System i

Zabezpečení Enterprise Identity Mapping

Verze 6, vydání 1

System i

Zabezpečení
Enterprise Identity Mapping

Verze 6, vydání 1

Poznámka

Před použitím těchto informací a produktu, který podporují, si prostudujte informace obsažené v tématu "Poznámky", na stránce 123.

Toto vydání se vztahuje na verzi 6, vydání 1, modifikaci 0 operačního systému IBM i5/OS (číslo produktu 5761–SS1)a na všechna následující vydání a modifikace, dokud nebude v nových vydáních uvedeno jinak. Tato verze nepracuje na modelech RISC (reduced instruction set computer) ani na modelech CISC.

Obsah

Enterprise Identity Mapping 1
Co je nového ve verzi V6R1 1
Soubor PDF pro EIM (Enterprise Identity Mapping) . . . 2
Přehled o produktu EIM 2
Koncepce produktu EIM 4
Řadič domény EIM 6
Doména EIM 6
Identifikátor EIM 8
Definice registru EIM 11
Definice systémových registrů 13
Definice aplikačních registrů 14
Definice skupinového registru 15
Přidružení EIM. 16
Vyhledávací informace 16
Přidružení identifikátorů 17
Přidružení zásad 21
Předvolené přidružení zásad domény 21
Předvolené přidružení zásad registru 23
Přidružení zásad filtru certifikátů 24
Vyhledávací operace EIM 26
Příklady vyhledávací operace: Příklad 1 29
Příklady vyhledávací operace: Příklad 2 30
Příklady vyhledávací operace: Příklad 3 32
Příklady vyhledávací operace: Příklad 4 34
Příklady vyhledávací operace: Příklad 5 35
Podpora a povolení zásad mapování EIM 37
Kontrola přístupu k EIM 38
Skupina kontroly přístupu k EIM: Oprávnění rozhraní API 41
Skupina kontroly přístupu k EIM: Oprávnění k úlohám EIM 43
Koncepce LDAP pro EIM 45
Rozlišovací jméno 46
Nadřazené rozlišovací jméno 47
Schéma LDAP a další pokyny týkající se EIM . . 47
Koncepce EIM pro i5/OS. 48
Pokyny pro EIM týkající se uživatelských profilů v systému i5/OS 48
Monitorování EIM v operačním systému i5/OS . . 50
Aplikace operačního systému i5/OS podporující EIM 50
Scénáře: EIM (Enterprise Identity Mapping) 50
Plánování EIM 50
Plánování EIM pro eServer 51
Požadavky nastavení EIM (Enterprise Identity Mapping) pro eServer 51
Identifikace potřebných dovedností a rolí 52
Plánování domény EIM (Enterprise Identity Mapping) 54
Plánování řadiče domény EIM (Enterprise Identity Mapping) 55
Vytvoření plánu pojmenování definice registru EIM (Enterprise Identity Mapping) 58
Vytvoření plánu mapování totožností 59
Plánování přidružení EIM (Enterprise Identity Mapping) 59
Vytvoření plánu pojmenování identifikátoru EIM 62
Pracovní formuláře pro implementaci EIM (Enterprise Identity Mapping) 63
Plánování vývoje aplikací EIM (Enterprise Identity Mapping) 65
Plánování EIM pro operační systém i5/OS 65
Nezbytné předpoklady instalace EIM (Enterprise Identity Mapping) pro systém i5/OS 66
Instalace požadovaných voleb produktu System i Navigator 66
Pokyny týkající se zálohování a obnovy EIM . . . 67
Zálohování a obnova dat domény EIM. . . . 67
Zálohování a obnova dat domény EIM. . . . 67
Konfigurace EIM 68
Vytvoření a vstup do nové lokální domény 69
Dokončení konfigurace EIM pro doménu 72
Vytvoření a vstup do nové vzdálené domény 73
Dokončení konfigurace EIM pro doménu 77
Vstup do existující domény 78
Dokončení konfigurace EIM pro doménu 82
Konfigurace zabezpečeného připojení k řadiči domény EIM 83
Správa EIM. 83
Správa domén EIM 84
Přidání domény EIM do složky Správa domén . . 84
Připojení k doméně EIM 84
Povolení přidružení zásad pro doménu 85
Testování mapování EIM. 85
Práce s výsledky testování a řešení problémů . . 86
Odstranění domény EIM ze složky Správa domén 88
Výmaz domény EIM a všech objektů konfigurace 88
Správa definic registrů EIM 88
Přidání definice systémového registru 89
Přidání definice aplikačního registru 89
Přidání definice skupinového registru 90
Přidání jména alias do definice registrů 90
Definice typu registru soukromého uživatele v EIM 91
Povolení podpory vyhledávání mapování a použití přidružení zásad pro cílový registr 92
Výmaz definice registru 93
Odstranění jména alias z definice registru 94
Přidání člena do definice skupinového registru . . 94
Správa identifikátorů EIM 95
Vytvoření identifikátoru EIM 95
Přidání jména alias do identifikátoru EIM 95
Odstranění jména alias z identifikátoru EIM . . . 96
Výmaz identifikátoru EIM 97
Přizpůsobení zobrazení identifikátorů EIM . . . 97
Správa přidružení EIM 97
Vytváření přidružení EIM 98
Vytvoření přidružení identifikátorů EIM . . . 98
Vytvoření přidružení zásad 99
Přidání vyhledávací informace k totožnosti cílového uživatele 105
Přidání vyhledávacích informací do totožnosti cílového uživatele v přidružení identifikátorů . 106

Přidání vyhledávacích informací do totožnosti cílového uživatele v přidružení zásad 106
Odstranění vyhledávací informace z totožnosti cílového uživatele 107
Odstranění vyhledávací informace pro totožnost cílového uživatele v přidružení identifikátorů . 107
Zobrazení všech přidružení identifikátorů pro identifikátor EIM. 109
Zobrazení všech přidružení zásad pro doménu . . 109
Zobrazení všech přidružení zásad pro definici registru. 110
Výmaz přidružení identifikátorů 110
Výmaz přidružení zásad. 111
Správa řízení přístupu uživatelů k EIM 112
Správa konfiguračních vlastností EIM 113
Odstraňování problémů s EIM 114
Odstraňování problémů s připojením k řadiči domény 114
Odstraňování všeobecných problémů s konfigurací a doménou EIM 115
Odstraňování problémů s mapováním EIM 117
Rozhraní API EIM 120
Informace související s EIM 121

Dodatek. Poznámky. 123
Ochranné známky 124
Ustanovení a podmínky 125

Enterprise Identity Mapping

Produkt EIM (Enterprise Identity Mapping) pro systém System i je implemetací i5/OS infrastruktury IBM, která administrátorům a vývojářům aplikací umožňuje vyřešit problém správy více registrů uživatelů v rámci celého podniku.

Většina podniků využívajících sítě čelí problémům s vícenásobnými registry uživatelů, což vyžaduje, aby měla každá osoba nebo entita v rámci podniku vlastní totožnost uživatele v každém z registrů. Potřeba vícenásobných registrů uživatelů však v konečném důsledku znamená rozsáhlé administrační problémy, které negativně ovlivňují jak uživatele, tak administrátory a také vývojáře aplikací. Produkt EIM (Enterprise Identity Mapping) poskytuje řešení pro jednodušší správu více uživatelských registrů a totožností uživatele ve vašem podniku. Toto řešení je navíc efektivní z hlediska nákladů.

Produkt EIM vám umožňuje vytvořit systém mapování totožností, nazývaný přidružení, mezi různými totožnostmi uživatele v různých registrech uživatelů, které se vztahují k jedné osobě ve vašem podniku. EIM také poskytuje běžnou sadu rozhraní API, která je možné používat na různých platformách k vytváření aplikací, které mohou využívat vytvořená mapování totožností k hledání vztahů mezi totožnostmi. Kromě toho můžete EIM použít ve spojení se službou ověření v síti, což je implementace produktu Kerberos v rámci systému i5/OS, a nastavit tak v systému prostředí s jediným přihlášením.

EIM je možné nakonfigurovat a spravovat prostřednictvím produktu System i Navigator, který je grafickým uživatelským rozhraním systému System i. Systém System i používá EIM k povolení rozhraní i5/OS k ověření uživatelů prostřednictvím služby síťového ověření. Aplikace, stejně jako operační systém i5/OS, mohou přijímat tikety protokolu Kerberos a využívat tak EIM k nalezení uživatelského profilu, který představuje stejnou osobu, jež je reprezentována tiketem protokolu Kerberos.

Více informací o tom, jak EIM pracuje i o jeho koncepcích, které vám mohou pomoci při využití EIM ve vašem podniku, naleznete v následujících tématech:

Co je nového ve verzi V6R1

Seznamte se s novými nebo významně změněnými informacemi v kolekci témat produktu EIM (Enterprise Identity Mapping).

Nové nebo vylepšené funkce produktu EIM

- V předchozích vydáních operačního systému i5/OS produkt EIM podporoval pouze mapování na jednu totožnost lokálního uživatele pro systém. V operačním systému i5/OS verze V6R1, produkt EIM podporuje výběr vícenásobného mapování totožností lokálního uživatele pro daný systém.

Kromě toho bylo aktualizováno téma jediné přihlášení a nyní poskytuje dokumentaci o implementaci produktu EIM jakožto součásti prostředí jediného přihlášení za účelem snížení objemu správy hesel. Toto téma poskytuje množství detailních scénářů zaměřených na běžné situace spojené s jediným přihlášením spolu s podrobnými instrukcemi pro jejich implementaci.

Informace o změnách a novinkách

Jako pomůcku při hledání informací o technických změnách použijte následující informace:

- Značka » označuje, kde nové či změněné informace začínají.
- Značka « označuje, kde nové či změněné informace končí.

Více informací o novinkách a změnách v tomto vydání naleznete v dokumentu Sdělení pro uživatele.

Soubor PDF pro EIM (Enterprise Identity Mapping)

Můžete si zobrazit a vytisknout soubor PDF s těmito informacemi.

Chcete-li si prohlédnout nebo stáhnout verzi ve formátu PDF, vyberte odkaz EIM (Enterprise Identity Mapping) (zhruba 1820 KB).

Kterýkoli z těchto dokumentů ve formátu PDF si můžete zobrazit nebo stáhnout:

- Network authentication services (asi 1398 KB) obsahuje informace o tom, jak nakonfigurovat službu síťového ověření ve spojení s EIM za účelem vytvoření prostředí jediného přihlášení.
- IBM Tivoli Directory Server for i5/OS (LDAP) (asi 1700 KB) obsahuje informace o rozšířené konfiguraci LDAP spolu s informacemi o konfiguraci serveru LDAP, který může být použit jako řadič domény.

Uložení souborů ve formátu PDF

Chcete-li uložit soubory ve formátu PDF na vaší pracovní stanici za účelem jejich prohlížení nebo tisku, postupujte takto:

1. Klepněte pravým tlačítkem myši na odkaz PDF ve vašem prohlížeči.
2. Klepněte na volbu, která uloží lokálně soubor PDF.
3. Vyberte místo v adresáři, kam si přejete soubor PDF uložit.
4. Klepněte na **Uložit**.

Stažení produktu Adobe Reader

Chcete-li zobrazovat či tisknout soubory ve formátu PDF, musíte mít nainstalovaný produkt Adobe Reader ve vašem systému. Jeho bezplatnou kopii si můžete stáhnout z webových stránek společnosti Adobe

(www.adobe.com/products/acrobat/readstep.html) .

Přehled o produktu EIM

EIM vám pomůže vyřešit problémy, které se vyskytují při správě více než jednoho uživatelského registru.

Dnešní síťová prostředí se skládají ze složitých skupin systémů a aplikací, což vyžaduje v konečném důsledku správu stále více a více registrů uživatelů. Právě problematika registrů uživatelů se stává docela závažným administračním problémem, který má vliv na jednotlivé uživatele, administrátory a samozřejmě také na vývojáře aplikací. Proto se dnes stále více společností zabývá novými technologiemi ověření a autorizace pro jednotlivé systémy a aplikace. EIM umožňuje administrátorům a vývojářům aplikací vyrovnávat se s těmito problémy daleko snadněji a s nižšími náklady, než kdy předtím.

Následující informace vám přiblíží problém současných přístupů a vysvětlí vám, proč je právě přístup EIM lepší než ostatní.

Problematika správy více registrů uživatelů

Většina administrátorů spravuje sítě, které zahrnují odlišné systémy a servery. Každý z těchto systémů či serverů si pak žádá jedinečný způsob správy různých registrů uživatelů. V těchto složitých sítích jsou administrátoři zodpovědni za správu každé totožnosti uživatele a každého jednotlivého hesla. Navíc administrátoři musí často tyto totožnosti a hesla synchronizovat. Uživatelé jsou zase zatěžováni tím, že si musí pamatovat mnoho totožností a hesel a uchovávat je synchronizované. Režijní náklady administrátorů a uživatelů jsou v tomto prostředí značné. V důsledku toho musí administrátoři vynakládat množství cenného času na řešení nepovedených pokusů o přihlášení a na opětovné nastavování zapomenutých hesel místo toho, aby se věnovali správě podniku.

Problém se správou více registrů uživatelů má také vliv na vývojáře aplikací, kteří se snaží vyvíjet vícevrstvé a heterogenní aplikace. Vývojáři rozumí tomu, že zákazníci mají svá data rozmístěná na velkém počtu odlišných typů

systémů, kde každý systém má své vlastní registry uživatelů. Proto pak musejí vytvářet chráněné registry uživatelů a přidružené sémantiky zabezpečení pro své aplikace. I když se tímto částečně vyřeší problém pro vývojáře aplikací, zvyšuje se tím režie pro administrátory a uživatele.

Současné přístupy

Některé současné přístupy ostatních společností k řešení problémů s vícenásobnými registry uživatelů jsou již dostupné, avšak všechny tyto přístupy nepřinášejí řešení, které by mohlo kompletně odstranit tento problém. Tak například LDAP (Lightweight Directory Access Protocol) poskytuje distribuované řešení registrů uživatelů. Avšak používání LDAP (nebo dalších v současnosti populárních produktů, jako je například Microsoft Passport) pro administrátora znamená, že musí spravovat ještě další registr uživatelů a sémantiku zabezpečení, nebo musí dokonce nahradit stávající aplikace, které byly vytvořeny pro používání těchto registrů.

Díky tomuto řešení administrátor stále musí spravovat několik bezpečnostních mechanismů pro individuální prostředky, čímž ale narůstá administrační režie a potenciálně se také zvyšuje pravděpodobnost vzniku bezpečnostních rizik. V případě, že vícenásobný mechanismus podporuje jediný prostředek, zvyšuje se šance na provedení změny oprávnění pomocí jednoho mechanismu a následné opomenutí změny oprávnění v jednom či více jiných mechanismů. Bezpečnostní riziko může například nastat v případě, je-li uživateli odmítnut přístup přes jedno prostředí, ale tento přístup je pak následně povolen přes jedno nebo více jiných prostředí.

Po dokončení této práce administrátoři zjistí, že opravdu daný problém celkově nevyřešili. Je všeobecně známé, že jednotlivé podniky již investovaly spoustu peněz do současných registrů uživatelů a k nim přidružených sémantik zabezpečení se snahou praktického využití těchto postupů. Vytvoření dalšího registru uživatelů a přidružené sémantiky zabezpečení řeší tento problém pro poskytovatele aplikací, nikoliv však už pro uživatele nebo administrátory.

Dalším možným řešením je využití prostředí jediného přihlášení. Několik dostupných produktů umožňuje administrátorům spravovat soubory, které obsahují všechny totožnosti uživatele a všechna hesla. Avšak tento přístup má také několik slabin:

- Tento přístup řeší pouze jeden zásadní problém, kterému musí uživatelé čelit. Ačkoliv je uživatelům sice umožněno přihlásit se do několika systémů zadáním jediné totožnosti a hesla, nevylučuje to u uživatele nutnost mít hesla do ostatních systémů, ani nutnost tato hesla spravovat.
- To vytváří další bezpečnostní riziko, jelikož jsou v těchto souborech uložena hesla jako čistý text nebo dešifrovatelná hesla. Hesla by nikdy neměla být uložena v souborech s čistým textem, ani být snadno přístupna každému, včetně administrátorů.
- Zmíněny přístup také neřeší problematiku vývojářů aplikací třetích stran, kteří vytvářejí heterogenní, vícevrstvé aplikace. Vývojáři stále musejí svým aplikacím poskytovat chráněné registry uživatelů.

I přes tyto zjevné nedostatky si podniky přesto vybírají některé z výše uvedených přístupů, protože tyto poskytují alespoň částečné řešení zmiňované problematiky více registrů uživatelů.

Přístup produktu EIM

Produkt EIM nabízí zcela nový přístup k jednotlivým problémům s cílem mnohem jednodušší správy více registrů uživatelů a totožností uživatele ve vícevrstvém a heterogenním prostředí. Produkt EIM je architekturou pro popis vztahů v podniku mezi jednotlivci nebo entitami (jako jsou třeba souborový server a tiskový server) a mezi mnoha totožnostmi, které je v podniku reprezentují. EIM navíc poskytuje balík rozhraní API, který umožňuje aplikacím klást otázky na tyto zmiňované vztahy.

Pokud jde o totožnost uživatele určité osoby v jednom registru uživatelů, můžete například určit, která totožnost uživatele v jiném registru reprezentuje tutéž osobu. Pokud je uživatel ověřován s jedinou totožností uživatele, můžete mapovat tuto totožnost uživatele na odpovídající totožnost v jiném registru uživatelů a uživatel již nemusí znovu poskytovat kredit pro ověření. Vy víte, kdo je uživatelem, a potřebujete pouze vědět, která totožnost uživatele reprezentuje tohoto uživatele v jiném registru uživatelů. Proto EIM poskytuje funkci všeobecného mapování totožností v daném podniku.

EIM umožňuje mapování totožností jeden-na-mnoho (jinak řečeno, jediný uživatel s více než jednou totožností uživatele v jediném registru uživatelů). Avšak administrátor nemusí mít specifické individuální mapování pro veškeré totožnosti uživatele v registru uživatelů. EIM také umožňuje mapování typu mnoho-na-jeden (jinými slovy, mapování více uživatelů směrem k jediné totožnosti uživatele v jediném registru uživatelů).

Schopnost mapování mezi jednotlivými totožnostmi uživatele v různých registrech uživatelů přináší mnoho výhod. Primárně jde především o to, že aplikace získají značnou flexibilitu, neboť mohou používat jeden registr uživatelů k ověření a zcela odlišný registr uživatelů k autorizaci. Administrátor by tak například mohl mapovat totožnost uživatele Windows v registru Kerberos na některý uživatelský profil i5/OS v jiném registru uživatelů, aby získal přístup k prostředkům i5/OS, pro které je uživatelský profil i5/OS autorizován.

EIM je otevřenou architekturou, kterou mohou administrátoři používat pro reprezentaci vztahů mapování totožností pro jakýkoliv registr. Nevyžaduje se kopírování existujících dat do nové schránky, ani úsilí o zachování synchronizace kopií. Jediná nová data, která EIM přináší, jsou informace o jednotlivých vztazích. EIM ukládá tyto data v adresáři LDAP, což poskytuje flexibilitu při správě těchto dat na jednom místě a umožňuje vytvářet kopie, kdekoliv je daná informace používána. V konečném důsledku EIM přináší podnikům a vývojářům aplikací flexibilitu a jednodušší práci v široké škále jednotlivých prostředí s daleko menšími náklady, než by vůbec kdy bylo možné dosáhnout bez takovéto podpory.

Produkt EIM používaný ve spojení se službou síťového ověření, tj. i5/OS implementací protokolu Kerberos poskytuje řešení pro jediné přihlášení. Aplikace mohou být napsány tak, aby používaly rozhraní API GSS a API EIM k potvrzení tiketu Kerberos a prováděly mapování na jinou, přidruženou totožnost uživatele v jiném registru uživatelů. Přidružení mezi uživatelskými totožnostmi, která umožňují toto mapování totožností, mohou být dosažena pomocí vytvoření přidruženého identifikátoru, který nepřímo přidružuje jednu totožnost uživatele k jiné přes identifikátor EIM nebo pomocí vytvoření přidružení zásad, které přímo přidružují jednu totožnost uživatele ve skupině k jediné specifické totožnosti uživatele.

Používání mapování totožností vyžaduje, aby administrátor provedl následující úkoly:

1. Nakonfigurovat doménu EIM v síti. Použijte průvodce konfigurací EIM a vytvořte řadič domény pro doménu a nakonfigurujte přístup k doméně. Pokud budete používat průvodce, můžete také vytvořit novou doménu EIM a vytvořit tak řadiče domény v lokálním nebo vzdáleném systému. Pokud doména EIM již existuje, můžete vybrat účast v existující doméně EIM.
2. Určete, kterým uživatelům (definovaným na serveru adresářů, který funguje jako hostitel pro řadič domény EIM) bude umožněna správa nebo přístup ke specifickým informacím v doméně EIM, a přiřaďte dané uživatele ke skupinám kontroly přístupu.
3. Vytvořte definice registrů EIM pro ty registry uživatelů, které budou účastny v doméně EIM. Ačkoli můžete definovat jakýkoliv registr uživatelů v doméně EIM, musíte také definovat registry uživatelů pro aplikace a operační systémy podporující EIM.
4. Na základě vašich potřeb implementace EIM určete, které z následujících úkolů provedete za účelem dokončení vaší konfigurace EIM:
   - Vytvoření identifikátorů EIM v doméně pro každého jedinečného uživatele a vytvoření přidružení identifikátorů pro tyto uživatele.
   - Vytvoření přidružení zásad.
   - Vytvoření kombinace těchto možností.

