistili, ako pracuje proces hľadania pre operáciu vyhľadávania, ktorá vracia cieľovú identitu užívateľa z predvoleného priradenia politiky registra.

Na obrázku 13, administrátor chce mapovať všetkých užívateľov pracovných staníc pracovnej plochy v registri Windows aktívneho adresára na jednotlivý i5/OS užívateľský profil s názvom všeobecný_užívateľ v registrii5/OS, ktorý je pomenovaný Systém_A v EIM. Autentifikačnou metódou, ktorú používa Windows je Kerberos a názov registra Windows Active Directory, ako ho definoval administrátor v EIM je Desktops. Jednou z identít užívateľa, z ktorých chce administrátor mapovať, je principál Kerberos s názvom sajones.

Administrátor vytvorí predvolené priradenie politiky registra s nasledujúcimi informáciami:

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

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



Táto konfigurácia umožňuje operáciu vyhľadávania mapovaní na mapovanie všetkých principálov Kerberos v registri Desktops, vrátane principálu sajones, na užívateľský profil i5/OS pomenovaný všeobecný_užívateľ, nasledovným spôsobom:

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

Operácia vyhľadávania prebieha týmto spôsobom:

1. Užívateľ sajones sa prihlási a autentifikuje do jeho prostredia Windows prostredníctvom principálu Kerberos v registri Desktops.
2. Užívateľ otvorí System i Navigator na prístup k údajom na systéme A.
3. i5/OS používa EIM API na vykonanie operácie vyhľadávania EIM použitím zdrojovej identity užívateľa sajones, zdrojového registra Desktops a cieľového registra Systém_A.
4. Operácia prehľadania EIM kontroluje, či je vyhľadávanie mapovaní povolené pre zdrojový register Desktops a cieľový register System_A. Sú povolené.

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

Niekedy operácia prehľadania EIM vráti nejednoznačný výsledok. Môže sa to stať napríklad, keď viac ako jedna cieľová identita užívateľa vyhovuje zadaným kritériám operácie vyhľadávania. Niektoré aplikácie povolené od EIM, vrátane i5/OS aplikácií a produktov, nie sú navrhnuté pre ošetrenie takýchto nejednoznačných výsledkov a môžu zlyhať alebo poskytnúť neočakávané výsledky. Pre vyriešenie tejto situácie budete musieť vykonať príslušné akcie. Napríklad budete musieť zmeniť vašu konfiguráciu EIM alebo definovať informácie na vyhľadanie pre každú cieľovú identitu užívateľa, aby sa predišlo viacerým zhodám v cieľovej identite užívateľa. Môžete tiež otestovať mapovanie, aby ste určili, či zmeny, ktoré ste vykonali fungujú tak, ako ste očakávali.

Príklady operácie vyhľadávania: Príklad 4

Použite tento príklad, aby ste zistili, ako pracuje proces hľadania pre operáciu vyhľadávania, ktorá vracia cieľovú identitu užívateľa v registri užívateľa, ktorý je členom definície skupinového registra.

Administrátor chce mapovať užívateľa Windows na i5/OS užívateľský profil. Kerberos je metóda autentifikácie, ktorú Windows používa a názov registra Kerberos, ako ho definoval administrátor v EIM, je Desktop_A. Identita užívateľa, ku ktorej administrátor chce mapovať, je principál Kerberos, s menom jday. Názov definície registra, i5/OS ako ho administrátor definoval v EIM, je Skupina_1 a identita užívateľa, ku ktorej chce administrátor mapovať, je užívateľský profil s názvom JOHND, ktorý existuje v troch individuálnych registroch: Systém_B, Systém_C a Systém_D. Každý z týchto individuálnych registrov je členom definície skupinového registra Skupina_1.

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

- Zdrojové priradenie pre principál Kerberos s názvom jday v registri Pracovná plocha_A.
- Cieľové priradenie pre užívateľský profil i5/OS s názvom JOHND v registri Skupina_1 .

Táto konfigurácia umožňuje operáciu vyhľadávania mapovaní pre mapovanie z principálu Kerberos na i5/OS užívateľský profil nasledovne:

Zdrojová identita užívateľa a register	**--->**	**Identifikátor EIM**	**--->**	**Cieľová identita užívateľa**
jday v registri Pracovná plocha_A	--->	John Day	--->	JOHND (v definícii skupinového registra Skupina_1)

Operácia vyhľadávania prebieha týmto spôsobom:

1. Užívateľ (jday) sa prihlasuje a autentifikuje pre Windows na Pracovná plocha_A.
2. Užívateľ otvorí System i Navigator na prístup k údajom na System_B.
3. i5/OS používa EIM API na vykonanie operácie vyhľadávania EIM použitím zdrojovej identity užívateľa jday, zdrojového registra Pracovná plocha_A a cieľového registra Systém_B.
4. Operácia prehľadania EIM kontroluje, či je vyhľadávanie mapovaní povolené pre zdrojový register (Pracovná plocha_A) a cieľový register (Systém_B).
5. Operácia vyhľadávania kontroluje špecifické individuálne zdrojové priradenie, ktoré sa zhoduje so zadanou zdrojovou identitou užívateľa jday v zdrojovom registri Pracovná plocha_A.

6. Operácia vyhľadávania používa porovnanie zhody zdrojového priradenia pre určenie príslušného názvu identifikátora EIM, ktorý je John Day.
7. Operácia vyhľadávania používa tento názov identifikátora EIM na hľadanie individuálneho cieľového priradenia pre identifikátor EIM, ktorý sa zhoduje so zadaným názvom cieľovej definície registra EIM Systém_B. (Neexistuje žiadny.)
8. Operácia vyhľadávania zisťuje, či či zdrojový register (Pracovná plocha_A) je členom akýchkoľvek definícií skupinového registra. (Nie je.)
9. Operácia vyhľadávania zisťuje, či cieľový register (Systém_B) je členom akýchkoľvek definícií skupinového registra. Je členom definície skupinového registra Skupina_1.
10. Operácia vyhľadávania používa tento názov identifikátora EIM na hľadanie cieľového priradenia identifikátora, ktorý sa zhoduje s názvom zadaného názvu cieľového registra EIM Skupina_1.
11. Existuje takéto individuálne cieľové priradenie a operácia vyhľadávania vracia cieľovú identitu užívateľa JOHND, ako je definované v cieľovom priradení.

Poznámka: V niektorých prípadoch vráti operácia vyhľadávania EIM nejednoznačné výsledky, kedy sa viacero cieľových užívateľských identít zhoduje so zadanými kritériami operácie vyhľadávania. Vzhľadom na to, že EIM nemôže vrátiť jedinú cieľovú užívateľskú identitu, aplikácie povolené EIM vrátane aplikácií a produktov i5/OS, ktoré nie sú navrhnuté na spracovanie týchto nejednoznačných výsledkov, môžu zlyhať alebo môžu poskytovať neočakávané výsledky. Pre vyriešenie tejto situácie budete musieť vykonať príslušné akcie. Napríklad budete musieť zmeniť vašu konfiguráciu EIM alebo definovať informácie na vyhľadanie pre každú cieľovú identitu užívateľa, aby sa predišlo viacerým zhodám v cieľovej identite užívateľa. Ak chcete zistiť, či vykonané zmeny fungujú tak, ako majú, môžete otestovať mapovanie.

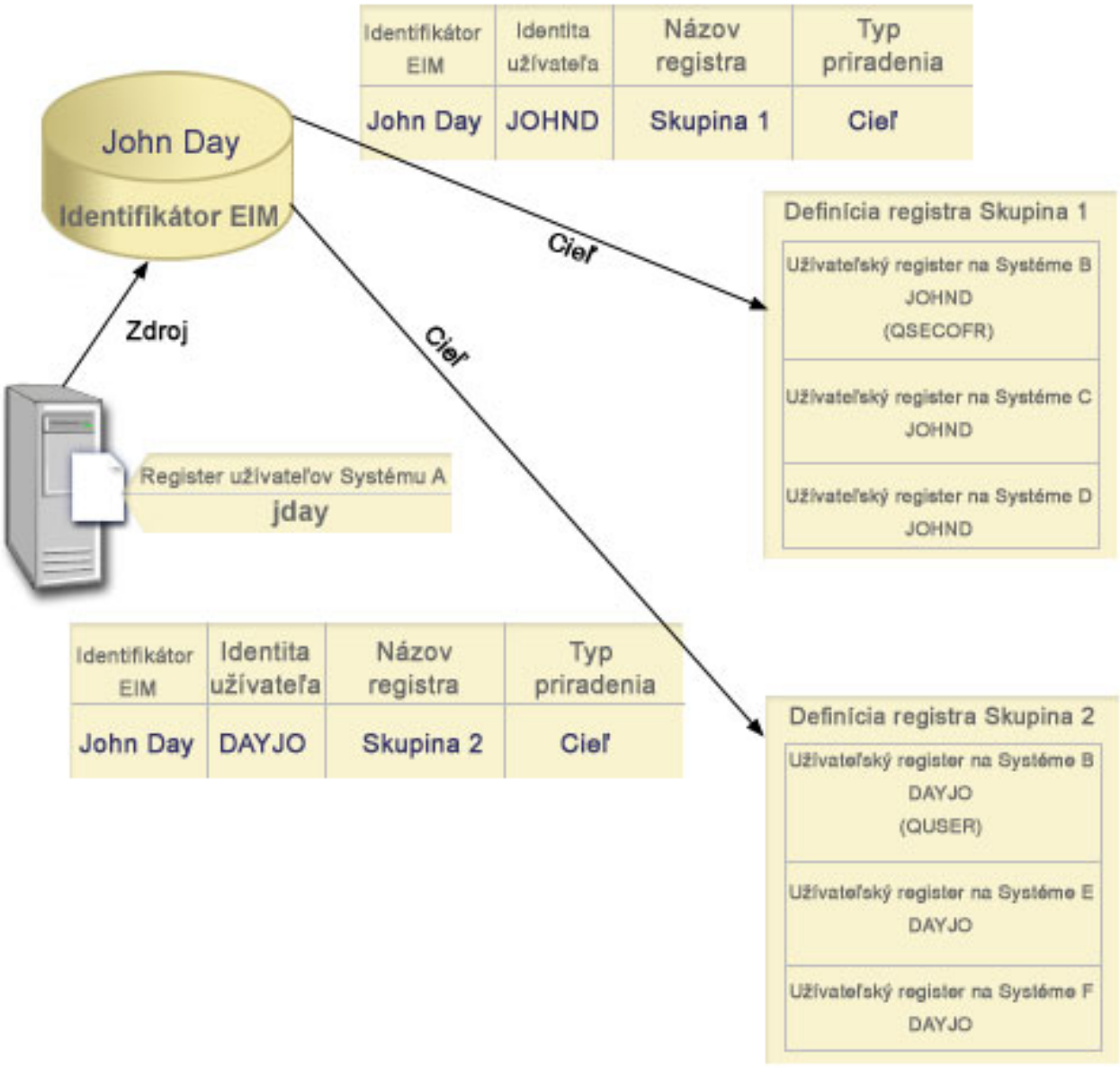
Príklady operácie vyhľadávania: Príklad 5

Použite tento príklad, ak sa chcete dozvedieť viac o operáciách vyhľadávania, ktoré produkujú nejednoznačné výsledky, ktorých súčasťou sú definície skupinových registrov.

V niektorých prípadoch mapovanie vyhľadávacej operácie vráti nejednoznačné výsledky, ak sa s určenými kritériami vyhľadávania zhoduje viac ako jedna identita cieľového užívateľa. Keďže situácia s nejednoznačnými výsledkami by mohla spôsobiť zlyhanie aplikácií, ktoré využívajú EIM, alebo to, že by produkovali neočakávané výsledky, musíte vykonať opatrenia na predídenie alebo riešenie takejto situácie.

Predovšetkým pamätajte, že vyhľadávacie operácie môžu vrátiť nejednoznačné výsledky, keď určíte jednotlivú definíciu registra užívateľskej identity ako člena viac než jednej definície skupinového registra. Ak je jednotlivá definícia registra užívateľa členom viacnásobnej definície skupinového registra a vytvoríte jednotlivé priradenia EIM alebo priradenia politiky, ktoré používajú definíciu skupinového registra buď ako zdrojový register alebo cieľový register, vyhľadávacie operácie môžu vrátiť nejednoznačné výsledky. Napríklad môžete použiť dve rôzne užívateľské identity pre dva rozličné typy systémových úloh, ktoré vykonávate: vykonávate úlohy ako bezpečnostný správca, ktoré si vyžadujú identitu užívateľa s autoritou QSECOFR, a vykonávate úlohy, ktoré si vyžadujú identitu užívateľa s autoritou QUSER. Ak sú obe vaše identity umiestnené v jedinom užívateľskom registri, ktorý je členom dvoch rôznych definícií skupinového registra, a vytvoríte cieľové priradenia identifikátora na obe cieľové identity užívateľa, vyhľadávacie operácie nájdu obe cieľové užívateľské identity a následne vrátia nejednoznačné výsledky.

Nasledujúci príklad popisuje možný výskyt tohto problému, keď zadáte jediný užívateľský register, ktorý je členom dvoch definícií skupinového registra, a určíte jednu z definícií skupinového registra ako cieľový register v dvoch jednotlivých priradeniach identifikátora EIM.



Príklad:

John Day má nasledovné užívateľské identity v definícii systémového registra s názvom System B:

- JOHND
- DAYJO

Užívateľský register System B je členom nasledovných definícií skupinového registra:

- Skupina 1
- Skupina 2

Identifikátor EIM John Day má dve cieľové priradenia s nasledujúcimi špecifikáciami:

- Cieľové priradenie: Cieľový register je Skupina 1, ktorá obsahuje identitu užívateľa JOHND v registri užívateľa System B.
- Cieľové priradenie: Cieľový register je Skupina 2, ktorá obsahuje identitu užívateľa DAYJO v registri užívateľa System B.

V tomto prípade mapovanie vyhľadávacej operácie vráti nejednoznačné výsledky, pretože s určenými kritériami vyhľadávania zhoduje viac ako jedna identita cieľového užívateľa; obe užívateľské identity (JOHND a DAYOJO) spĺňajú zadané vyhľadávacie kritériá.

Podobne mapovanie vyhľadávacej operácie môže vrátiť nejednoznačné výsledky, ak vytvoríte dve priradenia politiky (a nie jednotlivé priradenia identifikátora EIM), ktoré využívajú definície skupinového registra ako cieľový register.

Použite tento návod, ak chcete zabrániť operáciám vyhľadávania, ktoré produkujú nejednoznačné výsledky, ktorých súčasťou sú definície skupinových registrov:

- Zadajte jednotlivý užívateľský register ako člena nie viac než jednej definície skupinového registra.
- Dávajte pozor, keď vytvárate jednotlivé priradenia identifikátorov EIM alebo priradenia politiky, ktoré využívajú definície skupinového registra buď ako zdrojový alebo ako cieľový register. Overte si, či definícia skupinového registra nie je členom viac než jednej definície skupinového registra. Dávajte si pozor na to, či nie je člen cieľovej definície skupinového registra tiež členom inej definície skupinového registra, vyhľadávacie operácie môže vrátiť nejednoznačné výsledky.
- Ak máte situácie s nejednoznačnými výsledkami, pričom zadávate jednotlivé definície registra ako člena viacčlennej definície skupinového registra, a vytvoríte jedinečné priradenie identifikátora alebo priradenie politiky, ktorá využíva jednu z týchto definícií skupinových registrov buď ako zdrojový register alebo ako cieľový register, môžete definovať jedinečné vyhľadávacie informácie pre každú cieľovú identitu užívateľa v každom priradení na ďalšie upresňovanie vyhľadávania.

Môžete definovať nasledovné vyhľadávacie informácie pre každú cieľovú identitu používateľa v príklade o identite John Day:

- Pre JOHND: Definovať Administrátora ako vyhľadávaciu informáciu
- Pre DAYJO: Definovať Užívateľa ako vyhľadávaciu informáciu

Základné aplikácie i5/OS, ako napríklad System i Access for Windows, však nemôžu používať vyhľadávacie informácie na rozlišovanie medzi viacerými identitami cieľových užívateľov vrátenými operáciou vyhľadávania. Následne by ste mohli zvážiť predefinovanie priradení pre doménu, aby ste zabezpečili, že operácia vyhľadávania mapovania dokáže vrátiť jedinú cieľovú identitu užívateľa pre zaistenie, aby základné i5/OS aplikácie mohli úspešne vykonať operácie vyhľadávania a mapovať identity.

Súvisiace koncepty

"Definície skupinového registra" na strane 15
Logické zoskupovanie definícií registrov vám umožňuje redukovať množstvo práce, ktorú musíte vykonať, aby ste nakonfigurovali mapovanie EIM. Definíciu skupinového registra môžete riadiť podobným spôsobom, ako riadite definíciu individuálneho registra.

Operácie podpory a umožnenia politiky mapovaní EIM

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

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

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

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

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

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

Súvisiace koncepty

"Informácie na vyhľadanie" na strane 16
Pomocou EIM môžete poskytnúť voliteľné údaje, ktoré sa nazývajú vyhľadávacie informácie, na ďalšiu identifikáciu cieľovej užívateľskej identity. Táto cieľová identita užívateľa môže byť špecifikovaná buď v priradení identifikátora alebo v priradení politiky.

"Predvolené priradenia politiky domény" na strane 21
Predvolené priradenie politiky domény predstavuje jeden typ priradenia politiky, ktorý môžete použiť na vytvorenie mapovaní typu veľa-jeden medzi identitami užívateľov.

"Predvolené priradenia politiky registrov" na strane 23
Predvolené priradenie politiky registra predstavuje jeden typ priradenia politiky, ktorý môžete použiť na vytvorenie mapovaní typu veľa-jeden medzi identitami užívateľov.

"Vytváranie priradenia politiky" na strane 99
Priradenie politiky poskytuje prostriedky na priame definovanie vzťahu medzi viacerými identitami užívateľa v jednom alebo viacerých registroch a individuálnou cieľovou identitou užívateľa v inom registri.

Súvisiace úlohy

"Povolenie priradení politiky pre doménu" na strane 85
Priradenie politiky poskytuje prostriedky na vytváranie mapovaní veľa-na-jeden v situáciách, kde priradenia medzi identitami užívateľa a identifikátorom EIM neexistujú.

"Povolenie podpory vyhľadávaní mapovania a používanie priradení politiky pre cieľový register" na strane 92
Podpora politiky mapovania EIM umožňuje používanie priradení politiky ako spôsobu vytvárania viacerých mapovaní do jedného v situáciách, keď neexistujú priradenia medzi užívateľskými identitami a identifikátorom EIM. Priradenie politiky môžete použiť na mapovanie zdrojovej množiny viacerých identít užívateľa (namiesto jednej identity užívateľa) na jednu cieľovú identitu užívateľa v zadanom cieľovom registri užívateľov.

Riadenie prístupu EIM

Užívateľ EIM je užívateľ, ktorý vlastní riadenie prístupu na EIM na základe jeho členstva v preddefinovanej skupine užívateľov Lightweight Directory Access Protocol (LDAP) pre špecifickú doménu.

Zadanie riadenia prístupov EIM pre užívateľa pridá tohto užívateľa do špecifickej skupiny užívateľov LDAP pre konkrétnu doménu. Každá skupina LDAP má oprávnenie vykonávať konkrétne administračné úlohy EIM v tejto doméne. Jednotlivé administratívne úlohy a ich typy, vrátane operácií vyhľadávania, ktoré môže užívateľ EIM vykonať, sú určené skupinou riadenia prístupu, do ktorej patrí užívateľ EIM.

Poznámka: Ak chcete nakonfigurovať EIM, musíte dokázať, že ste dôveryhodný v rámci kontextu siete, nie v jednom konkrétnom systéme. Autorizácia na konfigurovanie EIM sa nezakladá na vašom i5/OS oprávnení užívateľského profilu, ale na vašom oprávnení riadenia prístupu na EIM. EIM je sieťový prostriedok, nie prostriedok pre akýkoľvek určitý systém; takže EIM nerozpoznáva mimoriadne oprávnenia špecifické pre i5/OS, ako sú *ALLOBJ a *SECADM, pre konfiguráciu. Akonáhle je však EIM nakonfigurované, oprávnenie pre vykonávanie úloh môže byť založené na mnohých rôznych typoch užívateľov, vrátane i5/OS užívateľských profilov. Napríklad IBM Tivoli Directory Server for i5/OS zaobchádza s profilmi i5/OS s mimoriadnym oprávnením *ALLOBJ a *IOSYSCFG ako s administrátormi adresára.

Pridávať ďalších užívateľov do skupiny riadenia prístupu k EIM alebo meniť nastavenia riadenia prístupu pre iných užívateľov môžu len užívatelia s oprávnením administrátora riadenia prístupu k EIM. Skôr, ako sa užívateľ stane

členom skupiny riadenia prístupu k EIM, musí mať záznam v adresárovom serveri, ktorý sa správa ako radič domény EIM. Rovnako, len konkrétne typy užívateľov sa môžu stať členmi skupiny riadenia prístupu k EIM. Identita užívateľa môže byť v tvare principál Kerberos, charakteristického názvu LDAP alebo ako i5/OS užívateľský profil, pokiaľ je identita užívateľa definovaná v adresárovom serveri.

Poznámka: Ak má byť typ užívateľa principál Kerberos dostupný v EIM, v systéme musí byť nakonfigurovaná služba sieťovej autentifikácie. Ak chcete mať typ užívateľského profilu i5/OS dostupný v EIM, musíte konfigurovať príponu systémového objektu na adresárovom serveri. Toto umožňuje, aby adresárový server odkazoval nai5/OS systémové objekty, ako sú i5/OS užívateľské profily.

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

Administrátor LDAP (Lightweight Directory Access Protocol)

Administrátor LDAP je špeciálny rozlišovací názov (DN) v adresári, ktorý je administrátorom pre celý adresár. Administrátor LDAP má preto prístup k všetkým administračným funkciám EIM aj k celému adresáru. Užívateľ s týmto oprávnením na riadenie prístupu môže vykonávať nasledujúce funkcie:

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

Administrátor EIM

Členstvo v tejto skupine riadenia prístupu umožňuje užívateľovi manažovať všetky údaje EIM v rámci tejto domény EIM. Užívateľ s týmto oprávnením na riadenie prístupu môže vykonávať nasledujúce funkcie:

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

- Pridávanie, odstraňovanie a vypisovanie informácií o riadení prístupu k EIM.
- Zmeňte a odstráňte poverovacie informácie pre užívateľa registra.

Administrátor identifikátorov

Členstvo v tejto skupine riadenia prístupu umožňuje užívateľovi pridávať a meniť identifikátory EIM a manažovať zdrojové a administratívne priradenia. Užívateľ s týmto oprávnením na riadenie prístupu môže vykonávať nasledujúce funkcie:

- Vytváranie identifikátorov EIM.
- Pridávanie a odstraňovanie zdrojových priradení.
- Pridávanie a odstraňovanie administratívnych priradení.
- Vykonávanie operácií prehľadania EIM.
- Načítavanie priradení identifikátora, priradení politiky, filtrov certifikátov, identifikátorov EIM a definícií registra EIM.

Operácie s mapovaním EIM

Členstvo v tejto skupine riadenia prístupu umožňuje užívateľovi vykonávať operácie vyhľadávania mapovaní EIM. Užívateľ s týmto oprávnením na riadenie prístupu môže vykonávať nasledujúce funkcie:

- Vykonávanie operácií prehľadania EIM.
- Načítavanie priradení identifikátora, priradení politiky, filtrov certifikátov, identifikátorov EIM a definícií registra EIM.

Administrátor registrov

Členstvo v tejto skupine riadenia prístupu umožňuje užívateľovi manažovať všetky definície registra EIM. Užívateľ s týmto oprávnením na riadenie prístupu môže vykonávať nasledujúce funkcie:

- Pridávanie a odstraňovanie cieľových priradení.
- Vytváranie a odstraňovanie priradení politiky.
- Vytváranie a odstraňovanie filtrov certifikátov.
- Aktivovanie a deaktivovanie vyhľadávania mapovaní pre register.
- Aktivovanie a deaktivovanie používania priradení politiky pre register.
- Vykonávanie operácií prehľadania EIM.
- Načítavanie priradení identifikátora, priradení politiky, filtrov certifikátov, identifikátorov EIM a definícií registra EIM.

Administrátor pre vybraté registre

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

- Vytváranie, odstraňovanie a vypisovanie cieľových priradení len pre určené definície registra EIM.
- Pridávanie a odstraňovanie predvolených priradení politiky domény.
- Pridávanie a odstraňovanie priradení politiky len pre určené definície registra.
- Pridávanie filtrov certifikátov len pre určené definície registra.
- Aktivovanie a deaktivovanie vyhľadávaní mapovania len pre určené definície registra.
- Aktivovanie a deaktivovanie používania priradení politiky len pre určené definície registra.

- Načítavanie identifikátorov EIM.
- Načítavanie priradení identifikátorov a filtrov certifikátov len pre určené definície registra.
- Načítavanie informácií o definícii registra EIM len pre určené definície registra.

Poznámka: Ak zadaná definícia registra je definícia skupinového registra, užívateľ s Administrátorom pre riadenie prístupu na vybraté registre má administrátorský prístup iba na túto skupinu, nie na členov skupiny.

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

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

Vyhľadávanie poverení

Táto skupina riadenia prístupu dovoľuje užívateľovi získať poverovacie informácie, akými sú napríklad heslá.

Ak užívateľ s takýmto riadením prístupu chce vykonať prídavnú operáciu EIM, užívateľ musí byť členom skupiny riadenia prístupu, ktorá poskytuje oprávnenie na požadovanú operáciu EIM. Napríklad, ak užívateľ s takýmto riadením prístupu chce získať cieľové priradenie zo zdrojového priradenia, užívateľ musí byť členom jednej z nasledujúcich skupín riadenia prístupu:

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

Súvisiace koncepty

“i5/OS faktory profilov užívateľov EIM” na strane 49
Schopnosť vykonávať úlohy v EIM nie je založená na vašom oprávnení užívateľského profilu i5/OS, ale na vašom oprávnení riadenia prístupov EIM.

“Identifikácia potrebných schopností a rolí” na strane 52
Mapovanie podnikovej identity (EIM) je nastavené tak, aby mohol byť jediný človek jednoducho zodpovedný za konfiguráciu a administráciu v malej organizácii. Vo väčšej organizácií môžete uprednostniť väčší počet rôznych osôb.

Súvisiace úlohy

“Riadenie prístupov užívateľov k EIM” na strane 112
Užívateľ EIM je taký užívateľ, ktorý má riadenie prístupov EIM založené na členstve v skupinách užívateľov preddefinovaného LDAP (Lightweight Directory Access Protocol). Špecifikovanie riadenia prístupu k EIM pre daného užívateľa pridá tohto užívateľa do špecifickej skupiny užívateľov LDAP.

Skupina riadenia prístupu k EIM: Oprávnenie rozhrania API

Tieto informácie zobrazujú tabuľky, ktoré sú organizované operáciou mapovania podnikovej identity (EIM), ktorú vykonáva API.

Každá z nasledujúcich tabuliek zobrazuje každé EIM API, rôzne EIM skupiny riadenia prístupu a či má táto skupina riadenia prístupu oprávnenie vykonávať konkrétnu funkciu EIM.

Tabuľka 1. Práca s doménami

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

Tabuľka 1. Práca s doménami (pokračovanie)

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

Tabuľka 2. Práca s identifikátormi

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

Tabuľka 3. Práca s registrami

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

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

API EIM	Administrátor LDAP	Administrátor EIM	Administrátor identifikátorov EIM	Hľadanie mapovaní EIM	Administrátor registrov EIM	X administrátor registrov EIM
eimAddAssociation (administratívne)	X	X	X	-	-	-
eimAddAssociation (zdrojové)	X	X	X	-	-	-
eimAddAssociation (zdrojové a cieľové)	X	X	X	-	X	X
eimAddAssociation (cieľové)	X	X	-	-	X	X

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

API EIM	Administrátor LDAP	Administrátor EIM	Administrátor identifikátorov EIM	Hľadanie mapovaní EIM	Administrátor registrov EIM	X administrátor registrov EIM
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 priradeniami politiky

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

Tabuľka 6. Práca s mapovaniami

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

Tabuľka 7. Práca s prístupom

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

Skupina riadenia prístupu EIM: Oprávnenie na úlohu EIM

Tieto informácie zobrazujú tabuľku, ktorá objasňuje vzťahy medzi rôznymi skupinami riadenia prístupu mapovania podnikovej identity (EIM) a úlohami EIM, ktoré môžu vykonať.

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

EIM nemá automaticky riadenie prístupu Administrátor LDAP.

Tabuľka 8. Tabuľka 1: Skupiny riadenia prístupu k EIM

Úloha EIM	**Administrátor EIM**	**Administrátor identifikátorov**	**Operácie vyhľadávania mapovaní EIM**	**Administrátor registrov**	**Administrátor pre vybraté registre**	**Vyhľadanie oprávnenia**
Vytvoriť doménu	-	-	-	-	-	
Vymazať doménu	X	-	-	-	-	
Upraviť doménu	X	-	-	-	-	
Povoliť/Zakázať priradenia politiky pre doménu	X	-	-	-	-	
Hľadať domény	X	-	-	-	-	
Pridať systémový register	X	-	-	-	-	
Pridať register aplikácií	X	-	-	-	-	
Odstrániť register	X	-	-	-	-	
Upraviť register	X	-	-	X	X	
Povoliť/Zakázať vyhľadávanie mapovaní pre register	X	-	-	X	X	
Povoliť/Zakázať priradenia politiky pre register	X	-	-	X	X	
Hľadať registre	X	X	X	X	X	
Pridať identifikátor	X	X	-	-	-	
Odstrániť identifikátor	X	-	-	-	-	
Upraviť identifikátor	X	X	-	-	-	
Hľadať identifikátory	X	X	X	X	X	
Opakovane získať priradené identifikátory	X	X	X	X	X	
Pridať/Odstrániť administratívne priradenie	X	X	-	-	-	
Pridať/Odstrániť zdrojové priradenie	X	X	-	-	-	

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

Úloha EIM	Administrátor EIM	Administrátor identifikátorov	Operácie vyhľadávania mapovaní EIM	Administrátor registrov	Administrátor pre vybraté registre	Vyhľadanie oprávnenia
Pridať/Odstrániť cieľové priradenie	X	-	-	X	X	
Pridať/Odstrániť priradenie politiky	X	-	-	X	X	
Pridať/Odstrániť filter certifikátov	X	-	-	X	X	
Hľadať filter certifikátov	X	X	X	X	X	
Hľadať priradenia	X	X	X	X	X	
Hľadať priradenia politiky	X	X	X	X	X	
Opakovane získať cieľové priradenie zo zdrojového priradenia	X	X	X	X	-	
Opakovane získať cieľové priradenie z identifikátora	X	X	X	X	X	
Upraviť užívateľov registrov	X	-	-	X	X	
Hľadať užívateľov registrov	X	X	X	X	X	
Upraviť alias registra	X	-	-	X	X	
Hľadať aliasy registrov	X	X	X	X	X	
Opakovane získať register z aliasu	X	X	X	X	X	
Pridať/Odstrániť riadenie prístupu k EIM	X	-	-	-	-	
Zobraziť členov skupiny riadenia prístupu	X	-	-	-	-	
Zobraziť riadenie prístupu k EIM pre konkrétneho užívateľa	X	-	-	-	-	

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

Úloha EIM	Administrátor EIM	Administrátor identifikátorov	Operácie vyhľadávania mapovaní EIM	Administrátor registrov	Administrátor pre vybraté registre	Vyhľadanie oprávnenia
Dotazovať riadenie prístupu k EIM	X	-	-	-	-	
Modifikovať oprávnenie	X	-	-	-	-	-
Načítať oprávnenie	X	-	-	-	-	X
1 - Ak je špecifikovaná definícia registra definíciou skupinového registra, užívateľ s oprávnením Administrátora pre riadenie prístupu k vybraným registrom má prístup administrátora len k skupine, nie k členom skupiny.						

Koncepty LDAP pre EIM

EIM používa server LDAP ako radič domény na ukladanie údajov EIM. V dôsledku toho by ste mali pochopiť niektoré koncepty LDAP, ktoré sa vzťahujú na konfigurovanie a používanie EIM vo vašom podniku. Napríklad rozlišovací názov LDAP môžete použiť ako identitu užívateľa na nakonfigurovanie EIM a autentifikovanie do radiča domén EIM.

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

Súvisiace koncepty

"Koncepty EIM" na strane 4
Konceptuálne pochopenie spôsobu fungovania EIM je potrebné pre úplné pochopenie spôsobu možného využitia EIM vo vašom podniku. Napriek tomu, že konfigurácia a implementácia rozhraní API mapovania EIM sa môže na rôznych platformách servera líšiť, základné pojmy EIM sú spoločné pre všetky platformy IBM eServer.

Charakteristický názov

Rozlišovací názov (DN) je LDAP záznam, ktorý jednoznačne identifikuje a popisuje záznam v adresárovom (LDAP) serveri. Použite konfiguračného sprievodcu EIM na konfigurovanie adresárového servera pre ukladanie informácií domény EIM. EIM používa adresárový server na ukladanie údajov EIM, preto môžete použiť rozlišovacie názvy ako prostriedky autentifikácie do radiča doemény EIM.

Rozlišovacie názvy obsahujú názov samotnej entity a názvy objektov nad ňou v adresári LDAP (v poradí odspodu nahor). Úplný rozlišovací názov môže byť napríklad cn=Tim Jones, o=IBM, c=US. Každá položka má aspoň jeden atribút, ktorý sa používa na pomenovanie danej položky. Tento pomenovací atribút sa nazýva relatívny rozlišovací názov (RDN) položky. Položka nad daným RDN sa nazýva charakteristický názov rodiča. V tomto príklade cn=Tim Jones pomenúva záznam, takže to je RDN. o=IBM, c=US je rodičovský DN pre cn=Tim Jones.

Keďže EIM používa adresárový server na ukladanie údajov EIM, charakteristický názov môžete použiť pre identitu užívateľa, ktorý sa autentifikuje do radiča domény. Charakteristický názov môžete použiť aj pre identitu užívateľa, ktorý konfiguruje EIM pre vašu platformu System i. Napríklad rozlišovací názov môžete použiť, keď robíte nasledujúce:

- Konfigurujete adresárový server, aby vystupoval ako radič domény EIM. Toto vykonáte vytvorením a použitím rozlišovacieho názvu, ktorý identifikuje administrátora LDAP pre adresárový server. Ak ešte nebol adresárový server nakonfigurovaný, môžete ho nakonfigurovať, keď použijete sprievodcu konfiguráciou EIM na vytvorenie a pripojenie novej domény.
- Používate Sprievodcu konfiguráciou EIM na výber typu identity užívateľa, ktorý má sprievodca použiť pri pripájaní k radiču domény EIM. Rozlišovací názov je jeden z typov užívateľov, ktorý môžete vybrať. Rozlišovací názov musí reprezentovať užívateľa, ktorý je autorizovaný vytvárať objekty v lokálnom názvovom priestore adresárového servera.

- Používate Sprievodcu konfiguráciou EIM na výber typu užívateľa na vykonávanie operácií EIM v mene funkcií operačného systému. Tieto operácie zahŕňajú operácie vyhľadávania mapovaní a vymazanie priradení, keď mažete lokálny i5/OS užívateľský profil. Rozlišovací názov je jeden z typov užívateľov, ktorý môžete vybrať.
- Pripájate sa k radiču domény kvôli správe EIM, napríklad kvôli manažovaniu registrov a identifikátorov a vykonaniu operácií vyhľadávania mapovaní.
- Vytvárate filtre certifikátov na určenie rozsahu priradenia politiky filtra certifikátov. Keď vytvoríte filter certifikátov, musíte poskytnúť informácie o rozlišovacom názve pre DN subjektu alebo DN vydavateľa alebo certifikát na určenie kritéria, ktoré filter používa na určenie certifikátov ovplyvnených priradením politiky.

Súvisiace koncepty

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

"Filtre certifikátov" na strane 26
Filter certifikátov definuje sadu podobných atribútov certifikátov s charakteristickým názvom pre skupinu užívateľských certifikátov v zdrojovom registri užívateľov X.509. Filter certifikátov môžete použiť ako základ priradenia politiky filtra certifikátov.

Súvisiace informácie

Koncepty adresárového servera

Rodičovský rozlišovací názov

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

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

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

Súvisiace koncepty

"Charakteristický názov" na strane 46
Rozlišovací názov (DN) je LDAP záznam, ktorý jednoznačne identifikuje a popisuje záznam v adresárovom (LDAP) serveri. Použite konfiguračného sprievodcu EIM na konfigurovanie adresárového servera pre ukladanie informácií domény EIM. EIM používa adresárový server na ukladanie údajov EIM, preto môžete použiť rozlišovacie názvy ako prostriedky autentifikácie do radiča doemény EIM.

Súvisiace informácie

Koncepty adresárového servera

Schéma LDAP a ostatné úvahy o EIM

Tieto informácie môžete použiť, aby ste sa dozvedeli, čo sa vyžaduje, aby adresárový server fungoval s EIM.

EIM vyžaduje, aby radič domény hosťoval na adresárovom serveri, ktorý podporuje protokol LDAP (Lightweight Directory Access Protocol) Verzia 3. Okrem toho, produkt adresárového servera musí byť schopný akceptovať schému EIM a rozumieť týmto atribútom a triedam objektov:

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

Súvisiace koncepty

“Radič domény EIM” na strane 5
Radič domény EIM je server LDAP (Lightweight Directory Access Protocol) nakonfigurovaný na riadenie jednej alebo viacerých domén EIM. Doména EIM pozostáva zo všetkých identifikátorov EIM, priradení EIM a registrov užívateľov zadefinovaných v tejto doméne. Systémy (klienti EIM) sú spojené s doménou EIM tým, že používajú údaje domény pre operácie prehľadania EIM.

Základné pojmy mapovania podnikovej identity pre i5/OS

EIM môžete implementovať na ľubovoľnú platformu IBM eServer. Keď však implementujete EIM na model System i, mali by ste byť oboznámený s niektorými informáciami špecifickými pre implementáciu System i.

Keď sa chcete dozvedieť viac o aplikáciách i5/OS povolených pre EIM, úvahách o užívateľskom profile a ostatných témach, ktoré pomáhajú pri efektívnom používaní EIM na platforme System i, pozrite si nasledujúce informácie:

Súvisiace koncepty

"Koncepty EIM" na strane 4
Konceptuálne pochopenie spôsobu fungovania EIM je potrebné pre úplné pochopenie spôsobu možného využitia EIM vo vašom podniku. Napriek tomu, že konfigurácia a implementácia rozhraní API mapovania EIM sa môže na rôznych platformách servera líšiť, základné pojmy EIM sú spoločné pre všetky platformy IBM eServer.

i5/OS faktory profilov užívateľov EIM

Schopnosť vykonávať úlohy v EIM nie je založená na vašom oprávnení užívateľského profilu i5/OS, ale na vašom oprávnení riadenia prístupov EIM.

Ak chcete nastaviť i5/OS na použitie EIM, musíte vykonať niektoré ďalšie úlohy. Pre tieto doplnkové úlohy musíte mať profil užívateľa i5/OS s príslušnými špeciálnymi právomocami.

Ak chcete nastaviť i5/OS na použitie EIM pomocou System i Navigator, váš užívateľský profil musí mať tieto mimoriadne oprávnenia:

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

Rozšírenie príkazov užívateľského profilu i5/OS pre identifikátory EIM

Keď nakonfigurujete EIM pre váš systém, nový parameter s názvom EIMASSOC môžete používať pre príkaz CRTUSRPRF (Create user profile) aj pre príkaz CHGUSRPRF (Change user profile). Tento parameter môžete použiť na definovanie priradení identifikátorov EIM pre konkrétny užívateľský profil pre lokálny register.

Pri používaní tohto parametra môžete zadať nasledujúce informácie:

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

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

Zvyčajne vytvárate cieľové priradenie pre profil i5/OS, najmä v prostredí jednoduchého prihlásenia. Po tom, čo príkaz vytvorí potrebné cieľové priradenie pre užívateľský profil (a identifikátor EIM, ak to je potrebné), budete zrejme potrebovať vytvoriť zodpovedajúce zdrojové priradenie. System i Navigator môžete použiť na vytvorenie zdrojového priradenia pre ďalšiu užívateľskú identitu, napríklad principálu Kerberos, s ktorým sa užívateľ prihlási do siete.

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

i5/OS heslá profilov užívateľov a EIM

Ak ste administrátor, vašim primárnym cieľom pri konfigurácii EIM ako súčasti prostredia jednoduchého prihlásenia je znížiť rozsah riadenia užívateľských hesiel, ktoré musíte vykonať pre typických koncových užívateľov vo vašom podniku. Viete, že pri používaní mapovania identity, ktoré poskytuje EIM, v kombinácií s autentifikáciou protokolom

Kerberos budú užívatelia musieť vykonávať menej prihlásení a pamätať a manažovať menej hesiel. Je to výhoda, pretože ste menej často volaný riešiť problémy s namapovanými identitami užívateľov, akými je napríklad prestavenie hesiel, keď ich užívatelia zabudnú. Napriek tomu sú vaše pravidlá bezpečnostnej politiky pre heslá účinné a stále musíte manažovať užívateľské profily pre užívateľov vždy, keď heslo exspiruje.

Pri využívaní prostredia jednoduchého prihlásenia budete možno chcieť zmeniť nastavenia hesiel pre užívateľské profily, ktoré sú cieľom mapovania identity. Užívateľ už ako cieľ mapovania identity nemusí poskytovať heslo pre užívateľský profil pri prístupe na platformu System i alebo prostriedok i5/OS povolený mapovaním EIM. Pre typických užívateľov môžete zmeniť nastavenie hesla na hodnotu *NONE a s užívateľským profilom sa nebude môcť použiť žiadne heslo. Majiteľ užívateľského profilu už nepotrebuje heslo z dôvodu mapovania identity a jednoduchého prihlásenia. Nastavenie hesla na *NONE je výhodné, pretože ani vy ani vaši užívatelia už nemusia riadiť uplynutie platnosti hesiel. Okrem toho, nikto nemôže použiť profil na priame prihlásenie na platformu System i ani do prostriedku i5/OS povoleného pomocou mapovania EIM. Môžete však chcieť, aby administrátori mali aj naďalej hodnotu hesla pre užívateľské profily pre prípad, ak sa budú niekedy musieť priamo prihlásiť na platformu System i. Ak je napríklad radič domény EIM vypnutý a mapovanie identity nie je možné vykonať, administrátor môže potrebovať priame prihlásenie na platformu System i, kým nebude problém s radičom domény odstránený.

Súvisiace koncepty

"Riadenie prístupu EIM" na strane 38
Užívateľ EIM je užívateľ, ktorý vlastní riadenie prístupu na EIM na základe jeho členstva v preddefinovanej skupine užívateľov Lightweight Directory Access Protocol (LDAP) pre špecifickú doménu.

Súvisiace informácie

Príkaz CRTUSRPRF (Create user profile)

i5/OS audit pre EIM

Na celkový bezpečnostný plán má významný vplyv výber auditu, ktorý vykonávate.

Ak nakonfigurujete a budete používať mapovanie podnikovej identity (EIM), budete možno chcieť nakonfigurovať podporu auditovania pre adresárový server na zabezpečenie, že poskytujete vhodnú úroveň sledovateľnosti, ktorú vyžaduje vaša bezpečnostná politika. Podpora auditovania môže byť užitočná, ak chcete napríklad zistiť, ktorý užívateľ namapovaný priradením politiky vykonal akciu vo vašom systéme alebo zmenil objekt.

Súvisiace informácie

Auditovanie adresárového servera

Aplikácie s povoleným EIM pre i5/OS

EIM môže používať viacero aplikácií i5/OS.

Nasledujúce aplikácie i5/OS možno nakonfigurovať na používanie mapovania podnikovej identity (EIM):

- Hostiteľské servery i5/OS (aktuálne používané System i Access for Windows
- a System i Navigator)
- Telnet Server (v súčasnosti používaný PC5250 a IBM Websphere host. serverom na požiadanie)
- QFileSrv.400 ODBC (umožňuje používanie jednoduchého prihlásenia cez SQL)
- JDBC (umožňuje používanie EIM prostredníctvom jazyka SQL)
- Distributed Relational Database Architecture (DRDA) (umožňuje použitie EIM pomocou SQL)
- IBM WebSphere Host On-Demand Verzia 8, (funkcia Web Express Logon)
- i5/OS NetServer
- QFileSvr.400

Scenáre: Mapovanie podnikovej identity

Pomocou týchto informácií sa dozviete, ako riadiť užívateľské identity v rôznych systémoch v prostredí jednoduchého prihlásenia.

EIM je technológia infraštruktúry IBM, ktorá vám umožní sledovanie a manažovanie identít užívateľov v podniku. Na implementáciu prostredia jednoduchého prihlásenia sa zvyčajne používa EIM s technológiou autentifikácie, napríklad službou sieťovej autentifikácie.

Súvisiace informácie

Scenáre jednoduchého prihlásenia

Plánovanie EIM

Skôr, ako nastavíte EIM, mali by ste vyvinúť plán implementácie EIM, ktorý zabezpečí úspešnú konfiguráciu EIM v prostredí System i alebo v prostredí zmiešaných platforiem.

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

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

Plánovanie mapovania podnikovej identity pre eServer

Plán implementácie je nevyhnutný pre úspešnú konfiguráciu a používanie EIM v podniku s viacerými platformami. Na vývoj vášho plánu implementácie potrebujete zhromaždiť informácie o systémoch, aplikáciách a užívateľoch EIM. Tieto získané informácie neskôr použijete pri rozhodnutiach o najlepšom spôsobe konfigurácie EIM pre prostredie s viacerými platformami.

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

Požiadavky nastavenia mapovania podnikovej identity pre eServer

Na úspešnú implementáciu EIM musíte spĺňať tri požiadavky: podniková alebo sieťová úroveň, systém a aplikácia.

Požiadavky na úrovni podniku alebo siete

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

Ďalším aspektom je dostupnosť administratívnych nástrojov. Jednou voľbou je použitie rozhraní API EIM vo vašich vlastných aplikáciách na vykonanie administratívnych funkcií. Ak plánujete používať IBM Tivoli Directory Server for i5/OS ako radič domény EIM, na riadenie EIM môžete použiť System i Navigator. Ak plánujete použiť produkt IBM Directory, môžete použiť pomocný program eimadmin, ktorý je súčasťou V1R4 LDAP SPE.

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

Systémové a aplikačné požiadavky

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

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

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

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

Nasledujúca tabuľka poskytuje informácie o podpore EIM poskytovanej platformami eServer. Informácie sú usporiadané podľa platformy, stĺpce majú nasledujúci význam:

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

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

Tabuľka 9. eServer EIM podpora

Platforma	Klient EIM (podpora rozhrania API)	Radič domény	Administratívne nástroje EIM
AIX na System p	AIX R5.2	IBM Directory V5.1	Nedostupné
Linux • SLES8 na PPC64 • Red Hat 7.3 na i386 • SLES7 na System z	Prevezmite jedno z tohto: • Klient IBM Directory V4.1 • Klient IBM Directory V5.1 • Klient LDAP v2.0.23	IBM Directory V5.1	Nedostupné
i5/OS na System i	i5/OS V5R3 alebo novšie vydanie	IBM Tivoli Directory Server for i5/OS	System i Navigator
Windows 2000 na System x	Prevezmite jedno z tohto: • Klient IBM Directory V4.1 • Klient IBM Directory V5.1	Klient IBM Directory V5.1	Nedostupné
z/OS na System z	z/OS V1R4 LDAP SPE OW57137	z/OS V1R4 LDAP	V1R4 LDAP SPE OW57137

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

Súvisiace informácie

Adresárový server IBM Tivoli

Identifikácia potrebných schopností a rolí

Mapovanie podnikovej identity (EIM) je nastavené tak, aby mohol byť jediný človek jednoducho zodpovedný za konfiguráciu a administráciu v malej organizácii. Vo väčšej organizácii môžete uprednostniť väčší počet rôznych osôb.

Počet ľudí, ktorých potrebujete vo vašom tíme závisí od vyžadovaných zručností jednotlivých členov tímu, typov platforiem zahrnutých vo vašej implementácií EIM a preferovanom spôsobe rozdelenia bezpečnostných rolí a zodpovednosti vo vašej organizácii.

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

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

Členovia tímu a ich úlohy

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

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

Poznámka: Administrátori EIM zohrávajú vo vašej organizácii dôležitú rolu a majú takú istú moc ako osoby, ktoré môžu vo vašich systémoch vytvárať identity užívateľov. Keď vytvoria priradenia EIM pre identity užívateľov, určia, kto môže pristupovať do vašich počítačových systémov a aké má pri prístupe privilégiá. IBM odporúča priradiť túto autoritu tým ľuďom, ktorým do veľkej miery dôverujete na základe bezpečnostnej politiky vašej spoločnosti.

Nasledujúca tabuľka obsahuje zoznam možných rolí členov tímu, úloh a zručnosti potrebných na konfiguráciu a riadenie EIM.

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

Tabuľka 10. Roly, úlohy a zručnosti pre konfiguráciu EIM

Rola	Autorizovaná úloha	Vyžadované zručnosti
Administrátor EIM	• Koordinácia operácií v doméne • Pridanie, odstránenie a zmena definícií registrov, identifikátorov EIM a priradení pre identity užívateľov • Oprávnenie radiča pre údaje v rámci domény EIM	Znalosť administratívnych nástrojov EIM
Administrátor identifikátorov EIM	• Vytvorenie a zmena identifikátorov EIM • Pridanie a odstránenie administratívnych a zdrojových priradení (nemôže pridať ani odstrániť cieľové priradenia)	Znalosť administratívnych nástrojov EIM

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

Rola	Autorizovaná úloha	Vyžadované zručnosti
Administrátor registrov EIM	Riadenie všetkých definícií registrov EIM: • Pridanie a odstránenie cieľových priradení (nemôže pridať ani odstrániť zdrojové a administratívne priradenia) • Aktualizácia definícií registrov EIM	Znalosti: • Všetkých registrov užívateľov, definovaných pre doménu EIM (napríklad informácie o identitách užívateľov) • Administratívnych nástrojov EIM
X administrátor registrov EIM	Riadenie konkrétnej definície registra EIM: • Pridanie a odstránenie cieľových priradení pre konkrétny register užívateľov (napríklad register X) • Aktualizácia konkrétnej definície registra EIM	Znalosti: • Konkrétneho registra užívateľov, definovaného pre doménu EIM (napríklad informácie o identitách užívateľov) • Administratívnych nástrojov EIM
Administrátor adresárového servera (LDAP)	• Inštalácia a konfigurácia adresárového servera (ak je to potrebné) • Prispôsobenie konfigurácie adresárového servera pre EIM • Vytvorenie domény EIM (pozrite si poznámku) • Definovanie užívateľov autorizovaných pre prístup k radiču domény EIM • Voliteľné: Definovanie prvého administrátora EIM **Poznámka:** Administrátor adresárového servera môže vykonávať všetky činnosti administrátora EIM.	Znalosti: • Inštalácie, konfigurácie a prispôsobenia adresárového servera • Administratívnych nástrojov EIM
Administrátor registrov užívateľov	• Nastavenie užívateľských profilov alebo identít užívateľov pre konkrétny register užívateľov • Voliteľné: Môže zastupovať administrátora registrov EIM pre konkrétny register užívateľov	Znalosti: • Nástrojov pre spravovanie registra užívateľov • Administratívnych nástrojov EIM
Systémový programátor alebo administrátor systému	Inštalácia potrebných softvérových produktov (môže zahŕňať inštaláciu EIM)	Znalosti: • Systémového programovania alebo administratívnych zručností • Inštalačných procedúr pre platformu
Aplikačný programátor	Písanie aplikácií používajúcich rozhrania API EIM	Znalosti: • Platformy • Programovacích zručností • Kompilácie programov

Súvisiace koncepty

"Riadenie prístupu EIM" na strane 38
Užívateľ EIM je užívateľ, ktorý vlastní riadenie prístupu na EIM na základe jeho členstva v preddefinovanej skupine užívateľov Lightweight Directory Access Protocol (LDAP) pre špecifickú doménu.

Plánovanie domény mapovania podnikovej identity

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

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

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

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

Tabuľka 11. Informácie potrebné na plánovanie domény EIM

Potrebné informácie	Rola
1. Existuje doména spĺňajúca potreby alebo je potrebné vytvoriť novú?	Administrátor EIM
2. Ktorý adresárový server bude predstavovať radič domény EIM? (Bližšie informácie o výbere radiča domény nájdete v "Plánovanie radiča domény mapovania podnikovej identity".)	Administrátor adresárového servera (LDAP) alebo administrátor EIM
3. Názov domény. (Môžete poskytnúť aj nepovinný opis.)	Administrátor EIM
4. Kde sa nachádza adresár na uloženie údajov domény EIM? **Poznámka:** V závislosti od vašej voľby systému hostiteľa adresárového servera a v závislosti od vašej voľby adresára na uloženie údajov domény EIM budete zrejme musieť vykonať niektoré konfiguračné úlohy adresárových služieb pred vytvorením domény.	Administrátor adresárového servera (LDAP) alebo administrátor EIM
5. Aplikácie a operačné systémy, ktoré sa budú nachádzať v doméne. Ak konfigurujete vašu prvú doménu, môže to byť len jeden systém. (Bližšie informácie nájdete v "Vývoj plánu pomenúvania definícií registra mapovania podnikovej identity" na strane 58.)	Tím EIM
6. Ľudia a entity, ktoré sa budú nachádzať doméne. **Poznámka:** Ak chcete, aby bolo úvodné testovanie ľahšie, môžete obmedziť počet účastníkov na jedného alebo dvoch.	Tím EIM

Plánovanie radiča domény mapovania podnikovej identity

Keď zhromažďujete informácie na zadefinovanie domény EIM, musíte zistiť, ktorý produkt adresárového servera sa bude správať ako radič domény EIM.

EIM vyžaduje, aby hostiteľom radiča domény bol adresárový server, ktorý podporuje protokol Lightweight Directory Access Protocol (LDAP) verzie 3. Okrem toho musí byť adresárový server schopný prijať schému LDAP a ďalšie faktory týkajúce sa EIM a podporovať určité atribúty a triedy objektov.

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

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

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

Naplánovať prístup k radiču domény

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

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

Vybrať typ viazania EIM

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

Jednoduché väzby
Jednoduchá väzba je pripojenie LDAP, v ktorom klient LDAP poskytuje serveru LDAP na autentifikáciu charakteristický názov väzby a heslo väzby. Rozlišovací názov a heslo viazania definuje administrátor LDAP v adresári LDAP. Ide o najslabšiu a najmenej bezpečnú formu autentifikácie, pretože rozlišovací názov a heslo viazania sa odosielajú nešifrované a dajú sa ľahko zistiť odpočúvaním. Môžete použiť CRAM-MD5 (challenge-response authentication mechanism), ak chcete pridať ďalšiu úroveň ochrany hesla viazania. Pri použití protokolu CRAM-MD5 klient odošle serveru na autentifikáciu hašovaciu hodnotu namiesto čistého hesla.

Autentifikácia servera pomocou SSL (Secure Sockets Layer) - autentifikácia na strane servera
Server LDAP môže byť nakonfigurovaný na pripojenia SSL alebo TLS (Transport Layer Security). Server LDAP používa na svoju autentifikáciu klientovi LDAP digitálny certifikát a vytvorí medzi nimi zašifrovanú komunikačnú reláciu. Pomocou certifikátu sa autentifikuje len server LDAP. Koncový užívateľ sa autentifikuje pomocou rozlišovacieho názvu a hesla viazania. Sila autentifikácie je taká istá ako v prípade jednoduchého viazania, ale všetky údaje sú zašifrované (vrátane rozlišovacieho názvu a hesla viazania).

Autentifikácia klienta pomocou SSL
Server LDAP môže byť nakonfigurovaný na vyžadovanie autentifikácie koncového užívateľa prostredníctvom digitálneho certifikátu namiesto charakteristického názvu a hesla väzby pre zabezpečené pripojenia SSL alebo TLS na server LDAP. Autentifikuje sa klient aj server a relácia je zašifrovaná. Táto voľba poskytuje silnejšiu úroveň autentifikácie užívateľa a chráni súkromie všetkých prenášaných údajov.

Autentifikácia Kerberos
Klient LDAP môže byť autentifikovaný na server pomocou lístka Kerberos ako voliteľnej náhrady charakteristického názvu a hesla väzby. Protokol Kerberos je dôveryhodný systém sieťovej autentifikácie tretej strany, ktorý umožňuje, aby principál (užívateľ alebo služba) preukázal svoju identitu inej službe v rámci nezabezpečenej siete. Autentifikácia principálov sa dokončí prostredníctvom centrálneho servera nazvaného distribučné centrum kľúčov (KDC). Centrum KDC autentifikuje užívateľa s lístkom Kerberos. Tieto lístky preukazujú identitu principálu iným službám v sieti. Po autentifikácii principálu týmito lístkami si môže principál a služba vymieňať zašifrované informácie s cieľovou službou. Táto voľba poskytuje silnejšiu úroveň autentifikácie užívateľa a chráni súkromie autentifikačných informácií.

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

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

Príklad pracovného listu plánovania: informácie o radiči domény

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

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

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

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

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

Tabuľka 13. Príklad pracovného listu plánovania identít viazania

Oprávnenie alebo rola EIM	**Identita viazania**	**Mechanizmus viazania**	**Potrebný dôvod**
Administrátor EIM	eimadmin@krbrealm1.com	kerberos	konfigurácia a riadenie EIM

Tabuľka 13. Príklad pracovného listu plánovania identít viazania (pokračovanie)

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

Vývoj plánu pomenúvania definícií registra mapovania podnikovej identity

Ak chcete používať EIM na mapovanie identity užívateľa v jednom registri užívateľov k ekvivalentnej identite užívateľa v inom registri užívateľov, musia byť oba registre užívateľov pre EIM definované.

Musíte vytvoriť definíciu registra EIM pre každý register užívateľov aplikácie alebo operačného systému, ktorý bude participovať v doméne EIM. Registre užívateľa môžu predstavovať registre operačného systému, ako napríklad Resource Access Control Facility (RACF) alebo i5/OS, distribuovaný register ako je Kerberos, alebo podskupinu systémového registra, ktorú používa aplikácia exkluzívne.

Doména EIM môže obsahovať definície registrov pre registre užívateľov, existujúce v inej platforme. Napríklad doména spravovaná radičom domény v i5/OS môže obsahovať definície registra pre platformy iné než i5/OS (ako napríklad register AIX). Aj keď môžete pre doménu EIM definovať ľubovoľný register užívateľov, musíte definovať registre užívateľov pre aplikácie a operačné systémy podporujúce EIM.

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

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

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

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

Názov definície registra	Typ registra užívateľov	Alias definície registra	Opis registra
System_C	Register užívateľov systémui5/OS	Pozrite si dokumentáciu aplikácie	Register užívateľov hlavného systému i5/OS na System C
System_A_WAS	WebSphere LTPA	app_23_alias_source	WebSphere LTPA register užívateľov na System A
System_B	Linux	Pozrite si dokumentáciu aplikácie	Linux register užívateľov na System B

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

Názov definície registra	Typ registra užívateľov	Alias definície registra	Opis registra
System_A	Register užívateľov systémui5/OS	app_23_alias_target app_xx_alias_target	Register užívateľov hlavného systému pre i5/OS na System A
System_D	Register užívateľov Kerberos	app_xx_alias_source	legal.mydomain.com Kerberos realm
System_4	Register užívateľov Windows 2000	Pozrite si dokumentáciu aplikácie	Register užívateľov aplikácie ľudských zdrojov v systéme 4

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

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

Vývoj plánu mapovania identity

Kritická časť úvodného procesu plánovania implementácie EIM vyžaduje určenie spôsobu používania mapovania identity vo vašom podniku.

Na mapovanie identít v EIM môžete použiť dve metódy:

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

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

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

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

Ak chcete vytvoriť plán mapovania identít, musíte vykonať toto:

Súvisiace koncepty

“Vytváranie priradení EIM” na strane 98
Existujú dva rôzne typy priradení EIM, ktoré môžete vytvoriť. Môžete vytvoriť priradenie identifikátora alebo priradenie politiky.

"Vytváranie priradenia politiky" na strane 99
Priradenie politiky poskytuje prostriedky na priame definovanie vzťahu medzi viacerými identitami užívateľa v jednom alebo viacerých registroch a individuálnou cieľovou identitou užívateľa v inom registri.

Plánovanie priradení mapovania podnikovej identity:

Priradenia sú položky vytvorené v doméne EIM na definovanie vzťahu medzi užívateľskými identitami v rôznych registroch užívateľov.

V EIM môžete vytvoriť jeden z dvoch typov priradení: priradenia identifikátorov, ktoré definujú mapovania typu veľa-jeden a priradenia politiky, ktoré definujú mapovania typu veľa-jeden. Priradenia politiky môžete používať namiesto alebo v kombinácii s priradeniami identifikátorov.

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

Môžete vytvoriť ľubovoľný z nasledujúcich typov priradení identifikátorov:

- **Cieľové priradenia**

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

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

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

Priradenie politiky vždy definuje cieľové priradenie.

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

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

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

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

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

Názov definície registra	Typ registra užívateľov	Alias definície registra	Opis registra	Typy priradení
System_C	Register užívateľov systémui5/OS	Pozrite si dokumentáciu aplikácie	Register užívateľov hlavného systému i5/OS na System C	Cieľové
System_A_WAS	WebSphere LTPA	app_23_alias_source	WebSphere LTPA register užívateľov na System A	Primárny zdroj
System_B	Linux	Pozrite si dokumentáciu aplikácie	Linux register užívateľov na System B	Zdrojové a cieľové
System_A	Register užívateľov systémui5/OS	app_23_alias_target app_xx_alias_target	Register užívateľov hlavného systému pre i5/OS na System A	Cieľové
System_D	Register užívateľov Kerberos	app_xx_alias_source	legal.mydomain.com Kerberos realm	Zdroj
System_4	Register užívateľov Windows 2000	Pozrite si dokumentáciu aplikácie	Register užívateľov aplikácie ľudských zdrojov v systéme 4	Administratívne
order.mydomain.com	Register užívateľov Windows 2000		Hlavný prihlasovací register pre zamestnancov oddelenia objednávok	Predvolená politika registra (zdrojový register)
System_A_order_app	Aplikácia oddelenia objednávok		Špecifický register aplikácie pre aktualizácie objednávok	Predvolená politika registra (cieľový register)
System_C_order_app	Aplikácia oddelenia objednávok		Špecifický register aplikácie pre aktualizácie objednávok	Predvolená politika registra (cieľový register)

Tabuľka 16. Príklad pracovného listu plánovania identifikátorov EIM

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

Tabuľka 17. Príklad pracovného listu plánovania priradení identifikátorov

Jedinečný názov identifikátora: _____John S Day_____		
Register užívateľov	**Identita užívateľa**	**Typy priradení**
WAS systému A	johnday	Zdroj
Linux na System B	jsd1	Zdrojové a cieľové
i5/OS na System C	JOHND	Cieľové
Register 4 v systéme ľudských zdrojov Windows 2000	JDAY	Administratívne

Tabuľka 18. Príklad pracovného listu plánovania priradení politiky

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

Vývoj plánu pomenúvania identifikátorov EIM:

Pri plánovaní potrieb mapovania identity EIM môžete vytvárať jedinečné identifikátory EIM pre užívateľov aplikácií povolených EIM a operačných systémov vo vašom podniku, keď chcete pre užívateľa vytvoriť mapovanie jeden-jeden medzi užívateľskými identitami. Používaním priradení identifikátorov na vytvorenie mapovaní typu veľa-jeden môžete maximalizovať výhody manažmentu hesiel, ktoré EIM poskytuje.

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

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

Tabuľka 19. Príklad pracovného listu plánovania identifikátorov EIM

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

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

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

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

Pracovné listy plánovania implementácie mapovania podnikovej identity

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

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

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

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

Príklad použitia tohto pracovného listu nájdete v téme Plán radiča domény EIM.

Tabuľka 21. Pracovný list plánovania identít viazania

EIM autorita alebo rola	**Spojovacia identita**	**Spojovací mechanizmus**	**Potrebný dôvod**

Tabuľka 21. Pracovný list plánovania identít viazania (pokračovanie)

Príklad použitia tohto pracovného listu nájdete v téme Plán radiča domény EIM.

Tabuľka 22. Pracovný list plánovania informácií o definícii registra EIM

Názov definície registra	**Typ užívateľského registra**	**Alias definície registra**	**Opis registra**	**Typy priradenia**

Príklad použitia tohto pracovného listu nájdete v téme Vývoj názvového plánu definície registra EIM.

Tabuľka 23. Pracovný list plánovania identifikátorov EIM

Názov jedinečného identifikátora	**Opis identifikátora alebo užívateľskej identity**	**Alias identifikátora**

Tabuľka 23. Pracovný list plánovania identifikátorov EIM (pokračovanie)

Príklad použitia tohto pracovného listu nájdete v téme Vývoj názvového plánu identifikátora EIM.

Tabuľka 24. Pracovný list plánovania priradení identifikátorov

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

Príklad použitia tohto pracovného listu nájdete v téme Plán priradení EIM.

Tabuľka 25. Pracovný list plánovania priradení politiky

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

Príklad použitia tohto pracovného listu nájdete v téme Plán priradení EIM.