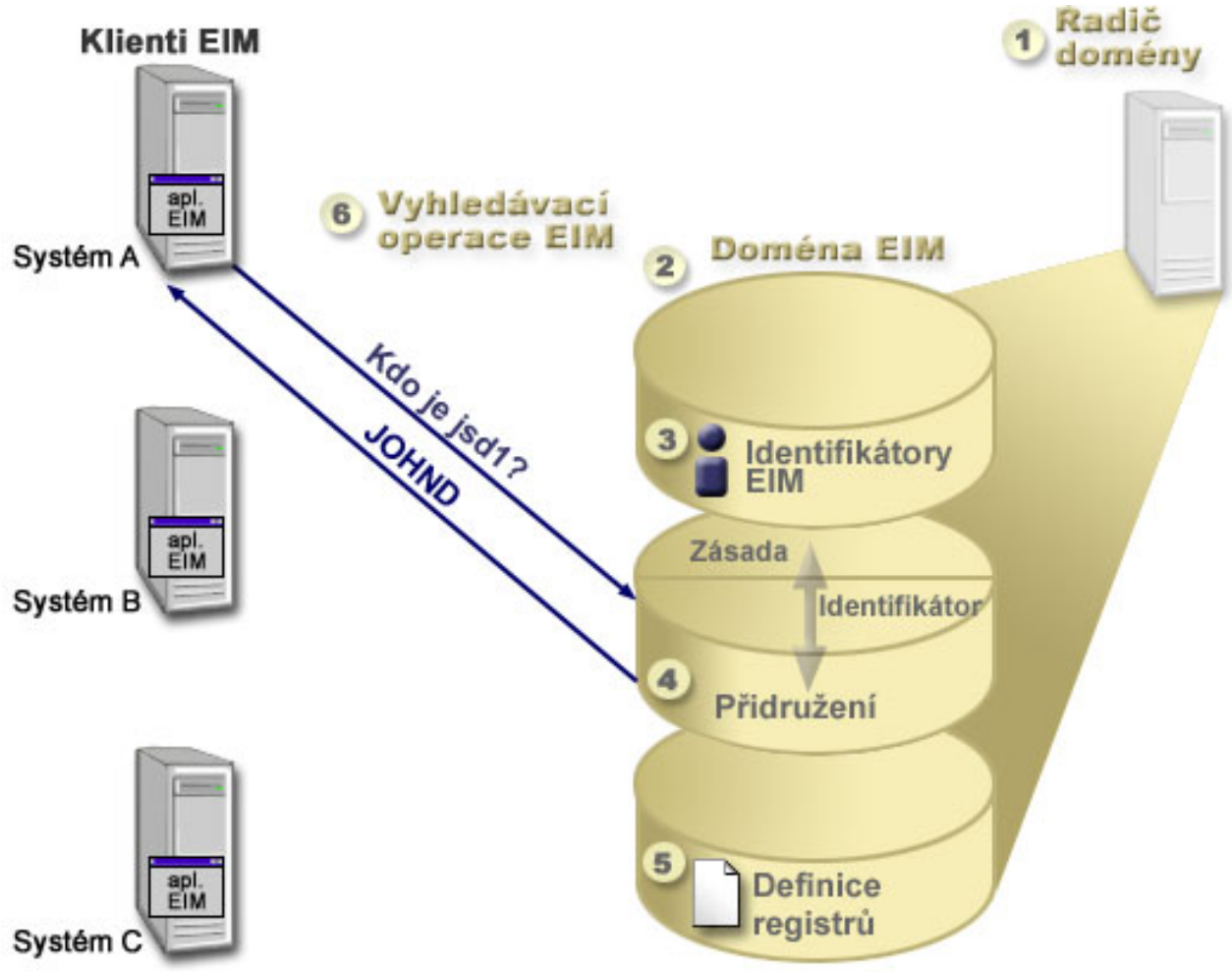
Související informace

Přehled jediného přihlášení

Koncepce produktu EIM

Abyste byli schopni celkově porozumět využití produktu EIM (Enterprise Identity Mapping) v rámci vašeho podniku, je nezbytné, abyste pochopili koncepce jeho fungování. Ačkoli se konfigurace a implementace pro určitá rozhraní API EIM může na jednotlivých platformách serverů lišit, jsou koncepce produktu EIM společné pro platformy IBM eServer.

Obrázek č. 1 ilustruje jeden příklad implementace EIM v podniku. Tři servery fungují jako klienti EIM a obsahují aplikace využívající EIM, které vyžadují data EIM pomocí vyhledávacích operací EIM 6 . Řadič domény 1 ukládá informace o doméně EIM 2 , která obsahuje identifikátor EIM 3 , přidružení 4 mezi těmito identifikátory EIM a uživatelskými totožnostmi a definicemi registrů EIM 5 .



Obrázek 1. Příklad implementace produktu EIM.

Více informací o koncepcích EIM eServer naleznete pod následujícími odkazy:

Související pojmy

“Koncepce LDAP pro EIM” na stránce 45
Produkt EIM využívá server LDAP jako řadič domény pro ukládání dat EIM. Je proto nutné, abyste dobře pochopili koncepce LDAP, které se vztahují přímo ke konfiguraci a používání EIM ve vašem podniku. Rozlišovací jméno LDAP můžete například používat jako totožnost uživatele pro konfiguraci EIM a pro ověření k řadiči domény EIM.

“Koncepce EIM pro i5/OS” na stránce 48
Produkt EIM můžete implementovat na jakékoliv platformě IBM eServer. Budete-li však implementovat produkt EIM v systému System i, měli byste znát určité informace, které jsou specifické pro implementaci v systému System i.

Řadič domény EIM

Doména EIM je server LDAP (Lightweight Directory Access Protocol), který je konfigurován pro správu jedné nebo více domén EIM. Doména EIM obsahuje všechny EIM identifikátory, přidružení EIM a uživatelské registry, které jsou definovány v doméně. Systémy (klienti EIM) se účastní domény tím způsobem, že používají data domény pro vyhledávací operace EIM.

V současné době můžete nakonfigurovat produkt IBM Tivoli Directory Server for i5/OS na některé platformy IBM eServer jako řadič domény EIM. Jakýkoliv systém podporující rozhraní API EIM se může účastnit domény jako klient. Tyto klientské systémy používají rozhraní API EIM ke kontaktu s řadičem domény EIM, aby mohly provádět vyhledávací operace. Umístění klienta EIM určuje, zda je řadič domény lokálním nebo vzdáleným systémem. Řadič domény je *lokální*, když je klient EIM spuštěný ve stejném systému jako řadič domény. Řadič domény je *vzdálený*, je-li klient EIM spuštěn v samostatném systému, jiném než je systém řadiče domény.

Poznámka: Pokud plánujete konfigurovat server adresářů ve vzdáleném systému, musí tento server adresářů poskytovat podporu pro EIM. EIM požaduje, aby server adresářů podporující LDAP (Lightweight Directory Access Protocol) verze 3 fungoval jako hostitel pro tento řadič domény. Dále musí být také tento server adresářů nakonfigurován tak, aby akceptoval schémata EIM. Produkt IBM Tivoli Directory Server for i5/OS poskytuje tuto podporu.

Související pojmy

"Vyhledávací operace EIM" na stránce 26
Aplikace nebo operační systém využívají rozhraní API EIM k provedení vyhledávací operace tak, aby aplikace nebo operační systém mohly provádět mapování od jedné totožnosti uživatele v jednom registru na další totožnost uživatele v jiném registru. Vyhledávací operace EIM je proces, kdy pomocí zadání některých známých a důvěryhodných informací aplikace nebo operační systém vyhledá neznámé přidružení totožnosti uživatele v daném cílovém registru.

"Schéma LDAP a další pokyny týkající se EIM" na stránce 47
Tyto informace použijte, chcete-li se dozvědět, co je třeba k tomu, aby server adresářů fungoval s produktem EIM (Enterprise Identity Mapping).

Doména EIM

Doména EIM je adresář v rámci serveru LDAP (Lightweight Directory Access Protocol), který obsahuje podniková data.

Doména EIM je kolekcí nejen všech identifikátorů EIM, veškerých přidružení EIM a všech registrů uživatelů, které jsou definovány v doméně, ale rovněž kontroly přístupu k těmto datům. Systémy (klienti EIM) se účastní domény tím způsobem, že používají data domény pro vyhledávací operace EIM.

Doména EIM je však odlišná od registru uživatelů. Registr uživatelů definuje sadu totožností uživatele známých a důvěryhodných na dané úrovni aplikace nebo operačního systému. Registr uživatelů obsahuje také potřebnou informaci pro ověření uživatele dané totožnosti. Navíc registr uživatelů obsahuje často některé další atributy, jako například preference uživatele, oprávnění systémů nebo také osobní informace pro danou totožnost.

Doména EIM se tedy *vztahuje* k totožnostem uživatele, které jsou definovány v registru uživatelů. Doména EIM obsahuje především informace o *vztazích* mezi totožnostmi v různých registrech uživatelů (uživatelské jméno, typ registru, instance registru) a mezi skutečnými lidmi nebo entitami, které tyto totožnosti reprezentují.

Obrázek č. 2 ukazuje data, která jsou uložena v rámci domény EIM. Tato data zahrnují identifikátory EIM, definice registrů EIM a jednotlivá přidružení EIM. Data EIM definují vztahy mezi totožnostmi uživatele a lidmi či entitami, které v podniku tyto totožnosti reprezentují.

Obrázek 2. Doména EIM a data uložená v doméně.

Data EIM zahrnují:

Definice registru EIM

Každá vytvořená definice registru představuje skutečný registr uživatelů (včetně informace o totožnosti uživatele), který existuje v systému v rámci podniku. Jakmile nadefinujete daný registr uživatelů v EIM tak, aby tento registr uživatelů mohl být součástí domény EIM, budete moci vytvořit dva typy definic registrů. Jeden typ se bude vztahovat k registrům uživatelů systému a druhý typ se pak bude vztahovat k uživatelům aplikačních registrů.

Identifikátory EIM

Každý vytvořený identifikátor EIM reprezentuje v rámci podniku jednoznačně danou osobu nebo entitu (jako je například tiskový server nebo souborový server). Pokud si přejete mít mapování typu jeden-na jeden mezi totožnostmi uživatele patřící osobě nebo entitě, můžete vytvořit identifikátor EIM, jež bude odpovídat právě dané osobě nebo určité entitě.

Přidružení EIM

Vytvořené přidružení EIM bude reprezentovat vztahy mezi totožnostmi uživatele. Musíte však definovat přidružení tak, aby klienti EIM mohli používat rozhraní API EIM k úspěšnému provádění vyhledávacích operací EIM. Tyto vyhledávací operace EIM pak vyhledávají pro definovaná přidružení doménu EIM. Existují dva různé typy přidružení, které je možné vytvořit:

Přidružení identifikátorů

Přidružení identifikátorů vám umožní definovat vztah jeden-na-jeden mezi totožnostmi uživatele přes identifikátor EIM definovaný pro jednotlivce. Každé vytvořené přidružení identifikátorů EIM reprezentuje jediný, specifický vztah mezi identifikátorem EIM a přidruženou totožností uživatele v rámci podniku. Přidružení identifikátorů poskytne informace, které vytvoří vazbu mezi identifikátorem EIM a určitou totožností uživatele v daném registru uživatelů, a umožní vám tak vytvořit pro uživatele mapování totožnosti typu jeden-na-jeden. Přidružení totožností jsou potřebná především tehdy, když mají jednotlivci totožnosti uživatele se zvláštními oprávněními a dalšími právy a vy je chcete výslovně řídit vytvořením mapování typu jeden-na-jeden mezi totožnostmi uživatele.

Přidružení zásad

Přidružení zásad vám umožní definovat vztahy mezi skupinou totožností uživatele v jednom či více registrech uživatelů a jedinou totožností uživatele v jiném registru uživatelů. Každé vytvořené přidružení zásad EIM má za následek mapování typu mnoho-na-jeden mezi zdrojovou skupinou totožností uživatele v jednom registru uživatelů a jednotlivou totožností cílového uživatele. Obvykle se přidružení zásad vytváří kvůli mapování skupiny uživatelů se stejnými požadavky na úroveň oprávnění pro jednotlivou totožnost uživatele s tímto oprávněním.

Související pojmy

"Definice registru EIM" na stránce 11
Definice registru EIM je záznam v rámci produktu EIM, který můžete vytvořit za účelem reprezentace aktuálního registru uživatelů, jenž se nachází v systému daného podniku. Registr uživatelů funguje jako adresář a obsahuje seznam platných totožností uživatele pro určitý systém nebo aplikaci.

"Identifikátor EIM"
Identifikátor EIM představuje v podniku určitou osobu či entitu. Typická síť se skládá z různých hardwarových platforem, aplikací a jejich přidružených registrů uživatelů. Většina platforem a také většina aplikací používá registry uživatelů specifické pro platformy nebo pro aplikace. Tyto registry uživatelů pak pro uživatele, kteří pracují se servery a aplikacemi, obsahují veškeré informace ohledně jejich identifikace.

"Vyhledávací operace EIM" na stránce 26
Aplikace nebo operační systém využívají rozhraní API EIM k provedení vyhledávací operace tak, aby aplikace nebo operační systém mohly provádět mapování od jedné totožnosti uživatele v jednom registru na další totožnost uživatele v jiném registru. Vyhledávací operace EIM je proces, kdy pomocí zadání některých známých a důvěryhodných informací aplikace nebo operační systém vyhledá neznámé přidružení totožnosti uživatele v daném cílovém registru.

Identifikátor EIM

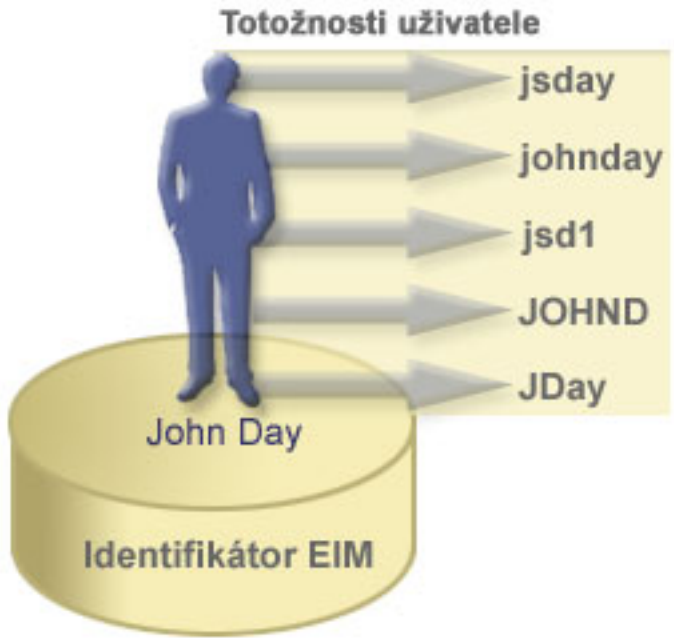
Identifikátor EIM představuje v podniku určitou osobu či entitu. Typická síť se skládá z různých hardwarových platforem, aplikací a jejich přidružených registrů uživatelů. Většina platforem a také většina aplikací používá registry uživatelů specifické pro platformy nebo pro aplikace. Tyto registry uživatelů pak pro uživatele, kteří pracují se servery a aplikacemi, obsahují veškeré informace ohledně jejich identifikace.

Chcete-li vytvořit jedinečné identifikátory pro osoby nebo pro entity ve vašem podniku, můžete využít možností nabízených produktem EIM. Můžete vytvořit přidružení identifikátorů nebo mapování totožnosti typu jeden-na-jeden mezi identifikátory EIM a různými totožnostmi uživatele, jež právě tyto identifikátory reprezentují. Tento proces vám tak značně usnadní výstavbu heterogenních a vícevrstvých aplikací. Tak bude i mnohem snazší vystavět a používat nástroje usnadňující nutnou administraci a správu každé totožnosti uživatele, kterou má každá osoba či entita v rámci podniku.

Identifikátor EIM reprezentující osobu

Na obrázku č. 3 můžete vidět příklad identifikátoru EIM, který představuje osobu jmenující se *John Day*, a jeho různé totožnosti v rámci podniku. V tomto případě má osoba *John Day* pět totožností ve čtyřech různých registrech uživatelů johnday, jsd1, JOHND, jsday a JDay.

Obrázek č. 3: Vztah mezi identifikátorem EIM pro osobu jmenující se *John Day* a jeho různými totožnostmi uživatele.

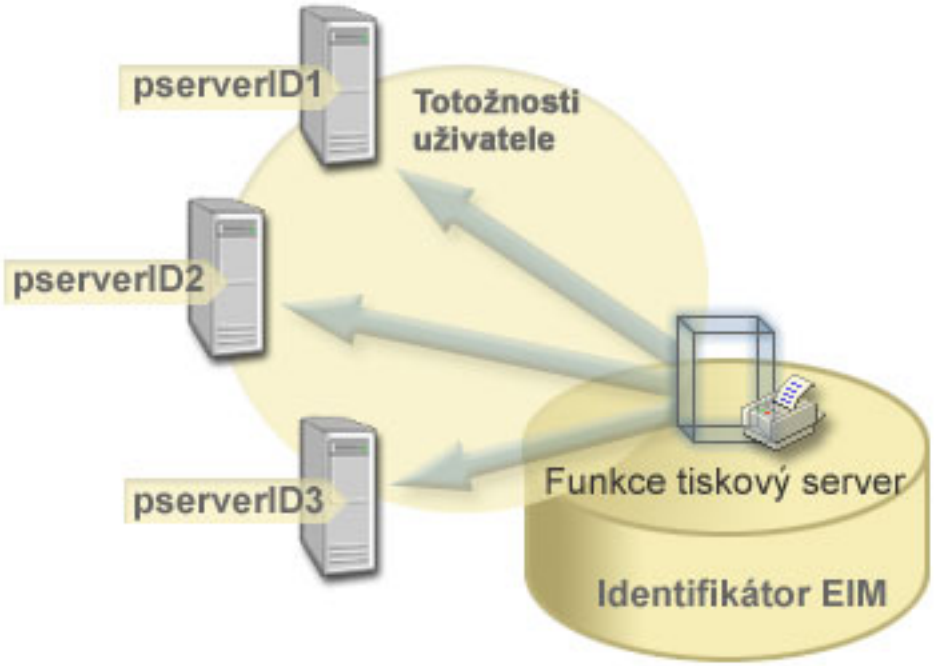


V EIM je možné vytvořit přidružení, která definují vztah mezi identifikátorem John Day a mezi každou z odlišných totožností uživatele pro osobu se jménem *John Day*. Vytvořením přidružení za účelem definování těchto vztahů můžete vy i ostatní zapisovat dané aplikace, které budou používat jednotlivá rozhraní API EIM pro vyhledávání potřebné, ale neznámé totožnosti uživatele založené na určité známé totožnosti uživatele.

Identifikátor reprezentující entitu

Kromě reprezentace uživatele mohou identifikátory EIM ve vašem podniku také reprezentovat určité entity (obrázek č. 4). Často například jde právě o funkci serveru tiskáren, která v podniku funguje ve více systémech. Na obrázku č. 4 funkce serveru tiskáren funguje ve třech různých systémech pod třemi různými totožnostmi uživatele pserverID1, pserverID2 a pserverID3.

Obrázek č. 4: Vztah mezi identifikátorem EIM, který reprezentuje funkci serveru tiskáren, a různými totožnostmi uživatele pro tuto funkci.



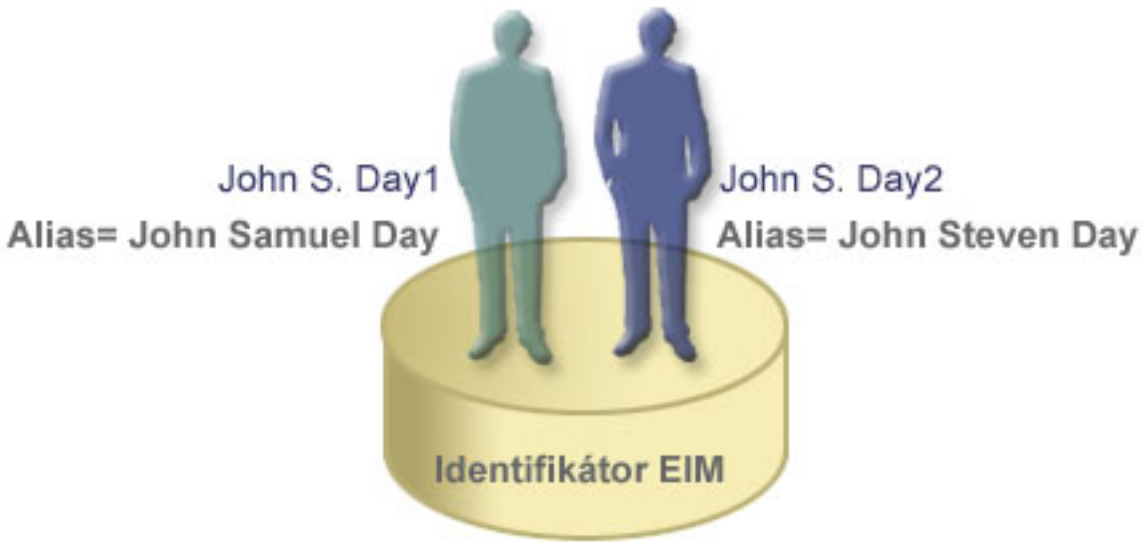
Pomocí EIM je možné vytvořit jeden identifikátor, který bude v celém podniku reprezentovat funkci serveru tiskáren. Jak příklad dokazuje, identifikátor EIM Funkce serveru tiskáren reprezentuje v podniku skutečnou entitu funkce serveru tiskáren. Přidružení jsou zde vytvořena za účelem definování vztahů mezi identifikátorem EIM (Funkce serveru tiskáren) a každou z totožností uživatele pro tuto funkci (pserverID1, pserverID2 a pserverID3). Tato přidružení umožňují vývojářům aplikací používat vyhledávací operace EIM k nalezení určité funkce serveru tiskáren. Poskytovatele aplikací pak mohou daleko snadněji zapisovat distribuované aplikace, které mnohem snadněji spravují funkci serveru tiskáren v celém podniku.

Identifikátory EIM a přiřazování jmen alias

Jména identifikátorů EIM musí být v rámci domény EIM jedinečná. Aliasy mohou být nápomocny tam, kde by používání jedinečných jmen mohlo být komplikované. Příkladem užitečnosti jmen alias identifikátorů EIM je situace, kdy jsou některá oficiální jména odlišná od jména, pod kterým je určitá osoba známa. Někdy mohou mít v podniku některé osoby stejné jméno, což může být v případě využívání vlastních jmen jako identifikátorů EIM matoucí.

Obrázek č. 5 ilustruje příklad, ve kterém se nachází v podniku stejné uživatelské jméno *John S. Day*. Administrátor pro jejich rozlišení vytvoří dva odlišné identifikátory EIM John S. Day1 a John S. Day2. To, který *John S. Day* je reprezentován jedním z těchto identifikátorů, však není ihned zřejmé.

Obrázek č. 5: Aliasy pro dva identifikátory EIM založené na sdíleném vlastním jménu *John S. Day*.



Využitím jmen alias může administrátor EIM poskytnout další informace o jednotlivcích zvlášť pro každý identifikátor EIM. Každý identifikátor EIM pak následně může mít za účelem identifikace toho, který *John S. Day* reprezentuje jaký identifikátor EIM, i více jmen alias. Další dodatečné jméno alias může například obsahovat zaměstnanecké číslo uživatele, číslo oddělení, pracovní titul nebo nějaký další rozlišovací atribut. V tomto případě: jméno alias pro John S. Day1 by mohlo být John Samuel Day a jméno alias pro John S. Day2 by mohl být John Steven Day.

Jméno alias můžete využít tedy jako pomoc při vyhledání určitého identifikátoru EIM. Například aplikace používající EIM by mohla zadat jméno alias, které sama používá, k vyhledání odpovídajícího identifikátoru EIM. Administrátor pak přidá tento jméno alias k identifikátoru EIM tak, aby aplikace mohla pro operace EIM využít spíše toto jméno alias než jedinečné jméno identifikátoru. Aplikace může také zadat tuto informaci, když využívá rozhraní API (eimGetTargetFromIdentifier()) k provádění vyhledávací operace EIM za účelem nalezení odpovídající totožnosti uživatele, kterou potřebuje.

Související pojmy

"Doména EIM" na stránce 6
Doména EIM je adresář v rámci serveru LDAP (Lightweight Directory Access Protocol), který obsahuje podniková data.