Plánovanie vývoja aplikácií pre mapovanie podnikovej identity

Aplikácia musí byť schopná používať rozhrania API mapovania EIM, aby mohla používať mapovanie podnikovej identity (EIM) a participovať v doméne.

Pozrite si dokumentáciu rozhrania API mapovania EIM a dokumentáciu EIM špecifickú pre platformu a zistite, či existujú nejaké mimoriadne aspekty plánovania, ktorým by ste mali pri písaní alebo adaptovaní aplikácií na používanie rozhraní API mapovania EIM rozumieť. Napríklad môžu existovať faktory týkajúce sa kompilácie aplikácií vytvorených v jazyku C alebo C++, ktoré obsahujú volania rozhraní API EIM. Takisto, v závislosti od platformy aplikácie môžu existovať ďalšie faktory týkajúce sa procesu zostavovania aplikácie.

Súvisiace úlohy

"Rozhrania API pre EIM" na strane 119
EIM poskytuje techniky pre manažment identít užívateľov medzi platformami. EIM má niekoľko aplikačných programových rozhraní (API), ktoré môžu aplikácie používať na vykonávanie operácií EIM v mene aplikácie alebo užívateľa aplikácie.

Plánovanie mapovania podnikovej identity pre i5/OS

Existuje viacero technológií a služieb, ktoré EIM obsahuje na platforme System i. Pred konfiguráciou EIM na váš server by ste sa mali rozhodnúť, akú funkčnosť chcete implementovať pomocou EIM a schopností jednoduchého prihlásenia.

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

Ak plánujte používať protokol Kerberos na autentifikáciu užívateľov ako súčasť implementácie jednoduchého prihlásenia, mali by ste takisto nakonfigurovať službu sieťovej autentifikácie.

Ak sa chcete dozvedieť viac o plánovaní konfigurácie EIM vášho systému, pozrite si nasledujúce informácie:

Súvisiace informácie

Služba plánovania sieťovej autentifikácie

Nevyhnutné podmienky inštalácie EIM pre i5/OS

Pracovný list plánovania uvádza služby, ktoré by ste mali nainštalovať pred konfiguráciou EIM.

Tabuľka 26. Plánovací pracovný list inštalácie EIM

Pracovný list pre plánovanie požiadaviek pre EIM	**Odpovede**
Používa váš systém i5/OS V5R4 alebo novšiu verziu?	
Sú vo vašom systéme nainštalované nasledujúce voľby a licenčné produkty? • Hostiteľské servery i5/OS (5761-SS1 Option 12) • System i Access for Windows (5761-XE1) • Qshell Interpreter (5761-SS1 Option 30) Potrebný, ak máte v úmysle konfigurovať službu sieťovej autentifikácie a tiež EIM. **Poznámka:** 5722 je kód produktu pre produkty a voľby i5/OS, pred V6R1.	
Je na osobnom počítači administrátora nainštalovaný System i Navigator vrátene nasledujúcich podkomponentov? • Sieť • Bezpečnosť (potrebná, ak máte v úmysle konfigurovať službu sieťovej autentifikácie a tiež EIM)	
Nainštalovali ste najnovší balík opráv System i Access for Windows? Najnovší balík opráv nájdete na System i Prístup	
Ak je adresárový server, napríklad adresárový server IBM Tivoli pre i5/OS aktuálne nakonfigurovaný a chcete ho použiť ako radič domény EIM, poznáte charakteristické meno (DN) a heslo administrátora LDAP?	
Ak je adresárový server aktuálne nakonfigurovaný, môže byť dočasne zastavený? (Bude to potrebné kvôli dokončeniu procesu konfigurácie EIM.)	
Máte špeciálne oprávnenia *SECADM, *ALLOBJ a *IOSYSCFG?	
Použili ste najnovšie dočasné opravy programu (PTF)?	

Inštalácia vyžadovaných volieb System i Navigator

Ak chcete povoliť prostredie jednoduchého prihlásenia s EIM a službou sieťovej autentifikácie, musíte nainštalovať voľbu **Sieť** aj voľbu **Bezpečnosť** z System i Navigator.

EIM sa nachádza pod voľbou **Sieť** a služba sieťovej autentifikácie sa nachádza pod voľbou **Bezpečnosť**. Ak neplánujete používať vo vašej sieti službu sieťovej autentifikácie, nemusíte inštalovať voľbu **Bezpečnosť** System i Navigator.

Ak chcete nainštalovať voľbu Network System i Navigator alebo zistiť, či máte túto voľbu už nainštalovanú, skontrolujte, či je System i Access for Windows nainštalovaný v osobnom počítači, ktorý používate na administráciu modelu System i.

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

1. Kliknite na **Start > Programs > System i Access for Windows > Selective Setup**.

2. Riaďte sa inštrukciami z dialógového okna. V dialógu **Component Selection** rozviňte **System i Navigator** a vyberte voľbu **Sieť**. Ak plánujete používať službu sieťovej autentifikácie, mali by ste tiež vybrať voľbu **Bezpečnosť**.
3. Pokračujte cez zvyšok **Selektívneho nastavovania**.

Súvisiace informácie

Služba sieťovej autentifikácie

Aspekty zálohy a obnovy pre EIM

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

Súvisiace informácie

Replikácia adresárového servera

Úlohy replikácie

Úvahy o ukladaní a obnove adresárového servera

Zálohovanie a obnova dát domény EIM:

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

Jedným zo spôsobov zálohovania údajov, vhodným najmä na účely obnovy pri nehode, je uloženie databázovej knižnice. Pri predvolených nastaveniach to je QUSRDIRDB. Ak je povolený protokol zmien changelog, mali by ste uložiť aj knižnicu QUSRDIRCL. Adresárový server v systéme, kde chcete obnoviť knižnicu, musí mať takú istú schému a konfiguráciu LDAP ako pôvodný adresárový server. Súbory, ktoré ukladajú tieto informácie sa nachádzajú v adresári /QIBM/UserData/OS400/DirSrv. Ďalšie konfiguračné údaje sú uložené v QUSRSYS/QGLDCFG (objekt *USRSPC) a QUSRSYS/QGLDVLDL (objekt *VLDL). Ak chcete mať kompletnú zálohu všetkého pre váš adresárový server, musíte uložiť obe knižnice, súbory integrovaného súborového systému a objekty QUSRSYS.

Napríklad na uloženie celého obsahu adresárového servera alebo jeho časti môžete použiť súbor LDIF. Ak chcete zálohovať informácie domény pre IBM Tivoli Directory Server pre radič domény i5/OS, vykonajte tieto kroky:

1. V System i Navigator rozviňte **Sieťové servery > > TCP/IP**.
2. Kliknite pravým tlačidlom myši na **Directory Server**, vyberte **Tools** a potom **Export file**, aby sa zobrazila stránka umožňujúca uviesť, ktoré časti obsahu adresárového servera sa majú vyexportovať do súboru.
3. Presuňte súbor exportu na platformu System i, ktorú chcete použiť ako svoj záložný adresárový server.
4. V System i Navigator na záložnom serveri rozviňte **Network > Servers > TCP/IP**.
5. Kliknite pravým tlačidlom myši na **Directory Server**, vyberte **Tools** a potom **Import**, aby ste zaviedli obsah presunutého súboru do nového adresárového servera.

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

Spôsob konfigurácie a používania replikačného adresárového servera závisí od typu replikačného modelu, ktorý budete používať.

Zálohovanie a obnova konfiguračných informácií EIM:

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

Pri ukladaní a obnove konfigurácie EIM sú dostupné tieto voľby:

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

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

Ďalej porozmýšľajte a naplánujte, ako budete zálohovať a obnovovať údaje služby sieťovej autentifikácie, ak ste túto službu nakonfigurovali ako súčasť implementácie prostredia jednoduchého prihlásenia.

Konfigurácia EIM

Konfiguračný sprievodca EIM umožňuje rýchlo a jednoducho vykonať základnú konfiguráciu EIM pre váš systém. Sprievodca vám poskytuje tri voľby pre konfiguráciu systému EIM.

Spôsob použitia sprievodcu pre konfiguráciu EIM v špecifickom systéme závisí na vašom celkovom pláne používania EIM vo vašom podniku a na vašich potrebách konfigurácie EIM. Mnohí administrátori chcú napríklad používať EIM v kombinácii so službou sieťovej autentifikácie na vytvorenie prostredia jednoduchého prihlásenia na viacerých systémoch a platformách bez potreby meniť východiskové bezpečnostné politiky. Sprievodca konfiguráciou EIM vám ich preto umožňuje konfigurovať službu sieťovej autentifikácie ako súčasť vašej konfigurácie EIM. Konfigurácia a používanie služby sieťovej autentifikácie však nie je nevyhnutné a povinné pre konfiguráciu a používanie EIM.

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

- Ktorú platformu System i chcete nakonfigurovať ako radič domény EIM pre doménu EIM? Konfiguračného sprievodcu EIM použite najprv na vytvorenie novej domény na tomto systéme a potom na konfiguráciu všetkých ďalších systémov na pripojenie k tejto doméne.
- Chcete nakonfigurovať službu sieťovej autentifikácie vo všetkých systémoch, ktoré konfigurujete pre EIM? Ak áno, môžete na vytvorenie základnej konfigurácie služby sieťovej autentifikácie na každom modeli System i použiť konfiguračného sprievodcu EIM. Musíte však vykonať aj iné úlohy pre dokončenie konfigurácie služby sieťovej autentifikácie.

Keď použijete konfiguračného sprievodcu EIM na vytvorenie základnej konfigurácie pre každú platformu System i, pred dokončením konfigurácie EIM musíte ešte vykonať niekoľko úloh konfigurácie EIM. Pozrite si Scenár: Povolenie jednoduchého prihlásenia, kde nájdete príklad, ako fiktívna spoločnosť nakonfigurovala prostredie jednoduchého prihlásenia pomocou služby sieťovej autentifikácie a EIM.

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

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

Pred použitím Sprievodcu konfiguráciou EIM musíte dokončiť všetky kroky pre “Plánovanie EIM” na strane 51, aby ste mohli presne určiť spôsob používania EIM. Ak konfigurujete EIM ako súčasť vytvárania prostredia jednoduchého prihlásenia, mali by ste tiež vykonať všetky kroky plánovania jednoduchého prihlásenia.

Ak chcete spustiť Sprievodcu konfiguráciou EIM, vykonajte tieto kroky:

1. Spustite System i Navigator.
2. Prihláste sa na systém, ktorý chcete nakonfigurovať pre EIM. Ak konfigurujete EIM na viacerých systémoch, začnite s tým, na ktorom chcete nakonfigurovať radič domény pre EIM.
3. Rozviňte **Network → Enterprise Identity Mapping**.

4. Pravým tlačidlom myši kliknite na **Configuration** a vyberte **Configure** na spustenie konfiguračného sprievodcu EIM.
5. Vyberte konfiguračnú voľbu EIM a postupujte podľa pokynov sprievodcu, potrebných pre jeho dokončenie.
6. Ak potrebujete zistiť, aké informácie treba zadať do jednotlivých polí, kliknite na tlačidlo **Help**.

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

Súvisiace informácie

Služba sieťovej autentifikácie

Jednoduché prihlásenie

Vytvorenie a pripojenie k novej lokálnej doméne

Pri použití Sprievodcu konfiguráciou EIM na vytvorenie a pripojenie k novej doméne môžete zvoliť, či chcete ako súčasť vytvorenia vašej konfigurácie EIM nakonfigurovať radič domény EIM v lokálnom systéme.

Ak treba, Sprievodca konfiguráciou EIM skontroluje, či poskytujete základné konfiguračné informácie pre adresárový server. Ak Kerberos nie je aktuálne nakonfigurovaný na platforme System i, sprievodca vás vyzve na spustenie sprievodcu konfiguráciou služby sieťovej autentifikácie.

Po dokončení Sprievodcu konfiguráciou EIM môžete vykonať tieto úlohy:

- Vytvoriť novú doménu EIM.
- Konfigurovať lokálny adresárový server, aby fungoval ako radič domény EIM.
- Konfigurovať službu sieťovej autentifikácie pre systém.
- Vytvoriť definície registru EIM pre lokálny register i5/OS a register Kerberos.
- Konfigurovať systém, aby sa stal účastníkom novej domény EIM.

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

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

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

1. V System i Navigator vyberte systém, pre ktorý chcete nakonfigurovať EIM a rozviňte **Network > Enterprise Identity Mapping**.
2. Kliknutím pravým tlačidlom myši na **Configuration** a výberom **Configure** spustíte sprievodcu konfiguráciou EIM.

   Poznámka: Ak bolo EIM predtým v systéme nakonfigurované, táto voľba bude označená **Reconfigure**.
3. Na stránke **Welcome** sprievodcu vyberte **Create and join a new domain** a kliknite na tlačidlo **Next**.
4. Na strane **Specify EIM Domain Location** vyberte **On the local Directory server** a kliknite na tlačidlo **Next**.

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

   Ak služba sieťovej autentifikácie nie je aktuálne nakonfigurovaná na platforme System i alebo sa na konfiguráciu prostredia jednoduchého prihlásenia vyžadujú ďalšie konfiguračné informácie sieťovej autentifikácie, zobrazí sa

stránka **Network Authentication Services Configuration**. Táto stránka vám umožňuje spustiť pomocníka Konfigurácie autentifikácie na sieti tak, aby ste mohli nakonfigurovať autentifikáciu na sieti. Alebo môžete nakonfigurovať službu sieťovej autentifikácie neskôr pomocou konfiguračného sprievodcu pre túto službu prostredníctvom System i Navigator. Po dokončení konfigurácie služby sieťovej autentifikácie pokračujete ďalej v Sprievodcovi konfiguráciou EIM.

5. Ak chcete konfigurovať službu sieťovej autentifikácie, vykonajte tieto kroky:
   a. Na strane **Configure Network Authentication Service** vyberte **Yes**, aby sa spustil Sprievodca konfiguráciou služby sieťovej autentifikácie. Pomocou tohto pomocníka môžete nakonfigurovať niekoľko rozhraní a služieb i5/OS, ktoré budú súčasťou prostredia Kerberos, ako aj nakonfigurovať prostredie jediného prihlásenia, ktoré používa aj EIM, aj autentifikačnú službu siete.
   b. Na strane **Specify Realm Information** zadajte názov predvoleného realmu v poli **Default realm**. Ak používate Microsoft Active Directory pre autentifikáciu pomocou Kerberos, vyberte **Microsoft Active Directory is used for Kerberos authentication** a kliknite na tlačidlo **Next**.
   c. Na strane **Specify KDC Information** zadajte plne kvalifikovaný názov servera Kerberos pre tento realm v poli **KDC**, potom v poli **Port** zadajte hodnotu 88 a kliknite na tlačidlo **Next**.
   d. Na strane **Specify Password Server Information** vyberte **Yes** alebo **No** pre nastavenie servera hesiel. Server hesiel umožňuje principálom meniť heslá v serveri Kerberos. Ak vyberiete voľbu **Yes**, zadajte názov servera hesiel v poli **Password server**. V poli **Port** použite predvolenú hodnotu 464 a kliknite na tlačidlo Next.
   e. Na stránke **Select Keytab Entries** vyberte **i5/OS Kerberos Authentication** a kliknite na **Next**.

      Poznámka: Ak chcete, aby tieto služby používali autentifikáciu Kerberos, môžete okrem toho vytvoriť aj položky súboru kľúčov pre IBM Tivoli Directory Server for i5/OS, i5/OS NetServer a IBM HTTP Server for i5/OS. Najskôr budete musieť vykonať ďalšiu konfiguráciu pre tieto služby predtým, než môžu používať autentifikáciu pomocou Kerberos.

   f. Na stránke **Create i5/OS Keytab Entry** zadajte a potvrďte heslo, a kliknite na **Next**. Toto isté heslo budete používať, keď budete pridávať principály i5/OS na server Kerberos.
   g. Voliteľný: Na strane **Create Batch File** vyberte **Yes**, potom zadajte nasledujúce informácie a kliknite na tlačidlo **Next**:
      - V poli **Batch file** zaktualizujte adresárovú cestu. Kliknite na tlačidlo **Browse**, ak chcete vyhľadať správnu adresárovú cestu alebo upravte cestu v poli **Batch file**.
      - V poli **Include password** vyberte **Yes**. To zaručí, že všetky heslá priradené k služobnému principálu i5/OS budú súčasťou dávkového súboru. Je dôležité nezabudnúť, že heslá sa zobrazujú ako čitateľný text a môže ich prečítať ktokoľvek s prístupom na čítanie toho dávkového súboru. Je preto dôležité ihneď po jeho použití dávkový súbor vymazať zo servera Kerberos aj z PC. Ak heslo nezahrniete, budete vyzvaný na zadanie hesla pri spustení dávkového súboru.

        Poznámka: Môžete tiež manuálne pridať principály služieb, vygenerované sprievodcom do Microsoft Active Directory. Ak chcete vedieť, ako to vykonať, pozrite si principály Add i5/OS pre server Kerberos

      - Na strane **Summary** zobrazte detaily konfigurácie služby sieťovej autentifikácie a kliknite na tlačidlo **Finish** pre návrat do Sprievodcu konfiguráciou EIM.
6. Ak lokálny adresárový server nie je práve nakonfigurovaný, po pokračovaní sprievodcu konfiguráciou EIM sa zobrazí strana **Configure Directory Server**. Ak chcete konfigurovať lokálny adresárový server, poskytnite tieto informácie:

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

   a. V poli **Port** použite predvolené číslo portu 389, alebo zadajte odlišné číslo portu, ak chcete používať nezabezpečené komunikácie EIM s adresárovým serverom.

b. V poli **Distinguished name** zadajte rozlišovací názov LDAP (DN), identifikujúci administrátora LDAP pre adresárový server. Sprievodca konfiguráciou EIM toto DN administrátora LDAP vytvorí a použije to pre konfiguráciu adresárového servera, aby fungoval ako radič domény pre novú vytváranú doménu.

c. V poli **Password** zadajte heslo pre administrátora LDAP.

d. V poli **Confirm password** zadajte heslo druhýkrát za účelom overenia.

e. Kliknite na tlačidlo **Next**.

7. Na strane **Specify Domain** poskytnite tieto informácie:

   a. V poli **Domain** zadajte názov domény EIM, ktorú chcete vytvoriť. Použite predvolený názov EIM, alebo použite ľubovoľný znakový reťazec, ktorý vám vyhovuje. Nemôžete však použiť špeciálne znaky, napríklad **= + < > , # ;** \ a *****.

   b. V poli **Description** zadajte opisný text domény.

   c. Kliknite na tlačidlo **Next**.

8. Na strane **Specify Parent DN for Domain** vyberte **Yes** pre špecifikovanie rodičovského DN pre práve vytváranú doménu, alebo zadajte **No**, ak chcete údaje EIM uložiť do adresára s príponou, ktorej názov je odvodený z názvu domény EIM.

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

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

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

   a. Vyberte **Local i5/OS**, ak chcete pridať definíciu registra pre register local. V poskytnutom poli pre názov definície registra použite buď predvolenú hodnotu registra, alebo pre názov definície registra zadajte odlišnú hodnotu. Názov registra EIM je ľubovoľný reťazec reprezentujúci typ registra a špecifickú inštanciu tohto registra.

   b. Vyberte **Kerberos**, ak chcete pridať definíciu registra pre register Kerberos. V poskytnutom poli pre názov definície registra použite buď predvolenú hodnotu registra, alebo pre názov definície registra zadajte odlišnú hodnotu. Predvolený názov definície registra je rovnaký ako názov realmu. Použitím predvoleného názvu a teda použitím názvu registra Kerberos, ktorý je rovnaký ako je názov realmu, môžete zvýšiť výkon získavania informácií z tohto registra. Ak treba, vyberte **Kerberos user identities are case sensitive**.

   c. Kliknite na tlačidlo **Next**.

10. Na strane **Specify EIM System User** vyberte **User Type**, ktorého systém použije pri vykonávaní operácií EIM v mene funkcií operačného systému. Medzi tieto operácie patrí mapovanie vyhľadávacích operácií a vymazávanie priradení počas vymazávania lokálnych profilov užívateľov i5/OS. Môžete vybrať jeden z týchto typov užívateľov: **Distinguished name and password**, **Kerberos keytab file and principal** alebo **Kerberos principal and password**. Typy užívateľov, ktoré môžete vybrať sa líšia podľa aktuálnej konfigurácie systému. Napríklad, ak Služba sieťovej autentifikácie nie je pre systém nakonfigurovaná, typy užívateľov Kerberos nemusia byť dostupné vo výbere. Vybratý typ užívateľa predurčuje ďalšie informácie, ktoré musíte poskytnúť pre dokončenie strany podľa týchto pokynov:

    Poznámka: Musíte špecifikovať užívateľa aktuálne definovaného v adresárovom serveri, ktorý je hostiteľom pre radič domény EIM. Vami zadaný užívateľ musí mať privilégiá minimálne na vykonanie vyhľadávania mapovaní a správu registra pre lokálny register užívateľov. Ak užívateľ, ktorého uvádzate, nemá tieto privilégiá, niektoré funkcie operačného systému týkajúce sa použitia jednoduchého prihlásenia a vymazávania užívateľských profilov môžu zlyhať.

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

- Ak vyberiete **Distinguished name and password**, poskytnite tieto informácie:
  - V poli **Distinguished name** zadajte rozlišovací názov LDAP (DN), identifikujúci užívateľa, ktorého systém použije pri vykonávaní operácií EIM.
  - V poli **Password** zadajte heslo pre rozlišovací názov.
  - V poli **Confirm password** zadajte heslo druhýkrát za účelom overenia.
- Ak vyberiete **Kerberos principal and password**, zadajte tieto informácie:
  - V poli **Principal** zadajte názov principálu Kerberos, ktorého systém použije pri vykonávaní operácií EIM
  - V poli **Realm** zadajte plne kvalifikovaný názov realmu Kerberos, ktorého je principál členom. Názov principálu a realmu jedinečne identifikujú užívateľov Kerberos v súbore kľúčov. Napríklad principál jsmith v realme ordept.myco.com je reprezentovaný v súbore kľúčov ako jsmith@ordept.myco.com.
  - V poli **Password** zadajte heslo pre daného užívateľa.
  - V poli **Confirm password** zadajte heslo druhýkrát za účelom overenia.
- Ak vyberiete **Kerberos keytab file and principal**, poskytnite tieto informácie:
  - V poli **Keytab file** zadajte úplnú cestu a názov súboru kľúčov, obsahujúceho principál Kerberos, ktorého systém použije pri vykonávaní operácií EIM. Alebo kliknite na **Browse** na prehľadávanie adresárov v integrovanom súborovom systéme System i na výber súboru na ukladanie kľúčov.
  - V poli **Principal** špecifikujte názov principálu Kerberos, ktorého systém použije pri vykonávaní operácií EIM.
  - V poli **Realm** zadajte plne kvalifikovaný názov realmu Kerberos, ktorého je principál členom. Názov principálu a realmu jedinečne identifikujú užívateľov Kerberos v súbore kľúčov. Napríklad principál jsmith v realme ordept.myco.com je reprezentovaný v súbore kľúčov ako jsmith@ordept.myco.com.
- Kliknite na **Verify Connection**, aby ste sa uistili, že sprievodca dokáže použiť zadané informácie o užívateľovi pre úspešné vytvorenie pripojenia k radiču domény EIM.
- Kliknite na tlačidlo **Next**.

11. Na paneli **Summary** skontrolujte vami zadané konfiguračné informácie. Ak sú všetky informácie správne, kliknite na tlačidlo **Finish**.

Ukončite konfiguráciu EIM pre doménu

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

1. Použite Sprievodcu konfiguráciou EIM v každom ďalšom serveri, ktorý chcete pripojiť k doméne.
2. Pridajte podľa potreby definície registra EIM do domény EIM pre ostatné platformy s výnimkou System i a aplikácie, ktoré chcete, aby participovali v doméne EIM. Tieto definície registra odkazujú na aktuálne registre užívateľov, ktoré musia byť účastníkmi domény. Môžete buď pridať definície systémových registrov alebo môžete pridať definície aplikačných registrov v závislosti na potrebách vašej implementácie EIM.
3. Na základe vašich potrieb implementácie EIM určite, či chcete:
   - Vytvoriť identifikátory EIM pre každého jedinečného užívateľa alebo entitu v doméne a vytvoriť priradenia pre tieto identifikátory.
   - Vytvoriť priradenia politiky pre mapovanie skupiny užívateľov do samostatnej cieľovej identity užívateľa.
   - Vytvoriť kombináciu z predošlých volieb.
4. Použite funkciu testovanie mapovania EIM, aby ste otestovali mapovania identít pre vašu konfiguráciu EIM.
5. Ak jediný vami vytvorený užívateľ EIM je DN pre administrátora LDAP, potom váš užívateľ EIM má vysokú úroveň oprávnenia pre všetky údaje v adresárovom serveri. Zvážte preto vytvorenie jedného alebo viacerých DN ako ďalších užívateľov, ktorí budú mať vhodnejšie a obmedzenejšie riadenie prístupu pre údaje EIM. Ak sa chcete dozvedieť viac o vytváraní DN pre adresárový server, pozrite si Distinguished names v Informačné centrum i5/OS .

Počet dodatočných užívateľov EIM, ktorých definujete závisí od prístupu vašej bezpečnostnej politiky k oddeleniu úloh týkajúcich sa bezpečnosti od zodpovednosti. Typicky môžete vytvoriť minimálne tieto dva typy DN:

- **Užívateľa s riadením prístupu Administrátor EIM**

  Toto DN administrátora EIM poskytuje príslušnú úroveň oprávnenia pre administrátora, ktorý je zodpovedný za správu domény EIM. DN tohto administrátora EIM môžete použiť na pripojenie k radiču domény, keď sú riadené všetky aspekty domény EIM pomocou System i Navigator.
- **Aspoň jedného užívateľa, ktorý má všetky tieto riadenia prístupu**:
  - Administrátor identifikátorov
  - Administrátor registrov
  - Operácie s mapovaním EIM

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

Poznámka: Ak chcete použiť tento nový DN pre systémového užívateľa namiesto DN administrátora LDAP, musíte zmeniť vlastnosti konfigurácie EIM pre platformu System i. Ak chcete vedieť, ako zmeniť DN systémového užívateľa, pozrite si tému Riadenie vlastností konfigurácie EIM.

Ďalej možno budete chcieť používať protokol SSL (Secure Sockets Layer) alebo protokol TLS (Transport Layer Security) pre konfiguráciu bezpečného pripojenia k radiču domény EIM, aby ste ochránili prenos údajov EIM. Ak povolíte SSL pre adresárový server, musíte aktualizovať konfiguračné vlastnosti EIM a zadať, že platforma System i používa bezpečné pripojenie SSL. Musíte tiež aktualizovať vlastnosti pre doménu a zadať, že EIM používa pripojenia SSL na riadenie domény prostredníctvom System i Navigator.

Poznámka: Možno budete musieť vykonať ďalšie úlohy, ak ste vytvorili základnú konfiguráciu služby sieťovej autentifikácie, najmä vtedy, ak implementujete prostredie jednoduchého prihlásenia. Informácie o týchto ďalších krokoch nájdete, ak si pozriete úplné konfiguračné kroky znázornené v scenári Povolenie jednoduchého prihlásenia pre i5/OS.

Vytvorenie a pripojenie k novej vzdialenej doméne

Pri použití Sprievodcu konfiguráciou EIM na vytvorenie a pripojenie k novej lokálnej doméne môžete zvoliť, či chcete ako súčasť vytvorenia vašej konfigurácie EIM nakonfigurovať adresárový server vo vzdialenom systéme, aby fungoval ako radič domény EIM.

Ak chcete nakonfigurovať EIM vo vzdialenom serveri, musíte zadať príslušné informácie pre pripájanie k vzdialenému adresárovému serveru. Ak Kerberos nie je aktuálne nakonfigurovaný na platforme System i, sprievodca vás vyzve na spustenie sprievodcu konfiguráciou služby sieťovej autentifikácie.

Poznámka: Adresárový server vo vzdialenom systéme musí poskytovať podporu pre EIM. EIM vyžaduje, aby hostiteľom radiča domény bol adresárový server podporujúci protokol LDAP (Lightweight Directory Access Protocol) verzie 3. Produkt adresárového servera musí mať nakonfigurovanú schému EIM. Napríklad produkt IBM Directory Server V5.1 poskytuje túto podporu. Bližšie informácie o požiadavkách radiča domény EIM nájdete v “Plánovanie radiča domény mapovania podnikovej identity” na strane 55.

Po dokončení Sprievodcu konfiguráciou EIM môžete vykonať tieto úlohy:

- Vytvoriť novú doménu EIM.
- Konfigurovať vzdialený adresárový server, aby fungoval ako radič domény EIM.
- Konfigurovať službu sieťovej autentifikácie pre systém.
- Vytvoriť definície registru EIM pre lokálny register i5/OS a register Kerberos.
- Konfigurovať systém, aby sa stal účastníkom novej domény EIM.

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

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

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

1. Skontrolujte, či je adresárový server vo vzdialenom systéme aktívny.
2. V System i Navigator vyberte systém, pre ktorý chcete nakonfigurovať EIM a rozviňte **Network > Enterprise Identity Mapping**.
3. Kliknutím pravým tlačidlom myši na **Configuration** a výberom **Configure** spustíte sprievodcu konfiguráciou EIM.

   Poznámka: Ak bolo EIM predtým v systéme nakonfigurované, táto voľba bude označená **Reconfigure**.
4. Na stránke **Welcome** sprievodcu vyberte **Create and join a new domain** a kliknite na tlačidlo **Next**.
5. Na strane **Specify EIM Domain Location** vyberte **On the local Directory server** a kliknite na tlačidlo **Next**.

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

   Ak služba sieťovej autentifikácie nie je aktuálne nakonfigurovaná na platforme System i alebo sa na konfiguráciu prostredia jednoduchého prihlásenia vyžadujú ďalšie konfiguračné informácie sieťovej autentifikácie, zobrazí sa stránka **Network Authentication Services Configuration**. Táto stránka vám umožňuje spustiť pomocníka Konfigurácie autentifikácie na sieti tak, aby ste mohli nakonfigurovať autentifikáciu na sieti. Alebo môžete nakonfigurovať službu sieťovej autentifikácie neskôr pomocou konfiguračného sprievodcu pre túto službu prostredníctvom System i Navigator. Po dokončení konfigurácie služby sieťovej autentifikácie pokračujete ďalej v Sprievodcovi konfiguráciou EIM.
6. Ak chcete konfigurovať službu sieťovej autentifikácie, vykonajte tieto kroky:
   a. Na strane **Configure Network Authentication Service** vyberte **Yes**, aby sa spustil Sprievodca konfiguráciou služby sieťovej autentifikácie. Pomocou tohto pomocníka môžete nakonfigurovať niekoľko rozhraní a služieb i5/OS, ktoré budú súčasťou prostredia Kerberos, ako aj nakonfigurovať prostredie jediného prihlásenia, ktoré používa aj EIM, aj autentifikačnú službu siete.
   b. Na strane **Specify Realm Information** zadajte názov predvoleného realmu v poli **Default realm**. Ak používate Microsoft Active Directory pre autentifikáciu pomocou Kerberos, vyberte **Microsoft Active Directory is used for Kerberos authentication** a kliknite na tlačidlo **Next**.
   c. Na strane **Specify KDC Information** zadajte plne kvalifikovaný názov servera Kerberos pre tento realm v poli **KDC**, potom v poli **Port** zadajte hodnotu 88 a kliknite na tlačidlo **Next**.
   d. Na strane **Specify Password Server Information** vyberte **Yes** alebo **No** pre nastavenie servera hesiel. Server hesiel umožňuje principálom meniť heslá v serveri Kerberos. Ak vyberiete voľbu **Yes**, zadajte názov servera hesiel v poli **Password server**. V poli **Port** použite predvolenú hodnotu 464 a kliknite na tlačidlo Next.
   e. Na stránke **Select Keytab Entries** vyberte **i5/OS Kerberos Authentication** a kliknite na **Next**.

      Poznámka: Ak chcete, aby tieto služby používali autentifikáciu Kerberos, môžete okrem toho vytvoriť aj položky kľúčov pre IBM Tivoli Directory Server for i5/OS, i5/OS NetServer a IBM HTTP Server for i5/OS server. Najskôr budete musieť vykonať ďalšiu konfiguráciu pre tieto služby predtým, než môžu používať autentifikáciu pomocou Kerberos.
   f. Na stránke **Create i5/OS Keytab Entry** zadajte a potvrďte heslo, a kliknite na **Next**. Toto isté heslo budete používať, keď budete pridávať principály i5/OS na server Kerberos.
   g. Voliteľný: Na strane **Create Batch File** vyberte **Yes**, potom zadajte nasledujúce informácie a kliknite na tlačidlo **Next**:
      - V poli **Batch file** zaktualizujte adresárovú cestu. Kliknite na tlačidlo **Browse**, ak chcete vyhľadať správnu adresárovú cestu alebo upravte cestu v poli **Batch file**.