Definice registru EIM

Definice registru EIM je záznam v rámci produktu EIM, který můžete vytvořit za účelem reprezentace aktuálního registru uživatelů, jenž se nachází v systému daného podniku. Registr uživatelů funguje jako adresář a obsahuje seznam platných totožností uživatele pro určitý systém nebo aplikaci.

Základní registr uživatelů obsahuje totožnosti uživatele a jejich hesla. Příkladem registru uživatelů je registr z/OS Security Server Resource Access Control Facility (RACF). Registry uživatelů mohou také obsahovat jiné informace. Například adresář LDAP (Lightweight Directory Access Protocol) obsahuje vázaná rozlišovací jména, hesla a kontroly přístupu k datům, která jsou uložena v LDAP. Dalším příkladem běžných registrů jsou činitelé ve sféře Kerberos nebo totožnosti uživatele v registru uživatelských profilů v doméně Windows Active Directory a v operačním systému i5/OS.

Rovněž lze definovat registr uživatelů, který je součástí jiných uživatelských registrů. Některé aplikace používají podmnožinu totožností uživatele v rámci jediné instance registru uživatelů. Tak například registr z/OS Security Server (RACF) může obsahovat určité registry uživatelů, které jsou podmnožinou uživatelů v rámci celkového registru uživatelů RACF.

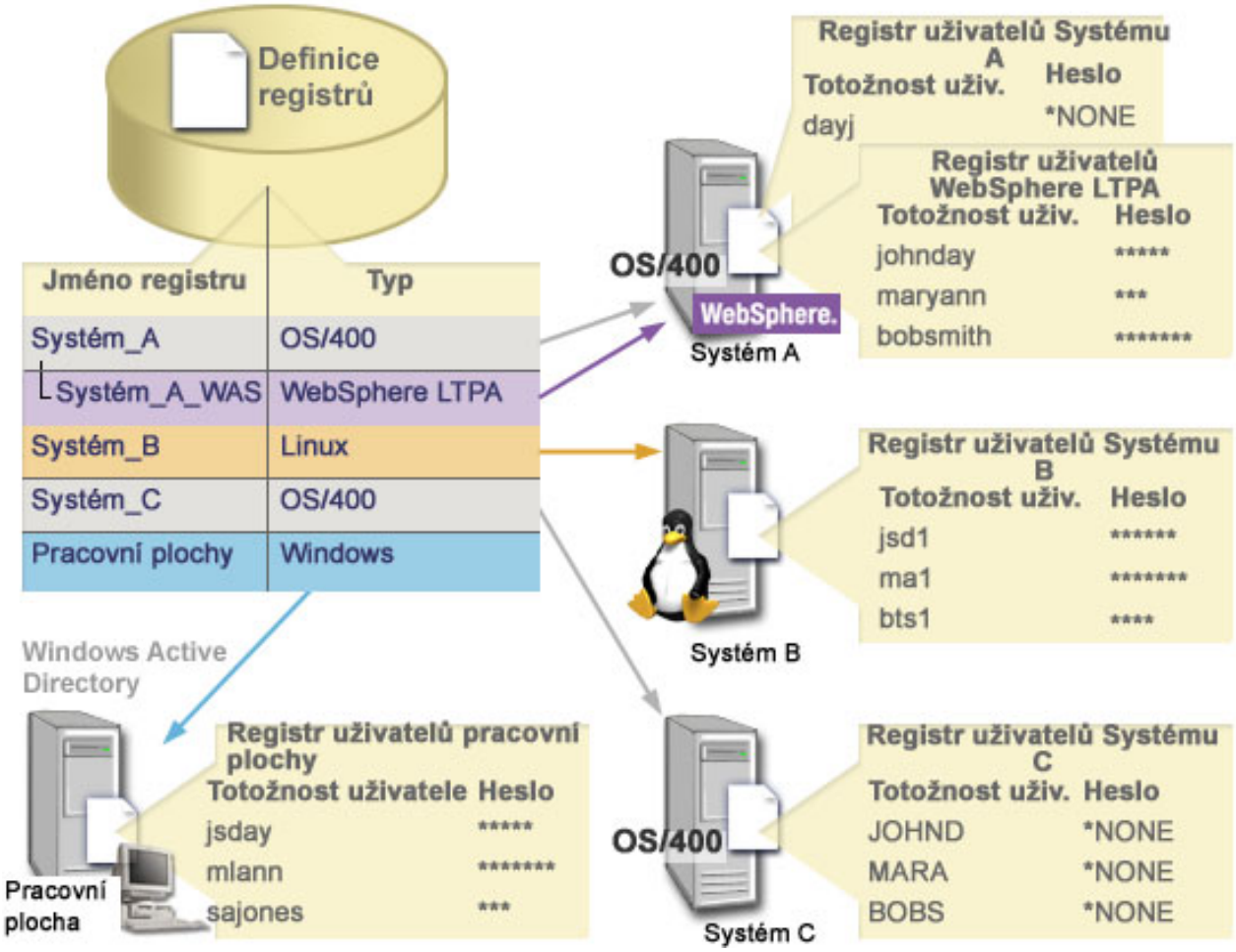
Definice registrů EIM poskytují informace týkající se registrů uživatelů v podniku. Administrátor definuje tyto registry v EIM zadáním následujících informací:

- Libovolné jedinečné jméno registru EIM. Každá definice registru reprezentuje specifickou instanci registru uživatelů. Následně byste měli tedy zvolit jméno definice registru EIM, které vám pomůže identifikovat přesnou instanci registru uživatelů. Například můžete zvolit hostitelské jméno TCP/IP pro registr uživatelů systému, nebo můžete hostitelské jméno zkombinovat se jménem aplikace pro registr uživatelů aplikace. Chcete-li vytvořit specifická jména definic registru EIM, můžete zvolit jakoukoliv kombinaci alfanumerických znaků (velká i malá písmena) a mezer.
- Typ registru uživatelů. Existuje určitý počet předvolených typů registrů uživatelů, pomocí nichž EIM pokrývá registry uživatelů ve většině operačních systémů. Tyto typy zahrnují:
  - AIX
  - Domino - dlouhé jméno
  - Domino - krátké jméno
  - Kerberos
  - Kerberos - rozlišování velikosti písmen
  - LDAP
  - - LDAP - krátké jméno
  - Linux
  - Novell Directory Server
  - - ostatní
  - - ostatní - citlivé na velikost písmen
  - i5/OS (nebo OS/400)
  - Tivoli Access Manager
  - RACF
  - Windows - lokální
  - Windows doména (Kerberos) (Tento typ rozlišuje velká a malá písmena.)
  - X.509

  Ačkoli tyto předvolené typy definice registru pokrývají většinu registrů uživatelů operačních systémů, budete možná muset vytvořit definici registru, pro kterou EIM nezahrnuje předvolený typ registru. Máte dvě možnosti, jak tuto situaci vyřešit. Můžete buď použít stávající definici registru, která odpovídá charakteristice registru uživatelů, nebo můžete definovat soukromý typ registru uživatelů. Například na obrázku č. 6 postupoval administrátor podle požadovaného postupu a definoval typ registru jako WebSphere LTPA pro definici registru aplikací Systém_A_WAS.

Na obrázku č. 6 vytvořil administrátor definice systémového registru EIM pro registr uživatelů reprezentující Systém A, Systém B, Systém C a Windows Active Directory, který obsahuje činitele Kerberos, pomocí nichž se uživatelé přihlašují na svých pracovních stanicích. Navíc vytvořil administrátor definici aplikačního registru pro WebSphere (R) LTPA (Lightweight Third-Party Authentication) provozovaného v Systému A. Jméno definice registru pak pomáhá administrátorovi identifikovat specifickou instanci typu registru uživatelů. Například IP adresa nebo hostitelské jméno často dostačuje pro mnoho typů registrů uživatelů. V tomto případě administrátor používá Systém_A_WAS, jako jméno definice aplikačního registru, k identifikaci této specifické instance aplikace WebSphere LTPA. Administrátor také zadá, že nadřazeným systémovým registrem pro definici aplikačního registru je registr Systém_A.

Obrázek č. 6: Definice registru EIM pro pět registrů uživatelů v podniku.



Poznámka: K dalšímu omezení nezbytné správy hesel uživatelů administrátor na obrázku č. 6 nastaví hesla uživatelských profilů i5/OS v Systému A a v Systému B na hodnotu *ŽÁDNÝ (*NONE). Administrátor v tomto případě provádí konfiguraci prostředí jediného přihlášení a jediná aplikace, se kterou jeho uživatelé pracují, je aplikace podporující EIM, jako např. produkt System i Navigator. Poté administrátor odstraní hesla z jejich uživatelských profilů i5/OS, aby jak uživatelé, tak administrátor mohli spravovat méně hesel.

Související pojmy

"Doména EIM" na stránce 6
Doména EIM je adresář v rámci serveru LDAP (Lightweight Directory Access Protocol), který obsahuje podniková data.

"Definice typu registru soukromého uživatele v EIM" na stránce 91
Při vytváření definice registru EIM můžete zadat jeden z předdefinovaných typů registru uživatelů, aby představoval skutečný registr uživatelů, který existuje v systému v rámci podniku.

Definice systémových registrů

Definice systémového registru je záznam vytvořený v produktu EIM za účelem reprezentace a popisu zvláštního registru uživatelů v rámci pracovní stanice nebo serveru.

Definici systémového registru EIM pro registr uživatelů můžete vytvořit v případě, když registr v rámci podniku bude mít jeden z následujících znaků:

- Registr je poskytován operačním systémem, jako například AIX, i5/OS, nebo jako produkt správy zabezpečení, například z/OS Security Server Resource Access Control Facility (RACF).

- Registr obsahuje totožnosti uživatele, které jsou jedinečné pro určitou aplikaci, například pro Lotus Notes.
- Registr obsahuje distribuované totožnosti uživatele, jako jsou činitelé Kerberos nebo rozlišovací jména LDAP (Lightweight Directory Access Protocol).

Vyhledávací operace EIM fungují správně, bez ohledu na to, jestli administrátor EIM definuje registr jako systémový nebo aplikační. Samostatné definice registrů umožňují, aby data mapování byla spravována na bázi aplikace. Odpovědnost za správu mapování specifických pro aplikaci může být přiřazena administrátorovi daného registru.

Související úlohy

"Přidání definice aplikačního registru" na stránce 89
Chcete-li vytvořit definici aplikačního registru, musíte být připojeni k doméně EIM, ve které chcete pracovat, a musíte mít řízení přístupu administrátora EIM.

Definice aplikačních registrů

Definice aplikačního registru je záznam v produktu EIM, který reprezentuje a popisuje podmnožiny totožností uživatele, jež jsou definovány v systémovém registru. Tyto totožnosti uživatele sdílí společnou sadu vlastností a charakteristik, které jim umožňují používat určitou aplikaci nebo sadu aplikací.

Definice aplikačních registrů také reprezentují registry uživatelů, které se nacházejí v rámci jiných registrů uživatelů. Tak například registr z/OS Security Server (RACF) může obsahovat určité registry uživatelů, které jsou podmnožinou uživatelů v rámci celkového registru uživatelů RACF. Kvůli tomuto vztahu musíte pro jakoukoliv definici aplikačního registru, kterou vytvoříte, zadat jméno nadřazeného systémového registru.

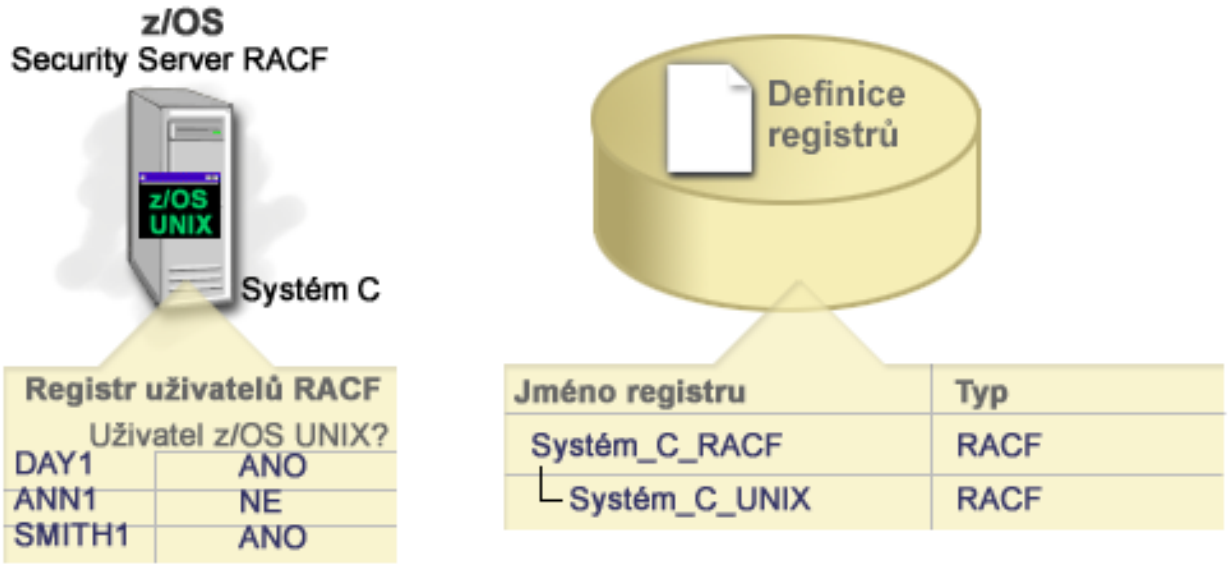
Definici aplikačního registru EIM můžete pro registr uživatelů vytvořit tehdy, pokud mají totožnosti uživatele v registru následující znaky:

- Totožnosti uživatele pro aplikaci nejsou uloženy v registru uživatelů, specifickém pro tuto aplikaci.
- Totožnosti uživatele pro aplikaci jsou uloženy v systémovém registru, který obsahuje totožnosti uživatele i pro jiné aplikace.

Vyhledávací operace EIM pak bude probíhat správně, bez ohledu na to, jestli administrátor EIM vytvoří pro registr uživatelů aplikaci nebo definici systémového registru. Samostatné definice registrů umožňují, aby data mapování byla spravována na bázi aplikace. Odpovědnost za správu mapování specifických pro aplikaci může být přiřazena administrátorovi daného registru.

Obrázek č. 7 ilustruje, jakým způsobem vytvořil administrátor EIM definici systémového registru, která bude reprezentovat registr z/OS Security Server RACF. Administrátor také vytvořil definici aplikačního registru za účelem reprezentace totožností uživatelů v rámci registru RACF, kteří využívají systémové služby z/OS(TM) UNIX System Services (z/OS UNIX). Systém C obsahuje registr uživatelů RACF, který dále obsahuje informace pro další tři totožnosti uživatele, DAY1, ANN1, a SMITH1. Dvě z těchto totožností uživatele (DAY1 a SMITH1) mají přístup k z/OS UNIX v Systému C. Tyto totožnosti uživatele jsou vlastně uživatelé RACF se zvláštními atributy, jež je identifikují jako uživatele z/OS UNIX. Administrátor EIM tak v definicích registrů EIM definoval Systém_C_RACF pro reprezentaci celkového registru uživatelů RACF. Dále administrátor také definoval Systém_C_UNIX pro reprezentaci totožností uživatele, které mají atributy z/OS UNIX.

Obrázek č. 7: Definice registrů EIM pro registr uživatelů RACF a pro uživatele z/OS UNIX.



Definice skupinového registru

Logické seskupování definic registru umožňuje zredukovat množství práce, které musíte provést, chcete-li konfigurovat mapování EIM. Definici skupinového registru lze spravovat obdobným způsobem jako definici individuálního registru.

Všichni uživatelé definice skupinového registru běžně obsahují alespoň jednu běžnou uživatelskou totožnost, ke které budete chtít vytvořit cílové nebo zdrojové přidružení. Seskupením členů dohromady umožníte vytvoření pouze jednoho přidružení (namísto více přidružení) uživatelské totožnosti k definici skupinového registru.

John Day se například přihlašuje do svého primárního systému s uživatelskou totožností jday a používá stejnou uživatelskou totožnost JOHND na více systémech. Takže uživatelský registr pro každý systém obsahuje uživatelskou totožnost JOHND. Normálně tedy John Day vytvoří oddělené cílové přidružení z identifikátoru EIM John Day na každý registr uživatele, který obsahuje uživatelskou totožnost JOHND. Chce-li snížit množství práce, které musí provést za účelem konfigurace mapování EIM, může vytvořit jednu definici registru se všemi uživatelskými registry, které obsahují uživatelskou totožnost JOHND jakožto člena této skupiny. Poté je schopen vytvořit jediné cílové přidružení z identifikátoru EIM - John Day k definici skupinového registru namísto několika cílových přidružení z identifikátoru EIM - John Day ke každé definici individuálního registru. Toto jediné cílové přidružení k definici skupinového registru umožňuje uživatelské totožnosti pana Johna Daye - jday mapovat uživatelskou totožnost JOHND.

Níže uvedené informace popisují definice skupinového registru:

- Všichni členové (definice individuálního registru) definice skupinového registru musí mít nastavenou stejnou citlivost na malá/velká písmena.
- Všichni členové (definice individuálního registru) definice skupinového registru musí být definováni v doméně EIM ještě předtím, než je můžete přidat do definice skupinového registru.
- Definice registru může být člen více než jedné skupiny. Měli byste se však vyhnout zadání registru individuálního uživatele jako člena více definic skupinového registru, protože vyhledávací operace mohou vrátit nejednoznačné výsledky. Definice skupinového registru nemůže být členem jiné definice skupinového registru.

Související pojmy

“Příklady vyhledávací operace: Příklad 5” na stránce 35
Tento příklad použijte, chcete-li se dozvědět více o vyhledávacích operacích, které vrací nejednoznačné výsledky zahrnující definice skupinového registru.

Přidružení EIM

Přidružení EIM (Enterprise Identity Mapping) je záznam, který vytvoříte v doméně EIM pro definici vztahu mezi totožnostmi uživatele v odlišných registrech uživatelů. Typ vytvořeného přidružení bude určovat, zda-li je definovaný vztah přímý či nepřímý.

Je možné vytvořit jeden ze dvou typů přidružení v EIM: přidružení identifikátorů a přidružení zásad. Přidružení zásad můžete používat namísto přidružení identifikátorů nebo v kombinaci s ním. To, jak budete přidružení používat, se bude odvíjet od vašeho celkového plánu implementace.

Další informace o práci s přidruženími naleznete v následujících tématech:

Vyhledávací informace

Produkt EIM poskytuje volitelná data, kterým se říká vyhledávací operace, pro další určení totožnosti cílového uživatele. Zmíněná totožnost cílového uživatele může být zadána buď v přidružení identifikátorů, nebo v přidružení zásad.

Vyhledávací informace je jedinečný znakový řetězec, který využívá buď rozhraní eimGetTargetFromSource API EIM, nebo rozhraní eimGetTargetFromIdentifier API EIM během operace vyhledávání mapování k dalšímu zpřesnění hledání totožnosti cílového uživatele, jenž je předmětem vyhledávací operace. Data, která pro vyhledávací informace zadáte, odpovídají parametru dodatečných informací pro registry uživatelů pro tato rozhraní API EIM.

Vyhledávací informace jsou nezbytné pouze v případě, kdy operace vyhledávání mapování může vrátit více než jednu totožnost cílového uživatele. Operace vyhledávání mapování vrací více totožností cílového uživatele, nastane-li jedna nebo více z následujících situací:

- Identifikátor EIM má více jednotlivých cílových přidružení ke stejnému cílovému registru.
- Více než jeden identifikátor EIM má tutéž totožnost uživatele specifikovanou ve zdrojovém přidružení a každý z těchto identifikátorů má cílové přidružení k témuž cílovému registru, ačkoliv totožnost uživatele specifikovaná pro každé cílové přidružení může být odlišná.
- Více než jedno předvolené přidružení zásad domény uvádí stejný cílový registr.
- Více než jedno předvolené přidružení zásad registru uvádí stejný zdrojový registr a stejný cílový registr.
- Více než jedno přidružení zásad filtru certifikátů uvádí stejný zdrojový registr X.509, filtr certifikátů a cílový registr.

Poznámka: Operace vyhledávání mapování, která vrací více než jednu totožnost cílového uživatele, může způsobit problém pro aplikace podporující EIM, včetně aplikací a produktů i5/OS, protože tyto nejsou navrženy pro práci s nejednoznačnými výsledky. Avšak základní aplikace i5/OS, jako například System i Access for Windows, nemohou využívat vyhledávací informace k rozlišování mezi více totožnostmi cílových uživatelů, které vrátila vyhledávací operace. Tudíž můžete zvážit nová definování přidružení pro doménu a zajistit tak, že operace vyhledávání mapování bude vracet jedinou totožnost cílového uživatele. Tak také zajistíte, že základní aplikace i5/OS budou moci úspěšně provádět vyhledávací operace a mapovat totožnosti.

Vyhledávací informace můžete používat, pokud se chcete vyhnout situacím, kdy operace vyhledávání mapování vrací více než jednu totožnost cílového uživatele. Jestliže chcete zabránit vyhledávacím operacím ve vracení několika totožností cílového uživatele, musíte definovat přesné vyhledávací informace pro každou totožnost cílového uživatele v každém přidružení. Vyhledávací informace musí být zadána pro operace vyhledávání mapování tak, aby tato operace mohla vrátit jedinečnou totožnost cílového uživatele. Jinak aplikace, které se spoléhají na EIM, nemusí být schopny určit přesnou totožnost cílového uživatele, kterou mají použít.

Například máte identifikátor EIM pojmenovaný John Day, který má dva uživatelské profily v Systému A. Jeden z těchto uživatelských profilů je JDUSER v Systému A a druhý je JDSECADM, který má zvláštní oprávnění administrátora systému. Existují dvě cílová přidružení pro identifikátor John Day. Jedno z těchto cílových přidružení je pro totožnost uživatele JDUSER v cílovém registru Systém_A a vyhledávací informace, zadaná pro JDUSER, bude oprávnění uživatele. Druhé cílové přidružení je pro totožnost uživatele JDSECADM v cílovém registru Systém_A a vyhledávací informace, zadaná pro JDSECADM, bude správce systému.

V případě, že operace vyhledávání mapování nezadá žádnou vyhledávací informaci, vyhledávací operace bude vracet obě totožnosti uživatele (JDUSER a JDSECADM). Naopak v případě, že operace vyhledávání mapování zadá vyhledávací informaci oprávnění uživatele, vrátí vyhledávací operace pouze totožnost uživatele JDUSER. A samozřejmě, pokud operace vyhledávání mapování zadá vyhledávací informaci správce systému, vrátí vyhledávací operace pouze totožnost uživatele JDSECADM.

Poznámka: Pokud vymažete poslední cílové přidružení pro totožnost uživatele (jedno, jestli se jedná o přidružení identifikátorů nebo o přidružení zásad), bude také z domény vymazána totožnost cílového uživatele spolu s veškerými vyhledávacími informacemi.

Jelikož je možné používat přidružení zásad certifikátů a také jiná přidružení mnoha různými způsoby, bude nutné předtím, než vytvoříte a začnete přidružení zásad certifikátů používat, důkladně porozumět tomu, jak pracuje podpora zásad mapování EIM a také tomu, jak fungují vyhledávací operace.

Související pojmy

"Podpora a povolení zásad mapování EIM" na stránce 37
Podpora zásad mapování produktu EIM (Enterprise Identity Mapping) vám umožní použít přidružení zásad stejně jako určitá přidružení identifikátorů v doméně EIM. Přidružení zásad můžete používat namísto přidružení identifikátorů nebo v kombinaci s ním.

"Vyhledávací operace EIM" na stránce 26
Aplikace nebo operační systém využívají rozhraní API EIM k provedení vyhledávací operace tak, aby aplikace nebo operační systém mohly provádět mapování od jedné totožnosti uživatele v jednom registru na další totožnost uživatele v jiném registru. Vyhledávací operace EIM je proces, kdy pomocí zadání některých známých a důvěryhodných informací aplikace nebo operační systém vyhledá neznámé přidružení totožnosti uživatele v daném cílovém registru.

"Předvolené přidružení zásad domény" na stránce 21
Předvolené přidružení zásad domény je typem přidružení zásad, který použijete k vytvoření mapování typu mnoho-na-jeden mezi totožnostmi uživatele.

"Předvolené přidružení zásad registru" na stránce 23
Předvolené přidružení zásad registru je typem přidružení zásad, které použijete k vytvoření mapování typu mnoho-na-jeden mezi totožnostmi uživatele.

Přidružení identifikátorů

Identifikátor EIM představuje v podniku určitou osobu nebo entitu. Přidružení identifikátorů EIM popisují vztah mezi identifikátorem EIM a jedinou totožností uživatele v registru uživatelů, která danou osobu také reprezentuje. Jestliže vytvoříte přidružení mezi identifikátorem EIM a všemi totožnostmi uživatele osoby nebo entity, umožníte tak ostatním jednoduše a kompletně pochopit, jak osoba nebo entita používá prostředky v podniku.

Totožnosti uživatele lze použít k ověření, autorizaci nebo k oběma těmto činnostem. *Ověření* je proces ověřování, zda entita nebo osoba, která poskytuje totožnost uživatele, má právo tuto totožnost převzít. Ověření se provádí tak, že osoba, která podává totožnost uživatele, musí zadat tajné nebo soukromé informace spojené s totožností uživatele, jako například heslo. *Autorizace* je proces, jehož prostřednictvím je zajišťováno, aby řádně ověřená totožnost uživatele mohla provádět funkce nebo přistupovat k prostředkům, k nimž je oprávněna přistupovat. V minulosti téměř všechny aplikace musely používat totožnosti v jednom registru uživatelů jak pro ověření, tak pro autorizaci. Nyní pomocí operací vyhledávání EIM mohou aplikace používat totožnosti v jednom registru uživatelů pro ověření, zatímco pro autorizaci mohou používat přiřazenou totožnost uživatele v jiném registru uživatelů.

Identifikátor EIM poskytne nepřímé přidružení mezi totožnostmi uživatele, což umožní aplikacím vyhledat odlišnou totožnost uživatele pro identifikátor EIM na základě známé totožnosti uživatele. EIM poskytne rozhraní API, která umožní aplikacím nalézt neznámou totožnost uživatele v určitém (cílovém) registru uživatelů poskytnutím známé totožnosti uživatele v nějakém jiném (zdrojovém) registru uživatelů. Tento proces se nazývá mapování totožností.

V EIM může administrátor definovat tři různé typy přidružení k popsání stavu mezi identifikátorem EIM a totožností uživatele. Přidružení identifikátorů může být zdrojové, cílové nebo administrační. To, jaký typ přidružení vytvoříte, závisí na tom, jak se používá totožnost uživatele. Například můžete vytvořit zdrojové a cílové přidružení pro totožnosti

uživatelů, které se mají podílet na mapování vyhledávacích operací. Je-li k ověření použita totožnost uživatele, obvykle pro ni vytvoříte zdrojové přidružení. Pro totožnosti uživatele, které jsou použity k autorizaci, pak vytvoříte cílová přidružení.

Dříve než vytvoříte přidružení identifikátorů, musíte vytvořit odpovídající identifikátor EIM a odpovídající definici registru EIM pro registr uživatelů, který obsahuje přidruženou totožnost uživatele. Přidružení definuje vztah mezi identifikátorem EIM a totožností uživatele pomocí následujících informací:

- Jméno identifikátoru EIM.
- Jméno totožnosti uživatele.
- Jméno definice registru EIM.
- Typ přidružení.
- Volitelné: vyhledávací informace pro bližší označení totožnosti cílového uživatele v cílovém přidružení.

Zdrojové přidružení

Zdrojové přidružení umožní totožnosti uživatele, aby se použila jako zdroj ve vyhledávací operaci EIM pro nalezení jiné totožnosti uživatele, která je přidružena ke stejnému identifikátoru EIM.

Použije-li se totožnost uživatele pro *ověření*, tato totožnost uživatele má mít cílové přidružení k identifikátoru EIM. Například můžete vytvořit zdrojové přidružení pro činitele Kerberos, protože se tato forma totožnosti uživatele používá pro ověření. Abyste zajistili úspěšné operace vyhledávání mapování pro identifikátory EIM, zdrojová a cílová přidružení se musí použít společně pro jeden identifikátor EIM.

Cílové přidružení

Cílové přidružení umožní totožnosti uživatele, aby byla vrácena jako výsledek vyhledávací operace EIM. Totožnosti uživatele, které představují koncové uživatele, běžně potřebují jen cílové přidružení.

Používá-li se totožnost uživatele pro *autorizaci* spíše než pro ověření, tato totožnost uživatele má mít cílové přidružení k identifikátoru EIM. Například můžete vytvořit cílové přidružení uživatelského profilu i5/OS, protože tato forma totožnosti uživatele určuje, jaké prostředky a jaká privilegia má uživatel v určitém systému System i. Abyste zajistili úspěšné operace vyhledávání mapování pro identifikátory EIM, zdrojová a cílová přidružení se musí použít společně pro jeden identifikátor EIM.

Vztah zdrojového a cílového přidružení

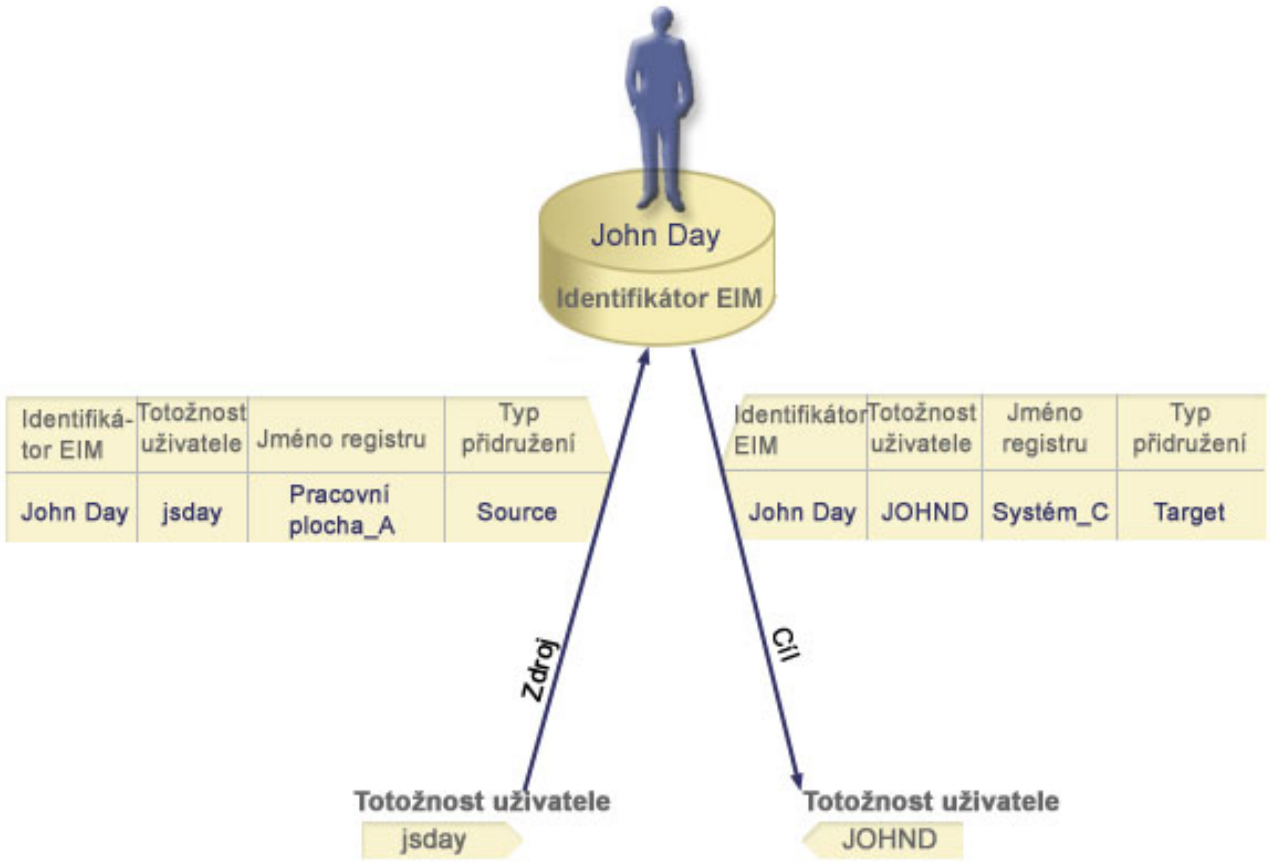
Abyste zajistili úspěšné operace vyhledávání mapování, potřebujete vytvořit alespoň jedno zdrojové a jedno nebo více cílových přidružení pro jeden identifikátor EIM. Obvykle vytvoříte cílové přidružení pro každou totožnost uživatele v registru uživatelů, které příslušná osoba může použít pro autorizaci v systému nebo v aplikaci, které odpovídá registr uživatelů.

Například uživatelé v podniku se normálně přihlašují a ověřují na pracovní ploše Windows a vstupují do systému System i, aby prováděli úlohy. Uživatelé se přihlašují na pracovní plochu pomocí činitele Kerberos a přihlašují se do systému System i pomocí uživatelského profilu i5/OS. Vaším cílem je vytvoření prostředí jediného přihlášení, kde se uživatelé ověřují na svých pracovních plochách pomocí činitele Kerberos a nemusí se již ručně ověřovat v systému System i.

K dosažení tohoto cíle vytvoříte zdrojové přidružení pro činitele Kerberos pro každého uživatele a identifikátor EIM daného uživatele. Pak vytvoříte cílové přidružení pro uživatelský profil i5/OS každého uživatele a identifikátor EIM daného uživatele. Tato konfigurace zajistí, že operační systém i5/OS může provádět operace vyhledávání mapování ke zjištění správného uživatelského profilu potřebného pro uživatele, který vstupuje do systému System i poté, co se ověřil na pracovní ploše. Operační systém i5/OS pak umožní uživateli přístup k prostředkům na serveru na základě odpovídajícího uživatelského profilu, aniž by požadoval ověření uživatele na serveru.

Obrázek č. 6 ukazuje jiný příklad, kdy administrátor EIM vytvoří dvě přidružení, zdrojové přidružení a cílové přidružení, pro identifikátor EIM John Day, aby definoval vztah mezi tímto identifikátorem a dvěma přidruženými totožnostmi uživatele. Administrátor vytvoří zdrojové přidružení pro jsday, činitele Kerberos v registru uživatelů Desktops. Administrátor rovněž vytvoří cílové přidružení pro JOHND, uživatelský profil operačního systému i5/OS v registru uživatelů Systém_C. Tato přidružení poskytují prostředek pro aplikace k získání neznámé totožnosti uživatele (cílové, JOHND) na základě známé totožnosti uživatele (zdrojové, jsday) jako součást vyhledávací operace EIM.

Obrázek č. 6: Cílová a zdrojová přidružení EIM pro identifikátor EIM John Day



Chceme-li jít v příkladu dále, budeme předpokládat, že administrátor EIM si uvědomí, že John Day používá stejný profil operačního systému i5/OS - jsd1 v pěti různých systémech. V této situaci musí administrátor vytvořit šest přidružení pro identifikátor EIM John Day a definovat tak vztah mezi tímto identifikátorem a přidruženou totožností uživatele v pěti registrech uživatele: zdrojové přidružení pro johnday a službu Kerberos v registru uživatele Desktop_A a pět cílových přidružení pro jsd1, uživatelský profil operačního systému i5/OS v pěti registrech uživatele: Systém_B, Systém_C, Systém_D, Systém_E a Systém_F. Chce-li zredukovat množství práce, které musí vykonat pro konfiguraci mapování EIM, vytvoří administrátor EIM definici skupinového registru. Mezi členy definice skupinového registru patří jména definice registru Systém_B, Systém_C, Systém_D, Systém_E a Systém_F. Seskupení členů dohromady umožní administrátorovi vytvořit jediné cílové přidružení s definicí skupinového registru a totožností uživatele namísto vytváření několika přidružení s definicemi individuálních registrů. Tato přidružení poskytují prostředek pro aplikace k získání neznámé totožnosti uživatele (cílové, jsd1) v pěti registrech uživatele, které jsou znázorněné jako členové definice skupinového registru, na základě známé totožnosti uživatele (zdrojové, johnday) jako součást vyhledávací operace EIM.

Pro některé uživatele může být nezbytné vytvoření obou, jak zdrojového, tak cílového přidružení, pro stejný registr uživatelů. To se vyžaduje, když jednotlivec používá jeden systém jako klienta i server, nebo pro jednotlivce, kteří se chovají jako administrátoři.

Poznámka: Totožnosti uživatele, které představují typické uživatele, běžně potřebují jen cílové přidružení.

Pro některé uživatele může být nezbytné vytvoření obou, jak zdrojového, tak cílového přidružení, pro stejný registr uživatelů. To se vyžaduje, když jednotlivec používá jeden systém jako klienta i server, nebo pro jednotlivce, kteří se chovají jako administrátoři.

Například administrátor používá funkci Centrální správa v produktu System i Navigator ke správě centrálního systému a několika koncových systémů. Funkce, které administrátor provádí, mohou začínat v centrálním systému nebo v koncovém systému. V této situaci byste vytvořili jak zdrojové přidružení, tak cílové přidružení pro každou z administrátorských totožností uživatele v obou systémech. Tím se zajistí to, že ať administrátor použije k přístupu do jiných systémů jakýkoliv systém, totožnost uživatele použitá k zahájení přístupu do jiného systému může být mapována na odpovídající totožnost uživatele pro následující systém, do něhož administrátor přistoupí.

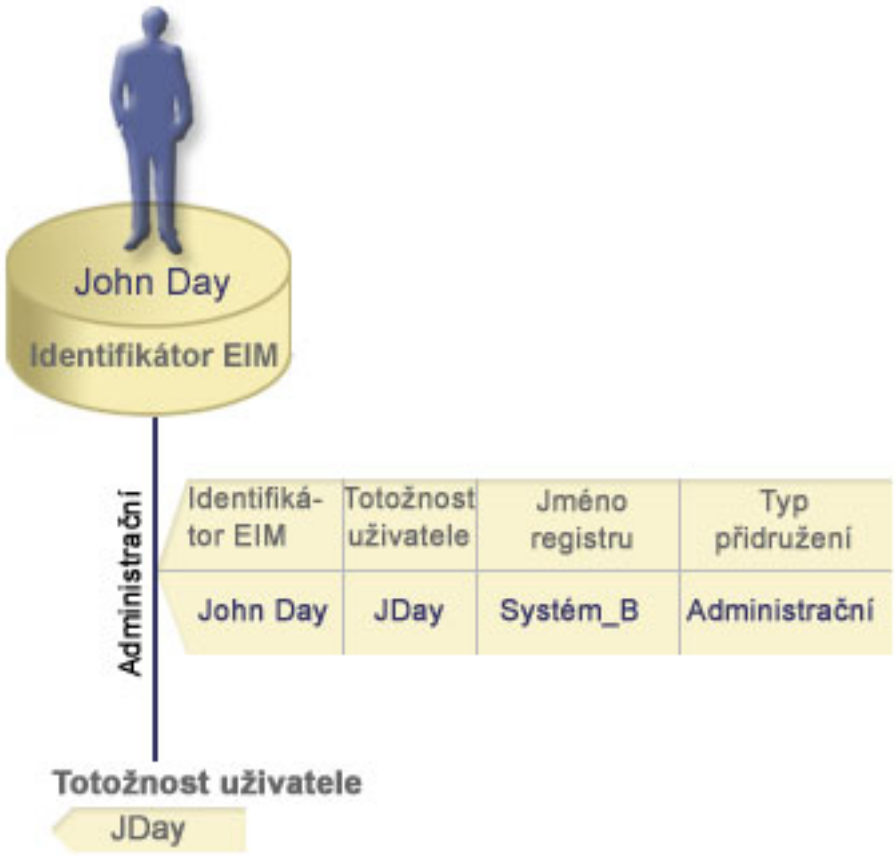
Administrační přidružení

Administrační přidružení identifikátorů EIM se běžně používá k zobrazení skutečnosti, že osoba či entita představovaná identifikátorem EIM vlastní totožnost uživatele, která vyžaduje speciální posouzení určitého systému. Tento typ přidružení lze použít například u utajovaných registrů uživatelů.

Kvůli speciální povaze administračních přidružení se tento typ přidružení nemůže účastnit vyhledávacích operací mapování EIM. V důsledku toho vyhledávací operace EIM, která dodává totožnost zdrojového uživatele s administračním přidružením, nevrátí žádné výsledky. Podobně, totožnost uživatele s administračním přidružením se nikdy nevrátí jako výsledek vyhledávací operace EIM.

Obrázek č. 7 ukazuje příklad administračního přidružení. V tomto příkladu zaměstnanec jménem John Day má totožnost uživatele John_Day v Systému A a totožnost uživatele JDay v Systému B, což je vysoce zabezpečený systém. Administrátor systému chce zajistit, aby si uživatelé ověřovali totožnost v Systému B pouze pomocí lokálního registru uživatelů tohoto systému. Administrátor nechce povolit aplikaci ověřovat John Day v systému pomocí jiného ověřovacího mechanismu. Pomocí administračního přidružení pro totožnost uživatele JDay v Systému B administrátor EIM vidí, že John Day v Systému B vlastní účet, ale EIM nevrátí informace o totožnosti JDay ve vyhledávacích operacích EIM. I když v tomto systému existují aplikace, které používají vyhledávací operace EIM, nemohou najít totožnosti uživatele, které mají administrační přidružení.

Obrázek č. 7: Administrační přidružení EIM identifikátoru EIM John Day



Přidružení zásad

Zásady mapování EIM umožňuje administrátorovi produktu EIM vytvářet a používat přidružení zásad, chce-li definovat vztah mezi několika totožnostmi uživatele v jednom nebo více registrech uživatelů a jedinou totožností uživatele v jiném registru uživatelů.

Přidružení zásad používá podporu zásad mapování EIM k vytvoření mapování typu mnoho-na-jeden mezi totožnostmi uživatele bez identifikátoru EIM. Přidružení zásad můžete použít namísto přidružení identifikátorů, která poskytují mapování typu jeden-na-jeden mezi identifikátorem EIM a jedinou totožností uživatele, nebo v kombinaci s nimi.

Přidružení zásad ovlivní pouze ty totožnosti uživatele, pro které neexistují určitá individuální přidružení EIM. Pokud určitá přidružení identifikátorů existují mezi identifikátorem EIM a totožnostmi uživatele, pak je totožnost cílového uživatele z přidružení identifikátorů vrácena aplikaci provádějící vyhledávací operaci, i když přidružení zásad existuje a použití přidružení zásad je povoleno.

Můžete vytvořit tři různé typy přidružení zásad:

Související pojmy

“Vyhledávací operace EIM” na stránce 26
Aplikace nebo operační systém využívají rozhraní API EIM k provedení vyhledávací operace tak, aby aplikace nebo operační systém mohly provádět mapování od jedné totožnosti uživatele v jednom registru na další totožnost uživatele v jiném registru. Vyhledávací operace EIM je proces, kdy pomocí zadání některých známých a důvěryhodných informací aplikace nebo operační systém vyhledá neznámé přidružení totožnosti uživatele v daném cílovém registru.

Předvolené přidružení zásad domény:

Předvolené přidružení zásad domény je typem přidružení zásad, který použijete k vytvoření mapování typu mnoho-na-jeden mezi totožnostmi uživatele.

Můžete použít předvolené přidružení zásad domény k mapování zdrojové sady totožností více uživatelů (v tomto případě všech uživatelů v doméně) na totožnost jediného cílového uživatele v určeném cílovém registru uživatelů. V předvoleném přidružení zásad domény jsou všichni uživatelé v doméně zdrojem přidružení zásad a mapují se na jediný cílový registr a totožnost cílového uživatele.

Chcete-li použít předvolená přidružení zásad domény, musíte povolit vyhledávání mapování pomocí přidružení zásad pro doménu. Také musíte povolit vyhledávání mapování pro zdrojový registr uživatele přidružení zásad. Nakonfigurujete-li toto ustanovení, registry uživatelů v přidružení zásad se mohou podílet na operacích vyhledávání mapování.

Předvolené přidružení zásad domény nabývá platnosti, když operace vyhledávání mapování neuspěje u přidružení identifikátorů, přidružení zásad filtru certifikátů, ani u předvoleného přidružení zásad registru pro cílový registr. Výsledkem je, že všechny totožnosti uživatele v doméně se mapují na jedinou totožnost cílového uživatele tak, jak je uvedeno v předvoleném přidružení zásad domény.

Například vytvoříte předvolené přidružení zásad domény s totožností cílového uživatele John_Day v cílovém registru Registry_xyz a nevytvoříte žádné přidružení identifikátorů nebo jiné přidružení zásad, které mapuje tuto totožnost uživatele. Tudíž, když je uveden Registry_xyz jako cílový registr ve vyhledávacích operacích, předvolená zásada domény zajistí, že totožnost cílového uživatele John_Day se vrátí pro všechny totožnosti uživatele v doméně, kterénemají definovaná žádná jiná přidružení.

Při definici předvoleného přidružení zásad registru uvádíte tyto dvě informace:

- **Cílový registr**. Cílový registr, který uvedete, je jméno definice registru EIM, které obsahuje totožnost uživatele, k níž se mapují všechny totožnosti uživatele v doméně.
- **Cílový uživatel**. Cílový uživatel je jméno totožnosti uživatele, která se vrátí jako cíl operace vyhledávání mapování EIM na základě tohoto přidružení zásad.

Pro každý registr v doméně můžete definovat předvolené přidružení zásad domény. Pokud se dvě nebo více přidružení zásad domény odkazují na stejný cílový registr, musíte pro každé z těchto přidružení zásad definovat jedinečné vyhledávací informace, abyste zajistili, že budou pro operace vyhledávání mapování navzájem rozlišitelné. Jinak mohou operace vyhledávání mapování vrátit více totožností cílového uživatele. Důsledkem těchto nejednoznačných výsledků pro aplikace spoléhající na EIM by mohlo být, že tyto aplikace nebudou schopny určit přesnou cílovou totožnost.