- V poli **Include password** vyberte **Yes**. To zaručí, že všetky heslá priradené k služobnému principálu i5/OS budú súčasťou dávkového súboru. Je dôležité nezabudnúť, že heslá sa zobrazujú ako čitateľný text a môže ich prečítať ktokoľvek s prístupom na čítanie toho dávkového súboru. Je preto dôležité ihneď po jeho použití dávkový súbor vymazať zo servera Kerberos aj z PC. Ak heslo nezahrniete, budete vyzvaný na zadanie hesla pri spustení dávkového súboru.

  Poznámka: Môžete tiež manuálne pridať principály služieb, vygenerované sprievodcom do Microsoft Active Directory. Ak chcete vedieť, ako to vykonať, pozrite si principály Add i5/OS pre server Kerberos .
- Na strane **Summary** zobrazte detaily konfigurácie služby sieťovej autentifikácie a kliknite na tlačidlo **Finish** pre návrat do Sprievodcu konfiguráciou EIM.

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

        Poznámka: Overte, že radič domény EIM je nakonfigurovaný pre používanie bezpečného pripojenia. V opačnom prípade môže pripojenie k radiču domény zlyhať.
      - V poli **Port** zadajte port TCP/IP, na ktorom adresárový server počúva. Ak je vybraté **Use secure connection**, predvoleným portom je port 636; v opačnom prípade je predvoleným portom port 389.
   c. Kliknite na **Verify Connection**, aby ste otestovali, či sprievodca dokáže zadané informácie použiť na vytvorenie pripojenia k vzdialenému radiču domény EIM.
   d. Kliknite na tlačidlo **Next**.
8. Na strane **Specify User For Connection** vyberte **User Type** pre pripojenie. Môžete vybrať jeden z týchto typov užívateľov: **Distinguished name and password**, **Kerberos keytab file and principal**, **Kerberos principal and password** alebo **User profile and password**. Tieto dva typy užívateľov Kerberos sú k dispozícii len vtedy, ak je služba sieťovej autentifikácie nakonfigurovaná pre lokálnu platformu System i. Vami vybratý typ užívateľa určuje ostatné informácie, ktoré musíte poskytnúť v tomto dialógovom okne:

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

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

   a. Ak vyberiete **Distinguished name and password**, poskytnite tieto informácie:
      - Do poľa **Distinguished name** zadajte rozlišovací názov administrátora LDAP (DN) a heslo, ktoré zabezpečí sprievodcovi dostatočné oprávnenia na administráciu domény EIM a objektov v tejto doméne.
      - V poli **Password** zadajte heslo pre rozlišovací názov.
      - V poli **Confirm password** zadajte heslo druhýkrát za účelom overenia.
   b. Ak vyberiete **Kerberos keytab file and principal**, poskytnite tieto informácie:
      - V poli **Keytab file** zadajte úplnú cestu a názov súboru kľúčov, obsahujúceho principál Kerberos, ktorého sprievodca použije pri pripájaní k doméne EIM. Alebo kliknite na **Browse** na prehľadávanie adresárov v integrovanom súborovom systéme i5/OS na výber súboru kľúčov.
      - V poli **Principal** zadajte názov principálu Kerberos, ktorý sa použije pre identifikáciu užívateľa.

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

c. Ak vyberiete **Kerberos principal and password**, zadajte tieto informácie:
   - V poli **Principal** zadajte názov principálu Kerberos, ktorého sprievodca použije pri pripájaní k doméne EIM.
   - V poli **Realm** zadajte plne kvalifikovaný názov realmu Kerberos, ktorého je principál členom. Názov principálu a realmu jedinečne identifikujú užívateľov Kerberos v súbore kľúčov. Napríklad principál jsmith v realme ordept.myco.com je reprezentovaný v súbore kľúčov ako jsmith@ordept.myco.com.
   - V poli **Password** zadajte heslo pre principál Kerberos.
   - V poli **Confirm password** zadajte heslo druhýkrát za účelom overenia.

d. Ak vyberiete **User profile and password**, poskytnite tieto informácie:
   - V poli **User profile** zadajte názov užívateľského profilu, ktorého sprievodca použije pri pripájaní k doméne EIM.
   - V poli **Password** zadajte heslo pre užívateľský profil.
   - V poli **Confirm password** zadajte heslo druhýkrát za účelom overenia.

e. Kliknite na **Verify Connection**, aby ste otestovali, či sprievodca dokáže zadané informácie o užívateľovi použiť pre úspešné vytvorenie pripojenia k radiču domény EIM.

f. Kliknite na tlačidlo **Next**.

9. Na strane **Specify Domain** poskytnite tieto informácie:
   a. V poli **Domain** zadajte názov domény EIM, ktorú chcete vytvoriť. Použite predvolený názov EIM, alebo použite ľubovoľný znakový reťazec, ktorý vám vyhovuje. Nemôžete však použiť špeciálne znaky, napríklad **= + < > , # ;** \ a *.
   b. V poli **Description** zadajte opisný text domény.
   c. Kliknite na tlačidlo **Next**.
10. V dialógovom okne **Specify Parent DN for Domain** vyberte **Yes** pre špecifikáciu rodičovského DN, ktoré sprievodca použije pre umiestnenie domény EIM, ktorú vytvárate. Toto DN predstavuje položku, ktorá sa v stromovej hierarchii informácií v adresároch nachádza hneď nad položkou domény s vašim názvom. Môžete zadať **No**, ak chcete údaje EIM uložiť do adresára s príponou, ktorej názov je odvodený z názvu domény EIM.

    Poznámka: Pri použití sprievodcu pre konfiguráciu domény vo vzdialenom radiči domény musíte pre danú doménu zadať príslušné rodičovské DN. Všetky potrebné objekty konfigurácie musia pre rodičovské DN existovať, inak môže konfigurácia EIM zlyhať, preto uprednostnite radšej prehľadanie pre príslušné rodičovské DN pred manuálnym zadaním informácií o DN. Ak chcete získať viac informácií o používaní rodičovského DN, kliknite na **Help**.
11. Na strane **Registry Information** špecifikujte, či chcete pridať lokálne registre užívateľov do domény EIM ako definície registrov. Vyberte jeden alebo oba typy registra užívateľov:

    Poznámka: Teraz nemusíte vytvárať definície registrov. Ak sa rozhodnete vytvoriť definície registra neskôr, pozrite si pridávanie definície systémového registra a vlastnosti konfigurácie EIM.
    a. Vyberte **Local i5/OS**, ak chcete pridať definíciu registra pre register local. V poskytnutom poli pre názov definície registra použite buď predvolenú hodnotu registra, alebo pre názov definície registra zadajte odlišnú hodnotu. Názov registra EIM je ľubovoľný reťazec reprezentujúci typ registra a špecifickú inštanciu tohto registra.
    b. Vyberte **Kerberos**, ak chcete pridať definíciu registra pre register Kerberos. V poskytnutom poli pre názov definície registra použite buď predvolenú hodnotu registra, alebo pre názov definície registra zadajte odlišnú hodnotu. Predvolený názov definície registra je rovnaký ako názov realmu. Použitím predvoleného názvu a teda použitím názvu registra Kerberos, ktorý je rovnaký ako je názov realmu, môžete zvýšiť výkon získavania informácií z tohto registra. Ak treba, vyberte **Identity užívateľa Kerberos rozlišujú veľkosť písmen**.
    c. Kliknite na tlačidlo **Next**.

12. Na strane **Specify EIM System User** vyberte **User Type**, ktorého systém použije pri vykonávaní operácií EIM v mene funkcií operačného systému. Medzi tieto operácie patrí mapovanie vyhľadávacích operácií a vymazávanie priradení počas vymazávania lokálnych profilov užívateľov i5/OS. Môžete vybrať jeden z týchto typov užívateľov: **Distinguished name and password**, **Kerberos keytab file and principal** alebo **Kerberos principal and password**. Typy užívateľov, ktoré môžete vybrať sa líšia podľa aktuálnej konfigurácie systému. Napríklad, ak služba sieťovej autentifikácie nie je pre systém nakonfigurovaná, typy užívateľov Kerberos nemusia byť dostupné vo výbere. Vybratý typ užívateľa predurčuje ďalšie informácie, ktoré musíte poskytnúť pre dokončenie strany podľa týchto pokynov:

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

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

    a. Ak vyberiete **Distinguished name and password**, poskytnite tieto informácie:
        - V poli **Distinguished name** zadajte rozlišovací názov LDAP (DN), identifikujúci užívateľa, ktorého systém použije pri vykonávaní operácií EIM.
        - V poli **Password** zadajte heslo pre rozlišovací názov.
        - V poli **Confirm password** zadajte heslo druhýkrát za účelom overenia.

    b. Ak vyberiete **Kerberos principal and password**, zadajte tieto informácie:
        - V poli **Principal** zadajte názov principálu Kerberos, ktorého systém použije pri vykonávaní operácií EIM
        - V poli **Realm** zadajte plne kvalifikovaný názov realmu Kerberos, ktorého je principál členom. Názov principálu a realmu jedinečne identifikujú užívateľov Kerberos v súbore kľúčov. Napríklad principál jsmith v realme ordept.myco.com je reprezentovaný v súbore kľúčov ako jsmith@ordept.myco.com.
        - V poli **Password** zadajte heslo pre daného užívateľa.
        - V poli **Confirm password** zadajte heslo druhýkrát za účelom overenia.

    c. Ak vyberiete **Kerberos keytab file and principal**, poskytnite tieto informácie:
        - V poli **Keytab file** zadajte úplnú cestu a názov súboru kľúčov, obsahujúceho principál Kerberos, ktorého systém použije pri vykonávaní operácií EIM. Alebo kliknite na **Browse** na prehľadávanie adresárov v integrovanom súborovom systéme System i na výber súboru na ukladanie kľúčov.
        - V poli **Principal** špecifikujte názov principálu Kerberos, ktorého systém použije pri vykonávaní operácií EIM.
        - V poli **Realm** zadajte plne kvalifikovaný názov realmu Kerberos, ktorého je principál členom. Názov principálu a realmu jedinečne identifikujú užívateľov Kerberos v súbore kľúčov. Napríklad principál jsmith v realme ordept.myco.com je reprezentovaný v súbore kľúčov ako jsmith@ordept.myco.com.

    d. Kliknite na **Verify Connection**, aby ste sa uistili, že sprievodca dokáže použiť zadané informácie o užívateľovi pre úspešné vytvorenie pripojenia k radiču domény EIM.

    e. Kliknite na tlačidlo **Next**.

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

Ukončite konfiguráciu EIM pre doménu

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

1. Použite sprievodcu konfiguráciou EIM na každom ďalšom serveri, ktorý chcete, aby sa pripojil do existujúcej domény. Bližšie informácie nájdete v téme “Pripojenie k existujúcej doméne” na strane 78.

2. Pridajte podľa potreby definície registra EIM do domény EIM pre ostatné platformy s výnimkou System i a aplikácie, ktoré chcete, aby participovali v doméne EIM. Tieto definície registra odkazujú na aktuálne registre užívateľov, ktoré musia byť účastníkmi domény. V závislosti od potrieb vašej implementácie EIM si pozrite "Pridávanie definície systémového registra" na strane 89 alebo "Pridávanie definície registra aplikácií" na strane 89.
3. Na základe vašich potrieb implementácie EIM určite, či chcete:
   a. "Vytváranie identifikátora EIM" na strane 95 pre každého jedinečného užívateľa alebo entitu v doméne a "Vytváranie priradenia identifikátora EIM" na strane 98 pre nich.
   b. "Vytváranie priradenia politiky" na strane 99 mapovať skupinu užívateľov pre jednu identitu cieľového užívateľa.
   c. Vytvorenie ich kombinácie.
4. Funkcia EIM "Testovanie mapovania EIM" na strane 85 sa používa na testovanie mapovaní identity pre vašu konfiguráciu EIM.
5. Ak jediný vami vytvorený užívateľ EIM je DN pre administrátora LDAP, potom váš užívateľ EIM má vysokú úroveň oprávnenia pre všetky údaje v adresárovom serveri. Zvážte preto vytvorenie jedného alebo viacerých DN ako ďalších užívateľov, ktorí budú mať vhodnejšie a obmedzenejšie riadenie prístupu pre údaje EIM. Ak sa chcete dozvedieť viac o vytváraní DN pre adresárový server, pozrite si tému Charakteristické názvy v Informačné centrum i5/OS . Počet dodatočných užívateľov EIM, ktorých definujete závisí od prístupu vašej bezpečnostnej politiky k oddeleniu úloh týkajúcich sa bezpečnosti od zodpovednosti. Typicky môžete vytvoriť minimálne tieto dva typy DN:
   - **Užívateľa s riadením prístupu Administrátor EIM**

     Toto DN administrátora EIM poskytuje príslušnú úroveň oprávnenia pre administrátora, ktorý je zodpovedný za správu domény EIM. DN tohto administrátora EIM môžete použiť na pripojenie k radiču domény, keď sú riadené všetky aspekty domény EIM pomocou System i Navigator.
   - **Aspoň jedného užívateľa, ktorý má všetky tieto riadenia prístupu**:
     – Administrátor identifikátorov
     – Administrátor registrov
     – Operácie s mapovaním EIM

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

   Poznámka: Ak chcete použiť tento nový DN pre systémového užívateľa namiesto DN administrátora LDAP, musíte zmeniť vlastnosti konfigurácie EIM pre platformu System i. Ak chcete vedieť, ako zmeniť DN systémového užívateľa, pozrite si tému "Riadenie vlastností konfigurácie EIM" na strane 112.

Možno budete musieť vykonať ďalšie úlohy, ak ste vytvorili základnú konfiguráciu služby sieťovej autentifikácie, najmä vtedy, ak implementujete prostredie jednoduchého prihlásenia. Informácie o týchto ďalších krokoch nájdete, ak si pozriete úplné konfiguračné kroky znázornené v scenári Povolenie jednoduchého prihlásenia pre i5/OS.

Pripojenie k existujúcej doméne

Použite sprievodcu konfiguráciou EIM na jednej platforme System i na konfiguráciu radiča domény a vytvorte doménu EIM a potom môžete použiť sprievodcu na konfiguráciu ostatných systémov na participáciu v doméne.

Po vytvorení domény EIM a konfigurácii radiča domény v jednom systéme môžete nakonfigurovať všetky ostatné platformy System i na pripojenie k existujúcej doméne EIM. Pri prechode sprievodcom musíte zadávať informácie o doméne, vrátane informácií o pripojení k radiču domény EIM. Ak na pripojenie k existujúcej doméne použijete Sprievodcu konfiguráciou EIM, sprievodca vám stále poskytuje možnosť spustenia Sprievodcu konfiguráciou služby sieťovej autentifikácie, ak si ako súčasť konfigurácie EIM v systéme zvolíte konfiguráciu Kerberos.

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

- Konfigurovať službu sieťovej autentifikácie pre systém.
- Vytvoriť definície registru EIM pre lokálny register i5/OS a register Kerberos.

- Konfigurovať systém, aby sa stal účastníkom domény EIM.

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

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

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

1. Skontrolujte, či je adresárový server vo vzdialenom systéme aktívny.
2. V System i Navigator vyberte systém, pre ktorý chcete nakonfigurovať EIM a rozviňte **Network > Enterprise Identity Mapping**.
3. Pravým tlačidlom myši kliknite na **Konfigurácia** a vyberte **Konfigurovať...**, aby sa spustil Sprievodca konfiguráciou EIM.

   Poznámka: Táto voľba je označená ako **Prekonfigurovať...**, ak už bolo EIM predtým v systéme nakonfigurované.
4. Na strane **Welcome** sprievodcu vyberte **Join an existing domain** a kliknite na tlačidlo **Next**.

   Poznámka: Ak služba sieťovej autentifikácie nie je momentálne nakonfigurovaná na modeli System i alebo sa na konfiguráciu prostredia jednoduchého prihlásenia vyžadujú ďalšie konfiguračné informácie sieťovej autentifikácie, zobrazí sa stránka **Network Authentication Services Configuration**. Táto stránka vám umožňuje spustiť pomocníka Konfigurácie autentifikácie na sieti tak, aby ste mohli nakonfigurovať autentifikáciu na sieti. Alebo môžete nakonfigurovať službu sieťovej autentifikácie neskôr pomocou konfiguračného sprievodcu pre túto službu prostredníctvom System i Navigator. Po dokončení konfigurácie služby sieťovej autentifikácie pokračujete ďalej v Sprievodcovi konfiguráciou EIM.
5. Ak chcete konfigurovať službu sieťovej autentifikácie, vykonajte tieto kroky:
   a. Na strane **Configure Network Authentication Service** vyberte **Yes**, aby sa spustil Sprievodca konfiguráciou služby sieťovej autentifikácie. Pomocou tohto pomocníka môžete nakonfigurovať niekoľko rozhraní a služieb i5/OS, ktoré budú súčasťou prostredia Kerberos, ako aj nakonfigurovať prostredie jediného prihlásenia, ktoré používa aj EIM, aj autentifikačnú službu siete.
   b. Na strane **Specify Realm Information** zadajte názov predvoleného realmu v poli **Default realm**. Ak používate Microsoft Active Directory pre autentifikáciu pomocou Kerberos, vyberte **Microsoft Active Directory is used for Kerberos authentication** a kliknite na tlačidlo **Next**.
   c. Na strane **Specify KDC Information** zadajte plne kvalifikovaný názov servera Kerberos pre tento realm v poli **KDC**, potom v poli **Port** zadajte hodnotu 88 a kliknite na tlačidlo **Next**.
   d. Na strane **Specify Password Server Information** vyberte **Yes** alebo **No** pre nastavenie servera hesiel. Server hesiel umožňuje principálom meniť heslá v serveri Kerberos. Ak vyberiete voľbu **Yes**, zadajte názov servera hesiel v poli **Password server**. V poli **Port** použite predvolenú hodnotu 464 a kliknite na tlačidlo Next.
   e. Na stránke **Select Keytab Entries** vyberte **i5/OS Kerberos Authentication** a kliknite na **Next**.

      Poznámka: Ak chcete, aby tieto služby používali autentifikáciu Kerberos, môžete okrem toho vytvoriť aj položky kľúčov pre IBM Tivoli Directory Server for i5/OS, i5/OS NetServer a IBM HTTP Server for i5/OS. Najskôr budete musieť vykonať ďalšiu konfiguráciu pre tieto služby predtým, než môžu používať autentifikáciu pomocou Kerberos.
   f. Na stránke **Create i5/OS Keytab Entry** zadajte a potvrďte heslo, a kliknite na **Next**. Toto isté heslo budete používať, keď budete pridávať principály i5/OS na server Kerberos.
   g. Voliteľný: Na strane **Create Batch File** vyberte **Yes**, potom zadajte nasledujúce informácie a kliknite na tlačidlo **Next**:
      - V poli **Batch file** zaktualizujte adresárovú cestu. Kliknite na tlačidlo **Browse**, ak chcete vyhľadať správnu adresárovú cestu alebo upravte cestu v poli **Batch file**.

- V poli **Include password** vyberte **Yes**. To zaručí, že všetky heslá priradené k služobnému principálu i5/OS budú súčasťou dávkového súboru. Je dôležité nezabudnúť, že heslá sa zobrazujú ako čitateľný text a môže ich prečítať ktokoľvek s prístupom na čítanie toho dávkového súboru. Je preto dôležité ihneď po jeho použití dávkový súbor vymazať zo servera Kerberos aj z PC. Ak heslo nezahrniete, budete vyzvaný na zadanie hesla pri spustení dávkového súboru.

  Poznámka: Môžete tiež manuálne pridať principály služieb, vygenerované sprievodcom do Microsoft Active Directory. Ak chcete vedieť, ako to vykonať, pozrite si principály Add i5/OS pre server Kerberos

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

6. Na strane **Specify Domain Controller** poskytnite tieto informácie:

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

   a. V poli **Domain controller name** zadajte názov systému, ktorý slúži ako radič pre doménu EIM, ku ktorej chcete, aby sa platforma System i pripojila.

   b. Kliknite na **Use secure connection (SSL or TLS)**, ak chcete použiť bezpečné pripojenie k radiču domény EIM. Pri výbere tejto voľby použije pripojenie buď protokol SSL (Secure Sockets Layer), alebo TLS (Transport Layer Security) na vytvorenie bezpečného pripojenia, aby ochránilo prenos údajov EIM cez nedôveryhodnú sieť, napríklad Internet.

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

   c. V poli **Port** zadajte port TCP/IP, na ktorom adresárový server počúva. Ak je vybraté **Use secure connection**, predvoleným portom je port 636; v opačnom prípade je predvoleným portom port 389.

   d. Kliknite na **Verify Connection**, aby ste otestovali, či sprievodca dokáže zadané informácie použiť na vytvorenie pripojenia k radiču domény EIM.

   e. Kliknite na tlačidlo **Next**.

7. Na strane **Specify User For Connection** vyberte **User Type** pre pripojenie. Môžete zvoliť niektorý z nasledujúcich typov užívateľa: **Distinguished name and password**, **Kerberos keytab file and principal**, **Kerberos principal and password**, alebo **User profile and password**. Tieto dva typy užívateľov Kerberos sú k dispozícii len vtedy, ak je služba sieťovej autentifikácie nakonfigurovaná pre lokálnu platformu System i. Vami vybratý typ užívateľa určuje ostatné informácie, ktoré musíte poskytnúť v tomto dialógovom okne:

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

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

   - Ak vyberiete **Distinguished name and password**, poskytnite tieto informácie:
     - V poli **Distinguished name** zadajte rozlišovací názov LDAP (DN), identifikujúci užívateľa s oprávnením na vytvorenie objektov v lokálnom názvovom priestore servera LDAP. Ak ste tohto sprievodcu už použili pre konfiguráciu servera LDAP v niektorom z predošlých krokov, zadajte rozlišovací názov administrátora LDAP, ktorý ste vtedy vytvorili.
     - V poli **Password** zadajte heslo pre rozlišovací názov.
     - V poli **Confirm password** zadajte heslo druhýkrát za účelom overenia.
   - Ak vyberiete **Kerberos keytab file and principal**, poskytnite tieto informácie:
     - V poli **Keytab file** zadajte úplnú cestu a názov súboru kľúčov, obsahujúceho principál Kerberos, ktorého sprievodca použije pri pripájaní k doméne EIM. Alebo kliknite na **Browse...** na prehľadávanie adresárov v integrovanom súborovom systéme System i na výber súboru kľúčov.

- V poli **Principal** zadajte názov principálu Kerberos, ktorý sa použije pre identifikáciu užívateľa.
- V poli **Realm** zadajte plne kvalifikovaný názov realmu Kerberos, ktorého je principál členom. Názov principálu a realmu jedinečne identifikujú užívateľov Kerberos v súbore kľúčov. Napríklad principál jsmith v realme ordept.myco.com je reprezentovaný v súbore kľúčov ako jsmith@ordept.myco.com.

• Ak vyberiete **Kerberos principal and password**, zadajte tieto informácie:
- V poli **Principal** zadajte názov principálu Kerberos, ktorého sprievodca použije pri pripájaní k doméne EIM.
- V poli **Realm** zadajte plne kvalifikovaný názov realmu Kerberos, ktorého je principál členom. Názov principálu a realmu jedinečne identifikujú užívateľov Kerberos v súbore kľúčov. Napríklad principál jsmith v realme ordept.myco.com je reprezentovaný v súbore kľúčov ako jsmith@ordept.myco.com.
- V poli **Password** zadajte heslo pre principál Kerberos.
- V poli **Confirm password** zadajte heslo druhýkrát za účelom overenia.

• Ak vyberiete **User profile and password**, poskytnite tieto informácie:
- V poli **User profile** zadajte názov užívateľského profilu, ktorého sprievodca použije pri pripájaní k doméne EIM.
- V poli **Password** zadajte heslo pre užívateľský profil.
- V poli **Confirm password** zadajte heslo druhýkrát za účelom overenia.

• Kliknite na **Verify Connection**, aby ste otestovali, či sprievodca dokáže zadané informácie o užívateľovi použiť pre úspešné vytvorenie pripojenia k radiču domény EIM.
• Kliknite na tlačidlo **Next**.

8. Na strane **Specify Domain** vyberte názov domény, do ktorej sa chcete pripojiť a kliknite na tlačidlo **Next**.
9. Na strane **Registry Information** špecifikujte, či chcete pridať lokálne registre užívateľov do domény EIM ako definície registrov. Vyberte jeden alebo oba typy registra užívateľov:
   • Vyberte **Local i5/OS**, ak chcete pridať definíciu registra pre register local. V poskytnutom poli pre názov definície registra použite buď predvolenú hodnotu registra, alebo pre názov definície registra zadajte odlišnú hodnotu. Názov registra EIM je ľubovoľný reťazec reprezentujúci typ registra a špecifickú inštanciu tohto registra.

     Poznámka: Teraz nemusíte vytvárať definície lokálneho registra i5/OS. Ak vyberiete neskoršie vytvorenie definícií registrov i5/OS, musíte pridať definície systémových registrov a zaktualizovať vlastnosti konfigurácie EIM.

   • Vyberte **Kerberos**, ak chcete pridať definíciu registra pre register Kerberos. V poskytnutom poli pre názov definície registra použite buď predvolenú hodnotu registra, alebo pre názov definície registra zadajte odlišnú hodnotu. Predvolený názov definície registra je rovnaký ako názov realmu. Použitím predvoleného názvu a teda použitím názvu registra Kerberos, ktorý je rovnaký ako je názov realmu, môžete zvýšiť výkon získavania informácií z tohto registra. Ak treba, vyberte **Identity užívateľa Kerberos rozlišujú veľkosť písmen**.

     Poznámka: Ak ste použili sprievodcu konfiguráciou EIM na ďalšom systéme na pridanie definície registra pre register Kerberos, pre ktorý má tento model System i principál, potom nemusíte pridať definíciu registra Kerberos ako súčasť tejto konfigurácie. Po dokončení tohto sprievodcu však budete musieť zadať názov tohto registra Kerberos vo vlastnostiach konfigurácie pre tento systém.

   • Kliknite na tlačidlo **Next**.
10. Na strane **Specify EIM System User** vyberte **User Type**, ktorého systém použije pri vykonávaní operácií EIM v mene funkcií operačného systému. Medzi tieto operácie patrí mapovanie vyhľadávacích operácií a vymazávanie priradení počas vymazávania lokálnych profilov užívateľov i5/OS. Môžete vybrať jeden z týchto typov užívateľov: **Distinguished name and password**, **Kerberos keytab file and principal** alebo **Kerberos principal and password**. Typy užívateľov, ktoré môžete vybrať sa líšia podľa aktuálnej konfigurácie systému. Napríklad, ak služba sieťovej autentifikácie nie je pre systém nakonfigurovaná, typy užívateľov Kerberos nemusia byť dostupné vo výbere. Vybratý typ užívateľa predurčuje ďalšie informácie, ktoré musíte poskytnúť pre dokončenie strany podľa týchto pokynov:

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

- Ak vyberiete **Distinguished name and password**, poskytnite tieto informácie:
  - V poli **Distinguished name** zadajte rozlišovací názov LDAP (DN), identifikujúci užívateľa, ktorého systém použije pri vykonávaní operácií EIM.
  - V poli **Password** zadajte heslo pre rozlišovací názov.
  - V poli **Confirm password** zadajte heslo druhýkrát za účelom overenia.
- Ak vyberiete **Kerberos principal and password**, zadajte tieto informácie:
  - V poli **Principal** zadajte názov principálu Kerberos, ktorého systém použije pri vykonávaní operácií EIM
  - V poli **Realm** zadajte plne kvalifikovaný názov realmu Kerberos, ktorého je principál členom. Názov principálu a realmu jedinečne identifikujú užívateľov Kerberos v súbore kľúčov. Napríklad principál jsmith v realme ordept.myco.com je reprezentovaný v súbore kľúčov ako jsmith@ordept.myco.com.
  - V poli **Password** zadajte heslo pre daného užívateľa.
  - V poli **Confirm password** zadajte heslo druhýkrát za účelom overenia.
- Ak vyberiete **Kerberos keytab file and principal**, poskytnite tieto informácie:
  - V poli **Keytab file** zadajte úplnú cestu a názov súboru kľúčov, obsahujúceho principál Kerberos, ktorého systém použije pri vykonávaní operácií EIM. Alebo kliknite na **Browse...** na prehľadávanie adresárov v integrovanom súborovom systéme System i na výber súboru kľúčov.
  - V poli **Principal** špecifikujte názov principálu Kerberos, ktorého systém použije pri vykonávaní operácií EIM.
  - V poli **Realm** zadajte plne kvalifikovaný názov realmu Kerberos, ktorého je principál členom. Názov principálu a realmu jedinečne identifikujú užívateľov Kerberos v súbore kľúčov. Napríklad principál jsmith v realme ordept.myco.com je reprezentovaný v súbore kľúčov ako jsmith@ordept.myco.com.
- Kliknite na **Verify Connection**, aby ste sa uistili, že sprievodca dokáže použiť zadané informácie o užívateľovi pre úspešné vytvorenie pripojenia k radiču domény EIM.
- Kliknite na tlačidlo **Next**.

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

Ukončite konfiguráciu EIM pre doménu

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

1. Pridajte podľa potreby definície registra EIM do domény EIM pre systémy, ktoré nepoužívajú systémy i5/OS a aplikácie, ktoré chcete, aby participovali v doméne EIM. Tieto definície registra odkazujú na aktuálne registre užívateľov, ktoré musia byť účastníkmi domény. Môžete buď pridať definície systémových registrov alebo môžete pridať definície aplikačných registrov v závislosti na potrebách vašej implementácie EIM.
2. Na základe vašich potrieb implementácie EIM určite, či chcete:
   - Vytvoriť identifikátory EIM pre každého jedinečného užívateľa alebo entitu v doméne a vytvoriť priradenia pre tieto identifikátory.
   - Vytvoriť priradenia politiky pre mapovanie skupiny užívateľov do samostatnej cieľovej identity užívateľa.
   - Vytvoriť kombináciu z predošlých volieb.
3. Použite funkciu testovanie mapovania EIM, aby ste otestovali mapovania identít pre vašu konfiguráciu EIM.
4. Ak jediný vami vytvorený užívateľ EIM je DN pre administrátora LDAP, potom váš užívateľ EIM má vysokú úroveň oprávnenia pre všetky údaje v adresárovom serveri. Zvážte preto vytvorenie jedného alebo viacerých DN ako ďalších užívateľov, ktorí budú mať vhodnejšie a obmedzenejšie riadenie prístupu pre údaje EIM. Ak sa chcete dozvedieť viac o vytváraní DN pre adresárový server, pozrite si tému Charakteristické názvy v Informačné centrum

i5/OS . Počet dodatočných užívateľov EIM, ktorých definujete závisí od prístupu vašej bezpečnostnej politiky k oddeleniu úloh týkajúcich sa bezpečnosti od zodpovednosti. Typicky môžete vytvoriť minimálne tieto dva typy DN:

- **Užívateľa s riadením prístupu Administrátor EIM**

  Toto DN administrátora EIM poskytuje príslušnú úroveň oprávnenia pre administrátora, ktorý je zodpovedný za správu domény EIM. DN tohto administrátora EIM môžete použiť na pripojenie k radiču domény, keď sú riadené všetky aspekty domény EIM pomocou System i Navigator.
- **Aspoň jedného užívateľa, ktorý má všetky tieto riadenia prístupu**:
  - Administrátor identifikátorov
  - Administrátor registrov
  - Operácie s mapovaním EIM

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

Poznámka: Ak chcete použiť tento nový DN pre systémového užívateľa namiesto DN administrátora LDAP, musíte zmeniť vlastnosti konfigurácie EIM pre platformu System i. Ak chcete vedieť, ako zmeniť DN systémového užívateľa, pozrite si tému Riadenie vlastností konfigurácie EIM.

Možno budete musieť vykonať ďalšie úlohy, ak ste vytvorili základnú konfiguráciu služby sieťovej autentifikácie, najmä vtedy, ak implementujete prostredie jednoduchého prihlásenia. Informácie o týchto ďalších krokoch nájdete, ak si pozriete úplné konfiguračné kroky znázornené v scenári Povolenie jednoduchého prihlásenia pre i5/OS.

Konfigurácia bezpečného pripojenia k radiču domény EIM

Možno budete chcieť použiť protokol SSL (Secure Sockets Layer) alebo protokol TLS (Transport Layer Security) na vytvorenie bezpečného pripojenia na radič domény EIM, aby sa ochránil prenos údajov EIM.