Protože lze použít přidružení zásad mnoha způsoby, které se překrývají, měli byste důkladně porozumět, jak funguje podpora zásad mapování EIM a vyhledávací operace předtím, než vytvoříte a použijete přidružení zásad.

Poznámka: Možná budete chtít vytvořit předvolené přidružení zásad domény s cílovou totožností uživatele, která existuje v definici skupinového registru. Všichni uživatelé v doméně jsou zdrojovým přidružením zásady a jsou mapováni na cílovou totožnost uživatele v cílové definici skupiny. Uživatelská totožnost, kterou definujete v předvoleném přidružení zásady, existuje v rámci členů definice skupinového registru.

John Day například používá stejný uživatelský profil operačního systému i5/OS - John_Day v pěti různých systémech: Systém B, systém C, systém D, systém E a systém F. Chce-li administrátor produktu EIM zredukovat množství práce, které musí provést pro konfiguraci mapování EIM, vytvoří definici skupinového registru s názvem Group_1. Členové definice registru zahrnují jména definice registru Systém_B, Systém_C, Systém_D, Systém_E a Systém_F. Seskupení členů dohromady umožní administrátorovi vytvořit jediné cílové přidružení s definicí skupinového registru a totožností uživatele namísto vytváření několika přidružení s definicemi individuálních registrů.

Administrátor EIM vytvoří předvolené přidružení zásad domény s totožností cílového uživatele John_Day v cílovém registru Group_1. V tomto případě se nepoužijí žádná další specifická přidružení

indentifikátorů nebo přidružení zásad. Tudíž, když je uveden registr s názvem Group_1 jako cílový registr ve vyhledávacích operacích, předvolená zásada domény zajistí, že totožnost cílového uživatele John_Day se vrátí pro všechny totožnosti uživatele v doméně, které nemají definovaná žádná speficická přidružení identifikátorů.

Související pojmy

"Vyhledávací informace" na stránce 16
Produkt EIM poskytuje volitelná data, kterým se říká vyhledávací operace, pro další určení totožnosti cílového uživatele. Zmíněná totožnost cílového uživatele může být zadána buď v přidružení identifikátorů, nebo v přidružení zásad.

"Podpora a povolení zásad mapování EIM" na stránce 37
Podpora zásad mapování produktu EIM (Enterprise Identity Mapping) vám umožní použít přidružení zásad stejně jako určitá přidružení identifikátorů v doméně EIM. Přidružení zásad můžete používat namísto přidružení identifikátorů nebo v kombinaci s ním.

Předvolené přidružení zásad registru:

Předvolené přidružení zásad registru je typem přidružení zásad, které použijete k vytvoření mapování typu mnoho-na-jeden mezi totožnostmi uživatele.

Můžete použít předvolené přidružení zásad registru k mapování zdrojové sady totožností více uživatelů (v tomto případě těch v jednom registru) na totožnost jediného cílového uživatele v určeném cílovém registru uživatelů. V předvoleném přidružení zásad registru jsou všichni uživatelé jednoho registru zdrojem přidružení zásad a mapují se na jediný cílový registr a cílového uživatele.

Chcete-li použít tato předvolená přidružení zásad registru, musíte povolit vyhledávání mapování pomocí přidružení zásad pro doménu. Také musíte povolit vyhledávání mapování pro zdrojový registr a povolit vyhledávání mapování a použití přidružení zásad pro cílový registr uživatelů přidružení zásad. Nakonfigurujete-li toto ustanovení, registry uživatelů v přidružení zásad se mohou podílet na operacích vyhledávání mapování.

Předvolené přidružení zásad registru nabývá platnosti, když operace vyhledávání mapování neuspěje u přidružení identifikátorů, přidružení zásad filtru certifikátů, ani u jiného předvoleného přidružení zásad registru pro cílový registr. Výsledkem je, že všechny totožnosti uživatele ve zdrojovém registru se mapují na jedinou totožnost cílového uživatele tak, jak je uvedeno v předvoleném přidružení zásad registru.

Například vytvoříte předvolené přidružení zásad registru mající zdrojový registr my_realm.com, což jsou činitelé v určité sféře Kerberos. Pro toto přidružení zásad také uvedete totožnost cílového uživatele general_user1 v cílovém registru i5/OS_system_reg, což je určitý uživatelský profil v registru uživatelů i5/OS. V tomto případě jste nevytvořili žádná přidružení identifikátorů nebo přidružení zásad, která jsou použitelná na totožnosti uživatele ve zdrojovém registru. Tudíž, je-li uveden i5/OS_system_reg jako cílový registr a my_realm.com je uveden jako zdrojový registr ve vyhledávacích operacích, předvolené přidružení zásad registru zajistí, že totožnost cílového uživatele general_user1 se vrátí pro všechny totožnosti uživatele v registru my_realm.com, které nemají definovaná žádná určitá přidružení identifikátorů nebo přidružení zásad filtru certifikátů.

Při definici předvoleného přidružení zásad registru uvádíte tyto tři informace:

- **Zdrojový registr**. Je to taková definice registru, kterou chcete, aby používalo přidružení zásad jako zdroj mapování. Všechny totožnosti uživatele v tomto zdrojovém registru uživatelů se namapují na zadaného cílového uživatele přidružení zásad.
- **Cílový registr**. Cílový registr, který uvedete, je jméno definice registru EIM. Cílový registr musí obsahovat totožnost cílového uživatele, na níž se namapují všechny totožnosti uživatele ve zdrojovém registru.
- **Cílový uživatel**. Cílový uživatel je jméno totožnosti uživatele, která se vrátí jako cíl operace vyhledávání mapování EIM na základě tohoto přidružení zásad.

Můžete definovat více než jedno předvolené přidružení zásad registru. Pokud se dvě nebo více přidružení zásad se stejným zdrojovým registrem odkazují na stejný cílový registr, musíte definovat jedinečné vyhledávací informace pro každé z těchto přidružení zásad, abyste zajistili, že je operace vyhledávání mapování rozeznají. Jinak mohou operace

vyhledávání mapování vrátit více totožností cílového uživatele. Důsledkem těchto nejednoznačných výsledků pro aplikace spoléhající na EIM by mohlo být, že tyto aplikace nebudou schopny určit přesnou cílovou totožnost.

Protože lze použít přidružení zásad mnoha způsoby, které se překrývají, měli byste důkladně porozumět, jak funguje podpora zásad mapování EIM a vyhledávací operace předtím, než vytvoříte a použijete přidružení zásad.

Poznámka: Možná budete chtít vytvořit předvolené přidružení zásad registru s cílovou totožností uživatele, která existuje v definici skupinového registru. Všichni uživatelé ve zdrojovém registru uživatelů jsou zdrojovým přidružením zásady a jsou mapováni na cílovou totožnost uživatele v cílové definici skupiny. Uživatelská totožnost, kterou definujete v předvoleném přidružení zásady registru, existuje v rámci členů definice skupinového registru.

John Day například používá stejný uživatelský profil operačního systému i5/OS - John_Day v pěti různých systémech: Systém_B, Systém_C, Systém_D, Systém_E a Systém_F. Chce-li administrátor produktu EIM zredukovat množství práce, které musí provést pro konfiguraci mapování EIM, vytvoří definici skupinového registru s názvem Group_1. Mezi členy definice skupinového registru patří jména definice registru Systém_B, Systém_C, Systém_D, Systém_E a Systém_F. Seskupení členů dohromady umožní administrátorovi vytvořit jediné cílové přidružení s definicí skupinového registru a totožností uživatele namísto vytváření několika přidružení s definicemi individuálních registrů.

Administrátor EIM vytvoří předvolené přidružení zásad registru mající zdrojový registr my_realm.com, což jsou činitelé v určité sféře Kerberos. Pro přidružení této zásady také zadá cílovou totožnost uživatele John_Day v cílovém registru Group_1. V tomto případě se nepoužijí žádná další specifická přidružení identifikátoru ani přidružení zásad. Tudíž, je-li uveden registr s názvem Group_1 jako cílový registr a my_realm.com je uveden jako zdrojový registr ve vyhledávacích operacích, předvolené přidružení zásad registru zajistí, že totožnost cílového uživatele general_user1 se vrátí pro všechny totožnosti uživatele v registru my_realm.com, které nemají definovaná žádná určitá přidružení identifikátorů.

Související pojmy

"Vyhledávací informace" na stránce 16
Produkt EIM poskytuje volitelná data, kterým se říká vyhledávací operace, pro další určení totožnosti cílového uživatele. Zmíněná totožnost cílového uživatele může být zadána buď v přidružení identifikátorů, nebo v přidružení zásad.

"Podpora a povolení zásad mapování EIM" na stránce 37
Podpora zásad mapování produktu EIM (Enterprise Identity Mapping) vám umožní použít přidružení zásad stejně jako určitá přidružení identifikátorů v doméně EIM. Přidružení zásad můžete používat namísto přidružení identifikátorů nebo v kombinaci s ním.

Přidružení zásad filtru certifikátů:

Přidružení zásad filtru certifikátů je typem přidružení zásad, který použijete k vytvoření mapování typu mnoho-na-jeden mezi totožnostmi uživatele. Můžete použít přidružení zásad filtru certifikátů k mapování zdrojové sady certifikátů na totožnost jediného cílového uživatele v určeném cílovém registru uživatelů.

V přidružení zásad filtru certifikátů uvedete sadu certifikátů v jediném registru X.509 jako zdroj přidružení zásad. Tyto certifikáty se mapují na jediný cílový registr a cílového uživatele, které zadáte. Na rozdíl od předvoleného přidružení zásad registru, kde jsou všichni uživatele v jediném registru také zdrojem přidružení zásad, rozsah přidružení zásad filtru certifikátů je mnohem flexibilnější. Jako zdroj v registru můžete uvést podmnožinu certifikátů. Filtr certifikátů, který zadáte pro přidružení zásad, určuje jeho rozsah.

Poznámka: Předvolené přidružení zásad registru vytvoříte a budete používat, pokud chcete mapovat všechny certifikáty v registru uživatelů X.509 na totožnost jednoho cílového uživatele.

Chcete-li použít tato přidružení zásad filtru certifikátů, musíte povolit vyhledávání mapování pomocí přidružení zásad pro doménu. Také musíte povolit vyhledávání mapování pro zdrojový registr a povolit vyhledávání mapování a použití

přidružení zásad pro cílový registr uživatelů přidružení zásad. Nakonfigurujete-li toto ustanovení, registry uživatelů v přidružení zásad se mohou podílet na operacích vyhledávání mapování.

Je-li digitální certifikát totožností zdrojového uživatele v operaci vyhledávání mapování EIM (poté, co požadující aplikace použije rozhraní API eimFormatUserIdentity() EIM k naformátování jména totožnosti uživatele), EIM nejprve zkontroluje, zda existuje přidružení identifikátorů mezi identifikátorem EIM a zadanou totožností uživatele. Neexistuje-li, EIM porovná DN v certifikátu s DN nebo částečnými DN zadanými ve filtru pro přidružení zásad. Pokud se informace o DN v certifikátu shodují s filtrem, EIM vrátí totožnost cílového uživatele uvedeného v přidružení zásad. Výsledkem je, že certifikáty ve zdrojovém registru X.509, které vyhovují kritériím filtru certifikátů, se mapují na jedinou totožnost cílového uživatele tak, jak je uvedeno v přidružení zásad filtru certifikátů.

Například vytvoříte přidružení zásad filtru certifikátů se zdrojovým registrem certificates.x509. Tento registr obsahuje certifikáty pro všechny zaměstnance firmy, včetně těch, které používají manažeři na personálním oddělení k přístupu k určitým soukromým interním webovým stránkám a dalším zdrojům, ke kterým přistupují pomocí systému System i. Pro toto přidružení zásad také uvedete totožnost cílového uživatele hr_managers v cílovém registru system_abc, což je určitý uživatelský profil v registru uživatelů i5/OS. Abyste zajistili, že tímto přidružením zásad jsou pokryté pouze certifikáty, které patří managerům personálního oddělení, uvedete filtr certifikátů s rozlišovacím jménem subjektu (SDN) ou=hrmgr,o=myco.com,c=us.

V tomto případě jste nevytvořili žádná přidružení identifikátorů nebo jiná přidružení zásad filtru certifikátů, která jsou použitelná na totožnosti uživatele ve zdrojovém registru. Tudíž, je-li uveden system_abc jako cílový registr a certificates.x509 je uveden jako zdrojový registr ve vyhledávacích operacích, předvolené přidružení zásad registru zajistí, že totožnost cílového uživatele hr_managers se vrátí pro všechny certifikáty v registru certificates.x509, které odpovídají uvedenému filtru certifikátů a které nemají definovaná žádná určitá přidružení identifikátorů.

Přidružení zásad filtru certifikátů definujete zadáním těchto informací:

- **Zdrojový registr**. Definice zdrojového registru, který uvedete, musí být registr uživatelů typu X.509. Zásada filtru certifikátů vytvoří přidružení mezi totožnostmi uživatele v tomto registru uživatelů X.509 a jednou určitou totožností cílového uživatele. Přidružení platí pouze pro ty totožnosti uživatele v registru, které odpovídají kritériím filtru certifikátů, který pro tuto zásadu zadáte.
- **Filtr certifikátů**. Filtr certifikátů definuje sadu podobných atributů certifikátu. Přidružení zásad filtru certifikátů mapuje jakékoliv certifikáty s těmito definovanými atributy v registru uživatelů X.509 na určitou totožnost cílového uživatele. Uvádíte filtr na základě kombinace rozlišovacího jména (SDN) subjektu a rozlišovacího jména vydávajícího shodného s certifikáty, jež chcete použít jako zdroj mapování. Filtr certifikátů, který pro zásadu uvedete, již musí existovat v doméně EIM.
- **Cílový registr**. Definice cílového registru, který uvedete, je registr uživatelů, který obsahuje totožnost uživatele, na níž chcete mapovat certifikáty, které se shodují s filtrem certifikátů.
- **Cílový uživatel**. Cílový uživatel je jméno totožnosti uživatele, která se vrátí jako cíl operace vyhledávání mapování EIM na základě tohoto přidružení zásad.

Jelikož je možné používat přidružení zásad certifikátů a také jiná přidružení mnoha různými způsoby, bude nutné předtím, než vytvoříte a začnete přidružení zásad certifikátů používat, důkladně porozumět tomu, jak pracuje podpora zásad mapování EIM a také tomu, jak fungují vyhledávací operace.

Poznámka: Možná budete chtít vytvořit přidružení zásad filtru certifkátů s cílovou totožností uživatele, která existuje v definici skupinového registru. Uživatelé ve zdrojovém registru, kteří splňují kritéria zadaná filtrem certifikátu, jsou zdrojem přiřazení zásady a jsou mapováni na totožnost cílového uživatele v cílové definici skupinového registru. Uživatelská totožnost, kterou definujete v přidružení zásad filtru certifikátů, existuje v rámci členů definice skupinového registru.

John Day například používá stejný uživatelský profil operačního systému i5/OS - John_Day v pěti různých systémech: Systém B, systém C, systém D, systém E a systém F. Chce-li administrátor produktu EIM zredukovat množství práce, které musí provést pro konfiguraci mapování EIM, vytvoří definici skupinového registru. Mezi členy definice skupinového registru patří jména definice registru Systém_B, Systém_C, Systém_D, Systém_E a Systém_F. Seskupení členů dohromady umožní administrátorovi

vytvořit jediné cílové přidružení s definicí skupinového registru a totožností uživatele namísto vytváření několika přidružení s definicemi individuálních registrů.

Administrátor EIM vytvoří přidružení zásad filtru certifikátů, kde definuje podmnožinu certifikátů v rámci jednoho registru X.509 jakožto zdroj přidružení zásad. Zadá cílovou totožnost uživatele John_Day v cílovém registru Group_1. V tomto případě se nepoužijí žádná další specifická přidružení identifikátoru nebo další zásady filtrování certifikátů. Pokud je tedy Group_1 zadána jako cílový registr pro operace vyhledávání, mapují se všechny certifikáty ve zdrojovém registru X.509, které vyhovují kritériím filtru certifikátů, na zadanou totožnost cílového uživatele.

Filtry certifikátů:

Filtr certifikátů definuje sadu podobných atributů certifikátu s rozlišujícím názvem pro skupinu uživatelských certifikátů ve zdrojovém registru uživatelů X.509. Dále můžete také využít filtr certifikátů jako základ pro přidružení zásad filtru certifikátů.

Filtr certifikátů v přidružení zásad určuje, které certifikáty v uvedeném zdrojovém registru X.509 se mapují na určitého cílového uživatele. Certifikáty, jejichž informace o DN subjektu a DN vyhovují kritériím filtru, se mapují na zadaného cílového uživatele během vyhledávacích operací mapování EIM (Enterprise Identity Mapping).

Například vytvoříte filtr certifikátů s rozlišovacím jménem subjektu (SDN) o=ibm,c=us. Všechny certifikáty s těmito DN jako součástmi jejich informací SDN odpovídají kritériím filtru, jako například certifikát s SDN cn=JohnDay,ou=LegalDept,o=ibm,c=us. Jestliže existuje více než jeden filtr certifikátů, jehož kritériím certifikát vyhovuje, dostane přednost ta konkrétní hodnota filtru certifikátů, které certifikát odpovídá přesněji. Například máte filtr certifikátů s SDN o=ibm,c=us a pak máte další filtr certifikátů s SDN ou=LegalDept,o=ibm,c=us. Je-li certifikát ve zdrojovém registru X.509 cn=JohnDay,ou=LegalDept,o=ibm,c=us, použije se druhý nebo ještě specifictější filtr certifikátů. Je-li certifikát ve zdrojovém registru X.509 s SDN cn=SharonJones,o=ibm,c=us, použije se méně specifický filtr certifikátů, protože tento certifikát lépe odpovídá kritériím.

Chcete-li definovat filtr certifikátů, můžete specifikovat jednu nebo obě následující možnosti:

- Rozlišovací jméno subjektu (SDN). Úplné nebo částečné DN, které zadáte pro filtr, musí odpovídat části DN subjektu digitálního certifikátu, který označuje majitele certifikátu. Můžete zadat úplný řetězec DN subjektu, nebo jedno či více částečných DN, které mohou zahrnovat úplné SDN.
- Rozlišovací jméno (IDN) vydávajícího. Úplné nebo částečné DN, které zadáte pro filtr, musí odpovídat části DN vydavatele digitálního certifikátu, který stanovuje Certifikační autorita, jež vydala daný certifikát. Můžete zadat úplný řetězec DN vydavatele, nebo jedno či více částečných DN, které mohou zahrnovat úplné IDN.

Existuje několik způsobů, které můžete použít k vytvoření filtru certifikátů, včetně použití rozhraní API eimFormatPolicyFilter (Formát filtru zásad EIM) k vygenerování filtrů certifikátů tak, že použijete certifikát jako šablonu k vytvoření potřebných DN ve správném pořadí a ve správném formátu pro SDN a IDN.

Související pojmy

“Rozlišovací jméno” na stránce 46
Rozlišovací jméno (DN) je záznam v LDAP (Lightweight Directory Access Protocol), který poskytuje jedinečnou identifikaci a popisuje záznam na serveru adresářů (LDAP). Pomocí průvodce konfigurací EIM provedete konfiguraci serveru adresářů, aby bylo možné ukládat informace o doméně EIM. Jelikož produkt EIM používá server adresářů k ukládání dat EIM, můžete použít rozlišovací jména jako prostředek ověření k řadiči domény EIM.

Související informace

Rozhraní API eimFormatPolicyFilter (Formát filtru zásad EIM)

Vyhledávací operace EIM

Aplikace nebo operační systém využívají rozhraní API EIM k provedení vyhledávací operace tak, aby aplikace nebo operační systém mohly provádět mapování od jedné totožnosti uživatele v jednom registru na další totožnost uživatele v jiném registru. Vyhledávací operace EIM je proces, kdy pomocí zadání některých známých a důvěryhodných informací aplikace nebo operační systém vyhledá neznámé přidružení totožnosti uživatele v daném cílovém registru.

Aplikace využívající rozhraní API EIM mohou provádět vyhledávací operace určitých informací pouze v případě, jsou-li tyto informace uloženy v doméně EIM. Aplikace může provádět jednu ze dvou typu vyhledávacích operací EIM podle typu informací, které jsou dodány aplikací jako zdroj vyhledávací operace EIM: totožnost uživatele nebo identifikátor EIM.

V případě, že aplikace nebo operační systém využívají rozhraní API eimGetTargetFromSource() za účelem získání totožnosti cílového uživatele pro daný cílový registr, pak aplikace nebo operační systém musí zadat *totožnost uživatele jako zdroj* pro vyhledávací operace. Aby totožnost uživatele mohla sloužit jako zdroj vyhledávací operace EIM, musí být pro totožnost uživatele definováno zdrojové přidružení identifikátorů, nebo musí být kryta přidružením zásad. Pokud aplikace nebo operační systém využívá rozhraní API, je nutné zadat tři druhy informací:

- Totožnost uživatele jako zdroj, neboli počáteční bod operace.
- Jméno definice registru EIM pro zdrojovou totožnost uživatele.
- Jméno definice registru EIM, který je cílem vyhledávací operace EIM. Tato definice registru popisuje registr uživatelů, jenž obsahuje totožnost uživatele, kterou aplikace hledá.

V případě, že aplikace nebo operační systém využívají rozhraní API eimGetTargetFromIdentifier() za účelem získání totožnosti uživatele pro daný cílový registr, pak aplikace nebo operační systém musí dodat *identifikátor EIM jako zdroj* pro vyhledávací operaci EIM. Pokud aplikace využívá toto rozhraní API, je nutné, aby aplikace dodala dva druhy informací:

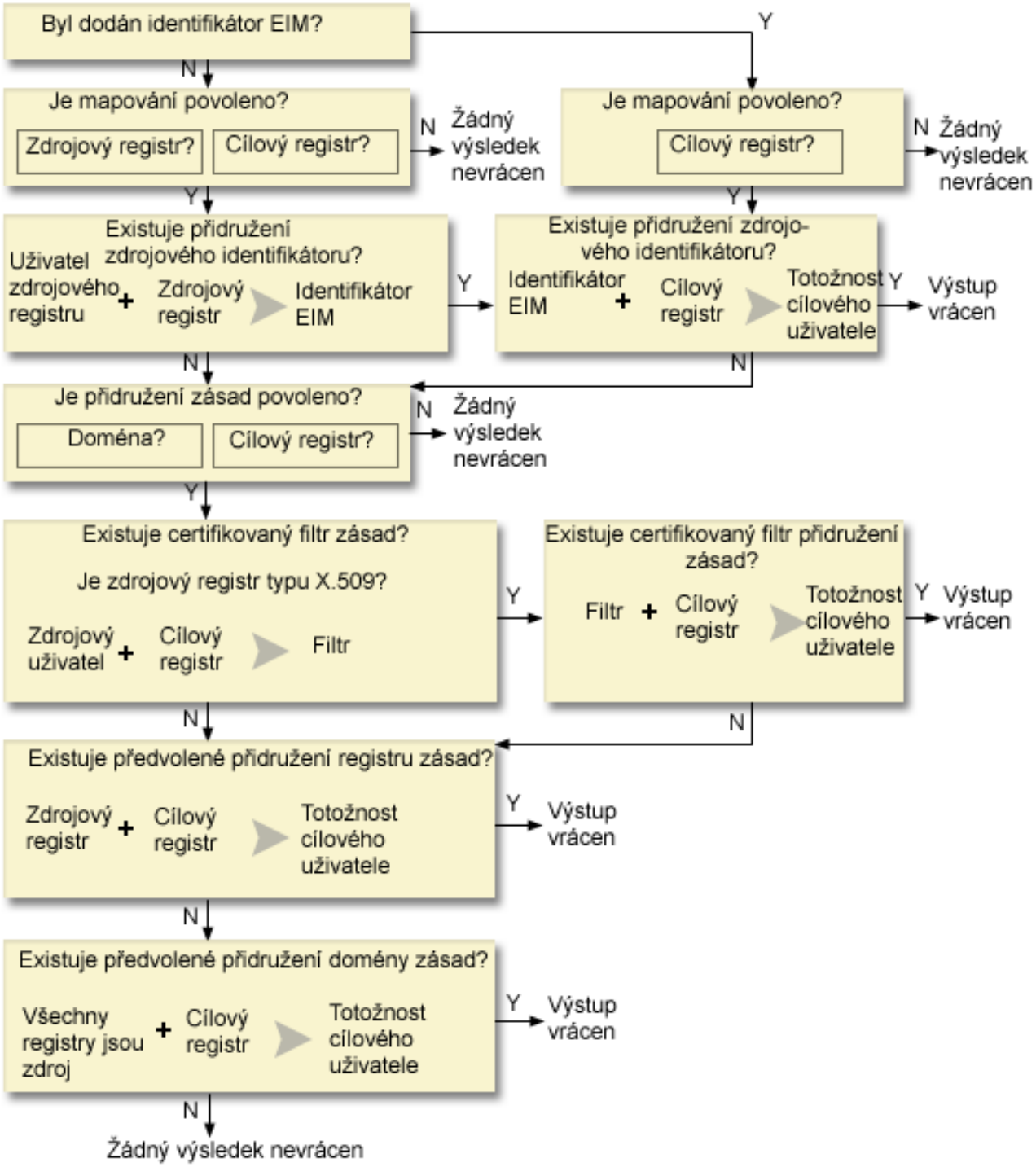
- Totožnost uživatele jako zdroj, neboli počáteční bod operace.
- Jméno definice registru EIM, který je cílem vyhledávací operace EIM. Tato definice registru popisuje registr uživatelů, jenž obsahuje totožnost uživatele, kterou aplikace hledá.

Aby se totožnost uživatele vrátila jako cíl jednotlivých typů vyhledávacích operací EIM, musí být pro totožnost uživatele definované cílové přidružení. Toto cílové přidružení může mít formu přidružení identifikátorů nebo přidružení zásad.

Dodaná informace bude předána EIM a vyhledávací operace EIM vyhledá a vrátí každou totožnost cílového uživatele. Vyhledávání probíhá, jak ilustruje obrázek č. 10, v následujícím pořadí:

1. Identifikátor cílového přidružení pro identifikátor EIM. Identifikátor EIM je identifikován jedním ze dvou způsobů: buď je dodán rozhraním API eimGetTargetFromIdentifier(), nebo je určen podle informací dodaných rozhraním API eimGetTargetFromSource().
2. Přidružení zásad filtru certifikátů.
3. Předvolené přidružení zásad registru.
4. Předvolené přidružení zásad domény.

Obrázek č. 10: Vývojový diagram obecného postupu zpracování vyhledávací operace EIM



Poznámka: V následujícím vývojovém diagramu vyhledávací operace nejprve zkontroluje definice individuálního registru, jako například zadaný zdrojový registr nebo cílový registr. Pokud vyhledávací operace selže při vyhledávání mapování pomocí definice individuálního registru, pak tato operace zjišťuje, zda je definice individuálního registru členem definice skupinového registru. Pokud je členem definice skupinového registru, vyhledávací operace zkontroluje definici skupinového registru, aby vyhověla požadavku vyhledávání mapování.

Vyhledávací operace probíhá tímto způsobem:

1. Vyhledávací operace zjišťuje, zda jsou povolena vyhledávání mapování. Vyhledávací operace určí, zda jsou vyhledávání mapování povolena jak pro uvedený zdrojový registr, tak pro uvedený cílový registr, nebo pro oba specifikované registry. Pokud nejsou vyhledávání mapování povolena pro jeden nebo oba registry, vyhledávací operace se ukončí, aniž by vrátila totožnost cílového uživatele.
2. Vyhledávací operace zkontroluje, zda existují přidružení identifikátorů, která odpovídají kritériím pro vyhledávání. Pokud byl poskytnut identifikátor EIM, vyhledávací operace bude využívat zadaného jména identifikátoru EIM. V opačném případě vyhledávací operace zkontroluje, zda existuje určité zdrojové přidružení identifikátoru, které odpovídá totožnosti zdrojového uživatele a zdrojovému registru. Pokud ano, vyhledávací operace jej použije k určení příslušného jména identifikátoru EIM. Vyhledávací operace pak použije jméno identifikátoru EIM k vyhledání individuálního cílového přidružení pro identifikátor EIM, který se shoduje se zadaným jménem definice cílového registru EIM. Existuje-li odpovídající individuální cílové přidružení identifikátorů, vyhledávací operace vrátí totožnost cílového uživatele definovanou v cílovém přidružení.
3. Vyhledávací operace zjišťuje, zda je povoleno použít přidružení zásad. Vyhledávací operace pomocí přidružení zásad zkontroluje, zda je v doméně povoleno vyhledávaní mapování pomocí přidružení zásad. Vyhledávací operace také zkontroluje, zda je povoleno cílovému registru použít přidružení zásad. Pokud není v doméně nebo registru povoleno použití přidružení zásad, vyhledávací operace se ukončí, aniž by vrátila totožnost cílového uživatele.
4. Vyhledávací operace hledá přidružení zásad filtru certifikátů. Vyhledávací operace zkontroluje, zda je zdrojový registr registrem typu X.509. Je-li typ registru X.509, vyhledávací operace zkontroluje, zda existuje přidružení zásad filtru certifikátů, které odpovídá jménům definice zdrojového a cílového registru. Vyhledávací operace zkontroluje, zda certifikáty zdrojového registru X.509 odpovídají nastavení, které bylo zadáno přidružením zásad filtru certifikátů. Existuje-li odpovídající přidružení zásad a existují-li certifikáty, které odpovídají kritériím filtrů certifikátů, vyhledávací operace vrátí příslušnou totožnost cílového uživatele pro toto přidružení zásad.
5. Vyhledávací operace hledá předvolená přidružení zásad registru.Vyhledávací operace zkontroluje, zda existuje předvolené přidružení zásad registru, které odpovídá jménu definice cílového registru. Existuje-li odpovídající přidružení zásad, vyhledávací operace vrátí příslušnou totožnost cílového uživatele pro přidružení zásad.
6. Vyhledávací operace hledá předvolená přidružení zásad domény. Vyhledávací operace zkontroluje, zda existuje předvolené přidružení zásad domény definované pro definici cílového registru. Existuje-li odpovídající přidružení zásad, vyhledávací operace vrátí přidruženou totožnost cílového uživatele pro toto přidružení zásad.
7. Vyhledávací operace nevrátí žádné výsledky.

Chcete-li se dozvědět více o operacích vyhledávání EIM (Enterprise Identity Mapping), najdete další informace v rámci těchto příkladů:

Související pojmy

"Doména EIM" na stránce 6
Doména EIM je adresář v rámci serveru LDAP (Lightweight Directory Access Protocol), který obsahuje podniková data.

"Přidružení zásad" na stránce 21
Zásady mapování EIM umožňuje administrátorovi produktu EIM vytvářet a používat přidružení zásad, chce-li definovat vztah mezi několika totožnostmi uživatele v jednom nebo více registrech uživatelů a jedinou totožností uživatele v jiném registru uživatelů.

"Řadič domény EIM" na stránce 6
Doména EIM je server LDAP (Lightweight Directory Access Protocol), který je konfigurován pro správu jedné nebo více domén EIM. Doména EIM obsahuje všechny EIM identifikátory, přidružení EIM a uživatelské registry, které jsou definovány v doméně. Systémy (klienti EIM) se účastní domény tím způsobem, že používají data domény pro vyhledávací operace EIM.

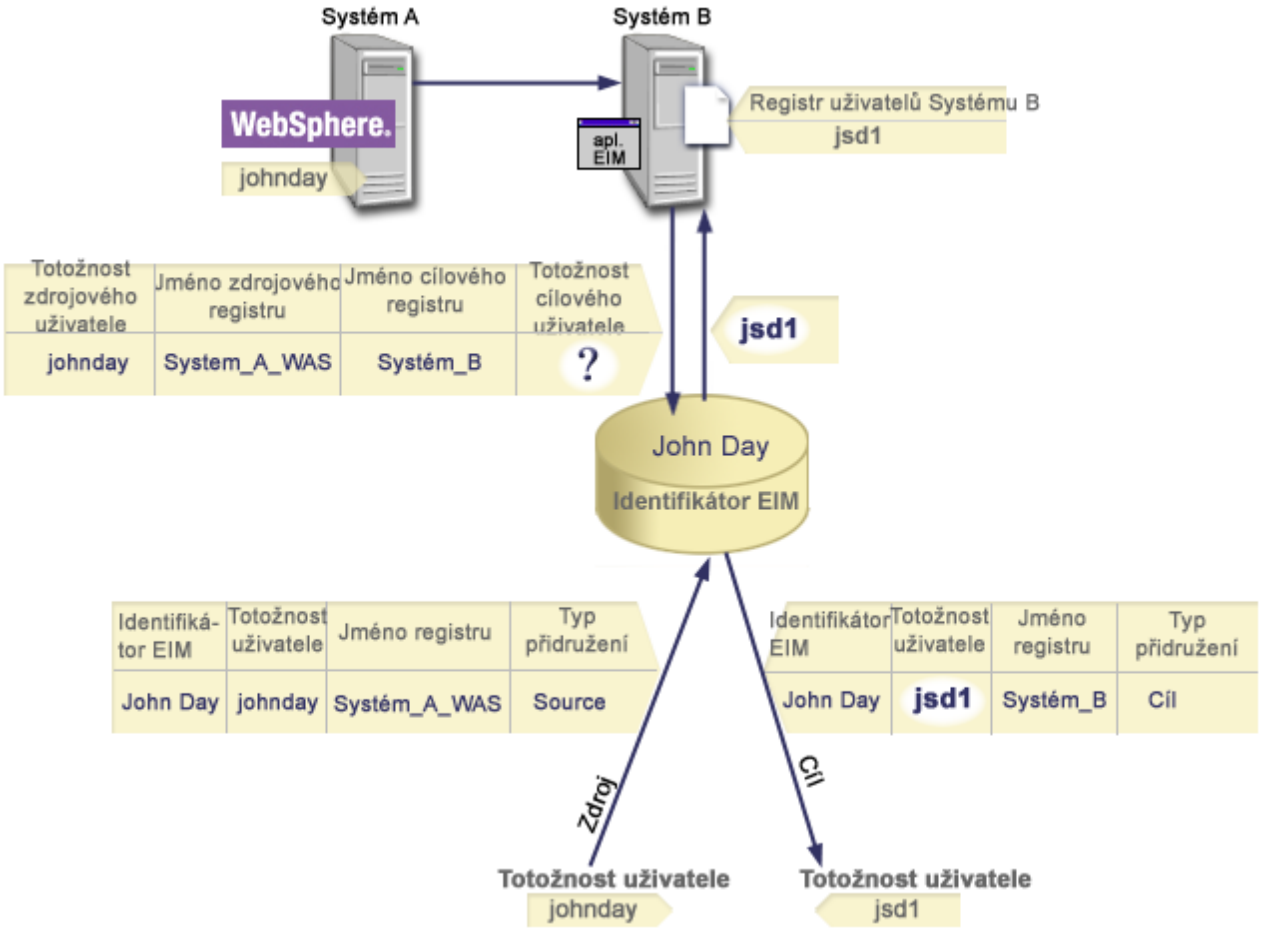
"Vyhledávací informace" na stránce 16
Produkt EIM poskytuje volitelná data, kterým se říká vyhledávací operace, pro další určení totožnosti cílového uživatele. Zmíněná totožnost cílového uživatele může být zadána buď v přidružení identifikátorů, nebo v přidružení zásad.

Příklady vyhledávací operace: Příklad 1

Tento příklad použijte, chcete-li se dozvědět více o tom, jak vyhledávací operace vrací cílovou totožnost uživatele z daných přidružení identifikátorů na základě známé totožnosti uživatele.

Na obrázku č. 11, se totožnost uživatele johnday ověřuje k serveru WebSphere Application Server použitím LPTA (Lightweight Third-Party Authentication) v Systému A. Server WebSphere Application Server v Systému A volá integrovaný program v Systému B pro přístup k datům v Systému B. Integrovaný program použije rozhraní API EIM k provedení vyhledávací operace v Systému A založené na totožnosti uživatele jako zdroje operace. Za účelem provedení operace zadá aplikace následující informace: johnday jako zdrojovou totožnost uživatele, Systém_A_WAS jako zdrojové jméno definice registru EIM a Systém_B jako cílové jméno definice registru EIM. Tyto zdrojové informace jsou předány EIM a vyhledávací operace EIM hledá zdrojové přidružení identifikátorů, které odpovídá zadané informaci. Prostřednictvím jména identifikátoru EIM John Day vyhledá vyhledávací operace EIM cílové přidružení identifikátorů pro identifikátor, jenž odpovídá cílovému jménu definice registru EIM pro Systém_B. Když je odpovídající cílové přidružení nalezeno, vyhledávací operace vrátí totožnost uživatele jsd1 zpět aplikaci.

Obrázek č. 11: Vyhledávací operace vrací cílovou totožnost uživatele z daných přidružení identifikátorů na základě známé totožnosti uživatele johnday.



Příklady vyhledávací operace: Příklad 2

Tento příklad použijte, chcete-li se dozvědět více o tom, jak vyhledávací operace vrací cílovou totožnost uživatele z daných přidružení identifikátorů na základě známé služby Kerberos.

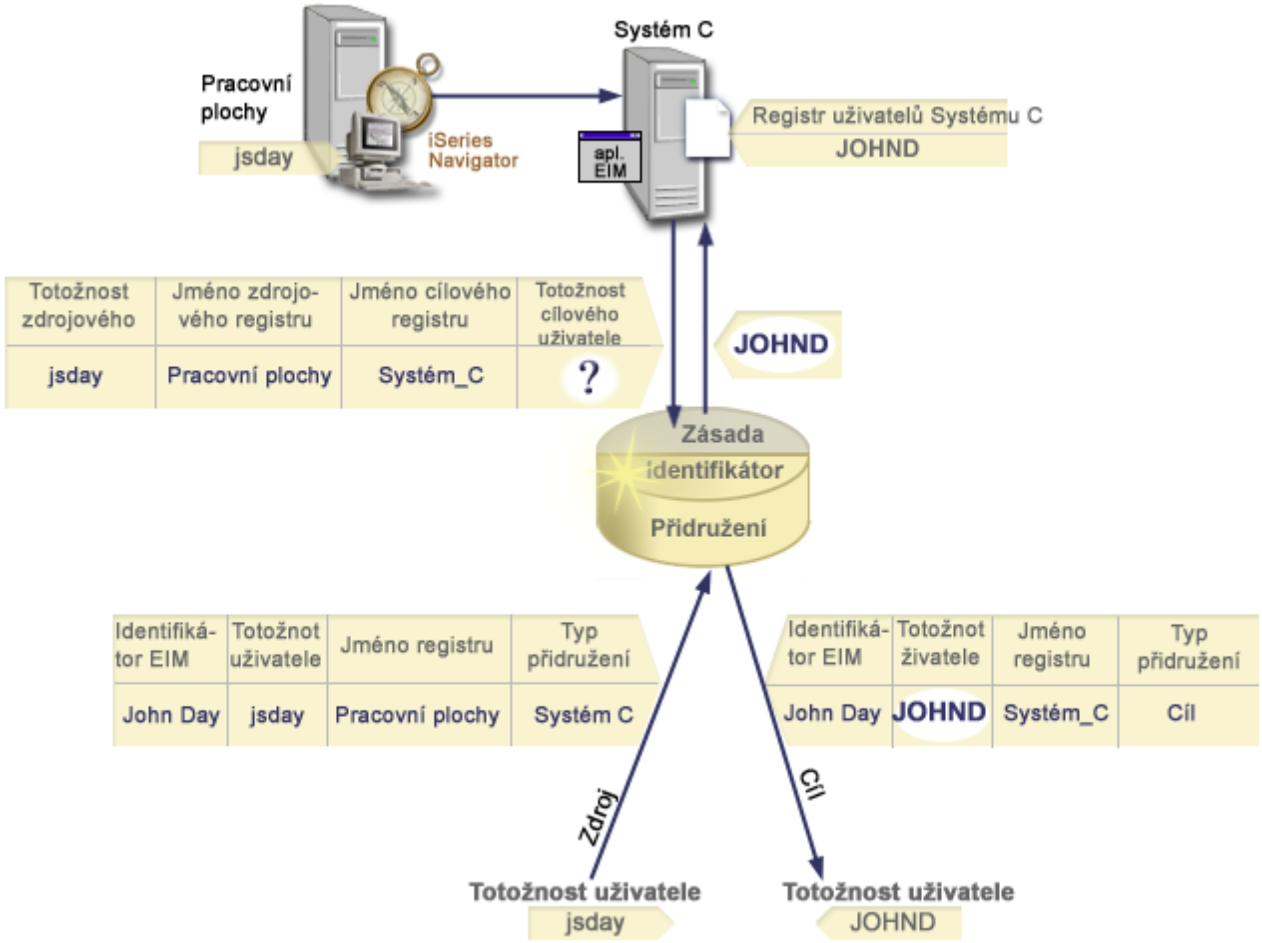
Na obrázku č. 12 chce administrátor mapovat uživatele operačního systému Windows v registru Windows Active Directory na profil uživatele operačního systému i5/OS. Windows používá sadu ověření Kerberos a jméno registru Windows Active Directory, jak je administrátor definoval v produktu EIM, bude Desktops. Totožnost uživatele, od níž

chce administrátor mapovat, je činitel Kerberos pojmenovaná jako jsday. Jméno registru i5/OS, jak jej administrátor definoval v EIM, je Systém_C, a totožnost uživatele, na kterou chce administrátor mapovat, je uživatelský profil jménem JOHND.

Administrátor vytvoří identifikátor EIM jménem John Day. Pak přidá dvě přidružení k tomuto identifikátoru EIM:

- Zdrojové přidružení pro činitele Kerberos jménem jsday v registru Desktops.
- Cílové přidružení pro uživatelský profil i5/OS jménem JOHND v registru Systém_C.

Obrázek č. 12: Vyhledávací operace EIM vrátí totožnost uživatele z daných přidružení identifikátorů na základě známého činitele Kerberos jsday.



Tato konfigurace umožňuje, aby se operace vyhledávání mapování mapovala z činitele Kerberos na uživatelský profil i5/OS následujícím způsobem:

Totožnost a registr zdrojového uživatele	**--->**	**Identifikátor EIM**	**--->**	**Totožnost cílového uživatele**
jsday v registru Desktops	--->	John Day	--->	JOHND (v registru Systém_C)

Vyhledávací operace probíhá tímto způsobem:

1. Uživatel jsday se přihlásí a ověřuje do Windows prostřednictvím činitele Kerberos v registru Windows Active Directory Desktops.

2. Uživatel otevře produkt System i Navigator, aby přistoupil k datům v systému Systém_C.
3. Operační systém i5/OS použije rozhraní API EIM k provedení vyhledávací operace EIM s totožností zdrojového uživatele jsday, zdrojovým registrem Desktops a cílovým registrem Systém_C.
4. Vyhledávací operace zkontroluje, zda jsou vyhledávání mapování povolena pro zdrojový registr Desktops a cílový registr Systém_C. Jsou.
5. Vyhledávací operace zkontroluje, zda dané zdrojové přidružení identifikátorů odpovídá zadané totožnosti zdrojového uživatele jsday ve zdrojovém registru Desktops.
6. Vyhledávací operace použije odpovídající zdrojové přidružení identifikátorů k určení příslušného jména identifikátoru EIM, kterým je John Day.
7. Vyhledávací operace použije toto jméno identifikátoru EIM k vyhledání cílového přidružení identifikátorů, které odpovídá zadanému jménu definice cílového registru EIM, kterým je Systém_C.
8. Takové cílové přidružení identifikátorů existuje a vyhledávací operace vrátí totožnost cílového uživatele jménem JOHND, jak bylo definováno v cílovém přidružení.
9. Po skončení operace vyhledávání mapování se produkt System i Navigator spustí pod uživatelským profilem JOHND. Oprávnění uživatele k přístupu k prostředkům a k provádění operací v rámci produktu System i Navigator je dáno spíše definovaným oprávněním pro uživatelský profil JOHND než definovaným oprávněním pro totožnost uživatele jsday.