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

1. Ak je potrebné, použite DCM (Digital Certificate Manager) na vytvorenie certifikátu pre adresárový server na používanie pre SSL.
2. Aktivujte SSL v lokálnom adresárovom serveri, ktorý hosťuje radič domény EIM.
3. Ak chcete uviesť, aby model System i používal bezpečné pripojenie SSL, zaktualizujte vlastnosti konfigurácie EIM. Ak chcete zaktualizovať konfiguračné vlastnosti EIM, vykonajte tieto kroky:
   a. V System i Navigator vyberte systém, na ktorom ste nakonfigurovali EIM a rozviňte **Network → Enterprise Identity Mapping**.
   b. Pravým tlačidlom myši kliknite na **Konfigurácia** a vyberte **Vlastnosti**.
   c. Na strane **Doména**, vyberte **Použitie bezpečného pripojenia (SSL alebo TLS)**, zadajte bezpečný port, na ktorom počúva adresárový server alebo akceptujte predvolenú hodnotu 636 v poli **Port** a kliknite na tlačidlo **OK**.
4. Ak chcete uviesť, aby EIM používalo pripojenie SSL pri riadení domény prostredníctvom System i Navigator, zaktualizujte vlastnosti domény EIM. Ak chcete zaktualizovať vlastnosti domény EIM, vykonajte tieto kroky:
   a. V System i Navigator vyberte systém, v ktorom ste nakonfigurovali EIM a rozviňte **Network → Enterprise Identity Mapping → Domain Management**.
   b. Vyberte doménu EIM, v ktorej chcete pracovať.
      - Ak doména EIM, s ktorou chcete pracovať, nie je uvedená pod zložkou **Domain Management**, pozrite si tému Pridávanie domény EIM do správy domén.
      - Ak nie ste práve pripojený na doménu EIM, v ktorej chcete pracovať, pozrite si tému Pripojenie k radiču domény EIM.
   c. Pravým tlačidlom myši kliknite na doménu EIM, ku ktorej ste teraz pripojený a vyberte **Vlastnosti**.
   d. Na strane **Doména**, vyberte **Použitie bezpečného pripojenia (SSL alebo TLS)**, zadajte bezpečný port, na ktorom počúva adresárový server alebo akceptujte predvolenú hodnotu 636 v poli **Port** a kliknite na tlačidlo **OK**.

Riadenie mapovania podnikovej identity

Po nakonfigurovaní EIM na platforme System i je mnoho administratívnych úloh, ktoré musíte v priebehu času vykonať pri riadení domény EIM a jej údajov.

Ak sa chcete dozvedieť viac o manažovaní EIM vo vašom podniku, pozrite si tieto strany:

Riadenie domén EIM (Managing Enterprise Identity)

Na riadenie všetkých svojich domén EIM použite System i Navigator.

Ak chcete riadiť ktorúkoľvek doménu EIM, táto musí byť uvedená alebo pridaná do zložky **Domain Managemet** pod zložkou **Network** v System i Navigator. Pri použití sprievodcu konfiguráciou EIM na vytvorenie a konfigurovanie novej domény EIM bude doména automaticky pridaná do zložky **Domain Management**, aby ste mohli manažovať túto doménu a informácie v nej obsiahnuté.

Na riadenie domény EIM, ktorá sa nachádza kdekoľvek v tej istej sieti, aj keď používaný systém neparticipuje v doméne, môžete použiť ľubovoľné pripojenie System i.

Pri manažovaní domény môžete vykonávať tieto úlohy:

Pridávanie domény EIM do zložky Domain Management

Ak pridávate doménu EIM do zložky Domain Management, musíte mať mimoriadne oprávnenie *SECADM a doména, ktorú chcete pridať, musí existovať predtým, ako ju budete pridávať do zložky Domain Management.

Ak chcete pridať existujúcu doménu EIM do zložky **Domain Managemet**, vykonajte tieto kroky:

1. Rozviňte **Network >Enterprise Identity Mapping**.
2. Kliknite pravým tlačidlom myši na zložku **Domain Management** a vyberte **Add Domain**.
3. V dialógovom okne **Add Domain** špecifikujte požadovanú doménu a zadajte informácie o pripojení. Alebo, ak chcete zobraziť zoznam domén, ktoré spravuje uvedený radič domény, kliknite na **Browse**.

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

Pripájanie k doméne EIM

Aby ste mohli pracovať s doménou EIM, musíte sa najprv pripojiť k radiču domény EIM. Na doménu EIM sa môžete pripojiť aj vtedy, keď váš model System i nie je aktuálne nakonfigurovaný na účasť v tejto doméne.

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

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

1. Rozviňte **Network > Enterprise Identity Mapping > Domain Management**.
2. Pravým tlačidlom myši kliknite na doménu, ku ktorej sa chcete pripojiť.

   Poznámka: Ak doména, s ktorou chcete pracovať, nie je uvedená pod zložkou **Domain Management**, musíte ju do tejto zložky pridať.
3. Pravým tlačidlom myši kliknite na doménu EIM, ku ktorej sa chcete pripojiť a vyberte **Connect**.

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

Povolenie priradení politiky pre doménu

Priradenie politiky poskytuje prostriedky na vytváranie mapovaní veľa-na-jeden v situáciách, kde priradenia medzi identitami užívateľa a identifikátorom EIM neexistujú.

Priradenie politiky môžete použiť na mapovanie zdrojovej množiny viacerých identít užívateľa (namiesto jednej identity užívateľa) na jednu cieľovú identitu užívateľa v zadanom cieľovom registri užívateľov. Skôr, ako budete môcť použiť priradenia politiky sa musíte uistiť, že ste povolili doméne používať priradenia politiky pre operácie vyhľadávania mapovaní.

Ak chcete podpore politiky mapovania povoliť používanie priradení politiky pre doménu, musíte byť pripojený na doménu EIM, v ktorej chcete pracovať a musíte mať riadenie prístupov administrátora EIM.

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

1. Rozviňte **Network > Enterprise Identity Mapping > Domain Management**.
2. Pravým tlačidlom myši kliknite na doménu EIM, v ktorej chcete pracovať a vyberte **Politika mapovania**.
   - Ak doména EIM, s ktorou chcete pracovať, nie je uvedená pod zložkou **Domain Management**, musíte ju do tejto zložky pridať.
   - Ak nie ste práve pripojený k doméne EIM, v ktorej chcete pracovať, musíte sa pripojiť k radiču domény EIM. (Voľba **Politika mapovania** je k dispozícii až po pripojení k doméne.)
3. Na strane **Všeobecné** vyberte **Povoliť vyhľadávanie mapovaní pomocou priradení politiky pre doménu**.
4. Kliknite na **OK**.

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

Súvisiace koncepty

"Operácie podpory a umožnenia politiky mapovaní EIM" na strane 37
Podpora politiky mapovania podnikovej identity (EIM) umožňuje používať v doméne EIM priradenia politiky a tiež špecifické priradenia identifikátorov. Priradenia politiky môžete používať namiesto alebo v kombinácii s priradeniami identifikátorov.

Testovanie mapovania EIM

Testovanie mapovania EIM umožňuje vykonať vyhľadávacie operácie mapovania EIM voči konfigurácii EIM. Testovaním si môžete overiť, či sa konkrétna identita zdrojového užívateľa správne mapuje na príslušnú identitu cieľového užívateľa. Testovanie zabezpečí, že vyhľadávacie operácie mapovania EIM môžu vrátiť na základe uvedených informácií správnu identitu cieľového užívateľa.

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

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

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

1. Rozviňte **Network > Enterprise Identity Mapping > Domain Management**.
2. Vyberte doménu EIM, v ktorej chcete pracovať.
   - Ak doména EIM, s ktorou chcete pracovať, nie je uvedená pod zložkou **Domain Management**, pozrite si tému Pridávanie domény EIM do správy domén.
   - Ak nie ste práve pripojený k doméne EIM, v ktorej chcete pracovať, pozrite si tému Connect to the EIM domain controller.
3. Pravým tlačidlom myši kliknite na doménu EIM, ku ktorej ste pripojený a vyberte **Test a Mapping**
4. V dialógovom okne **Test a Mapping** uveďte nasledujúce informácie:
   a. V poli **Source registry** zadajte názov definície registra, týkajúcej sa registra užívateľov, ktorý chcete použiť ako zdroj testu operácie vyhľadávania mapovaní.
   b. V poli **Source user** zadajte názov užívateľskej identity, ktorú chcete použiť ako zdroj testu operácie vyhľadávania mapovaní.
   c. V poli **Target registry** zadajte názov definície registra, týkajúcej sa registra užívateľov, ktorý chcete použiť ako cieľ testu operácie vyhľadávania mapovaní.
   d. Voliteľné: V poli **Lookup information** zadajte akúkoľvek informáciu vyhľadávania, definovanú pre cieľového užívateľa.
5. Ak potrebujete zistiť, aké informácie treba zadať do jednotlivých polí dialógového okna, kliknite na tlačidlo **Help**.
6. Kliknite na **Test** a pozrite si výsledky operácie vyhľadávania mapovania, ktoré sa vám zobrazia.

   Poznámka: Ak operácia vyhľadania mapovania vracia nejednoznačné výsledky, dialógové okno Test a Mapping - Results je zobrazené s indikáciou chybového hlásenia a zoznamom cieľových užívateľov, ktorých operácia vyhľadávania nájde.
   a. Ak chcete odstrániť nejednoznačné výsledky, vyberte cieľového užívateľa a kliknite na **Details**.
   b. Dialóg Test mapovania - Podrobnosti je zobrazený s indikáciou informácií o výsledkoch operácie vyhľadávania mapovaní pre zadaného cieľového užívateľa. Kliknite na Pomoc pre podrobnejšie informácie o výsledkoch operácie vyhľadávania mapovaní.
   c. Kliknite na **Close**, aby ste zatvorili dialógové okno **Test a Mapping - Results** .
7. Pokračujte v testovaní vašej konfigurácie alebo kliknite na **Close**, ak chcete ukončiť testovanie.

Súvisiace koncepty

“Odstraňovanie problémov s mapovaním EIM” na strane 116
Existuje množstvo bežných problémov, ktoré môžu spôsobiť úplné zlyhanie alebo neočakávané fungovanie mapovaní EIM. Informácie o probléme, ktorý môže spôsobovať zlyhanie mapovania EIM a možnom riešení tohto problému, nájdete v nasledujúcej tabuľke. Ak mapovania EIM zlyhávajú, budete asi musieť prejsť každým riešením a vyriešiť problém alebo problémy spôsobujúce zlyhania mapovaní.

Práca s výsledkami testu a riešenie problémov:

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

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

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

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

- Podpora priradenia politiky na úrovni domény nie je povolená. Budete musieť povoliť priradenia politiky pre doménu.
- Podpora vyhľadávania mapovaní alebo priradenia politiky na úrovni registra nie je povolená. Budete musieť povoliť podporu vyhľadávania mapovaní a používania priradení politiky pre cieľový register.
- Cieľové alebo zdrojové priradenie pre identifikátor EIM nie je správne nakonfigurované. Napríklad neexistuje zdrojové priradenie pre principál Kerberos (alebo užívateľa systému Windows) alebo je nesprávne. Je tiež možné, že cieľové priradenie určuje nesprávnu identitu užívateľa. Zobrazte všetky priradenia identifikátorov pre identifikátor EIM a skontrolujte priradenia pre konkrétny identifikátor.
- Priradenie politiky nie je správne nakonfigurované. Zobrazte všetky priradenia politiky pre doménu, aby ste overili informácie o zdroji a cieli pre všetky priradenia politiky, zadefinované v doméne.
- Definícia registra a identity užívateľov sa nezhodujú z dôvodu rozlišovania veľkosti písmen. Môžete vymazať a znovu vytvoriť register alebo vymazať a znovu vytvoriť priradenie so správnou veľkosťou písma.

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

- Identifikátor EIM má viaceré individuálne cieľové priradenia k rovnakému cieľovému registru.
- Viac ako jeden identifikátor EIM má v zdrojovom priradení zadanú tú istú identitu užívateľa a každý z nich má cieľové priradenie k tomu istému cieľovému registru, aj keď identita užívateľa zadaná pre každé cieľové priradenie môže byť rôzna.
- Viac ako jedno predvolené priradenie politiky domény určuje ten istý cieľový register.
- Viac ako jedno predvolené priradenie politiky registra určuje ten istý zdrojový register a ten istý cieľový register.
- Viac ako jedno priradenie politiky filtra certifikátov určuje ten istý zdrojový register X.509, filter certifikátov a cieľový register.

Operácia vyhľadávania mapovaní, ktorá vracia viac ako jednu cieľovú identitu užívateľa, môže spôsobovať problémy pre aplikácie dovolené od EIM, vrátane i5/OS aplikácií a produktov. Musíte preto určiť príčinu nejednoznačných výsledkov a druh akcie, potrebnej na vyriešenie tejto situácie. V závislosti od príčiny môžete vykonať niektoré z nasledujúcich krokov:

- Test vráti viaceré nežiaduce identity cieľového užívateľa. To znamená, že konfigurácia priradenia pre túto doménu nie je správna pretože:
  - Cieľové alebo zdrojové priradenie pre identifikátor EIM nie je správne nakonfigurované. Napríklad neexistuje zdrojové priradenie pre principál Kerberos (alebo užívateľa systému Windows) alebo je nesprávne. Je tiež možné, že cieľové priradenie určuje nesprávnu identitu užívateľa. Zobrazte všetky priradenia identifikátorov pre identifikátor EIM a skontrolujte priradenia pre konkrétny identifikátor.
  - Priradenie politiky nie je správne nakonfigurované. Zobrazte všetky priradenia politiky pre doménu, aby ste overili informácie o zdroji a cieli pre všetky priradenia politiky, zadefinované v doméne.
- Test vráti viaceré identity cieľového užívateľa a tieto výsledky zodpovedajú spôsobu, akým ste nakonfigurovali priradenia, takže pre každú identitu cieľového užívateľa musíte špecifikovať informácie na vyhľadanie. Jedinečné informácie na vyhľadanie musíte zadefinovať pre všetky identity cieľového užívateľa, ktoré majú rovnaký zdroj (buď identifikátor EIM pre priradenia identifikátora alebo zdrojový register užívateľov pre priradenia politiky). Zadefinovaním informácií na vyhľadanie pre každú identitu cieľového užívateľa zabezpečujete, že operácia vyhľadávania vráti jednu identitu cieľového užívateľa namiesto všetkých možných identít cieľového užívateľa. Pozrite si tému Pridávanie vyhľadávacích informácií do identity cieľového užívateľa. Musíte zadať tieto informácie vyhľadávania o operácii vyhľadávania mapovaní.

  Poznámka: Tento prístup funguje, len keď má aplikácia povolené používať informácie na vyhľadanie. Základné aplikácie i5/OS ako napríklad System i Access for Windows však nemôžu používať vyhľadávacie

informácie na rozlíšenie medzi viacerými cieľovými užívateľskými identitami vrátenými operáciou vyhľadávania. Následne by ste mohli zvážiť predefinovanie priradení pre doménu, aby ste zabezpečili, že operácia vyhľadávania mapovania dokáže vrátiť jedinú cieľovú identitu užívateľa pre zaistenie, aby základné i5/OS aplikácie mohli úspešne vykonať operácie vyhľadávania a mapovať identity.

Odstránenie domény EIM zo zložky Domain Management

Doménu EIM, ktorú už nechcete spravovať, môžete zo zložky **Domain Management** odstrániť. Odstránenie domény zo zložky **Domain Management** však **nie** je to isté, ako vymazanie domény a nevymaže údaje domény z radiča domény.

Na odstránenie domény nepotrebujete žiadne riadenie prístupov EIM.

Doménu EIM, ktorú už nechcete ďalej spravovať, môžete odstrániť zo zložky **Domain Management**; vykonajte nasledujúce kroky:

1. Rozviňte **Network >Enterprise Identity Mapping**.
2. Kliknite pravým tlačidlom myši na **Domain Management** a vyberte **Remove Domain**.
3. Vyberte doménu EIM, ktorú chcete odstrániť zo zložky **Domain Management**.
4. Kliknite na tlačidlo **OK**, aby sa odstránila doména.

Súvisiace úlohy

"Vymazanie domény EIM a všetkých konfiguračných objektov"
Aby ste mohli vymazať doménu EIM, musíte najprv vymazať všetky definície registrov a všetky identifikátory EIM v doméne. Ak nechcete vymazať doménu a všetky údaje v nej, ale nechcete už doménu spravovať, môžete ju odstrániť.

Vymazanie domény EIM a všetkých konfiguračných objektov

Aby ste mohli vymazať doménu EIM, musíte najprv vymazať všetky definície registrov a všetky identifikátory EIM v doméne. Ak nechcete vymazať doménu a všetky údaje v nej, ale nechcete už doménu spravovať, môžete ju odstrániť.

Ak chcete vymazať doménu EIM, musíte mať riadenie prístupov EIM na jednej z týchto úrovní:

- Administrátor LDAP.
- Administrátor EIM.

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

Poznámka: Okno Prebieha vymazávanie sa zobrazí počas daného stavu, až kým sa proces vymazávania neukončí.

Súvisiace úlohy

"Odstránenie domény EIM zo zložky Domain Management"
Doménu EIM, ktorú už nechcete spravovať, môžete zo zložky **Domain Management** odstrániť. Odstránenie domény zo zložky **Domain Management** však **nie** je to isté, ako vymazanie domény a nevymaže údaje domény z radiča domény.

Riadenie definícií registrov EIM

Ak chcete, aby boli registre užívateľov a v nich obsiahnuté užívateľské identity prítomné v doméne EIM, musíte pre ne vytvoriť definície registrov. Potom môžete manažovať spôsob účasti registrov užívateľov a ich identít užívateľov v EIM manažovaním len týchto definícií registrov EIM.

Pri manažovaní definícií domén môžete vykonávať tieto úlohy:

Súvisiace koncepty

"Vytváranie priradenia politiky" na strane 99
Priradenie politiky poskytuje prostriedky na priame definovanie vzťahu medzi viacerými identitami užívateľa v jednom alebo viacerých registroch a individuálnou cieľovou identitou užívateľa v inom registri.

Súvisiace úlohy

"Vymazanie priradenia politiky" na strane 111
Ak chcete vymazať priradenie politiky, musíte byť pripojený na doménu EIM, v ktorej chcete pracovať a musíte mať riadenie prístupov EIM ako administrátor registrov alebo administrátor EIM.

Pridávanie definície systémového registra

Ak chcete vytvoriť definíciu systémového registra, musíte byť pripojený do domény EIM, v ktorej chcete pracovať a musíte mať riadenie prístupov administrátora EIM.

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

1. Rozviňte **Network > Enterprise Identity Mapping > Domain Management**.
2. Vyberte doménu EIM, v ktorej chcete pracovať.
   - Ak doména EIM, s ktorou chcete pracovať, nie je uvedená pod zložkou Domain Management, pozrite si tému "Pridávanie domény EIM do zložky Domain Management" na strane 84.
   - Ak nie ste práve pripojený do domény EIM, v ktorej chcete pracovať, pozrite si tému "Pripájanie k doméne EIM" na strane 84.
3. Rozviňte doménu EIM, ku ktorej ste teraz pripojený.
4. Kliknite pravým tlačidlom myši na **User Registries**, vyberte **Add Registry** a potom **System**.
5. V dialógovom okne **Add system Registry** zadajte nasledujúce informácie o definícii systémového registra:
   a. Názov definície systémového registra.
   b. Typ definície registra.
   c. Opis definície systémového registra.
   d. (Voliteľné.) URL registra užívateľov.
   e. Ak to je potrebné, jeden alebo viac aliasov pre definíciu systémového registra.
6. Ak chcete uložiť informácie a pridať definíciu registra do domény EIM, kliknite na tlačidlo **OK**.

Pridávanie definície registra aplikácií

Ak chcete vytvoriť definíciu registra aplikácií, musíte byť pripojený do domény EIM, v ktorej chcete pracovať a musíte mať riadenie prístupov administrátora EIM.

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

1. Rozviňte **Network > Enterprise Identity Mapping > Domain Management**.
2. Vyberte doménu EIM, v ktorej chcete pracovať.
   - Ak doména EIM, s ktorou chcete pracovať, nie je uvedená pod zložkou Domain Management, pozrite si tému "Pridávanie domény EIM do zložky Domain Management" na strane 84.
   - Ak nie ste práve pripojený do domény EIM, v ktorej chcete pracovať, pozrite si tému "Pripájanie k doméne EIM" na strane 84.
3. Rozviňte doménu EIM, ku ktorej ste teraz pripojený.
4. Kliknite pravým tlačidlom myši na **User Registries**, vyberte **Add Registry** a potom **Application**.
5. V dialógovom okne **Add Application Registry**, zadajte nasledujúce informácie o definícii registra aplikácií:
   a. Názov definície registra aplikácií.
   b. Názov definície systémového registra, ktorej podsadou je vami definovaný register užívateľov aplikácie. Definícia systémového registra, ktorú zadávate, musí už existovať v EIM, ináč vytvorenie registra aplikácií zlyha.
   c. Typ definície registra.
   d. Opis definície registra aplikácií.

e. Ak to je potrebné, jeden alebo viac aliasov pre definíciu registra aplikácií.

6. Ak potrebujete zistiť, aké informácie treba zadať do jednotlivých polí, kliknite na tlačidlo **Help**.
7. Ak chcete uložiť informácie a pridať definíciu registra do domény EIM, kliknite na tlačidlo **OK**.

Súvisiace koncepty

"Definície systémového registra" na strane 13
Definícia systémového registra je záznam, ktorý vytvárate v EIM na reprezentovanie a popis jedinečného registra užívateľa v rámci pracovnej stanice alebo servera.

Pridanie definície skupinového registra

Ak chcete vytvoriť definíciu skupinového registra, musíte byť pripojený do domény EIM, v ktorej chcete pracovať a musíte mať riadenie prístupov administrátora EIM.

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

1. Rozviňte **Network → Enterprise Identity Mapping → Domain Management**.
2. Vyberte doménu EIM, v ktorej chcete pracovať.
   a. Ak doména EIM, s ktorou chcete pracovať, nie je uvedená pod zložkou Domain Management, pozrite si tému Pridávanie domény EIM do zložky Domain Management.
   b. Ak nie ste práve pripojený do domény EIM, v ktorej chcete pracovať, pozrite si tému Pripojenie k radiču domény EIM.
3. Rozviňte doménu EIM, ku ktorej ste pripojený.
4. Kliknite pravým tlačidlom myši na **User Registries**, vyberte **Add Registry** a potom **Group.**
5. V dialógovom okne Pridať skupinový register zadajte informácie o definícii skupinového registra nasledovným spôsobom:
   a. Názov definície skupinového registra.
   b. Vyberte **Group registry members are case sensitive**, ak všetky členy skupinového registra rozlišujú veľké a malé písmená.
   c. Opis definície skupinového registra.
   d. Ak to je potrebné, jeden alebo viac aliasov pre definíciu skupinového registra.
6. Ak potrebujete zistiť, aké informácie treba zadať do jednotlivých polí, kliknite na tlačidlo **Help**.
7. Ak chcete uložiť informácie a pridať definíciu registra do domény EIM, kliknite na tlačidlo **OK**.

Pridávanie aliasu do definície registra

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

Podpora tohto aliasu umožňuje programátorom písať aplikácie bez nutnosti vopred poznať ľubovoľný názov definície registra EIM, zvolený administrátorom, ktorý aplikáciu implementuje. Dokumentácia k aplikácii môže administrátorovi EIM oznámiť alias, ktorý používa daná aplikácia. Vďaka tejto informácii môže administrátor priradiť tento alias k definícii registra EIM, reprezentujúcej skutočný register užívateľov, ktorý chce administrátor použiť pre aplikáciu.

Ak chcete pridať alias do definície registra, musíte byť pripojený do domény, s ktorou chcete pracovať, a musíte mať riadenie prístupov EIM na jednej z týchto úrovní:

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

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

1. Rozviňte **Network > Enterprise Identity Mapping > Domain Management**.
2. Vyberte doménu EIM, v ktorej chcete pracovať.

- Ak doména EIM, s ktorou chcete pracovať, nie je uvedená pod zložkou Domain Management, pozrite si tému "Pridávanie domény EIM do zložky Domain Management" na strane 84.
- Ak nie ste práve pripojený do domény EIM, v ktorej chcete pracovať, pozrite si tému "Pripájanie k doméne EIM" na strane 84.

3. Rozviňte doménu EIM, ku ktorej ste teraz pripojený.
4. Kliknite na zložku **User Registries**, aby sa zobrazil zoznam definícií registrov v doméne.

   Poznámka: Ak máte riadenie prístupu Administrátor pre vybraté registre, zoznam bude obsahovať len tie definície registra, na ktoré máte oprávnenie.
5. Kliknite pravým tlačidlom myši na definíciu registra, do ktorého chcete pridať alias a vyberte **Properties**.
6. Vyberte stranu **Aliases** a zadajte názov a typ aliasu, ktorý chcete pridať.

   Poznámka: Môžete zadať typ aliasu, ktorý nie je zahrnutý v zozname typov.
7. Ak potrebujete zistiť, aké informácie treba zadať do jednotlivých polí, kliknite na tlačidlo **Help**.
8. Kliknite na tlačidlo **Add**.
9. Kliknite na tlačidlo **OK**, aby sa uložili vaše zmeny v definícii registra.

Definovanie typu registra súkromného užívateľa v EIM

Keď vytvárate definíciu registra EIM, môžete zadať jedno číslo z preddefinovaných typov registra užívateľov na reprezentáciu aktuálneho registra užívateľov, ktorý sa nachádza v systéme v rámci podniku.

Preddefinované typy definícií registrov zahŕňajú väčšinu registrov užívateľov operačného systému. Možno budete musieť vytvoriť definíciu registra, pre ktorú EIM nezahŕňa preddefinovaný typ registra. V tejto situácii máte dve možnosti. Buď môžete použiť existujúcu definíciu registra, ktorá zodpovedá charakteristikám vášho registra užívateľov, alebo môžete definovať súkromný typ registra užívateľov.

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

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

Identifikátory OID je možné získať dvomi spôsobmi:

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

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

- Americký národný štandardizačný inštitút (ANSI) je registračnou entitou pre USA pre názvy organizácií pod globálnym registračným procesom vytvoreným Medzinárodnou štandardizačnou organizáciou (ISO) a Medzinárodnou telekomunikačnou úniou (ITU). Informačný leták vo formáte Microsoft Word obsahujúci informácie o Registered Application Provider Identifier (RID) sa nachádza na webovej stránke ANSI Public Document Library

http://public.ansi.org/ansionline/Documents/ . Výberom **Other Services > Registration Programs** môžete vyhľadať hárok faktov. Rozsah ANSI OID pre organizácie je 2.16.840.1. ANSI účtuje za priradenie rozsahu OID poplatok. Samotné priradenie rozsahu OID od ANSI trvá približne dva týždne. ANSI priradí číslo (NEWNUM) na vytvorenie nového rozsahu OID; napríklad: 2.16.840.1.NEWNUM.

- Vo väčšine krajín a regiónov je register OID spravovaný národnými organizáciami. Pokiaľ ide o rozsahy ANSI, sú to väčšinou rozsahy priradené pod OID 2.16. Nájdenie autority OID pre konkrétnu krajinu alebo región môže byť trochu náročnejšie. Adresy pre národné členské organizácie ISO nájdete na adrese:

  http://www.wssn.net/WSSN/listings/links_national.html . Tieto informácie obsahujú poštovú adresu a adresu elektronickej pošty. V niektorých prípadoch je uvedená aj webová lokalita.
- IANA (Internet Assigned Numbers Authority) priraďuje súkromné čísla podnikov (identifikátory OID) v rozsahu 1.3.6.1.4.1. IANA dodnes priradila rozsahy viac ako 7500 spoločnostiam. Stránka so žiadosťou sa nachádza na

  adrese http://www.iana.org/cgi-bin/enterprise.pl , pod číslami súkromných podnikov. Registrácia v IANA trvá zvyčajne jeden týždeň. OID od IANA sú k dispozícii bezplatne. IANA priradí číslo (NEWNUM), takže nový rozsah OID bude 1.3.6.1.4.1.NEWNUM.
- Federálna vláda USA spravuje Computer Security Objects Registry (CSOR). CSOR predstavuje pomenovaciu autoritu pre rozsah 2.16.840.1.101.3 a práve registruje objekty pre bezpečnostné označenia, kryptografické algoritmy a politiky certifikátov. Identifikátory OID politík certifikátov sú definované v rozsahu 2.16.840.1.101.3.2.1. CSOR poskytuje identifikátory OID agentúram federálnej vlády USA. Bližšie informácie o

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

Súvisiace koncepty

“Definície registrov EIM” na strane 11
Definícia registra EIM je položka v EIM, ktorú vytvoríte na reprezentovanie aktuálneho registra užívateľov existujúceho v systéme v rámci podniku. Register užívateľov slúži ako adresár a obsahuje zoznam platných identít užívateľov pre konkrétny systém alebo aplikáciu.

Povolenie podpory vyhľadávaní mapovania a používanie priradení politiky pre cieľový register

Podpora politiky mapovania EIM umožňuje používanie priradení politiky ako spôsobu vytvárania viacerých mapovaní do jedného v situáciách, keď neexistujú priradenia medzi užívateľskými identitami a identifikátorom EIM. Priradenie politiky môžete použiť na mapovanie zdrojovej množiny viacerých identít užívateľa (namiesto jednej identity užívateľa) na jednu cieľovú identitu užívateľa v zadanom cieľovom registri užívateľov.

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

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

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

Ak chcete vyhľadávaniu mapovaní povoliť použitie priradení politiky pre cieľový register, musíte byť pripojený k doméne EIM, v ktorej chcete pracovať a musíte mať jednu z týchto úrovní: “Riadenie prístupu EIM” na strane 38

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

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

1. Rozviňte **Network > Enterprise Identity Mapping > Domain Management**.
2. Vyberte doménu EIM, v ktorej chcete pracovať.
   - Ak doména EIM, s ktorou chcete pracovať, nie je uvedená pod zložkou **Domain Management**, pozrite si “Pridávanie domény EIM do zložky Domain Management” na strane 84.
   - Ak nie ste práve pripojený k doméne EIM, v ktorej chcete pracovať, pozrite si tému Pripojenie k radiču domény EIM.
3. Ak chcete zobraziť zoznam definícií registra pre doménu, vyberte **Registre užívateľov**.

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

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

Súvisiace koncepty

“Operácie podpory a umožnenia politiky mapovaní EIM” na strane 37
Podpora politiky mapovania podnikovej identity (EIM) umožňuje používať v doméne EIM priradenia politiky a tiež špecifické priradenia identifikátorov. Priradenia politiky môžete používať namiesto alebo v kombinácii s priradeniami identifikátorov.

Vymazanie definície registra

Keď vymažete definíciu registra z domény EIM, neovplyvníte register užívateľov, na ktorý definícia registra odkazuje, ale tento register užívateľov už nebude môcť participovať v doméne EIM.

Keď vymazávate definíciu registra, musíte zvážiť tieto veci:

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

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

Ak chcete vymazať definíciu registra EIM, vykonajte tieto kroky:

1. Rozviňte **Network > Enterprise Identity Mapping > Domain Management**.
2. Vyberte doménu EIM, v ktorej chcete pracovať.
   - Ak doména EIM, s ktorou chcete pracovať, nie je uvedená pod zložkou **Domain Management**, pozrite si “Pridávanie domény EIM do zložky Domain Management” na strane 84.
   - Ak nie ste práve pripojený k doméne EIM, s ktorou chcete pracovať, pozrite si tému Pripojenie k radiču domény EIM.
3. Rozviňte doménu EIM, ku ktorej ste pripojený.

4. Kliknite na **User Registries**, aby sa zobrazil zoznam definícií registrov pre doménu.

   Poznámka: Ak máte riadenie prístupu Administrátor pre vybraté registre, zoznam bude obsahovať len tie definície registra, na ktoré máte oprávnenie.
5. Pravým tlačidlom myši kliknite na register užívateľov, ktorý chcete vymazať a vyberte **Delete**.
6. Kliknite na tlačidlo **Yes** v dialógovom okne **Confirmation**, aby sa vymazali definície registra.

Odstránenie aliasu z definície registra

Ak chcete odstrániť alias z definície registra EIM, musíte byť pripojený na doménu EIM, v ktorej chcete pracovať a musíte mať riadenie prístupov EIM ako administrátor registrov, administrátor vybratých registrov alebo administrátor EIM.

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

1. Rozviňte **Network > Enterprise Identity Mapping > Domain Management**.
2. Vyberte doménu EIM, v ktorej chcete pracovať.
   - Ak doména EIM, s ktorou chcete pracovať, nie je uvedená pod zložkou **Domain Management**, pozrite si “Pridávanie domény EIM do zložky Domain Management” na strane 84.
   - Ak nie ste práve pripojený k doméne EIM, s ktorou chcete pracovať, pozrite si tému Pripojenie k radiču domény EIM.
3. Rozviňte doménu EIM, ku ktorej ste pripojený.
4. Kliknite na **Registre užívateľov**, aby sa zobrazil zoznam definícií registrov pre doménu.