Příklady vyhledávací operace: Příklad 3

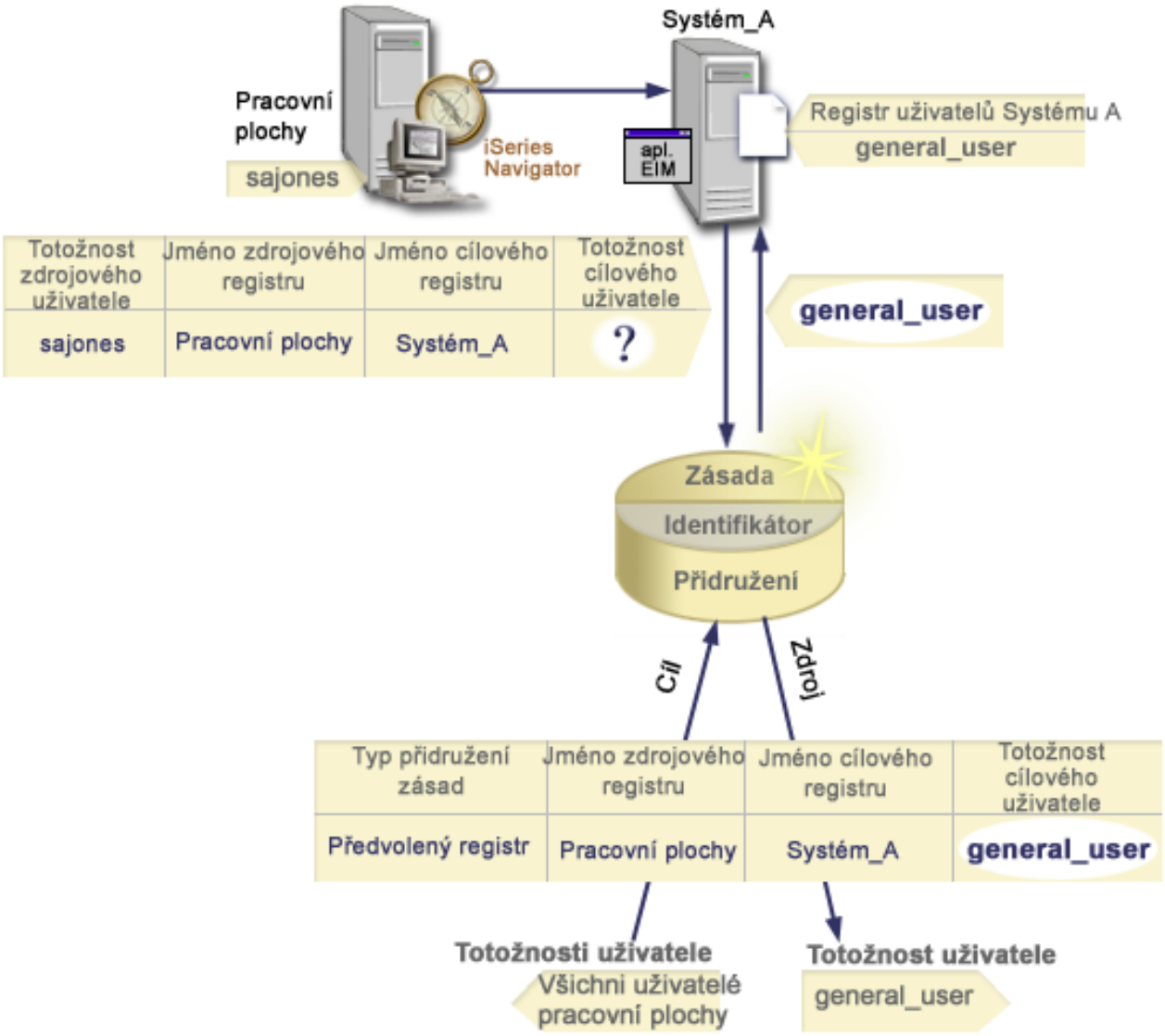
Tento příklad použijte, chcete-li se dozvědět více o tom, jak vyhledávací operace vrací cílovou totožnost uživatele z předvoleného přidružení zásady registru.

Na obrázku č. 13 chce administrátor mapovat všechny uživatele pracovních stanic v registru Windows Active Directory na jediný uživatelský profil i5/OS se jménem general_user v registru i5/OS, který v EIM pojmenoval jako Systém_A. Windows používá sadu ověření Kerberos a jméno registru Windows Active Directory, jak je administrátor definoval v produktu EIM, bude Desktops. Jedna z totožností uživatele, od které chce administrátor mapovat, je činitel Kerberos se jménem sajones.

Administrátor vytvoří předvolené přidružení zásad registru s následujícími informacemi:

- Zdrojový registr Desktops.
- Cílový registr Systém_A.
- Totožnost cílového uživatele general_user.

Obrázek č. 13: Vyhledávací operace vrátí totožnost cílového uživatele z předvoleného přidružení zásad registru.



Tato konfigurace umožňuje operaci vyhledávání mapování mapovat všechny činitele Kerberos v registru Desktops, včetně činitele sajones, k uživatelskému profilu i5/OS se jménem general_user následujícím způsobem:

Totožnost a registr zdrojového uživatele	**--->**	**Předvolené přidružení zásad registru**	**--->**	**Totožnost cílového uživatele**
sajones v registru Desktops	--->	Předvolené přidružení zásad registru	--->	general_user (v registru Systém_A)

Vyhledávací operace probíhá tímto způsobem:

1. Uživatel sajones se přihlásí a ověřuje na plochu Windows pomocí jeho činitele Kerberos v registru Desktops.
2. Uživatel otevře produkt System i Navigator, aby přistoupil k datům v systému System A.
3. Operační systém i5/OS používá rozhraní API EIM k provádění vyhledávací operace EIM s totožností zdrojového uživatele sajones, se zdrojovým registrem Desktops a s cílovým registrem Systém_A.
4. Vyhledávací operace EIM zkontroluje, zda jsou vyhledávání mapování povolena pro zdrojový registr Desktops a cílový registr Systém_A. Jsou.

5. Vyhledávací operace zkontroluje, zda dané zdrojové přidružení identifikátorů odpovídá zadané totožnosti zdrojového uživatele sajones ve zdrojovém registru Desktops. Nenajde však odpovídající zásadu identifikátorů.
6. Vyhledávací operace zkontroluje, zda je doméně umožněno používat přidružení zásad. Je.
7. Vyhledávací operace zkontroluje, zda je v cílovém registru (Systém_A) povoleno použití přidružení zásad. Je.
8. Vyhledávací operace zkontroluje, zda je zdrojový registr (Desktops) totožný s registrem X.509. Není.
9. Vyhledávací operace zkontroluje, zda existuje předvolené přidružení zásad registru, které odpovídá jménu definice zdrojového registru (Desktops) a jménu definice cílového registru (Systém_A).
10. Pokud existuje, vyhledávací informace vrátí general_user jako totožnost cílového uživatele.

Někdy se může stát, že vyhledávací operace EIM vrátí nejednoznačné výsledky. To nastane například tehdy, když více než jedna totožnost cílového uživatele odpovídá zadaným kritériím vyhledávací operace. Některé aplikace podporující EIM, včetně aplikací a produktů operačního systému i5/OS, nejsou schopny s těmito nejednoznačnými údaji zacházet, a proto mohou selhat nebo přinést neočekávané výsledky. Vyřešení této situace vyžaduje zásah operátora. Aby bylo možné zabránit například vzniku vícenásobné shody totožností cílového uživatele, budete potřebovat buď pozměnit vaši konfiguraci EIM, nebo definovat vyhledávací informaci pro každou totožnost cílového uživatele zvlášť. Rovněž můžete mapování otestovat a tím se ujistíte, že změny, které jste provedli, fungují podle vašich představ.

Příklady vyhledávací operace: Příklad 4

Tento příklad použijte, chcete-li se dozvědět více o tom, jak vyhledávací operace vrací cílovou totožnost uživatele v uživatelském registru, který je členem definice skupinového registru.

Administrátor chce mapovat uživatele operačního systému Windows na uživatelský profil operačního systému i5/OS. Kerberos je metoda ověření, kterou používá operační systém Windows, a jméno registru Kerberos, které administrátor definoval v aplikaci EIM (Enterprise Identity Mapping), zní Desktop_A. Totožnost uživatele, kterou chce administrátor mapovat, je služba Kerberos se jménem jday. Jméno registru i5/OS, jak jej administrátor definoval v EIM, je Group_1 a uživatelská totožnost, na kterou chce administrátor mapovat, je uživatelský profiol se jménem JOHND, který existuje ve třech individuálních registrech: Systém_B, Systém_C a Systém_D. Každý z těchto individuálních registrů je členem definice skupinového registru Group_1.

Administrátor vytvoří identifikátor EIM jménem John Day. Pak přidá dvě přidružení k tomuto identifikátoru EIM:

- Zdrojové přidružení pro činitele Kerberos jménem jday v registru Desktop_A.
- Cílové přidružení pro uživatelský profil i5/OS jménem JOHND v registru.

Tato konfigurace umožňuje, aby se operace vyhledávání mapování mapovala z činitele Kerberos na uživatelský profil i5/OS následujícím způsobem:

Totožnost a registr zdrojového uživatele	**--->**	**Identifikátor EIM**	**--->**	**Totožnost cílového uživatele**
jday v registru Desktop_A	--->	John Day	--->	JOHND (v definici skupinového registru Group_1)

Vyhledávací operace probíhá tímto způsobem:

1. Uživatel (jday) se přihlásí a je ověřena jeho totožnost v systému Windows na Desktop_A.
2. Uživatel otevře produkt System i Navigator, aby přistoupil k datům v systému Systém_B.
3. Operační systém i5/OS použije rozhraní API EIM k provedení vyhledávací operace EIM s totožností zdrojového uživatele jday, zdrojovým registrem Desktop_A a cílovým registrem Systém_B.
4. Vyhledávací operace EIM zkontroluje, zda jsou vyhledávání mapování povolena pro zdrojový registr (Desktop_A) a cílový registr (Systém_B).
5. Vyhledávací operace zkontroluje, zda dané zdrojové přidružení odpovídá zadané totožnosti zdrojového uživatele sajones ve zdrojovém registru Desktops.

6. Vyhledávací operace použije odpovídající zdrojové přidružení k určení příslušného jména identifikátoru EIM, kterým je John Day.
7. Vyhledávací operace použije toto jméno identifikátoru EIM k vyhledání individuálního cílového přidružení, které odpovídá zadanému jménu definice cílového registru EIM, kterým je Systém_C.
8. Vyhledávací operace zkontroluje, zda je zdrojový registr (Desktop_A) členem nějaké skupiny definicí registru. (Není.)
9. Vyhledávací operace zkontroluje, zda je cílový registr (Systém_B) členem nějaké skupiny definicí registru. Je členem definice skupinového registru Group_1.
10. Vyhledávací operace použije toto jméno identifikátoru EIM k vyhledání cílového individuálního přidružení, které odpovídá zadanému jménu definice cílového registru EIM, kterým je Systém_C.
11. Takové cílové individuální přidružení existuje a vyhledávací operace vrátí totožnost cílového uživatele jménem JOHND, jak bylo definováno v cílovém přidružení.

Poznámka: V některých případech vyhledávací operace EIM vrací nejednoznačné výsledky, když zadaným kritériím pro danou operaci vyhledávání odpovídá více než jedna totožnost cílového uživatele. Protože EIM nemůže vrátit jednu cílovou uživatelskou totožnost, mohou aplikace využívající EIM, včetně aplikací a produktů operačního systému i5/OS, které nejsou navrženy tak, aby uměly zacházet s těmito nejednoznačnými výsledky, selhat nebo vrátit neočekávané výsledky. Vyřešení této situace vyžaduje zásah operátora. Aby bylo možné zabránit například vzniku vícenásobné shody totožností cílového uživatele, budete potřebovat buď pozměnit vaši konfiguraci EIM, nebo definovat vyhledávací informaci pro každou totožnost cílového uživatele zvlášť. Můžete testovat mapování a ujistit se tak, že změny, které jste provedli, fungují podle vašich představ.

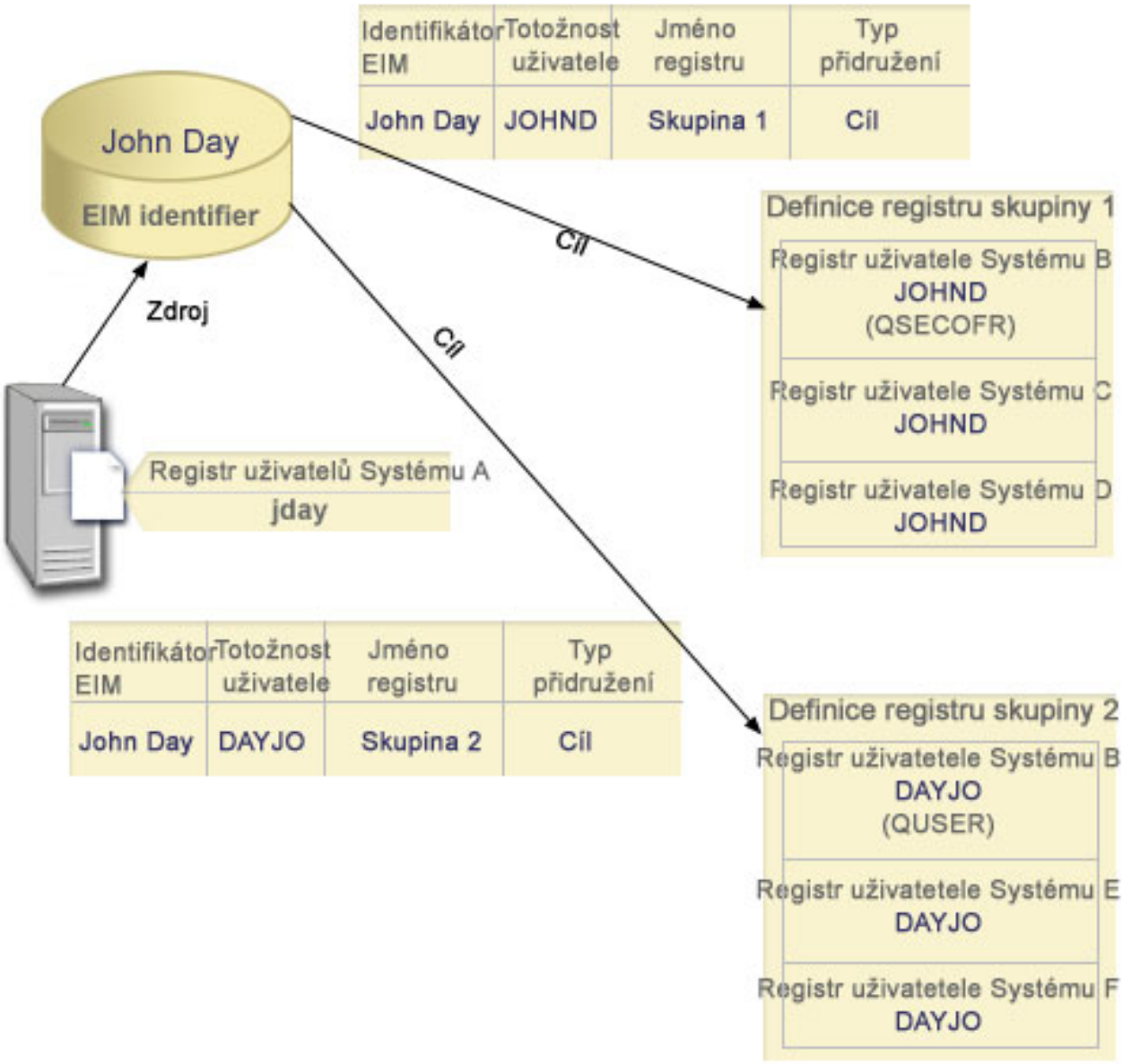
Příklady vyhledávací operace: Příklad 5

Tento příklad použijte, chcete-li se dozvědět více o vyhledávacích operacích, které vrací nejednoznačné výsledky zahrnující definice skupinového registru.

V některých případech vyhledávací operace vrací nejednoznačné výsledky, když zadaným kritériím pro dané vyhledávání odpovídá více než jedna totožnost cílového uživatele. Protože situace s nejednoznačnými výsledky mohou způsobit selhání nebo neočekávané výsledky u aplikací, které využívají EIM, musíte podniknout patřičné kroky, aby jste se na takovou situaci připravili.

Zvláště byste si měli být vědomi toho, že vyhledávací operace mohou vrátit nejednoznačné výsledky, pokud zadáte definici registru jednotlivého uživatele jako člena více než jedné definice skupinového registru. Pokud definice registru jednoho člena je členem definic registru více skupiny a vytvoříte přidružení jednotlivého identifikátoru EIM nebo přidružení zásad, která využívají definice skupinového registru jakožto buď zdrojový registr, nebo cílový registr, mohou vyhledávací operace vrátit nejednoznačné výsledky. Můžete například použít dvě různé uživatelské totožnosti pro dva různé typy systémových úloh, které provedete: jakožto administrátor systému provedete úlohy, které vyžadují uživatelskou totožnost s oprávněním QSECOFR, a provedete typické úlohy uživatele, které vyžadují uživatelskou totožnost s oprávněním QUSER. Pokud jsou obě totožnosti uživatele umístěné v rámci jednoho uživatelského registru, který je členem dvou různých definic skupinového registru, a vytvoříte cílové přidružení identifikátoru na obě cílové totožnosti uživatele, najde vyhledávací operace obě cílové totožnosti uživatele a následně vrátí nejednoznačné výsledky.

Níže uvedený příklad popisuje, jak může dojít k tomuto problému, pokud zadáte registr individuálního uživatele jakožto člena dvou definic skupinového registru a zadáte jednu z definic skupinového registru jako cílový registr ve dvou přidruženích individuálních identifikátorů EIM.



Příklad:

John Day má tyto uživatelské totožnosti v rámci definice systémového registru, který se nazývá uživatelský registr System B:

- JOHND
- DAYJO

Uživatelský registr System B je členem těchto definic skupinového registru:

- Skupina 1
- Skupina 2

Identifikátor EIM John Day má dvě cílové přidružení s těmito specifikacemi:

- Cílové přidružení: Cílový registr je Skupina 1 a obsahuje uživatelskou totožnost JOHND v uživatelském registru System B.

- Cílové přidružení: Cílový registr je Skupina 2 a obsahuje uživatelskou totožnost DAYJO v uživatelském registru System B .

V tomto případě vyhledávací operace vrací nejednoznačné výsledky, protože zadaným kritériím pro dané vyhledávání odpovídá více než jedna totožnost cílového uživatele; obě totožnosti uživatele (JOHND a DAYOJO) odpovídají zadaným kritériím vyhledávání.

Obdobně mohou vyhledávací operace mapování vrátit nejednoznačné výsledky, pokud vytvoříte dvě přidružení zásad (místo přidružení jednotlivých identifikátorů EIM), které využívají definice skupinového registru jako cílové registry.

Chcete-li zabránit tomu, aby vyhledávací operace vracely nejednoznačné výsledky zahrnující definice skupinového registru, zvažte tyto pokyny:

- Zadejte registr jednoho uživatele jako člena ne více než jedné definice skupinového registru.
- Dbejte zvýšené opatrnosti při vytváření jednotlivých přidružení identifikátorů EIM nebo přidružení zásad, které využívají definice skupinového registru buď jako zdrojový registr, nebo cílový registr. Ověřte, že definice skupinového registru není členem více než jedné definice skupinového registru. Buďte si vědomi toho, že pokud členem cílové definice skupinového registru je rovněž členem jiné definice skupinového registru, mohou vrátit vyhledávací operace nejednoznačné výsledky.
- Pokud dojde k situaci s nejednoznačnými výsledky, kdy zadáte definici individuálního registru jakožto člena více definic skupinového registru a vytvoříte přidružení individuálního identifikátoru nebo přidružení zásad využívající jednu z těchto definic skupinového registru buď jako zdrojový registr, nebo jako cílový registr, můžete zpřesnit vyhledávání definováním jednoznačné vyhledávací informace pro každou cílovou totožnost uživatele v každém přidružení.

V příkladu s panem John Day můžete pro každou cílovou totožnost uživatele definovat následující vyhledávací informace:

- Pro JOHND: Definujte jakožto vyhledávací informaci Administrator.
- Pro DAYJO: Definujte jakožto vyhledávací informaci User.

Avšak základní aplikace i5/OS, jako například System i Access for Windows, nemohou využívat vyhledávací informace k rozlišování mezi více totožnostmi cílových uživatelů, které vrátila vyhledávací operace. Tudíž můžete zvážit nová definování přidružení pro doménu a zajistit tak, že operace vyhledávání mapování bude vracet jedinou totožnost cílového uživatele. Tak také zajistíte, že základní aplikace i5/OS budou moci úspěšně provádět vyhledávací operace a mapovat totožnosti.

Související pojmy

"Definice skupinového registru" na stránce 15
Logické seskupování definic registru umožňuje zredukovat množství práce, které musíte provést, chcete-li konfigurovat mapování EIM. Definici skupinového registru lze spravovat obdobným způsobem jako definici individuálního registru.

Podpora a povolení zásad mapování EIM

Podpora zásad mapování produktu EIM (Enterprise Identity Mapping) vám umožní použít přidružení zásad stejně jako určitá přidružení identifikátorů v doméně EIM. Přidružení zásad můžete používat namísto přidružení identifikátorů nebo v kombinaci s ním.

Podpora zásad mapování EIM poskytuje prostředek k povolení a zakázání použití přidružení zásad pro celou doménu, stejně jako pro každý specifický cílový registr uživatelů. EIM vám také umožní nastavit, zda se obecně určitý registr může účastnit v operacích vyhledávání mapování. Podporu zásad mapování lze tedy použít pro přesnější kontrolu toho, jak operace vyhledávání mapování vrací výsledky.

Předvolené nastavení domény EIM znamená, že vyhledávání mapování využívající přidružení zásad jsou pro doménu zakázána. Je-li použití přidružení zásad pro doménu zakázáno, všechny operace vyhledávání mapování vrací výsledky pouze pomocí určitých přidružení identifikátorů mezi totožnostmi uživatele a identifikátory EIM.

Předvolené nastavení každého individuálního registru je takové, že účast vyhledávání mapování je povolena a použití přidružení zásad je zakázáno. Povolíte-li použití přidružení zásad pro individuální cílový registr, musíte také zajistit, aby bylo nastavení povoleno pro doménu.

Účast ve vyhledávání mapování a použití přidružení zásad lze nakonfigurovat pro každý registr jedním ze tří způsobů:

- Operace vyhledávání mapování nelze vůbec použít pro určitý registr. Jinými slovy, aplikace, která provádí vyhledávací operaci mapování zahrnující tento registr, selže při navrácení výsledků.
- Operace vyhledávání mapování mohou použít určitá přidružení identifikátorů pouze mezi totožnostmi uživatele a identifikátory EIM. Pro registr jsou povolena vyhledávání mapování, ale použití přidružení zásad je pro registr zakázáno.
- Operace vyhledávání mapování mohou použít určitá přidružení identifikátorů, pokud existují, a přidružení zásad, pokud určitá přidružení identifikátorů neexistují (všechna nastavení jsou povolena).

Související pojmy

"Vyhledávací informace" na stránce 16
Produkt EIM poskytuje volitelná data, kterým se říká vyhledávací operace, pro další určení totožnosti cílového uživatele. Zmíněná totožnost cílového uživatele může být zadána buď v přidružení identifikátorů, nebo v přidružení zásad.

"Předvolené přidružení zásad domény" na stránce 21
Předvolené přidružení zásad domény je typem přidružení zásad, který použijete k vytvoření mapování typu mnoho-na-jeden mezi totožnostmi uživatele.

"Předvolené přidružení zásad registru" na stránce 23
Předvolené přidružení zásad registru je typem přidružení zásad, které použijete k vytvoření mapování typu mnoho-na-jeden mezi totožnostmi uživatele.

"Vytvoření přidružení zásad" na stránce 99
Přidružení zásad umožňuje přímé definování vztahů mezi více totožnostmi uživatele v jednom či více registrech a jednotlivou totožností cílového uživatele v jiném registru.

Související úlohy

"Povolení přidružení zásad pro doménu" na stránce 85
Přidružení zásad umožňuje různé způsoby vytváření mapování typu mnoho-na-jeden v situaci, kdy neexistuje přidružení mezi totožnostmi uživatele a identifikátorem EIM.

"Povolení podpory vyhledávání mapování a použití přidružení zásad pro cílový registr" na stránce 92
Podpora zásad mapování EIM (Enterprise Identity Mapping) vám umožňuje používat přidružení zásad jako prostředek k vytvoření mapování typu mnoho-na-jeden tam, kde neexistuje přidružení mezi totožnostmi uživatele a identifikátorem EIM. Přidružení zásad můžete použít pro mapování zdrojové sady více totožností uživatele (spíše než jedné totožnosti uživatele) k jedné totožnosti cílového uživatele v daném cílovém registru uživatelů.