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

Pridávanie člena do definície skupinového registra

Ak chcete pridať člena do definície skupinového registra, musíte byť pripojený do domény EIM, v ktorej chcete pracovať a musíte mať riadenie prístupov EIM ako administrátor EIM, administrátor registra, administrátor pre vybraté registre (pre definíciu skupinového registra, do ktorého chcete pridať člena, aj pre jednotlivého člena, ktorého chcete pridať).

Ak chcete pridať člen definície skupinového registra, vykonajte tieto kroky:

1. Rozviňte **Network → Enterprise Identity Mapping → Domain Management**
2. Vyberte doménu EIM, v ktorej chcete pracovať.
   a. Ak doména EIM, s ktorou chcete pracovať, nie je uvedená pod zložkou Domain Management, pozrite si tému Pridávanie domény EIM do zložky Domain Management.
   b. Ak nie ste práve pripojený do domény EIM, v ktorej chcete pracovať, pozrite si tému Pripojenie k radiču domény EIM.
3. Rozviňte doménu EIM, ku ktorej ste pripojený.
4. 4. Kliknite na zložku **User Registries**, aby sa zobrazil zoznam definícií registrov v doméne.
5. 5. Kliknite pravým tlačidlom myši na definíciu skupinového registra, do ktorého chcete pridať člena a vyberte **Properties**
6. 6. Vyberte stránku **Members** a kliknite na **Add**.
7. 7. V okne **Add EIM Group Registry member** vyberte jednu alebo viac definícií registra a kliknite na **OK**. Obsah zoznamu je rôzny v závislosti na type vášho riadenia prístupu k EIM, a je obmedzený na definície registrov s rovnakým pravidlom používania veľkých a malých písmen ako majú ostatné členy skupiny
8. 8. Kliknite na tlačidlo **OK**, aby ste zatvorili okno.

Správa identifikátorov EIM

Túto informáciu použite, ak sa chcete dozvedieť ako vytvoriť a spravovať identifikátory EIM pre doménu.

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

Implementácia prostredia jednoduchého prihlásenia uľahčuje proces správy užívateľských identít aj pre užívateľov, najmä v prípade, keď prejdú na iné oddelenie alebo do inej oblasti v rámci podniku. Povolenie jednoduchého prihlásenia môže pre týchto užívateľov znížiť potrebu pamätať si nové užívateľské mená a heslá pre nové systémy.

Poznámka: Spôsob vytvárania a používania identifikátorov EIM závisí na potrebách vašej organizácie. Ak sa chcete dozvedieť viac, pozrite si “Vývoj plánu pomenúvania identifikátorov EIM” na strane 62.

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

Súvisiace informácie

Jednoduché prihlásenie

Vytváranie identifikátora EIM

Ak chcete vytvoriť identifikátor EIM, musíte byť pripojený k doméne EIM, v ktorej chcete pracovať a musíte mať riadenie prístupov EIM ako administrátor identifikátorov alebo administrátor EIM.

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

1. Rozviňte **Network > Enterprise Identity Mapping > Domain Management**.
2. Vyberte doménu EIM, v ktorej chcete pracovať.
   - Ak doména EIM, s ktorou chcete pracovať, nie je uvedená pod zložkou **Domain Management**, pozrite si “Pridávanie domény EIM do zložky Domain Management” na strane 84.
   - Ak nie ste práve pripojený k doméne EIM, v ktorej chcete pracovať, pozrite si “Pripájanie k doméne EIM” na strane 84.
3. Rozviňte doménu EIM, ku ktorej ste pripojený.
4. Pravým tlačidlom myši kliknite na **Identifiers** a vyberte **New identifier**.
5. V dialógovom okne **New EIM Identifier** poskytnite informácie o identifikátore EIM podľa týchto pokynov:
   a. Názov pre identifikátor.
   b. Či má systém generovať jedinečný názov, ak treba.
   c. Opis identifikátora.
   d. Jeden alebo viac aliasov pre identifikátor, ak treba.
6. Ak potrebujete zistiť, aké informácie treba zadať do jednotlivých polí, kliknite na tlačidlo **Help**.
7. Po zadaní vyžadovaných informácií kliknite na tlačidlo **OK**, aby sa vytvoril identifikátor EIM.

Poznámka: Ak vytvoríte veľké množstvo identifikátorov EIM, niekedy bude trvať dlhý čas, kým sa zobrazí zoznam identifikátorov pri rozvinutí zložky **Identifikátory**. Ak chcete zlepšiť výkon, keď máte veľký počet identifikátorov EIM, pozrite si “Prispôsobenie zobrazenia identifikátorov EIM” na strane 97.

Pridávanie aliasu do identifikátora EIM

Môžete chcieť vytvoriť alias na poskytnutie ďalšej charakteristickej informácie pre identifikátor EIM. Aliasy môžu pomôcť pri hľadaní špecifického identifikátora EIM pri vykonávaní operácie prehľadania EIM. Aliasy môžu byť užitočné napríklad v situáciách, kedy sa oficiálne meno osoby odlišuje od mena, pod ktorým je osoba známa.

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

Ak chcete pridať alias k identifikátoru EIM, musíte byť pripojený k doméne EIM, v ktorej chcete pracovať a musíte mať “Riadenie prístupu EIM” na strane 38 na jednej z týchto úrovní:

- Administrátor EIM.
- Administrátor identifikátorov

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

1. Rozviňte **Network > Enterprise Identity Mapping > Domain Management**.
2. Vyberte doménu EIM, v ktorej chcete pracovať.
   - Ak doména EIM, s ktorou chcete pracovať, nie je uvedená pod zložkou **Domain Management**, pozrite si “Pridávanie domény EIM do zložky Domain Management” na strane 84.
   - Ak nie ste práve pripojený k doméne EIM, v ktorej chcete pracovať, pozrite si “Pripájanie k doméne EIM” na strane 84.
3. Rozviňte doménu EIM, ku ktorej ste pripojený.
4. Kliknite na **Identifiers** v pravej záložke, čím zobrazíte zoznam identifikátorov EIM v doméne.

   Poznámka: Zobrazenie zoznamu identifikátorov pri pokuse o rozvinutie zložky **Identifiers** môže niekedy trvať dlho. Ak chcete zlepšiť výkon, keď máte v doméne veľký počet identifikátorov EIM, pozrite si “Prispôsobenie zobrazenia identifikátorov EIM” na strane 97.
5. Pravým tlačidlom myši kliknite na identifikátor EIM, ku ktorému chcete pridať alias a vyberte **Properties**.
6. V poli **Alias** zadajte názov aliasu, ktorý chcete pridať k tomuto identifikátoru EIM a kliknite na tlačidlo **Add**.
7. Kliknite na tlačidlo **OK**, aby sa uložili zmeny pre identifikátor EIM.

Odstránenie aliasu z identifikátora EIM

Ak chcete odstrániť alias z identifikátora EIM, musíte byť pripojený k doméne, v ktorej chcete pracovať a musíte mať riadenie prístupov ako administrátor identifikátorov alebo administrátor EIM.

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

1. Rozviňte **Network > Enterprise Identity Mapping > Domain Management**.
2. Vyberte doménu EIM, v ktorej chcete pracovať.
   - Ak doména EIM, s ktorou chcete pracovať, nie je uvedená pod zložkou **Domain Management**, pozrite si “Pridávanie domény EIM do zložky Domain Management” na strane 84.
   - Ak nie ste práve pripojený k doméne EIM, v ktorej chcete pracovať, pozrite si “Pripájanie k doméne EIM” na strane 84.
3. Rozviňte doménu EIM, ku ktorej ste pripojený.
4. Kliknite na **Identifiers** v pravej záložke, čím zobrazíte zoznam identifikátorov EIM v doméne.

   Poznámka: Zobrazenie zoznamu identifikátorov pri pokuse o rozvinutie zložky **Identifiers** môže niekedy trvať dlho. Ak chcete zlepšiť výkon, keď máte v doméne veľký počet identifikátorov EIM, pozrite si “Prispôsobenie zobrazenia identifikátorov EIM” na strane 97.
5. Pravým tlačidlom myši kliknite na identifikátor EIM, ku ktorému chcete pridať alias a vyberte **Properties**.
6. Vyberte alias, ktorý chcete odstrániť a kliknite na tlačidlo **Remove**.
7. Kliknutím na **OK** uložíte vaše zmeny.

Vymazanie identifikátora EIM

Ak chcete vymazať identifikátor EIM, musíte byť pripojený na doménu EIM, v ktorej chcete pracovať a musíte mať riadenie prístupov administrátora EIM.

Ak chcete vymazať identifikátor EIM, vykonajte tieto kroky:

1. Rozviňte **Network > Enterprise Identity Mapping > Domain Management**.
2. Vyberte doménu EIM, v ktorej chcete pracovať.
   - Ak doména EIM, s ktorou chcete pracovať, nie je uvedená pod zložkou **Domain Management**, pozrite si “Pridávanie domény EIM do zložky Domain Management” na strane 84.
   - Ak nie ste práve pripojený k doméne EIM, s ktorou chcete pracovať, pozrite si tému Pripojenie k radiču domény EIM.
3. Rozviňte doménu EIM, ku ktorej ste teraz pripojený.
4. Kliknite na **Identifikátory**.

   Poznámka: Zobrazenie zoznamu identifikátorov pri pokuse o rozvinutie zložky **Identifikátory** môže niekedy trvať dlho. Ak chcete zvýšiť výkon pri veľkom počte identifikátorov EIM v doméne, pozrite si časť “Prispôsobenie zobrazenia identifikátorov EIM”.
5. Vyberte identifikátor EIM, ktorý chcete vymazať. Ak chcete vymazať viacero identifikátorov, pri výbere identifikátorov EIM stlačte kláves **Ctrl**.
6. Pravým tlačidlom myši kliknite na vybraté identifikátory EIM a vyberte **Vymazať**.
7. V dialógovom okne **Potvrdenie vymazania** kliknite na tlačidlo **Áno**, aby sa vymazali vybraté identifikátory EIM.

Prispôsobenie zobrazenia identifikátorov EIM

Pri pokuse o rozvinutie zložky identifikátorov môže zobrazenie zoznamu identifikátorov niekedy trvať dlho. Ak máte veľký počet identifikátorov EIM v doméne a chcete zlepšiť výkon, môžete prispôsobiť zobrazenie pre zložku identifikátorov.

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

1. Rozviňte **Network —> Enterprise Identity Mapping —> Domain Management**.
2. Vyberte doménu EIM, v ktorej chcete pracovať.
   - Ak doména EIM, s ktorou chcete pracovať, nie je uvedená pod zložkou **Domain Management**, pozrite si “Pridávanie domény EIM do zložky Domain Management” na strane 84.
   - Ak nie ste práve pripojený do domény EIM, v ktorej chcete pracovať, pozrite si tému “Pripájanie k doméne EIM” na strane 84.
3. Pravým tlačidlom myši kliknite na zložku **Identifiers** a vyberte **Customize this View**.
4. Zadajte kritériá, ktoré chcete použiť pre zobrazenie identifikátorov EIM v doméne. Ak chcete znížiť počet zobrazených identifikátorov EIM, zadajte znaky, ktoré chcete použiť pre triedenie identifikátorov. V názve identifikátora môžete zadať jeden alebo viac zástupných znakov (*). Napríklad môžete ako vaše kritérium triedenia v poli **Identifiers** zadať *JOHNSON*. Výsledky budú zahŕňať všetky identifikátory EIM, kde je znakový reťazec JOHNSON definovaný ako časť názvu identifikátora EIM a tiež budú zahŕňať identifikátory EIM, kde je znakový reťazec JOHNSON definovaný ako časť aliasu pre identifikátor EIM.
5. Kliknutím na **OK** uložíte vaše zmeny.

Mapovanie priradení EIM

EIM umožňuje vytvárať a riadiť dva druhy priradení, ktoré definujú priame alebo nepriame vzťahy medzi identitami užívateľa: priradenia identifikátorov a priradenia politiky. EIM vám dovoľuje vytvárať a manažovať priradenia identifikátorov medzi identifikátormi EIM a ich identitami užívateľa, ktoré vám dovoľujú definovať nepriame, ale špecifické, individuálne vzťahy medzi identitami užívateľa.

EIM vám tiež dovoľuje vytvoriť priradenia politiky na opísanie vzťahu medzi viacerými identitami užívateľa v jednom alebo viacerých registroch a individuálnej cieľovej identity užívateľa v inom registri. Priradenia politiky používajú

podporu politík mapovania EIM na vytvorenie mapovaní typu veľa-jeden medzi identitami užívateľov bez použitia identifikátora EIM. Oba typy priradení definujú vzťahy medzi identitami užívateľov v podniku, manažovanie priradení je dôležitým prvkom pri manažovaní EIM.

Údržba priradení v doméne je kľúč k zjednodušeniu administratívnych úloh vyžadovaných na vedenie záznamov o užívateľoch, ktorý majú kontá v rôznych systémoch v sieti. Keď implementujete bezpečnú sieť jednoduchého prihlásenia, priradenia identifikátorov a priradenia politiky musia byť udržiavané v aktuálnom stave.

S priradeniami môžete vykonávať nasledujúce riadiace úlohy:

Vytváranie priradení EIM

Existujú dva rôzne typy priradení EIM, ktoré môžete vytvoriť. Môžete vytvoriť priradenie identifikátora alebo priradenie politiky.

Priradenie identifikátora môžete vytvoriť na nepriame definovanie vzťahu medzi dvomi užívateľskými identitami, ktoré používa jeden užívateľ. Priradenie identifikátora opisuje vzťah medzi identifikátorom EIM a identitou užívateľa v registri užívateľov. Priradenia identifikátorov vám dovoľujú vytvoriť mapovania typu jeden-jeden medzi identifikátormi EIM a jednotlivými, rôznymi identitami užívateľa, ktoré súvisia s užívateľom, ktorý je reprezentovaný identifikátorom EIM.

Priradenie politiky môžete vytvoriť na priame definovanie vzťahu medzi viacerými identitami užívateľa v jednom alebo viacerých registroch a jednou identitou cieľového užívateľa v inom registri. Priradenia politiky používajú podporu politík mapovania EIM na vytvorenie mapovaní typu veľa-jeden medzi identitami užívateľov bez použitia identifikátora EIM. Priradenia politiky vám umožnia rýchlo vytvoriť veľké množstvo mapovaní medzi identitami užívateľa v rôznych registroch užívateľov.

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

Súvisiace koncepty

“Vývoj plánu mapovania identity” na strane 59
Kritická časť úvodného procesu plánovania implementácie EIM vyžaduje určenie spôsobu používania mapovania identity vo vašom podniku.

“Vytváranie priradenia politiky” na strane 99
Priradenie politiky poskytuje prostriedky na priame definovanie vzťahu medzi viacerými identitami užívateľa v jednom alebo viacerých registroch a individuálnou cieľovou identitou užívateľa v inom registri.

Súvisiace úlohy

“Vytváranie priradenia identifikátora EIM”
Priradenia identifikátora definujú vzťah medzi identifikátorom EIM a užívateľskou identitou osoby alebo entity vo vašom podniku, na ktorú identifikátor EIM odkazuje.

Vytváranie priradenia identifikátora EIM:

Priradenia identifikátora definujú vzťah medzi identifikátorom EIM a užívateľskou identitou osoby alebo entity vo vašom podniku, na ktorú identifikátor EIM odkazuje.

Môžete vytvoriť tri typy priradení identifikátorov: cieľové, zdrojové a administratívne. Ak chcete zabrániť prípadným problémom s priradeniami a so spôsobom, akým mapujú identity, pozrite si “Vývoj plánu mapovania identity” na strane 59.

Ak chcete vytvoriť priradenie identifikátora, musíte byť pripojený na doménu EIM, v ktorej chcete pracovať a musíte mať riadenie prístupov EIM vyžadované typom priradenia, ktoré chcete vytvoriť.

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

- Administrátor identifikátorov

- Administrátor EIM.

Ak chcete vytvoriť cieľové priradenie, musíte mať riadenie prístupu k EIM na jednej z týchto úrovní:
- Administrátor identifikátorov
- Administrátor pre vybraté registre (definície registra, ktorá odkazuje na register užívateľov, obsahujúci cieľovú identitu užívateľa)
- Administrátor EIM.

Ak chcete vytvoriť priradenie identifikátora, vykonajte tieto kroky:
1. Rozviňte **Network > Enterprise Identity Mapping > Domain Management**.
2. Vyberte doménu EIM, v ktorej chcete pracovať.
   - Ak doména EIM, s ktorou chcete pracovať, nie je uvedená pod zložkou **Domain Management**, pozrite si “Pridávanie domény EIM do zložky Domain Management” na strane 84.
   - Ak nie ste práve pripojený k doméne EIM, v ktorej chcete pracovať, pozrite si “Pripájanie k doméne EIM” na strane 84.
3. Rozviňte doménu EIM, ku ktorej ste teraz pripojený.
4. Kliknite na **Identifiers**, aby sa zobrazil zoznam identifikátorov EIM pre túto doménu.

   Poznámka: Zobrazenie zoznamu identifikátorov pri pokuse o rozvinutie zložky **Identifiers** môže niekedy trvať dlho. Ak chcete zlepšiť výkon, keď máte v doméne veľký počet identifikátorov EIM, pozrite si “Prispôsobenie zobrazenia identifikátorov EIM” na strane 97.
5. Pravým tlačidlom myši kliknite na identifikátor EIM, ku ktorému chcete pridať association a vyberte **Properties...**.
6. Vyberte stránku **Associations** a kliknite na **Add**.
7. V dialógovom okne **Add Association** zadajte nasledujúce informácie na definovanie priradenia:
   - Názov registra, ktorý obsahuje identitu užívateľa, ktorú chcete priradiť identifikátoru EIM. Zadajte presný názov existujúcej definície registra alebo ho vyhľadajte.
   - Názov identity užívateľa, ktorú chcete priradiť identifikátoru EIM.
   - Typ priradenia. Priradenie môže mať jeden z týchto troch typov:
     - Administratívne
     - Zdroj
     - Cieľové
8. Ak potrebujete zistiť, aké informácie treba zadať do jednotlivých polí, kliknite na tlačidlo **Help**.
9. Voliteľné. Ak chcete zobraziť pre cieľové priradenie dialógové okno **Add Association - Advanced**, kliknite na tlačidlo **Advanced...**. Ak sa chcete vrátiť do dialógového okna **Add Association**, zadajte informácie na vyhľadanie pre cieľovú identitu užívateľa a kliknite na tlačidlo **OK**.
10. Ak chcete vytvoriť priradenie, kliknite po zadaní vyžadovaných informácií na tlačidlo **OK**.

Súvisiace koncepty

“Vytváranie priradení EIM” na strane 98
Existujú dva rôzne typy priradení EIM, ktoré môžete vytvoriť. Môžete vytvoriť priradenie identifikátora alebo priradenie politiky.

Vytváranie priradenia politiky:

Priradenie politiky poskytuje prostriedky na priame definovanie vzťahu medzi viacerými identitami užívateľa v jednom alebo viacerých registroch a individuálnou cieľovou identitou užívateľa v inom registri.

Priradenia politiky používajú podporu politiky mapovania EIM na vytvorenie mapovaní typu veľa-jeden medzi identitami užívateľa bez zahrnutia identifikátora EIM. Vzhľadom na to, že priradenia politiky môžete použiť viacerými súbežnými spôsobmi, mali by ste pred vytvorením a použitím priradení politiky dôkladne porozumieť podpore politiky

mapovania EIM a spôsobu fungovania vyhľadávacích operácií. Ak chcete predchádzať prípadným problémom s priradeniami a spôsobom, akým mapujú identity, skôr ako začnete definovať priradenia, musíte vyvinúť celkový plán mapovania identít pre váš podnik.

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

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

Súvisiace koncepty

"Riadenie definícií registrov EIM" na strane 88
Ak chcete, aby boli registre užívateľov a v nich obsiahnuté užívateľské identity prítomné v doméne EIM, musíte pre ne vytvoriť definície registrov. Potom môžete manažovať spôsob účasti registrov užívateľov a ich identít užívateľov v EIM manažovaním len týchto definícií registrov EIM.

"Vytváranie priradení EIM" na strane 98
Existujú dva rôzne typy priradení EIM, ktoré môžete vytvoriť. Môžete vytvoriť priradenie identifikátora alebo priradenie politiky.

"Operácie podpory a umožnenia politiky mapovaní EIM" na strane 37
Podpora politiky mapovania podnikovej identity (EIM) umožňuje používať v doméne EIM priradenia politiky a tiež špecifické priradenia identifikátorov. Priradenia politiky môžete používať namiesto alebo v kombinácii s priradeniami identifikátorov.

"Vývoj plánu mapovania identity" na strane 59
Kritická časť úvodného procesu plánovania implementácie EIM vyžaduje určenie spôsobu používania mapovania identity vo vašom podniku.

Vytváranie predvoleného priradenia politiky domény:

Ak chcete vytvoriť predvolené priradenie politiky domény, musíte byť pripojený na doménu EIM, v ktorej chcete pracovať a musíte mať riadenie prístupov EIM ako administrátor EIM alebo administrátor registrov.

Priradenie politiky opisuje vzťah medzi viacerými identitami užívateľa a jednou identitou užívateľa v cieľovom registri užívateľov. Priradenie politiky môžete použiť na opísanie vzťahu medzi zdrojovou množinou viacerých identít užívateľa a jednou identitou cieľového užívateľa v určenom cieľovom registri užívateľov. Priradenia politiky používajú podporu politík mapovania EIM na vytvorenie mapovaní typu veľa-jeden medzi identitami užívateľov bez použitia identifikátora EIM.

Poznámka: Priradenia politiky môžete používať rôznymi spôsobmi prekrývania, preto musíte sa dôkladne oboznámiť s podporou politiky mapovania EIM skôr, než priradenia politiky vytvoríte a začnete používať. Ak sa chcete vyhnúť možným problémom s priradeniami a spôsobom mapovania identít, musíte skôr ako začnete definovať priradenia, vytvoriť celkový plán mapovania identít pre váš podnik.

V predvolenom priradení politiky domény sú všetci užívatelia v doméne zdrojom priradenia politiky a sú mapovaní na jeden cieľový register a cieľového užívateľa. Predvolené priradenie politiky domény môžete definovať pre každý register v doméne. Ak sa dve alebo viac priradení politiky domény týka rovnakého cieľového registra, pre každé z týchto priradení politiky môžete zadefinovať jedinečné informácie na vyhľadanie, aby ste zabezpečili, že operácie vyhľadávania mapovaní môžu medzi nimi rozlíšiť. V opačnom prípade môžu operácie vyhľadávania mapovaní vrátiť viacero cieľových identít užívateľov. Následkom týchto nejednoznačných výsledkov môže byť neschopnosť aplikácií spoliehajúcich sa na EIM určiť presnú cieľovú identitu, ktorá sa má použiť.

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

1. Rozviňte **Network > Enterprise Identity Mapping > Domain Management**.
2. Pravým tlačidlom myši kliknite na doménu EIM, v ktorej chcete pracovať a vyberte **Mapping Policy**
   - Ak doména EIM, s ktorou chcete pracovať, nie je uvedená pod zložkou **Domain Management**, pozrite si "Pridávanie domény EIM do zložky Domain Management" na strane 84.

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

3. Na strane General vyberte **Enable mapping lookups using policy associations for domain**.
4. Vyberte stránku **Domain** a kliknite na **Add**.
5. V dialógovom okne **Add Default Domain Policy Association** uveďte nasledujúce požadované informácie:
   - Názov definície **Target registry** pre priradenie politiky.
   - Názov identity **Target user** pre priradenie politiky.
6. Ak potrebujete viac detailov o dokončení tohto a následných dialógových okien, kliknite na **Help**.
7. Voliteľné. Kliknutím na **Advanced** zobrazíte dialógové okno **Add Association - Advanced**. Zadajte **Lookup information** pre priradenie politiky a kliknite na **OK**, aby ste sa vrátili do dialógového okna **Add Default Domain Policy Association**.

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

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

Vytváranie predvoleného priradenia politiky registra:

Ak chcete vytvoriť predvolené priradenie politiky registra, musíte byť pripojený na doménu EIM, v ktorej chcete pracovať a musíte mať riadenie prístupov EIM ako administrátor registra alebo administrátor EIM.

Priradenie politiky opisuje vzťah medzi viacerými identitami užívateľa a jednou identitou užívateľa v cieľovom registri užívateľov. Priradenie politiky môžete použiť na opísanie vzťahu medzi zdrojovou množinou viacerých identít užívateľa a jednou identitou cieľového užívateľa v určenom cieľovom registri užívateľov. Priradenia politiky používajú podporu politík mapovania EIM na vytvorenie mapovaní typu veľa-jeden medzi identitami užívateľov bez použitia identifikátora EIM.

Poznámka: Priradenia politiky môžete používať rôznymi spôsobmi prekrývania, preto musíte sa dôkladne oboznámiť s podporou politiky mapovania EIM skôr, než priradenia politiky vytvoríte a začnete používať. Taktiež, ak chcete zabrániť prípadným problémom s priradeniami a so spôsobom, akým mapujú identity, skôr ako začnete definovať priradenia, musíte vyvinúť celkový plán mapovania identít pre váš podnik.

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

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

1. Rozviňte **Network > Enterprise Identity Mapping > Domain Management**.
2. Vyberte doménu EIM, v ktorej chcete pracovať.
   - Ak doména EIM, s ktorou chcete pracovať, nie je uvedená pod zložkou **Domain Management**, pozrite si “Pridávanie domény EIM do zložky Domain Management” na strane 84.

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

3. Na strane Všeobecné vyberte **Povoliť vyhľadávanie mapovaní pomocou priradení politiky pre doménu**.
4. Na strane Všeobecné vyberte **Povoliť vyhľadávanie mapovaní pomocou priradení politiky pre doménu**.
5. V dialógovom okne **Add Default Registry Policy Association** uveďte nasledujúce požadované informácie:
   - Názov definície **zdrojového registra** pre priradenie politiky.
   - Názov definície **cieľového registra** pre priradenie politiky.
   - Názov identity **cieľového užívateľa** pre priradenie politiky.
6. Ak potrebujete viac detailov o dokončení tohto a následných dialógových okien, kliknite na **Help**.
7. Voliteľné. Kliknutím na **Advanced** zobrazíte dialógové okno **Add Association - Advanced**. Zadajte **lookup information** pre priradenie politiky a kliknite na **OK**, aby ste sa vrátili do dialógového okna **Add Default Registry Policy Association**. Ak sa dve alebo viac priradení politiky s rovnakým zdrojovým registrom týka rovnakého cieľového registra, musíte pre každú z identít cieľového užívateľa v týchto priradeniach politiky definovať jedinečné informácie na vyhľadanie. Zadefinovaním informácií na vyhľadanie pre každú identitu cieľového užívateľa v tejto situácii zabezpečte, aby operácie vyhľadávania mapovaní mohli medzi nimi rozlišovať. V opačnom prípade môžu operácie vyhľadávania mapovaní vrátiť viacero cieľových identít užívateľov. Následkom týchto nejednoznačných výsledkov môže byť neschopnosť aplikácií spoliehajúcich sa na EIM určiť presnú cieľovú identitu, ktorá sa má použiť.
8. Ak chcete vytvoriť nové priradenie politiky, kliknite na **OK** a vráťte sa na stránku **Registry**. Nové predvolené priradenie politiky registra sa teraz zobrazí v tabuľke **Predvolené priradenia politiky**.
9. Skontrolujte, či je nové priradenie politiky pre cieľový register aktivované.
10. Kliknite na **OK**, aby ste uložili vaše zmeny a zatvorili dialógové okno **Politika mapovania**.

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

Vytváranie priradenia politiky filtra certifikátov:

Ak chcete vytvoriť priradenie politiky filtra certifikátov, musíte byť pripojený na doménu EIM, v ktorej chcete pracovať a musíte mať riadenie prístupov EIM ako administrátor registrov alebo administrátor EIM.

Priradenie politiky opisuje vzťah medzi zdrojo množinou viacerých identít užívateľa a jednou identitou cieľového užívateľa v určenom cieľovom registri užívateľov. Priradenia politiky používajú podporu politík mapovania EIM na vytvorenie mapovaní typu veľa-jeden medzi identitami užívateľov bez použitia identifikátora EIM.

Poznámka: Priradenia politiky môžete používať rôznymi spôsobmi prekrývania, preto musíte sa dôkladne oboznámiť s podporou politiky mapovania EIM skôr, než priradenia politiky vytvoríte a začnete používať. Ak chcete predchádzať prípadným problémom s priradeniami a spôsobom, akým mapujú identity, skôr ako začnete definovať priradenia, musíte vyvinúť celkový plán mapovania identít pre váš podnik.

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

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

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

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

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

1. Rozviňte **Network > Enterprise Identity Mapping > Domain Management**.
2. Pravým tlačidlom myši kliknite na doménu EIM, v ktorej chcete pracovať a vyberte **Mapping Policy**
   - Ak doména EIM, s ktorou chcete pracovať, nie je uvedená pod zložkou **Domain Management**, pozrite si “Pridávanie domény EIM do zložky Domain Management” na strane 84.
   - Ak nie ste práve pripojený k doméne EIM, v ktorej chcete pracovať, pozrite si tému Connect to the EIM domain controller.
3. Na strane General vyberte **Enable mapping lookups using policy associations for domain**.
4. Vyberte stránku **Certificate Filter** a kliknutím na **Add** zobrazte dialógové okno **Add Certificate Filter Policy Association**.
5. Ak potrebujete viac detailov o dokončení tohto a následných dialógových okien, kliknite na **Help**.
6. Na zadefinovanie priradenia politiky uveďte nasledujúce požadované informácie:
   a. Zadajte názov definície registra užívateľov X.509, ktorý sa bude používať ako **zdrojový register X.509** pre priradenie politiky. Alebo kliknutím na **Browse** ho vyberte zo zoznamu definícií registrov pre doménu.
   b. Kliknite na **Select**, aby sa zobrazilo dialógové okno **Select Certificate Filter** a vyberte existujúci filter certifikátov, ktorý sa použije ako základ pre nové priradenie politiky filtra certifikátov.

      Poznámka: **Musíte** použiť existujúci filter certifikátov. Ak filter certifikátov, ktorý chcete používať, nie je uvedený, kliknite na **Add** na vytvorenie nového filtra certifikátov.
   c. Zadajte názov definície registra pre **cieľový register** alebo kliknutím na **Browse** ho vyberte zo zoznamu existujúcich definícií registrov pre doménu.
   d. Zadajte meno **cieľového užívateľa** na ktorého sa majú mapovať všetky certifikáty v **zdrojovom registri X.509**, ktoré sa zhodujú s filtrom certifikátov. Alebo kliknutím na **Browse** ho vyberte zo zoznamu užívateľov známych doméne.
   e. Voliteľné. Kliknutím na **Advanced** zobrazíte dialógové okno **Add Association - Advanced**. Zadajte **Lookup information** pre identitu cieľového užívateľa a kliknite na **OK**, aby ste sa vrátili do dialógového okna **Add Certificate Filter Policy Association**.

      Poznámka: Ak sa dve alebo viac priradení politiky s kritériami rovnakého zdrojového registra X.509 a kritériami rovnakého filtra certifikátov týkajú rovnakého cieľového registra, musíte v každom z týchto priradení politiky definovať jedinečné informácie na vyhľadanie pre identity cieľového užívateľa. Zadefinovaním informácií na vyhľadanie pre každú identitu cieľového užívateľa v tejto situácii zabezpečte, aby operácie vyhľadávania mapovaní mohli medzi nimi rozlišovať. V opačnom prípade môžu operácie vyhľadávania mapovaní vrátiť viacero cieľových identít užívateľov. Následkom týchto nejednoznačných výsledkov môže byť neschopnosť aplikácií spoliehajúcich sa na EIM určiť presnú cieľovú identitu, ktorá sa má použiť.
7. Ak chcete vytvoriť priradenie politiky filtra certifikátov, kliknite na **OK** a vráťte sa na stranu **Cerificate Filter**. Nové priradenie politiky sa zobrazí v zozname.
8. Skontrolujte, či je nové priradenie politiky pre cieľový register aktivované.
9. Kliknite na **OK**, aby ste uložili vaše zmeny a zatvorili dialógové okno **Mapping Policy**.

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

Vytváranie filtra certifikátov:

Filter certifikátov definuje sadu podobných atribútov certifikátov s charakteristickým názvom pre skupinu užívateľských certifikátov v zdrojovom registri užívateľov X.509. Filter certifikátov môžete použiť ako základ priradenia politiky filtra certifikátov.

Filter certifikátov v priradení politiky určuje, ktoré certifikáty v zadanom zdrojovom registri X.509 sa majú namapovať k zadanému cieľovému užívateľovi. Tie certifikáty, ktoré majú informáciu Subject DN a Issuer DN, ktoré vyhovujú kritériam filtra, sú namapované do špecifikovaného cieľového užívateľa počas operácií vyhľadávania mapovania EIM.

Ak chcete vytvoriť filter certifikátov, musíte byť pripojený k doméne EIM, v ktorej chcete pracovať a musíte mať “Riadenie prístupu EIM” na strane 38 na jednej z týchto úrovní:

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

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

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

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

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

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

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

1. Rozviňte **Network > Enterprise Identity Mapping > Domain Management**.
2. Pravým tlačidlom myši kliknite na doménu EIM, v ktorej chcete pracovať a vyberte **Mapping Policy**
   - V prípade, že doména EIM, v ktorej chcete pracovať sa nenachádza v **Správe domén**, pozrite si časť “Pridávanie domény EIM do zložky Domain Management” na strane 84.
   - Ak nie ste práve pripojený k doméne EIM, v ktorej chcete pracovať, pozrite si tému Pripojenie k radiču domény EIM.
3. Vyberte stránku **Filter certifikátov** a kliknutím na **Filtre certifikátov** zobrazte dialógové okno **Filtre certifikátov**.

   Poznámka: Ak kliknete na **Filtre certifikátov** a nevyberiete priradenie politiky, zobrazí sa dialógové okno **Prehľadávať registre EIM**. Toto dialógové okno vám umožní vybrať register X.509 zo zoznamu definícií registra X.509 v doméne, pre ktorú chcete zobraziť filtre certifikátov. Obsah zoznamu je rôzny v závislosti od typu vášho riadenia prístupu k EIM.

4. Kliknutím na **Add** zobrazíte dialógové okno **Add Certificate Filter**.
5. V dialógovom okne **Add Certificate Filter** sa musíte rozhodnúť, či chcete pridať jeden filter certifikátov alebo vytvoriť filter certifikátov na základe konkrétneho digitálneho certifikátu. Ak potrebujete viac detailov o dokončení tohto a následných dialógových okien, kliknite na **Help**.
   a. Ak vyberiete **Add a single certificate filter**, môžete zadať informácie o konkrétnom úplnom alebo čiastočnom **DN subjektu**, o úplnom alebo čiastočnom **DN vydavateľa** alebo o oboch. Ak chcete vytvoriť filter certifikátov, kliknite na **OK** a vráťte sa do dialógového okna **Certificate Filters**. Filter sa teraz zobrazí v zozname.
   b. Ak sa vyberiete **Generate certificate filter from a digital certificate**, kliknite na **OK**, aby sa zobrazilo dialógové okno **Generate Certificate Filters**.
      1) Zakódovanú verziu informácií certifikátu vo formáte base64, ktorú ste predtým skopírovali do odkladacej schránky, vložte do poľa **Informácie o certifikáte**.
      2) Kliknite na **OK**, aby sa vytvoril zoznam možných filtrov certifikátov podľa **DN subjektu** a **DN vydavateľa** certifikátu.
      3) Z dialógového okna **Prehľadávať filtre certifikátov** vyberte jeden alebo viacero týchto filtrov certifikátov. Kliknutím na tlačidlo **OK** sa vrátite do dialógového okna **Výber filtrov certifikátov**, kde sú teraz zobrazené vybraté filtre certifikátov.
   c. Ak vyberiete **Vygenerovať filter certifikátov zo zdrojového priradenia pre užívateľa X.509**, kliknite na **OK** na zobrazenie dialógového okna **Generovať filtre certifikátov**. Toto dialógové okno zobrazuje zoznam identít užívateľov X.509, ktorí majú v doméne zdrojové priradenie s identifikátorom EIM.
      1) Vyberte identitu užívateľa X.509, ktorého digitálny certifikát chcete použiť na vytvorenie jedného alebo viacerých kandidátov filtra certifikátov a kliknite na **OK**.
      2) Kliknite na **OK**, aby sa vytvoril zoznam možných filtrov certifikátov podľa **DN subjektu** a **DN vydavateľa** certifikátu.
      3) Z dialógového okna **Browse Certificate Filters** vyberte jeden alebo viacero týchto možných filtrov certifikátov. Kliknite na **OK**, aby ste sa vrátili do dialógového okna **Select Certificate Filters**, kde sú teraz zobrazené vybraté filtre certifikátov.

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

Pridávanie vyhľadávacích informácií do identity cieľového užívateľa

Vyhľadávacie informácie sú voliteľné jedinečné identifikačné údaje pre identitu cieľového užívateľa definovaného v priradení. Toto priradenie môže byť buď cieľovým priradením identifikátora alebo priradením politiky.

Informácie na vyhľadanie sú potrebné, len keď operácia vyhľadávania mapovaní môže vrátiť viac ako jednu cieľovú identitu užívateľa. Táto situácia môže spôsobiť problémy pre aplikácie povolené od EIM, vrátane aplikácií a produktov i5/OS, ktoré nie sú navrhnuté pre ošetrenie nejednoznačných výsledkov.

Keď je to potrebné, môžete pridať informácie na vyhľadanie pre každú cieľovú identitu užívateľa, čím poskytnete detailnejšie identifikačné informácie, ktoré viac opisujú každú cieľovú identitu užívateľa. Ak definujete informácie na vyhľadanie pre cieľovú identitu užívateľa, musia sa poskytnúť operácii vyhľadávania mapovaní, aby táto operácia vrátila jedinečnú cieľovú identitu užívateľa. Inak aplikácie, ktoré sa spoliehajú na EIM nebudú schopné určiť presnú cieľovú identitu na použitie.

Poznámka: Ak nechcete, aby boli operácie prehľadania EIM schopné vracať viac ako jednu cieľovú identitu užívateľa, mali by ste namiesto používania informácií na vyhľadanie opraviť konfiguráciu vašich priradení. Bližšie informácie nájdete v “Odstraňovanie problémov s mapovaním EIM” na strane 116.

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

Pridanie informácií na vyhľadanie k cieľovej identite užívateľa v priradení identifikátora:

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

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

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

1. Rozviňte **Network > Enterprise Identity Mapping > Domain Management**.
2. Vyberte doménu EIM, v ktorej chcete pracovať.
   - Ak doména EIM, s ktorou chcete pracovať, nie je uvedená pod zložkou **Domain Management**, pozrite si “Pridávanie domény EIM do zložky Domain Management” na strane 84.
   - Ak nie ste práve pripojený k doméne EIM, v ktorej chcete pracovať, pozrite si tému Connect to the EIM domain controller.
3. Rozviňte doménu EIM, ku ktorej ste pripojený.
4. Kliknite na **Identifiers**, aby sa zobrazil zoznam identifikátorov EIM pre túto doménu.

   Poznámka: Zobrazenie zoznamu identifikátorov pri pokuse o rozvinutie zložky **Identifiers** môže niekedy trvať dlho. Ak chcete zvýšiť výkon v prípade veľkého počtu identifikátorov EIM v doméne, môžete prispôsobiť zobrazenie adresára **Identifiers** obmedzením hodnoty vyhľadávania, použitej pre zobrazenie identifikátorov. Kliknite pravým tlačidlom myši na **Identifiers**, vyberte **Customize this view > Include** a zadajte kritériá zobrazenia, ktoré sa použijú na vygenerovanie zoznamu identifikátorov EIM, ktoré budú súčasťou zobrazenia.
5. Kliknite pravým tlačidlom myši na identifikátor EIM a vyberte **Properties**.
6. Vyberte stránku **Associations**, vyberte cieľové priradenie, do ktorého chcete pridať vyhľadávacie informácie a kliknite na **Details**. Ak potrebujete zistiť, aké informácie treba zadať do jednotlivých polí, kliknite na tlačidlo **Help**.
7. V dialógovom okne **Association - Details** zadajte **Lookup information**, ktoré chcete používať na ďalšiu identifikáciu cieľovej identity užívateľa v tomto priradení a kliknite na tlačidlo **Add**.
8. Opakujte tento krok pre každú položku informácií na vyhľadanie, ktorú chcete pridať k priradeniu.
9. Kliknite na **OK**, aby sa uložili vaše zmeny a aby ste sa vrátili do dialógového okna **Association - Details**.
10. Kliknite na tlačidlo **OK**, aby ste zatvorili okno.

Pridanie informácií na vyhľadanie k cieľovej identite užívateľa v priradení politiky:

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

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

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

1. Rozviňte **Network > Enterprise Identity Mapping > Domain Management**.
2. Vyberte doménu EIM, v ktorej chcete pracovať.
   - Ak doména EIM, s ktorou chcete pracovať, nie je uvedená pod zložkou **Domain Management**, pozrite si “Pridávanie domény EIM do zložky Domain Management” na strane 84.
   - Ak nie ste práve pripojený do domény EIM, v ktorej chcete pracovať, pozrite si tému Pripojenie k radiču domény EIM.
3. V dialógovom okne **Mapping Policy** môžete použiť strany na zobrazenie priradení politiky pre doménu.

4. Nájdite a vyberte priradenie politiky pre cieľový register obsahujúci cieľovú identitu užívateľa, ku ktorej chcete pridať informácie na vyhľadanie.
5. Kliknutím na **Details** zobrazíte dialóg **Policy Association - Details** pre vybratý typ priradenia politiky. Ak potrebujete zistiť, aké informácie treba zadať do jednotlivých polí, kliknite na tlačidlo **Help**.
6. Zadajte **Lookup information**, ktoré chcete používať na ďalšiu identifikáciu cieľovej identity užívateľa v tomto priradení a kliknite na tlačidlo **Add**. Opakujte tento krok pre každú položku informácií na vyhľadanie, ktorú chcete pridať k priradeniu.
7. Kliknite na **OK**, aby sa uložili vykonané zmeny a aby ste sa vrátili do pôvodného okna **Policy Association - Details**.
8. Kliknite na tlačidlo **OK**, aby ste zatvorili okno.

Odstránenie vyhľadávacích informácií z identity cieľového užívateľa

Vyhľadávacie informácie sú voliteľné jedinečné identifikačné údaje pre identitu cieľového užívateľa definovaného v priradení. Toto priradenie môže byť buď cieľovým priradením identifikátora alebo priradením politiky.

Informácie na vyhľadanie sú potrebné, len keď operácia vyhľadávania mapovaní môže vrátiť viac ako jednu cieľovú identitu užívateľa. Táto situácia môže spôsobiť problémy pre aplikácie povolené od EIM, vrátane aplikácií a produktov i5/OS, ktoré nie sú navrhnuté pre ošetrenie nejednoznačných výsledkov.

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

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

Odstránenie informácií na vyhľadanie pre cieľovú identitu užívateľa v priradení identifikátora:

Keď chcete odstrániť informácie na vyhľadanie pre cieľovú identitu užívateľa v priradení identifikátora, musíte byť pripojený k doméne EIM, v ktorej chcete pracovať a musíte mať “Riadenie prístupu EIM” na strane 38 na jednej z týchto úrovní:

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

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

1. Rozviňte **Network > Enterprise Identity Mapping > Domain Management**.
2. Vyberte doménu EIM, v ktorej chcete pracovať.
   - Ak doména EIM, s ktorou chcete pracovať, nie je uvedená pod zložkou **Domain Management**, pozrite si “Pridávanie domény EIM do zložky Domain Management” na strane 84.
   - Ak nie ste práve pripojený na doménu EIM, v ktorej chcete pracovať, pozrite si tému Pripojenie k radiču domény EIM.
3. Rozviňte doménu EIM, ku ktorej ste pripojený.
4. Kliknite na **Identifikátory**, aby sa zobrazil zoznam identifikátorov EIM pre túto doménu.

   Poznámka: Zobrazenie zoznamu identifikátorov pri pokuse o rozvinutie zložky **Identifikátory** môže niekedy trvať dlho. Ak chcete zvýšiť výkon v prípade veľkého počtu identifikátorov EIM v doméne, môžete prispôsobiť zobrazenie adresára **Identifikátory** obmedzením hodnoty vyhľadávania, použitej pre

zobrazenie identifikátorov. Pravým tlačidlom myši kliknite na **Identifikátory**, vyberte **Prispôsobiť toto zobrazenie > Zahrnúť** a zadajte kritéria zobrazenia, ktoré sa použijú pri generovaní zoznamu identifikátorov EIM, ktoré majú byť zahrnuté do zobrazenia.

5. Kliknite pravým tlačidlom myši na identifikátor EIM a vyberte **Vlastnosti**.
6. Vyberte stránku **Priradenia**, vyberte cieľové priradenie pre identitu užívateľa, pre ktorú chcete odstrániť vyhľadávacie informácie a kliknite na **Podrobnosti**.
7. V dialógovom okne **Priradenie - Detaily** vyberte informácie na vyhľadanie, ktoré chcete odstrániť z cieľovej identity užívateľa a kliknite na **Odstrániť**.

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

Odstránenie informácií na vyhľadanie pre cieľovú identitu užívateľa v priradení politiky:

Keď chcete odstrániť informácie na vyhľadanie pre cieľovú identitu užívateľa v priradení politiky, musíte byť pripojený k doméne EIM, v ktorej chcete pracovať a musíte mať "Riadenie prístupu EIM" na strane 38 na niektorej z týchto úrovní:

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

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

1. Rozviňte **Network > Enterprise Identity Mapping > Domain Management**.
2. Vyberte doménu EIM, v ktorej chcete pracovať.
   - Ak doména EIM, s ktorou chcete pracovať, nie je uvedená pod zložkou **Domain Management**, pozrite si "Pridávanie domény EIM do zložky Domain Management" na strane 84.
   - Ak nie ste práve pripojený na doménu EIM, v ktorej chcete pracovať, pozrite si tému Pripojenie k radiču domény EIM.
3. V dialógovom okne **Politika mapovania** môžete použiť strany na zobrazenie priradení politiky pre doménu.
4. Nájdite a vyberte priradenie politiky pre cieľový register, ktorý obsahuje cieľovú identitu užívateľa, pre ktorú chcete odstrániť informácie na vyhľadanie.
5. Kliknutím na **Podrobnosti** zobrazíte dialóg **Priradenia politiky - podrobnosti** pre vybratý typ priradenia politiky.
6. Vyberte informácie na vyhľadanie, ktoré chcete odstrániť z cieľovej identity užívateľa a kliknite na **Odstrániť**.

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

Zobrazenie všetkých priradení identifikátorov pre identifikátory EIM

Ak chcete zobraziť všetky priradenia pre identifikátor EIM, musíte byť pripojený na doménu EIM, v ktorej chcete pracovať a na vykonanie tejto úlohy musíte mať určitú úroveň riadenia prístupov EIM.

Na zobrazenie všetkých priradení potrebujete ľubovoľnú úroveň riadenia prístupu, okrem riadenia prístupu Administrátor pre vybraté registre. Táto úroveň riadenia prístupu vám dovoľuje zobraziť a filtrovať len tie priradenia pre registre, na ktoré máte explicitné oprávnenie, ak tiež nemáte oprávnenie na riadenie prístupu operácií vyhľadávania mapovaní EIM.

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

Ak chcete zobraziť priradenia identifikátora, vykonajte tieto kroky:

1. Rozviňte **Network > Enterprise Identity Mapping > Domain Management**.
2. Vyberte doménu EIM, v ktorej chcete pracovať.
   - Ak doména EIM, s ktorou chcete pracovať, nie je uvedená pod zložkou **Domain Management**, pozrite si "Pridávanie domény EIM do zložky Domain Management" na strane 84.
   - Ak nie ste práve pripojený k doméne EIM, v ktorej chcete pracovať, pozrite si tému Pripojenie na radič domény EIM.
3. Rozviňte doménu EIM, ku ktorej ste pripojený.
4. Kliknite na **Identifiers**, aby sa zobrazil zoznam identifikátorov EIM pre túto doménu.

   Poznámka: Zobrazenie zoznamu identifikátorov pri pokuse o rozvinutie zložky **Identifiers** môže niekedy trvať dlho. Ak chcete zvýšiť výkon v prípade veľkého počtu identifikátorov EIM v doméne, môžete prispôsobiť zobrazenie adresára **Identifiers** obmedzením hodnoty vyhľadávania, použitej pre zobrazenie identifikátorov. Kliknite pravým tlačidlom myši na **Identifiers**, vyberte **Customize this view > Include** a zadajte kritériá zobrazenia, ktoré sa použijú na vygenerovanie zoznamu identifikátorov EIM, ktoré budú súčasťou zobrazenia.
5. Vyberte identifikátor EIM, kliknite pravým na identifikátor EIM a zvoľte **Properties**.
6. Ak chcete zobraziť zoznam identít užívateľa, priradených vybratému identifikátoru EIM vyberte stranu **Associations**.
7. Kliknite na tlačidlo **OK**, aby ste zatvorili okno.

Zobrazenie všetkých priradení politiky pre doménu

Ak chcete zobraziť všetky priradenia politiky zadefinované pre doménu, musíte byť pripojený na doménu EIM, v ktorej chcete pracovať a na vykonanie tejto úlohy musíte mať určitú úroveň riadenia prístupov EIM.

Na zobrazenie všetkých priradení politiky potrebujete ľubovoľnú úroveň riadenia prístupu, okrem riadenie prístupu Administrátor pre vybraté registre. Táto úroveň riadenia prístupu vám dovoľuje zobraziť a filtrovať len tie priradenia pre registre, na ktoré máte explicitné oprávnenie. Následne, s týmto riadením prístupu nemôžete zobraziť žiadne predvolené priradenia politiky domény, ak tiež nemáte oprávnenie na riadenie prístupu operácií vyhľadávania mapovaní EIM.

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

1. Rozviňte **Network > Enterprise Identity Mapping > Domain Management**.
2. Pravým tlačidlom myši kliknite na doménu EIM, v ktorej chcete pracovať a vyberte **Politika mapovania**
   - Ak doména EIM, s ktorou chcete pracovať, nie je uvedená pod zložkou **Domain Management**, pozrite si "Pridávanie domény EIM do zložky Domain Management" na strane 84.
   - Ak nie ste práve pripojený k doméne EIM, v ktorej chcete pracovať, pozrite si tému Pripojenie k radiču domény EIM.
3. Podľa nasledujúcich krokov vyberte stranu na zobrazenie priradení politiky definovaných pre doménu:
   a. Ak chcete zobraziť predvolené priradenia politiky domény, definované pre doménu a zistiť, či je priradenie politiky povolené na úrovni registra, vyberte stranu **Doména**.
   b. Ak chcete zobraziť predvolené priradenia politiky domény, definované pre doménu, vyberte stranu **Register**. Môžete tiež zobraziť, ktoré zdrojové a cieľové registre ovplyvňujú priradenia politiky.
   c. Ak chcete zobraziť priradenia politiky filtra certifikátov, definované a povolené na úrovni registra, vyberte stranu **Filter certifikátov**.
4. Kliknite na tlačidlo **OK**, aby ste zatvorili okno.

Zobrazenie všetkých priradení politiky pre definíciu registra

Ak chcete zobraziť všetky priradenia politiky zadefinované pre špecifický register, musíte byť pripojený na doménu EIM, v ktorej chcete pracovať a na vykonanie tejto úlohy musíte mať určitú úroveň riadenia prístupov EIM.

Na zobrazenie všetkých priradení politiky potrebujete ľubovoľnú úroveň riadenia prístupu, okrem riadenie prístupu Administrátor pre vybraté registre. Táto úroveň riadenia prístupu vám dovoľuje zobraziť a filtrovať len tie priradenia pre

registre, na ktoré máte explicitné oprávnenie. Následne, s týmto riadením prístupu nemôžete zobraziť žiadne predvolené priradenia politiky domény, ak tiež nemáte oprávnenie na riadenie prístupu operácií vyhľadávania mapovaní EIM.

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

1. Rozviňte **Network > Enterprise Identity Mapping > Domain Management**.
2. Vyberte doménu EIM, v ktorej chcete pracovať.
   - Ak doména EIM, s ktorou chcete pracovať, nie je uvedená pod zložkou **Domain Management**, pozrite si “Pridávanie domény EIM do zložky Domain Management” na strane 84.
   - Ak nie ste práve pripojený k doméne EIM, v ktorej chcete pracovať, pozrite si tému Pripojenie k radiču domény EIM.
3. Pravým tlačidlom myši kliknite na definíciu registra, s ktorou chcete pracovať a vyberte **Politika mapovania**.
4. Podľa nasledujúcich krokov vyberte stranu na zobrazenie priradení politiky definovaných pre zadanú definíciu registra:
   - Ak chcete zobraziť predvolené priradenia politiky domény definované pre register, vyberte stranu **Doména**.
   - Ak chcete zobraziť predvolené priradenia politiky registra definované a povolené pre register, vyberte stranu **Register**.
   - Ak chcete zobraziť priradenia politiky certifikátu filtrov, definované a povolené pre register, vyberte stranu **Filter certifikátov**.
5. Kliknite na tlačidlo **OK**, aby ste zatvorili okno.

Vymazanie priradenia identifikátora

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

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

- Administrátor identifikátorov
- Administrátor EIM.

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

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

Ak chcete vymazať priradenie identifikátora, vykonajte tieto kroky.

1. Rozviňte **Network > Enterprise Identity Mapping > Domain Management**.
2. Vyberte doménu EIM, v ktorej chcete pracovať.
   - Ak doména EIM, s ktorou chcete pracovať, nie je uvedená pod zložkou **Domain Management**, pozrite si “Pridávanie domény EIM do zložky Domain Management” na strane 84.
   - Ak nie ste práve pripojený do domény EIM, v ktorej chcete pracovať, pozrite si tému Pripojenie k radiču domény EIM.
3. Rozviňte doménu EIM, ku ktorej ste pripojený.
4. Kliknite na **Identifiers**, aby sa zobrazil zoznam identifikátorov EIM pre túto doménu.

   Poznámka: Zobrazenie zoznamu identifikátorov pri pokuse o rozvinutie zložky **Identifiers** môže niekedy trvať dlho. Ak chcete zvýšiť výkon pri veľkom počte identifikátorov EIM v doméne, môžete prispôsobiť zobrazenie zložky **Identifiers** obmedzením vyhľadávacieho kritéria použitého na zobrazenie identifikátorov. Kliknite pravým tlačidlom myši na **Identifiers**, vyberte **Customize this view > Include** a zadajte kritériá zobrazenia, ktoré sa použijú na vygenerovanie zoznamu identifikátorov EIM, ktoré budú súčasťou zobrazenia.

5. Vyberte identifikátor EIM, kliknite pravým na identifikátor EIM a zvoľte **Properties**.
6. Ak chcete zobraziť zoznam identít užívateľa, priradených vybratému identifikátoru EIM vyberte stranu **Associations**.
7. Ak chcete vymazať priradenie, vyberte ho a kliknite na tlačidlo **Remove**.

   Poznámka: Keď kliknete na **Remove**, nezobrazí sa žiadna výzva na potvrdenie.
8. Kliknutím na **OK** uložíte vaše zmeny.

Poznámka: Keď odstránite cieľové priradenie, všetky operácie vyhľadávania mapovaní pre cieľový register, ktoré sa spoliehajú na použitie vymazaného priradenia môžu zlyhať, ak pre ovplyvnený cieľový register neexistujú ďalšie priradenia (buď priradenia politiky, alebo priradenia identifikátorov).

Jediný spôsob definovania identity užívateľa v EIM je zadanie identity užívateľa ako súčasti priradenia, buď priradenia identifikátora, alebo priradenia politiky. Následne, keď vymažete posledné cieľové priradenie pre identitu užívateľa (odstránením samotného cieľového priradenia alebo odstránením priradenia politiky), daná identita užívateľa už nie je definovaná v EIM. Následne, názov identity užívateľa a všetky informácie na vyhľadanie pre danú identitu užívateľa sa stratia.

Vymazanie priradenia politiky

Ak chcete vymazať priradenie politiky, musíte byť pripojený na doménu EIM, v ktorej chcete pracovať a musíte mať riadenie prístupov EIM ako administrátor registrov alebo administrátor EIM.

Ak chcete vymazať priradenie politiky, vykonajte tieto kroky:

1. Rozviňte **Network > Enterprise Identity Mapping > Domain Management**.
2. Vyberte doménu EIM, v ktorej chcete pracovať.
   - Ak doména EIM, s ktorou chcete pracovať, nie je uvedená pod zložkou **Domain Management**, pozrite si “Pridávanie domény EIM do zložky Domain Management” na strane 84.
   - Ak nie ste práve pripojený k doméne EIM, v ktorej chcete pracovať, pozrite si tému Pripojenie k radiču domény EIM.
3. Vyberte vhodnú stranu pre typ priradenia politiky, ktorú chcete vymazať.
4. Na danej strane vyberte vhodné priradenie politiky a kliknite na tlačidlo **Odstrániť**.

   Poznámka: Keď kliknete na **Odstrániť**, nezobrazí sa žiadna výzva na potvrdenie.
5. Kliknite na tlačidlo **OK**, aby sa zatvorilo dialógové okno **Politika mapovania** a uložili vaše zmeny.

Poznámka: Keď odstránite cieľové priradenie politiky, všetky operácie vyhľadávania mapovaní pre cieľový register, ktoré využívajú vymazané priradenie politiky môžu zlyhať, ak ostatné priradenia (priradenia politiky alebo priradenia identifikátorov) neexistujú pre ovplyvnený cieľový register.

Jediný spôsob definovania identity užívateľa v EIM je zadanie identity užívateľa ako súčasti priradenia, buď priradenia identifikátora, alebo priradenia politiky. Následne, keď vymažete posledné cieľové priradenie pre identitu užívateľa (odstránením samotného cieľového priradenia alebo odstránením priradenia politiky), daná identita užívateľa už nie je definovaná v EIM. Následne, názov identity užívateľa a všetky informácie na vyhľadanie pre danú identitu užívateľa sa stratia.

Súvisiace koncepty

“Riadenie definícií registrov EIM” na strane 88
Ak chcete, aby boli registre užívateľov a v nich obsiahnuté užívateľské identity prítomné v doméne EIM, musíte pre ne vytvoriť definície registrov. Potom môžete manažovať spôsob účasti registrov užívateľov a ich identít užívateľov v EIM manažovaním len týchto definícií registrov EIM.

Riadenie prístupov užívateľov k EIM

Užívateľ EIM je taký užívateľ, ktorý má riadenie prístupov EIM založené na členstve v skupinách užívateľov preddefinovaného LDAP (Lightweight Directory Access Protocol). Špecifikovanie riadenia prístupu k EIM pre daného užívateľa pridá tohto užívateľa do špecifickej skupiny užívateľov LDAP.

Každá skupina LDAP má oprávnenie na vykonávanie rôznych administratívnych úloh EIM v doméne. Jednotlivé administratívne úlohy a ich typy, vrátane operácií vyhľadávania, ktoré môže užívateľ EIM vykonať, sú určené skupinou riadenia prístupu, do ktorej patrí užívateľ EIM.

Pridávať ďalších užívateľov do skupiny riadenia prístupu k EIM alebo meniť nastavenia riadenia prístupu pre iných užívateľov môžu len užívatelia s riadením prístupu Administrátor LDAP alebo EIM. Skôr, ako sa užívateľ stane členom skupiny riadenia prístupu k EIM, musí mať záznam v adresárovom serveri, ktorý sa správa ako radič domény EIM. Rovnako len konkrétne typy užívateľov sa môžu stať členmi skupiny riadenia prístupu k EIM: principály Kerberos, rozlišované mená a užívateľské profily i5/OS.

Poznámka: Ak chcete mať v EIM k dispozícii užívateľský typ principálu Kerberos, v systéme musí byť nakonfigurovaná služba sieťovej autentifikácie. Ak chcete mať typ užívateľského profilu i5/OS dostupný v EIM, musíte konfigurovať príponu systémového objektu na adresárovom serveri. Toto umožňuje, aby adresárový server odkazoval nai5/OS systémové objekty, ako sú i5/OS užívateľské profily.

Ak chcete manažovať riadenie prístupu pre existujúceho užívateľa adresárového servera alebo chcete pridať existujúceho užívateľa adresára do skupiny riadenia prístupu k EIM, vykonajte tieto kroky:

1. Rozviňte **Network > Enterprise Identity Mapping > Domain Management**.
2. Vyberte doménu EIM, v ktorej chcete pracovať.
   - Ak doména EIM, s ktorou chcete pracovať, nie je uvedená pod zložkou **Domain Management**, pozrite si “Pridávanie domény EIM do zložky Domain Management” na strane 84.
   - Ak nie ste práve pripojený k doméne EIM, v ktorej chcete pracovať, pozrite si tému Pripojenie k radiču domény EIM.
3. Pravým tlačidlom myši kliknite na doménu EIM, na ktorú ste pripojený a vyberte **Access Control**
4. V dialógovom okne **Edit EIM Access Control** vyberte **User type**, aby sa zobrazili polia potrebné pre poskytnutie informácií identifikujúcich užívateľa.
5. Zadajte vyžadované informácie o užívateľovi pre identifikáciu užívateľa, ktorému chcete manažovať riadenie prístupu k EIM a kliknite na tlačidlo **OK**, aby sa zobrazil panel **Edit EIM Access Control**. Ak potrebujete zistiť, aké informácie treba zadať do jednotlivých polí, kliknite na tlačidlo **Help**.
6. Vyberte jednu alebo viac skupín **riadenia prístupu** pre užívateľa a kliknite na tlačidlo **OK**, aby ste pridali tohto užívateľa do vybratej skupiny. Kliknite na tlačidlo **Help**, kde nájdete detailnejšie informácie o oprávneniach každej skupiny a nájdete informácie o akýchkoľvek špeciálnych požiadavkách.
7. Po poskytnutí vyžadovaných informácií kliknite na tlačidlo **OK**, aby sa uložili vaše zmeny.

Súvisiace koncepty

“Riadenie prístupu EIM” na strane 38
Užívateľ EIM je užívateľ, ktorý vlastní riadenie prístupu na EIM na základe jeho členstva v preddefinovanej skupine užívateľov Lightweight Directory Access Protocol (LDAP) pre špecifickú doménu.

Súvisiace informácie

Služba sieťovej autentifikácie

Riadenie vlastností konfigurácie EIM

Manažovať môžete niekoľko rôznych vlastností konfigurácie EIM vášho servera. Zvyčajne to nepotrebujete často.

Avšak, občas sa vyskytne situácia, kedy potrebujete urobiť zmeny do vlastností konfigurácie. Napríklad, ak sa váš systém vypína a potrebujete znovu vytvoriť vlastnosti konfigurácie EIM, môžete na tomto mieste buď znovu spustiť konfiguračného sprievodcu EIM alebo zmeniť vlastnosti. Iný príklad je, že ak ste nevybrali vytvorenie definícií registra pre lokálne registre v Sprievodcovi konfiguráciou EIM, definičné informácie registra môžete zaktualizovať tu.

Vlastnosti, ktoré môžete zmeniť, sú nasledovné:

- Doménu EIM, ktorej účastníkom je server.
- Informácie o pripojení pre radič domény EIM.
- Identita užívateľa, ktorú systém používa na vykonávanie operácií EIM v mene funkcií operačného systému.
- Názvy definícií registrov, ktoré sa týkajú aktuálnych registrov užívateľov, ktoré môže systém používať, keď vykonáva operácie EIM v mene funkcií operačného systému. Tieto názvy definícií registrov sa týkajú lokálnych registrov užívateľov, ktoré môžete vytvoriť počas behu sprievodcu konfiguráciou EIM.

  Poznámka: Ak ste vybrali nevytvorenie názvov definícií lokálneho registra v sprievodcovi konfiguráciou EIM, pretože registre už boli definované pre doménu EIM alebo preto, lebo ich chcete zadefinovať pre doménu neskôr, musíte zaktualizovať vlastnosti konfigurácie systému týmito názvami definícií registrov na tomto mieste. Systém potrebuje tieto informácie o definíci registra na vykonávanie operácií EIM v mene funkcií operačného systému.

Ak chcete zmeniť konfiguračné vlastnosti EIM, musíte mať tieto špeciálne oprávnenia:

- Špeciálne oprávnenie administrátora bezpečnosti (*SECADM).
- Všetky objekty (*ALLOBJ)

Ak chcete zmeniť vlastnosti konfigurácie EIM pre vašu platformu System i, vykonajte tieto kroky:

1. Rozviňte **Network >Enterprise Identity Mapping**.
2. Pravým tlačidlom myši kliknite na **Configuration** a vyberte **Properties**.
3. Vykonajte zmeny v konfiguračných informáciách EIM.
4. Ak chcete zistiť, aké informácie treba zadať do jednotlivých polí dialógového okna, kliknite na tlačidlo **Help**.
5. Ak sa chcete uistiť, že všetky zadané informácie umožnia systému úspešne vytvoriť pripojenie k radiču domény EIM, kliknite na tlačidlo **Verify Configuration**.
6. Kliknutím na **OK** uložíte vaše zmeny.

Poznámka: Ak ste nepoužili sprievodcu konfiguráciou EIM na vytvorenie alebo pripojenie domény, nepokúšajte sa vytvoriť konfiguráciu EIM ručným zadaním vlastností konfigurácie. Použitím sprievodcu na vytvorenie základnej konfigurácie EIM sa môžete vyhnúť potencionálnym konfiguračným problémom, pretože sprievodca spraví viac, ako len nakonfigurovanie vlastností.

Odstraňovanie problémov s EIM

Na vyriešenie niektorých základných problémov, ktoré môžu vzniknúť pri konfigurácii a používaní EIM použite nasledujúce metódy.

EIM sa skladá z viacerých technológií a mnohých aplikácií a funkcií. Problém sa preto môže vyskytnúť vo viacerých oblastiach. Nasledujúce informácie opisujú niekoľko bežných problémov a chýb, ku ktorým môže dôjsť pri používaní EIM a niekoľko návrhov na opravenie chýb a problémov.

Súvisiace informácie

Odstraňovanie problémov s konfiguráciou jednoduchého prihlásenia

Odstraňovanie problémov pripojenia k radiču domény

Pri pripájaní k radiču domény môže k problémom prispieť množstvo faktorov. Ak chcete zistiť, ako odstrániť problémy pripojenia k radiču domény, pozrite si nasledujúcu tabuľku

Tabuľka 27. Bežné problémy s pripojením radiča domény EIM a ich riešenia

Možný problém	Možné riešenia
Ak používate System i Navigator na riadenie EIM, nemôžete sa pripojiť k radiču domény.	Informácie o pripojení radiča domény pre doménu, ktorú chcete riadiť sú možno zadané nesprávne. Vykonajte tieto kroky na overenie informácií o pripojení domény: • Rozviňte **Network-->Enterprise Identity Mapping-->Network->Domain Management**. Kliknite pravým tlačidlom na doménu, ktorú chcete riadiť a vyberte **Vlastnosti**. • Skontrolujte správnosť názvu pre **Domain controller** a pre **Parent DN**, ak je zadané. • Overte, či sú informácie pre **Connection** pre radič domény správne. Presvedčte sa, či je číslo pre **Port** správne. Ak je vybraté **Use secure connection (SSL or TLS)**, adresárový server musí byť nakonfigurovaný na použitie SSL. Kliknite na **Verify Connection**, aby ste overili, že môžete používať zadané informácie na úspešné vytvorenie pripojenia k radiču domény. • Overte, či sú informácie o užívateľovi v paneli **Connect to Domain Controller** správne.
Operačný systém alebo aplikácie sa nemôžu pripojiť k radiču domény a pristupovať k údajom EIM. Napríklad operácie vyhľadávania mapovaní EIM vykonávané pre systém zlyhávajú. Môže k tomu dôjsť, pretože konfigurácia EIM v systéme alebo systémoch je nesprávna.	Skontrolujte vašu konfiguráciu EIM. V systéme, do ktorého sa chcete autentifikovať, rozviňte **Network-->Enterprise Identity Mapping-->Configuration**. Pravým tlačidlom myši kliknite na zložku **Configuration**, vyberte **Properties** a skontrolujte nasledujúce: • Strana **Domain**: – Názov radiča domény a čísla portov sú správne. – Kliknite na tlačidlo **Verify Configuration** a skontrolujte, či je radič domény aktívny. – Názov lokálneho registra je zadaný správne. – Názov registra Kerberos je zadaný správne. – Skontrolujte, či je vybraté **Enable EIM operations for this system**. • Strana **System user**: – Špecifikovaný užívateľ má dostatočné riadenie prístupu k EIM na vykonanie vyhľadávania mapovaní a heslo pre užívateľa je platné. Pozrite si online pomoc, kde sa dozviete o rozdielnych typoch oprávnení užívateľov. **Poznámka:** Ak ste zmenili heslo užívateľa systému v adresárovom serveri, musíte to zmeniť aj tu. Ak sa tieto heslá nezhodujú, užívateľ systému nemôže vykonávať funkcie EIM operačného systému a operácie vyhľadávania mapovaní zlyhajú. – Kliknite na tlačidlo **Verify Connection** a skontrolujte správnosť zadaných informácií o užívateľovi.
Konfiguračné informácie sa zdajú správne, ale nemôžete sa pripojiť k radiču domény.	• Presvedčte sa, či je adresárový server, ktorý vystupuje ako radič domény EIM, aktívny. Ak je radič domény platformou System i, môžete použiť System i Navigator a vykonať tieto kroky: 1. Rozviňte **Sieť> Servery > TCP/IP**. 2. Skontrolujte, že adresárový server má stav **Started**. Ak je server zastavený, kliknite pravým tlačidlom myši na **Directory Server** a vyberte **Start**

Po overení informácií o pripojení a aktivity adresárového servera sa pokúste pripojiť k radiču domény vykonaním týchto krokov:

1. Rozviňte **Network > Enterprise Identity Mapping > Domain Management**.
2. Pravým tlačidlom myši kliknite na doménu EIM, ku ktorej sa chcete pripojiť a vyberte **Connect**.
3. Zadajte typ užívateľa a vyžadované informácie o užívateľovi, ktoré sa majú použiť pre pripojenie k radiču domény EIM.
4. Kliknite na tlačidlo **OK**.

Odstraňovanie bežných problémov konfigurácie EIM a domény

Existuje veľa všeobecných problémov, ku ktorým môže dôjsť pri konfigurácii EIM pre váš systém, ako aj problémov, ktoré sa môžu vyskytnúť počas prístupu k doméne EIM. Ak sa chcete dozvedieť viac o niektorých bežných problémoch a ich možných riešeniach, pozrite si nasledujúcu tabuľku.

Tabuľka 28. Bežné problémy s konfiguráciou EIM a doménou a ich riešenia

Možný problém	Možné riešenia
Sprievodca konfiguráciou EIM sa javí ako zaseknutý počas spracovania kroku **Finish**.	Sprievodca môže čakať na spustenie radiča domény. Overte, či sa počas štartovania adresárového servera nevyskytli žiadne chyby. Pre platformy System i skontrolujte protokol úlohy QDIRSRV v podsystéme QSYSWRK. Ak chcete skontrolovať protokol úloh, vykonajte tieto kroky: 1. V System i Navigator rozviňte **Riadenie práce> Podsystémy > Qsyswrk**. 2. Pravým tlačidlom myši kliknite na **Qdirsrv** a vyberte **Protokol úlohy**.
Keď používate Sprievodcu konfiguráciou EIM na vytvorenie domény vo vzdialenom systéme, dostali ste túto chybovú správu: ″The parent distinguished name (DN) you entered is not valid. The DN must exist on the remote directory server. Specify or select a new or existing parent DN.’	Rodičovské DN uvedené pre vzdialenú doménu, neexistuje. Ak sa chcete dozvedieť viac o konfiguračnom sprievodcovi EIM, pozrite si “Vytvorenie a pripojenie k novej vzdialenej doméne” na strane 73. Môžete si tiež pozrieť online pomoc, kde nájdete detailné informácie o špecifikovaní rodičovského DN, keď vytvárate doménu.
Dostanete správu oznamujúcu, že doména EIM neexistuje.	Ak ste nevytvorili doménu EIM, použite sprievodcu konfiguráciou EIM. Tento sprievodca pre vás vytvorí doménu EIM alebo vám umožní nakonfigurovať existujúcu doménu EIM. Ak ste vytvorili doménu EIM, presvedčte sa, že uvedený užívateľ je členom skupiny “Riadenie prístupu EIM” na strane 38 s dostatočným oprávnením na prístup k nej.
Dostanete správu oznamujúcu, že objekt EIM (identifikátor, register, priradenie, priradenie politiky alebo filter certifikátov), sa nenašiel alebo že nemáte oprávnenie na údaje EIM.	Overte, či objekt EIM existuje a či je špecifikovaný užívateľ členom skupiny “Riadenie prístupu EIM” na strane 38 s dostatočným oprávnením na tento objekt.

Tabuľka 28. Bežné problémy s konfiguráciou EIM a doménou a ich riešenia (pokračovanie)

Možný problém	Možné riešenia
Zobrazenie zoznamu identifikátorov pri pokuse o rozvinutie zložky **Identifikátory** môže niekedy trvať dlho.	Toto sa môže stať, ak existuje veľké množstvo identifikátorov EIM v doméne. Keď to chcete vyriešiť, môžete upraviť zobrazenie zložky **Identifikátory** obmedzením vyhľadávacieho kritéria použitého na zobrazenie identifikátorov. Ak chcete prispôsobiť zobrazenie pre identifikátory EIM, vykonajte tieto kroky: 1. V System i Navigator rozviňte **Network> Enterprise Identity Mapping > Domain Managemet**. 2. Rozviňte doménu, ktorej identifikátory chcete zobraziť. 3. Kliknite pravým tlačidlom myši na **Identifiers** a vyberte **Customize this view > Include**. 4. Zadajte zobrazovacie kritérium, ktoré sa použije pre generovanie zoznamu identifikátorov EIM, ktoré sa zahrnú do zobrazenia. **Poznámka:** Môžete použiť hviezdičku (*) ako zástupný znak. 5. Kliknite na **OK**. Najbližšie, keď kliknete na **Identifiers**, zobrazia sa len tie identifikátory EIM, ktoré vyhovujú vami zadanému kritériu.
Ak riadite EIM prostredníctvom System i Navigator, dostanete chybu, ktorá uvádza, že identifikátor EIM je už neplatný.	Pripojenie k radiču domény bolo prerušené. Ak chcete obnoviť pripojenie k radiču domény, vykonajte tieto kroky: 1. V System i Navigator rozviňte **Network> Enterprise Identity Mapping > Domain Managemet**. 2. Kliknite pravým tlačidlom myši na doménu, s ktorou chcete pracovať a vyberte **Reconnect**. 3. Zadajte informácie pre pripojenie. 4. Kliknite na **OK**.
Keď používate protokol Kerberos pre autentifikáciu s EIM, do protokolu úlohy sa zapíše diagnostická správa CPD3E3F.	Táto správa sa vygeneruje vždy, keď zlyhá autentifikácia alebo operácia mapovania identity. Táto diagnostická správa obsahuje hlavné aj vedľajšie stavové kódy označujúce miesto vzniku problému. Väčšina bežných problémov je zdokumentovaná v správe spolu s informáciami o obnove. Odstraňovanie problému začnite prečítaním pomocných informácií z diagnostickej správy. Pozrite si aj tému Odstraňovanie problémov konfigurácie jednoduchého prihlásenia.

Odstraňovanie problémov s mapovaním EIM

Existuje množstvo bežných problémov, ktoré môžu spôsobiť úplné zlyhanie alebo neočakávané fungovanie mapovaní EIM. Informácie o probléme, ktorý môže spôsobovať zlyhanie mapovania EIM a možnom riešení tohto problému, nájdete v nasledujúcej tabuľke. Ak mapovania EIM zlyhávajú, budete asi musieť prejsť každým riešením a vyriešiť problém alebo problémy spôsobujúce zlyhania mapovaní.

Tabuľka 29. Bežné problémy s mapovaním EIM a ich riešenia

Možný problém	Možné riešenia
Informácie o pripojení pre radič domény nemusia byť správne alebo radič domény nemusí byť aktívny.	Ak sa chcete dozvedieť viac o overovaní informácií o pripojení pre radič domény a či je radič domény aktívny, pozrite si tému Problémy s pripojením radiča domény.

Tabuľka 29. Bežné problémy s mapovaním EIM a ich riešenia (pokračovanie)

Možný problém	Možné riešenia
Operácie vyhľadávania mapovaní EIM, vykonávané systémom zlyhávajú. Môže k tomu dôjsť, pretože konfigurácia EIM v systéme alebo systémoch je nesprávna.	Skontrolujte vašu konfiguráciu EIM. V systéme, do ktorého sa chcete autentifikovať, rozviňte **Network-->Enterprise Identity Mapping-->Configuration**. Pravým tlačidlom myši kliknite na zložku **Konfigurácia**, vyberte **Vlastnosti** a skontrolujte nasledujúce: • Strana **Doména**: – Názov radiča domény a čísla portov sú správne. – Kliknite na tlačidlo **Skontrolovať konfiguráciu** a skontrolujte, či je radič domény aktívny. – Názov lokálneho registra je zadaný správne. – Názov registra Kerberos je zadaný správne. – Skontrolujte, či je vybraté **Povoliť operácie EIM pre tento systém**. • Strana **Užívateľ systému**: – Zadaný užívateľ má dostatočné riadenie prístupu k EIM na vykonanie vyhľadávania mapovaní a heslo užívateľa je platné. Ak sa chcete dozvedieť viac o rôznych typoch užívateľských splnomocnení, pozrite si online pomoc. **Poznámka:** Ak ste zmenili heslo užívateľa systému v adresárovom serveri, musíte to zmeniť aj tu. Ak sa tieto heslá nezhodujú, užívateľ systému nemôže vykonávať funkcie EIM operačného systému a operácie vyhľadávania mapovaní zlyhajú. – Kliknite na tlačidlo **Skontrolovať pripojenie** a skontrolujte správnosť zadaných informácií o užívateľovi.

Tabuľka 29. Bežné problémy s mapovaním EIM a ich riešenia (pokračovanie)

Možný problém	Možné riešenia
Operácia vyhľadávania mapovaní môže vracať viaceré cieľové identity užívateľov. Toto môže nastať pri jednej alebo viacerých z nasledujúcich situácií: • Identifikátor EIM má viaceré samostatné cieľové priradenia k jednému cieľovému registru. • Viac ako jeden identifikátor EIM má v zdrojovom priradení zadanú tú istú identitu užívateľa a každý z nich má cieľové priradenie k tomu istému cieľovému registru, aj keď identita užívateľa zadaná pre každé cieľové priradenie môže byť rôzna. • Viac ako jedno predvolené priradenie politiky domény určuje ten istý cieľový register. • Viac ako jedno predvolené priradenie politiky registra určuje ten istý zdrojový register a ten istý cieľový register. • Viac ako jedno priradenie politiky filtra certifikátov určuje ten istý zdrojový register X.509, filter certifikátov a cieľový register.	Použite funkciu Test mapovania EIM , aby ste overili, či konkrétna identita zdrojového užívateľa správne mapuje na príslušnú identitu cieľového užívateľa. Riešenie problému závisí od výsledkov testu podľa týchto pokynov: • Test vráti viaceré nežiaduce identity cieľového užívateľa kvôli jednému z nasledujúcich dôvodov: – Toto môže indikovať, že konfigurácia priradenia domény nie je správna kvôli jednému z nasledujúceho: - Cieľové alebo zdrojové priradenie pre identifikátor EIM nie je správne nakonfigurované. Napríklad neexistuje zdrojové priradenie pre princípal Kerberos (alebo užívateľa systému Windows) alebo je nesprávne. Je tiež možné, že cieľové priradenie určuje nesprávnu identitu užívateľa. Zobrazte všetky priradenia identifikátorov pre identifikátor EIM a skontrolujte priradenia pre konkrétny identifikátor. - Priradenie politiky nie je správne nakonfigurované. Zobrazte všetky priradenia politiky pre doménu, aby ste overili informácie o zdroji a cieli pre všetky priradenia politiky, zadefinované v doméne. – Toto môže indikovať, že definície skupinového registra, ktoré obsahujú spoločných členov, sú zdrojové alebo cieľové registre pre priradenia identifikátora EIM alebo priradenia politiky. Použite podrobnosti poskytnuté operáciou vyhľadávania testu mapovania, aby ste určili, či zdrojové alebo cieľové registre sú definície skupinového registra. Ak sú, skontrolujte vlastnosti definícií skupinového registra, aby ste určili, či definície skupinového registra obsahujú spoločných členov. – Test vracia viaceré cieľové identity a tieto výsledky sú vhodné vzhľadom na spôsob konfigurácie priradení. V tejto situácii potrebujete zadať informácie na vyhľadanie pre každú cieľovú identitu užívateľa na zabezpečenie vrátenia jednej cieľovej identity užívateľa operáciou vyhľadávania, a nie všetkých možných cieľových identít užívateľov. Pozrite si tému Pridávanie vyhľadávacích informácií do identity cieľového užívateľa. **Poznámka:** Tento prístup funguje, len keď má aplikácia povolené používať informácie na vyhľadanie. Základné aplikácie i5/OS, napríklad System i Access for Windows, však nemôžu používať vyhľadávacie informácie na rozlíšenie medzi viacerými cieľovými užívateľskými identitami vrátenými operáciou vyhľadávania. Následne by ste mohli zvážiť predefinovanie priradení pre doménu, aby ste zabezpečili, že operácia vyhľadávania mapovania dokáže vrátiť jedinú cieľovú identitu užívateľa pre zaistenie, aby základné i5/OS aplikácie mohli úspešne vykonať operácie vyhľadávania a mapovať identity.

Tabuľka 29. Bežné problémy s mapovaním EIM a ich riešenia (pokračovanie)

Možný problém	Možné riešenia
Operácie prehľadania EIM nevracajú žiadne výsledky a priradenia pre doménu sú nakonfigurované.	Použite funkciu Test mapovania EIM , aby ste overili, či konkrétna identita zdrojového užívateľa správne mapuje na príslušnú identitu cieľového užívateľa. Skontrolujte, že ste pre test poskytli správne informácie. Ak sú správne a test nevracia žiadne výsledky, problém môže byť spôsobený jedným z nasledujúcich dôvodov: • Konfigurácia priradenia je nesprávna. Skontrolujte vašu konfiguráciu priradenia pomocou informácií o riešení problému poskytnutých v predchádzajúcej položke. • Podpora priradenia politiky na úrovni domény nie je povolená. Budete musieť povoliť priradenia politiky pre doménu. • Podpora vyhľadávania mapovaní alebo priradenia politiky na úrovni registra nie je povolená. Budete musieť povoliť podporu vyhľadávania mapovaní a používania priradení politiky pre cieľový register. • Definícia registra a identity užívateľov sa nezhodujú z dôvodu rozlišovania veľkosti písmen. Môžete vymazať a znovu vytvoriť register alebo priradenie so správnou veľkosťou písma.

Súvisiace úlohy

"Testovanie mapovania EIM" na strane 85
Testovanie mapovania EIM umožňuje vykonať vyhľadávacie operácie mapovania EIM voči konfigurácii EIM. Testovaním si môžete overiť, či sa konkrétna identita zdrojového užívateľa správne mapuje na príslušnú identitu cieľového užívateľa. Testovanie zabezpečí, že vyhľadávacie operácie mapovania EIM môžu vrátiť na základe uvedených informácií správnu identitu cieľového užívateľa.

Rozhrania API pre EIM

EIM poskytuje techniky pre manažment identít užívateľov medzi platformami. EIM má niekoľko aplikačných programových rozhraní (API), ktoré môžu aplikácie používať na vykonávanie operácií EIM v mene aplikácie alebo užívateľa aplikácie.

Tieto rozhrania API môžete použiť na vykonávanie operácií vyhľadávania mapovaní identity, rôznych funkcií manažmentu a konfigurácie EIM, ako aj na zmenu informácií a vytváranie dotazov. Všetky tieto rozhrania API sú podporované v platformách IBM.

Rozhrania API EIM sa delia do týchto kategórií:

- Operácie s deskriptormi a pripojeniami EIM
- Administrácia domény EIM
- Operácie s registrom
- Operácie s identifikátormi EIM
- Manažovanie priradení EIM
- Operácie vyhľadávania mapovaní EIM
- Manažovanie autorizácie EIM

Aplikácie, ktoré používajú tieto rozhrania API na manažovanie alebo používajú informácie EIM v doméne EIM sa zvyčajne držia tohto programovacieho modelu:

1. Získanie deskriptora EIM
2. Pripojenie k doméne EIM

3. Normálne aplikačné spracovanie
4. Použitie API pre správu EIM alebo operácie vyhľadávania mapovania identity EIM
5. Normálne aplikačné spracovanie
6. Zrušenie deskriptora EIM pred ukončením

Súvisiace koncepty

“Plánovanie vývoja aplikácií pre mapovanie podnikovej identity” na strane 65
Aplikácia musí byť schopná používať rozhrania API mapovania EIM, aby mohla používať mapovanie podnikovej identity (EIM) a participovať v doméne.

Súvisiace informácie

Rozhrania API mapovania podnikovej identity (EIM)

Súvisiace informácie pre mapovanie podnikovej identity

Publikácie IBM Redbooks a ostatné kolekcie tém informačného centra obsahujú informácie týkajúce sa kolekcie tém EIM. Ľubovoľný z týchto súborov PDF môžete zobraziť alebo vytlačiť.

Publikácie IBM Redbook

- Jednoduché prihlásenie založené na Windows a rámec EIM v IBM eServer iSeries Server
- Horúce témy iSeries Access for Windows V5R2: Prispôsobené obrázky, Správa aplikácií, SSL a Kerberos

Ostatné informácie

- Jediné prihlásenie
- Služba sieťovej autentifikácie
- IBM Tivoli Directory Server for i5/OS (LDAP)

Pojmy a podmienky

Oprávnenia na používanie týchto publikácií sú predmetom nasledujúcich pojmov a podmienok.

Osobné použitie: Tieto publikácie môžete reprodukovať pre svoje osobné, nekomerčné použitie za podmienky zachovania všetkých informácií o autorských právach. Bez výslovného povolenia autora ich nemôžete distribuovať, zobrazovať ani odvádzať práce z týchto publikácií ani žiadnej ich časti.

Komerčné použitie: Tieto publikácie môžete reprodukovať, distribuovať a zobrazovať výlučne vo vašej spoločnosti za podmienky zachovania všetkých informácií o autorských právach. Bez výslovného povolenia od autora nemôžete odvádzať práce z týchto publikácií ani reprodukovať, distribuovať a zobrazovať tieto publikácie ani žiadne ich časti.

S výnimkou ako je uvedené v týchto podmienkach, na publikácie ľubovoľné informácie, údaje, softvér alebo iné tu obsiahnuté intelektuálne vlastníctvo nemáte žiadne oprávnenia, licencie ani práva, vyjadrené ani implikované.

Spoločnosť IBM si vyhradzuje právo odobrať tu uvedené oprávnenia vždy, podľa vlastného uváženia, keď použitie týchto publikácií škodí autorovi, alebo ak spoločnosť IBM, že pokyny hore nie sú striktne dodržiavané.

Tieto informácie nemôžete prevziať ani exportovať okrem prípadu, ak to dovoľujú všetky aplikovateľné zákony a regulácie, vrátane všetkých zákonov a regulácií USA pre export.

SPOLOČNOSŤ IBM NERUČÍ ZA OBSAH TÝCHTO PUBLIKÁCIÍ. PUBLIKÁCIE SÚ POSKYTNUTÉ ″TAK AKO SÚ″ BEZ ZÁRUKY AKÉHOKOĽVEK DRUHU, VYJADRENEJ ALEBO IMPLIKOVANEJ, VRÁTANE (ALE NEOBMEDZENE) IMPLIKOVANÝCH ZÁRUK PREDAJNOSTI, NEPOŠKODENIA A VHODNOSTI NA KONKRÉTNY ÚČEL.

Príloha. Právne vyhlásenia

Tieto informácie boli vyvinuté pre produkty a služby ponúkané v USA.

IBM nemusí ponúkať produkty, služby alebo vlastnosti opisované v tomto dokumente v iných krajinách. Informácie o aktuálne dostupných produktoch a službách vo vašej krajine získate od predstaviteľa lokálnej pobočky IBM. Žiadny odkaz na produkt, program alebo službu IBM nie je myslený tak a ani neimplikuje, že sa môže používať len tento produkt, program alebo služba od IBM. Namiesto nich sa môže použiť ľubovoľný funkčne ekvivalentný produkt, program alebo služba, ktorá neporušuje intelektuálne vlastnícke právo IBM. Vyhodnotenie a kontrola činnosti produktu, programu alebo služby inej ako od IBM je však na zodpovednosti užívateľa.

IBM môže vlastniť patenty alebo nevybavené prihlášky patentov, týkajúce sa predmetu opísaného v tomto dokumente. Získanie tohto dokumentu vám nedáva žiadnu licenciu na tieto patenty. Žiadosti o licencie môžete zasielať písomne na:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Žiadosti o licencie týkajúce sa dvojbajtových (DBCS) informácií smerujte na oddelenie intelektuálneho vlastníctva IBM vo vašej krajine alebo ich pošlite písomne na:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

Nasledujúci odsek sa netýka Veľkej Británie ani žiadnej inej krajiny, kde sú takéto vyhlásenia nezlučiteľné s lokálnym zákonom: SPOLOČNOSŤ INTERNATIONAL BUSINESS MACHINES POSKYTUJE TÚTO PUBLIKÁCIU "TAK AKO JE" BEZ ZÁRUKY AKÉHOKOĽVEK DRUHU, VYJADRENEJ ALEBO IMPLIKOVANEJ, VRÁTANE (ALE NEOBMEDZENE) IMPLIKOVANÝCH ZÁRUK NEPOŠKODENIA, PREDAJNOSTI ALEBO VHODNOSTI NA KONKRÉTNY ÚČEL. Niektoré štáty nedovoľujú zrieknutie sa vyjadrených alebo mlčky predpokladaných záruk v určitých transakciách, preto sa vás toto vyhlásenie nemusí týkať.

Tieto informácie môžu obsahovať technické nepresnosti alebo typografické chyby. Tieto informácie sa periodicky menia; tieto zmeny budú začlenené do nových vydaní publikácie. IBM môže kedykoľvek bez ohlásenia spraviť zmeny a/alebo vylepšenia v produkte(och) a/alebo programe(och) opísanom v tejto publikácii.

Všetky odkazy v týchto informáciách na webové lokality iné ako od IBM sú poskytnuté len pre pohodlie a v žiadnom prípade neslúžia ako potvrdenie obsahu týchto webových lokalít. Materiály na týchto webových lokalitách nie sú časťou produktov IBM a použitie týchto webových lokalít je na vaše vlastné riziko.

IBM môže použiť alebo distribuovať všetky vami poskytnuté informácie ľubovoľným spôsobom bez toho, aby voči vám vznikli akékoľvek záväzky.

Vlastníci licencií na tento program, ktorí chcú o ňom získať informácie za účelom povolenia: (i) výmeny informácií medzi nezávisle vytvorenými programami a inými programami (vrátane tohto) a (ii) vzájomného použitia vymieňaných informácií by mali kontaktovať:

IBM Corporation
Software Interoperability Coordinator, Department 49XA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Takéto informácie môžu byť dostupné, môžu byť predmetom príslušných pojmov a podmienok a v niektorých prípadoch sú dostupné za poplatok.

Spoločnosť IBM poskytuje licenčný program opísaný v tomto dokumente a všetky preň dostupné licenčné materiály na základe podmienok zákazníckej zmluvy IBM, medzinárodnej licenčnej zmluvy na programy IBM, licenčnej zmluvy IBM pre počítačový kód alebo inej porovnateľnej zmluvy medzi zmluvnými stranami.

Všetky údaje o výkone, uvádzané v tomto dokumente boli získané v riadenom prostredí. Výsledky získané v iných prevádzkových prostrediach sa môžu podstatne odlišovať. Niektoré merania boli vykonané v systémoch vývojovej úrovne a nie je žiadna záruka, že tieto merania budú rovnaké vo všeobecne dostupných systémoch. Okrem toho, niektoré výsledky boli odhadnuté extrapoláciou. Skutočné výsledky sa môžu odlišovať. Užívatelia tohto dokumentu by si mali overiť použiteľnosť týchto údajov pre svoje špecifické prostredie.

Informácie o produktoch iných ako od IBM boli získané od poskytovateľov týchto produktov, z ich uverejnených oznámení alebo z iných, verejne dostupných zdrojov. IBM netestovala tieto produkty a nemôže potvrdiť presnosť ich výkonu, kompatibilitu ani žiadne iné tvrdenie týkajúce sa produktov iných ako od IBM. Otázky k schopnostiam produktov iných ako od IBM by ste mali adresovať poskytovateľom týchto produktov.

Všetky vyhlásenia týkajúce sa budúceho smerovania alebo úmyslov IBM sú predmetom zmeny alebo zrušenia bez ohlásenia a vyjadrujú len zámery a ciele.

Všetky ceny IBM sú navrhované predajné ceny stanovené spoločnosťou IBM, sú aktuálne a sú predmetom zmeny bez ohlásenia. Ceny dílerov môžu byť odlišné.

Tieto informácie slúžia len na plánovacie účely. Tu uvedené informácie sú predmetom zmeny pred sprístupnením opisovaných produktov.

Tieto informácie obsahujú príklady údajov a hlásení používaných v každodenných firemných operáciách. Kvôli ich čo najlepšej ilustrácii obsahujú tieto príklady mená osôb, názvy spoločností, pobočiek a produktov. Všetky tieto mená a názvy sú vymyslené a akákoľvek podobnosť s menami, názvami a adresami používanými skutočnými osobami a spoločnosťami je čisto náhodná.

LICENCIA NA AUTORSKÉ PRÁVA:

Tieto informácie obsahujú vzorové aplikačné programy v zdrojovom kóde, ktoré ilustrujú programovacie techniky v rôznych platformách. Tieto vzorové programy môžete kopírovať, upravovať a distribuovať v ľubovoľnej forme bez platenia poplatku spoločnosti IBM, za účelom vývoja, použitia, marketingu alebo distribúcie aplikačných programov vyhovujúcich aplikačnému programovému rozhraniu pre prevádzkovú platformu, pre ktorú sú napísané tieto vzorové programy. Tieto príklady neboli dôkladne otestované pri všetkých podmienkach. IBM preto nemôže garantovať alebo predpokladať spoľahlivosť, použiteľnosť ani funkciu týchto programov.

Každá kópia alebo časť týchto vzorových programov alebo odvodená práca musí obsahovať túto poznámku o autorských právach:

© (meno vašej spoločnosti) (rok). Časti tohto kódu sú odvodené od vzorových programov spoločnosti IBM. © Copyright IBM Corp. _uveďte rok alebo roky_. Všetky práva vyhradené.

Ak si prezeráte elektronickú kópiu týchto informácií, nemusia byť zobrazené fotografie ani farebné ilustrácie.

Ochranné známky

Nasledujúce pojmy sú ochranné známky spoločnosti International Business Machines v USA, v iných krajinách alebo v oboch:

AIX
Distributed Relational Database Architecture

Domino
DRDA
eServer
i5/OS
IBM
iSeries
Lotus Notes
NetServer
OS/400
pSeries
RACF
RDN
System i
Tivoli
WebSphere
xSeries
z/OS

Adobe, logo Adobe, PostScript a logo PostScript sú registrované ochranné známky alebo ochranné známky spoločnosti Adobe Systems Incorporated v USA alebo iných krajinách.

Linux je registrovaná ochranná známka Linusa Torvaldsa v USA alebo iných krajinách.

Microsoft, Windows, Windows NT a logo Windows sú ochranné známky spoločnosti Microsoft v USA alebo iných krajinách.

UNIX je registrovaná ochranná známka spoločnosti The Open Group v USA a iných krajinách.

Ostatné názvy spoločnosti, produktov alebo služieb môžu byť ochranné alebo servisné známky iných subjektov.

Pojmy a podmienky

Oprávnenia na používanie týchto publikácií sú predmetom nasledujúcich pojmov a podmienok.

Osobné použitie: Tieto publikácie môžete reprodukovať pre svoje osobné, nekomerčné použitie za podmienky zachovania všetkých informácií o autorských právach. Bez výslovného povolenia autora ich nemôžete distribuovať, zobrazovať ani odvádzať práce z týchto publikácií ani žiadnej ich časti.

Komerčné použitie: Tieto publikácie môžete reprodukovať, distribuovať a zobrazovať výlučne vo vašej spoločnosti za podmienky zachovania všetkých informácií o autorských právach. Bez výslovného povolenia od autora nemôžete odvádzať práce z týchto publikácií ani reprodukovať, distribuovať a zobrazovať tieto publikácie ani žiadne ich časti.

S výnimkou ako je uvedené v týchto podmienkach, na publikácie ľubovoľné informácie, údaje, softvér alebo iné tu obsiahnuté intelektuálne vlastníctvo nemáte žiadne oprávnenia, licencie ani práva, vyjadrené ani implikované.

Spoločnosť IBM si vyhradzuje právo odobrať tu uvedené oprávnenia vždy, podľa vlastného uváženia, keď použitie týchto publikácií škodí autorovi, alebo ak spoločnosť IBM, že pokyny hore nie sú striktne dodržiavané.

Tieto informácie nemôžete prevziať ani exportovať okrem prípadu, ak to dovoľujú všetky aplikovateľné zákony a regulácie, vrátane všetkých zákonov a regulácií USA pre export.

SPOLOČNOSŤ IBM NERUČÍ ZA OBSAH TÝCHTO PUBLIKÁCIÍ. PUBLIKÁCIE SÚ POSKYTNUTÉ ″TAK AKO SÚ″ BEZ ZÁRUKY AKÉHOKOĽVEK DRUHU, VYJADRENEJ ALEBO IMPLIKOVANEJ, VRÁTANE (ALE NEOBMEDZENE) IMPLIKOVANÝCH ZÁRUK PREDAJNOSTI, NEPOŠKODENIA A VHODNOSTI NA KONKRÉTNY ÚČEL.

Vytlačené v USA