Kontrola přístupu k EIM

Uživatel EIM je uživatel, který vlastní kontrolu přístupu k produktu EIM. Tato kontrola přístupu k EIM je založena na skutečnosti, že uživatel je členem předvolené skupiny uživatelů LDAP (Lightweight Directory Access Protocol) pro danou doménu.

Zadáním řízení přístupu k EIM pro uživatele přidáte tohoto uživatele k určité skupině uživatelů LDAP pro konkrétní doménu. Každá skupina uživatelů LDAP má oprávnění k provádění určitých administračních úkolů EIM pro tuto doménu EIM. Jak a jaké typy administračních úloh, včetně vyhledávacích operací, může uživatel provádět, určuje skupina pro kontrolu přístupu, do níž uživatel EIM náleží.

Poznámka: Při konfiguraci EIM budete muset dokázat, že jste důvěryhodní v kontextu celé sítě, a nikoli pouze v jednom systému. Oprávnění ke konfiguraci EIM je založeno spíše na vašem oprávnění ke kontrole přístupu k EIM, než na vašem oprávnění daném uživatelským profilem i5/OS. EIM je síťový prostředek, nikoli prostředek pro jeden konkrétní systém. Proto také EIM nemůže rozpoznat zvláštní oprávnění ke konfiguraci specifická pro operační systém i5/OS, jako jsou například oprávnění *ALLOBJ a *SECADM. Jakmile bude produkt EIM nakonfigurován, oprávnění k provádění jednotlivých úkolů se pak bude moci zakládat na větším počtu odlišných typů uživatelů, včetně uživatelských profilů i5/OS. Například produkt

IBM Tivoli Directory Server for i5/OS zachází s profily operačního systému i5/OS se zvláštním oprávněním *ALLOBJ a *IOSYSCFG jako s administrátory adresářů.

Pouze uživatelé, kteří mají kontrolu přístupu administrátora EIM, mohou přidávat jiné uživatele do skupiny kontroly přístupu nebo měnit nastavení jiných uživatelů. Dříve než se uživatel může stát členem skupiny kontroly přístupu k EIM, musí mít přístup k serveru adresářů, jenž vystupuje jako řadič domény EIM. Členem skupiny kontroly přístupu k EIM se tedy může stát pouze určitý typ uživatelů. Totožnost uživatele může být ve formě činitele Kerberos, rozlišovacího jména LDAP nebo uživatelského profilu i5/OS, dokud je totožnost uživatele definována na serveru adresářů.

Poznámka: Chcete-li, aby byl v EIM dostupný typ uživatele činitele Kerberos, musí být v systému nakonfigurována služba síťového ověření. Aby byl k dispozici pro EIM uživatelský profil i5/OS, musíte na serveru adresářů nakonfigurovat systémovou příponu objektu. To umožní serveru adresářů odkazovat se na systémové objekty i5/OS, jako jsou uživatelské profily i5/OS.

Následující informace jsou stručným popisem funkcí, které může provádět každá skupina oprávnění EIM:

Administrátor LDAP (Lightweight Directory Access Protocol)

Administrátor LDAP je zvláštní rozlišovací jméno (DN) v adresáři, jenž je administrátorem pro celý adresář. Znamená to, že administrátor LDAP má přístup ke všem administračním funkcím EIM, stejně jako k celému adresáři. Uživatel s touto kontrolou přístupu může provádět následující funkce:

- Vytvořit doménu.
- Vymazat doménu.
- Vytvořit nebo odstranit identifikátory EIM.
- Vytvořit nebo odstranit definice registrů EIM.
- Vytvořit nebo odstranit zdrojová, cílová a administrační přidružení.
- Vytvořit nebo odstranit přidružení zásad.
- Vytvořit nebo odstranit filtry certifikátů.
- Povolit nebo zakázat používání přidružení zásad pro doménu.
- Povolit nebo zakázat vyhledávání mapování pro registr.
- Povolit nebo zakázat používání přidružení zásad pro registr.
- Provádět vyhledávací operace EIM.
- Vyhledat přidružení identifikátorů, přidružení zásad, filtr certifikátů, identifikátory EIM a definice registrů EIM.
- Přidat, odstranit nebo vypsat seznam informací o kontrole přístupu k EIM.
- Měnit a odstraňovat informace o oprávnění pro uživatelský registr.

Administrátor EIM

Členství v této skupině kontroly přístupu uživateli umožňuje spravovat veškerá data EIM v rámci domény EIM. Uživatel s touto kontrolou přístupu může provádět následující funkce:

- Vymazat doménu.
- Vytvořit nebo odstranit identifikátory EIM.
- Vytvořit nebo odstranit definice registrů EIM.
- Vytvořit nebo odstranit zdrojová, cílová a administrační přidružení.
- Vytvořit nebo odstranit přidružení zásad.
- Vytvořit nebo odstranit filtry certifikátů.
- Povolit nebo zakázat používání přidružení zásad pro doménu.
- Povolit nebo zakázat vyhledávání mapování pro registr.
- Povolit nebo zakázat používání přidružení zásad pro registr.

- Provádět vyhledávací operace EIM.
- Vyhledat přidružení identifikátorů, přidružení zásad, filtr certifikátů, identifikátory EIM a definice registrů EIM.
- Přidat, odstranit nebo vypsat seznam informací o kontrole přístupu k EIM.
- Měnit a odstraňovat informace o oprávnění pro uživatelský registr.

Administrátor identifikátorů

Členství v této skupině kontroly přístupu umožňuje uživateli přidávat a měnit identifikátory EIM a také spravovat zdroj a administrační přidružení. Uživatel s touto kontrolou přístupu může provádět následující funkce:

- Vytvářet identifikátory EIM.
- Přidat nebo odstranit zdrojová přidružení.
- Přidat nebo odstranit administrační přidružení.
- Provádět vyhledávací operace EIM.
- Vyhledat přidružení identifikátorů, přidružení zásad, filtr certifikátů, identifikátory EIM a definice registrů EIM.

Operace mapování EIM.

Členství v této skupině kontroly přístupu umožňuje uživateli řídit operace vyhledávání mapování EIM. Uživatel s touto kontrolou přístupu může provádět následující funkce:

- Provádět vyhledávací operace EIM.
- Vyhledat přidružení identifikátorů, přidružení zásad, filtr certifikátů, identifikátory EIM a definice registrů EIM.

Administrátor registrů

Členství v této skupině kontroly přístupu umožňuje uživateli spravovat veškeré definice registrů EIM. Uživatel s touto kontrolou přístupu může provádět následující funkce:

- Přidat nebo odstranit cílová přidružení.
- Vytvořit nebo odstranit přidružení zásad.
- Vytvořit nebo odstranit filtry certifikátů.
- Povolit nebo zakázat vyhledávání mapování pro registr.
- Povolit nebo zakázat používání přidružení zásad pro registr.
- Provádět vyhledávací operace EIM.
- Vyhledat přidružení identifikátorů, přidružení zásad, filtr certifikátů, identifikátory EIM a definice registrů EIM.

Administrátor pro vybrané registry

Členství v této skupině kontroly přístupu uživateli umožňuje spravovat informace EIM pouze pro dané definice registrů uživatelů (jako je Registry_X). Členství v této skupině také umožňuje uživateli přidávat nebo odstraňovat cílová přidružení pouze pro danou definici registru uživatelů. K tomu, aby uživatel s touto kontrolou přístupu mohl využívat veškerých výhod operací vyhledávání mapování a přidružení zásad, měl by mít také kontrolu přístupu k **operacím mapování EIM**. Tato kontrola přístupu umožňuje uživateli provádět pro dané autorizované definice registru následující funkce:

- Vytvořit, odstranit nebo procházet seznam cílových přidružení pouze pro dané definice registrů EIM.
- Přidat nebo odstranit předvolená přidružení zásad domény.
- Přidat nebo odstranit přidružení zásad pouze pro dané definice registrů.
- Přidat filtry certifikátů pouze pro dané definice registrů.
- Povolit nebo zakázat vyhledávání mapování pouze pro dané definice registrů.
- Povolit nebo zakázat používání přidružení zásad pouze pro dané definice registrů.
- Vyhledat identifikátory EIM.
- Vyhledat přidružení identifikátorů a filtru certifikátů pouze pro dané definice registrů.

- Vyhledat informace o definici registru EIM pouze pro dané definice registrů.

Poznámka: Pokud je zadaná definice registru definicí registru skupiny, uživatel, který má oprávnění administrátora pro zvolený přístup k registrům, má přístup administrátora pouze ke skupině, a nikoliv ke členům skupiny.

Uživatel s oběma oprávněními kontroly přístupu **Administrátora pro vybrané registry** a **Operace vyhledávání mapování EIM** má možnost provádět následující funkce:

- Přidat nebo odstranit přidružení zásad pouze pro dané registry.
- Provádět vyhledávací operace EIM.
- Vyhledávat veškerá přidružení identifikátorů, přidružení zásad, filtru certifikátů a definice registrů EIM.

Vyhledání pověření

Tato skupina kontroly přístupu umožňuje uživateli načíst informace o oprávnění, například hesla.

Pokud chce uživatel s touto kontrolou přístupu provést další operace EIM, musí být tento uživatel členem skupiny kontroly přístupu, která poskytuje oprávnění pro požadovanou operaci EIM. Pokud například uživatel s touto kontrolou přístupu chce načíst cílové přidružení ze zdrojového přidružení, musí být tento uživatel členem jedné z těchto skupiny kontroly přístupu:

- Administrátor EIM.
- Administrátor identifikátorů.
- Operace vyhledávání mapování EIM.
- Administrátor registrů.

Související pojmy

"Pokyny pro EIM týkající se uživatelských profilů v systému i5/OS" na stránce 48
Schopnost provádět úkoly v produktu EIM (Enterprise Identity Mapping) není založena na oprávnění vašeho uživatelského profilu i5/OS, ale spíše na oprávnění řízení přístupu EIM.

"Identifikace potřebných dovedností a rolí" na stránce 52
Produkt EIM je navržen tak, že v malé organizaci může být za jeho konfiguraci a administraci snadno zodpovědná jediná osoba. Ve větší organizaci může být tato odpovědnost rozložena na více lidí.

Související úlohy

"Správa řízení přístupu uživatelů k EIM" na stránce 112
Uživatel EIM je uživatel, který vlastní oprávnění řízení přístupu EIM na základě členství v předdefinovaných skupinách uživatelů LDAP (Lightweight Directory Access Protocol). Uvedení kontroly přístupu k EIM pro uživatele přidá uživatele do určité skupiny uživatelů LDAP.

Skupina kontroly přístupu k EIM: Oprávnění rozhraní API

Tyto in formace zobrazují tabulky, které jsou organizovány operací produkt EIM (Enterprise Identity Mapping), kterou provádí rozhraní API.

Každá z následujících tabulek ukazuje jednotlivá rozhraní API EIM, různé skupiny kontroly přístupu k EIM a rovněž informaci o tom, zda má skupina kontroly přístupu oprávnění provádět určitou funkci produktu EIM.

Tabulka 1. Práce s doménami

Rozhraní API EIM	Administrátor LDAP	Administrátor EIM	Administrátor identifikátorů	Vyhledávání mapování EIM	Administrátor registrů	Administrátor pro vybraný registr
eimChangeDomain	X	X	-	-	-	-
eimCreateDomain	X	-	-	-	-	-
eimDeleteDomain	X	X	-	-	-	-
eimListDomains	X	X	-	-	-	-

Tabulka 2. Práce s identifikátory

Rozhraní API EIM	Administrátor LDAP	Administrátor EIM	Administrátor identifikátorů EIM	Vyhledávání mapování EIM	Administrátor registrů EIM	Administrátor registrů X 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

Tabulka 3. Práce s registry

Rozhraní API EIM	Administrátor LDAP	Administrátor EIM	Administrátor identifikátorů EIM	Vyhledávání mapování EIM	Administrátor registrů EIM	Administrátor registrů X 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	-	-	-	-

Tabulka 4. Práce s přidruženími identifikátorů. Pro rozhraní API eimAddAssociation() a eimRemoveAssociation() jsou k dispozici čtyři parametry určující typ přidružení, které je buď přidáváno, nebo odstraňováno. Oprávnění k těmto rozhraním API se liší v závislosti na typu přidružení specifikovaného v těchto parametrech. V níže uvedené tabulce je pro každé z těchto rozhraní API uveden typ přidružení.

Rozhraní API EIM	Administrátor LDAP	Administrátor EIM	Administrátor identifikátorů EIM	Vyhledávání mapování EIM	Administrátor registrů EIM	Administrátor registrů X EIM
eimAddAssociation (administrační)	X	X	X	-	-	-
eimAddAssociation (zdroj)	X	X	X	-	-	-
eimAddAssociation (zdroj a cíl)	X	X	X	-	X	X
eimAddAssociation (cíl)	X	X	-	-	X	X
eimListAssociations	X	X	X	X	X	X
eimRemoveAssociation (administrační)	X	X	X	-	-	-
eimRemoveAssociation (zdroj)	X	X	X	-	-	-
eimRemoveAssociation (zdroj a cíl)	X	X	X	-	X	X
eimRemoveAssociation (cíl)	X	X	-	-	X	X

Tabulka 5. Práce s přidruženími zásad

Rozhraní API EIM	Administrátor LDAP	Administrátor EIM	Administrátor identifikátorů EIM	Vyhledávání mapování EIM	Administrátor registrů EIM	Administrátor registrů X 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	-	-	-	-	-	

Tabulka 6. Práce s mapováním

Rozhraní API EIM	Administrátor LDAP	Administrátor EIM	Administrátor identifikátorů EIM	Vyhledávání mapování EIM	Administrátor registrů EIM	Administrátor registrů X EIM
eimGetAssociatedIdentifier	X	X	X	X	X	X
eimGetTargetFromIdentifier	X	X	X	X	X	X
eimGetTargetFromSource	X	X	X	X	X	X

Tabulka 7. Práce s přístupem

Rozhraní API EIM	Administrátor LDAP	Administrátor EIM	Administrátor identifikátorů EIM	Vyhledávání mapování EIM	Administrátor registrů EIM	Administrátor registrů X EIM
eimAddAccess	X	X	-	-	-	-
eimListAccess	X	X	-	-	-	-
eimListUserAccess	X	X	-	-	-	-
eimQueryAccess	X	X	-	-	-	-
eimRemoveAccess	X	X	-	-	-	-

Skupina kontroly přístupu k EIM: Oprávnění k úlohám EIM

Tyto informace popisují tabulku, která zobrazuje vztahy mezi různými skupinami kontroly přístupu k produktu EIM (Enterprise Identity Mapping) a operacemi EIM, které mohou provádět.

Přestože administrátor LDAP není v tabulce uveden, tato úroveň kontroly přístupu se vyžaduje k vytvoření nové domény EIM. Administrátor LDAP má rovněž stejnou kontrolu přístupu jako administrátor EIM, avšak administrátor EIM automaticky stejnou kontrolu přístupu jako administrátor LDAP nemá.

Tabulka 8. Tabulka 1: Skupiny kontroly přístupu k EIM

Úloha EIM	Administrátor EIM	Administrátor identifikátorů	Operace vyhledávání mapování EIM	Administrátor registrů	Administrátor pro vybraný registr	Vyhledat pověření
Vytvořit doménu	-	-	-	-	-	
Vymazat doménu	X	-	-	-	-	
Modifikovat doménu	X	-	-	-	-	
Povolit/Zakázat přidružení zásad pro doménu	X	-	-	-	-	
Prohledat domény	X	-	-	-	-	

Tabulka 8. Tabulka 1: Skupiny kontroly přístupu k EIM (pokračování)

Úloha EIM	Administrátor EIM	Administrátor identifikátorů	Operace vyhledávání mapování EIM	Administrátor registrů	Administrátor pro vybraný registr	Vyhledat pověření
Přidat systémový registr	X	-	-	-	-	
Přidat aplikační registr	X	-	-	-	-	
Odstranit registr	X	-	-	-	-	
Modifikovat registr	X	-	-	X	X	
Povolit/Zakázat vyhledávání mapování pro registr	X	-	-	X	X	
Povolit/Zakázat přidružení zásad pro registr	X	-	-	X	X	
Prohledat registry	X	X	X	X	X	
Přidat identifikátor	X	X	-	-	-	
Odstranit identifikátor	X	-	-	-	-	
Modifikovat identifikátor	X	X	-	-	-	
Prohledat identifikátory	X	X	X	X	X	
Načíst přidružené identifikátory	X	X	X	X	X	
Přidat/Odstranit administrační přidružení	X	X	-	-	-	
Přidat/Odstranit zdrojové přidružení	X	X	-	-	-	
Přidat/Odstranit cílové přidružení	X	-	-	X	X	
Přidat/Odstranit přidružení zásad	X	-	-	X	X	
Přidat/Odstranit filtr certifikátů	X	-	-	X	X	
Vyhledat filtr certifikátů	X	X	X	X	X	
Prohledat přidružení	X	X	X	X	X	

Tabulka 8. Tabulka 1: Skupiny kontroly přístupu k EIM (pokračování)

Úloha EIM	Administrátor EIM	Administrátor identifikátorů	Operace vyhledávání mapování EIM	Administrátor registrů	Administrátor pro vybraný registr	Vyhledat pověření
Prohledat přidružení zásad	X	X	X	X	X	
Získat cílové přidružení ze zdrojového přidružení	X	X	X	X	-	
Získat cílové přidružení z identifikátoru	X	X	X	X	X	
Modifikovat uživatele registru	X	-	-	X	X	
Prohledat uživatele registru	X	X	X	X	X	
Modifikovat jméno alias registru	X	-	-	X	X	
Prohledat jména alias registrů	X	X	X	X	X	
Získat registr z jména alias	X	X	X	X	X	
Přidat/Odstranit kontrolu přístupu k EIM	X	-	-	-	-	
Zobrazit členy skupin pro kontrolu přístupu	X	-	-	-	-	
Zobrazit kontrolu přístupu k EIM určitého uživatele	X	-	-	-	-	
Dotázat se na kontrolu přístupu k EIM	X	-	-	-	-	
Modifikovat pověření	X	-	-	-	-	-
Načíst pověření	X	-	-	-	-	X
1 - Pokud je zadaná definice registru definicí skupinového registru, uživatel, který má oprávnění administrátora pro zvolený přístup k registrům, má přístup administrátora pouze ke skupině, a nikoliv ke členům skupiny.						

Koncepce LDAP pro EIM

Produkt EIM využívá server LDAP jako řadič domény pro ukládání dat EIM. Je proto nutné, abyste dobře pochopili koncepce LDAP, které se vztahují přímo ke konfiguraci a používání EIM ve vašem podniku. Rozlišovací jméno LDAP můžete například používat jako totožnost uživatele pro konfiguraci EIM a pro ověření k řadiči domény EIM.

Chcete-li správně porozumět konfiguraci a používání EIM, prostudujte si především následující koncepce LDAP:

Související pojmy

“Koncepce produktu EIM” na stránce 4
Abyste byli schopni celkově porozumět využití produktu EIM (Enterprise Identity Mapping) v rámci vašeho podniku, je nezbytné, abyste pochopili koncepce jeho fungování. Ačkoli se konfigurace a implementace pro určitá rozhraní API EIM může na jednotlivých platformách serverů lišit, jsou koncepce produktu EIM společné pro platformy IBM eServer.

Rozlišovací jméno

Rozlišovací jméno (DN) je záznam v LDAP (Lightweight Directory Access Protocol), který poskytuje jedinečnou identifikaci a popisuje záznam na serveru adresářů (LDAP). Pomocí průvodce konfigurací EIM provedete konfiguraci serveru adresářů, aby bylo možné ukládat informace o doméně EIM. Jelikož produkt EIM používá server adresářů k ukládání dat EIM, můžete použít rozlišovací jména jako prostředek ověření k řadiči domény EIM.

Rozlišovací jméno se skládá ze samotného záznamu a také ze jmen objektů (v pořadí zdola nahoru), které se nacházejí v adresáři LDAP nad ním. Příkladem úplného rozlišovacího jména tak může být cn=Tim Jones, o=IBM, c=US. Každý záznam má minimálně jeden atribut, který je využíván k pojmenování tohoto záznamu. Tento atribut pojmenování se nazývá relativní rozlišovací jméno záznamu (RDN). Záznam, který je umístěn nad daným RDN, se nazývá Nadřazené rozlišovací jméno. V tomto případě cn=Tim Jones pojmenovává záznam, je to tedy RDN. o=IBM, c=US jsou nadřazená DN pro cn=Tim Jones.

Jelikož EIM využívá server adresářů k ukládání dat EIM, můžete rozlišovací jméno použít pro totožnost uživatele, která se ověřuje k řadiči domény. Dále je také možno využít rozlišovací jméno pro totožnost uživatele, která konfiguruje produkt EIM ve vašem systému System i. Rozlišovací jméno můžete použít v následujících případech:

- Při konfiguraci serveru adresářů jako řadiče domény. Toto provedete vytvořením a používáním rozlišovacího jména, jež identifikuje administrátora LDAP pro server adresářů. Pokud nebyl již dříve server adresářů nakonfigurován, můžete tak učinit pomocí průvodce konfigurací EIM při vytvoření a vstupu do nové domény.
- Při použití průvodce konfigurací EIM, když vybíráte typ totožnosti uživatele, kterou bude průvodce používat pro připojení k řadiči domény. Rozlišovací jméno bude právě jeden z typů uživatele, který můžete vybrat. Rozlišovací jméno musí reprezentovat uživatele, který je oprávněn k vytváření objektů v lokálním prostoru pro jména na serveru adresářů.
- Při použití průvodce konfigurací EIM pro výběr typu uživatele k provádění operací EIM v zastoupení funkcí operačního systému. Tyto operace zahrnují operace vyhledávání mapování a výmaz přidružení v případě vymazávání lokálního uživatelského profilu i5/OS. Rozlišovací jméno bude právě jeden z typů uživatele, který můžete vybrat.
- Při připojování k řadiči domény pro administraci EIM, například pro správu registrů a identifikátorů k provádění operací vyhledávání mapování.
- Při vytváření filtrů certifikátů k určení rozsahu přidružení zásad filtru certifikátů. Když vytváříte filtr certifikátů, musíte dodat informaci o rozlišovacím jméně, buď pro DN subjektu, nebo pro DN vydávajícího, a také certifikát. Tak specifikujete kritéria, která bude filtr používat pro určení, jaké certifikáty budou ovlivněny přidružením zásad.

Související pojmy

“Nadřazené rozlišovací jméno” na stránce 47
Nadřazené rozlišovací jméno (DN) je záznam v prostoru pro jména serveru adresářů LDAP (Lightweight Directory Access Protocol). Záznamy serveru LDAP jsou řazeny hierarchicky, a to ve struktuře, která může odrážet politické, geografické, organizační a doménové hranice. Rozlišovací jméno DN je označeno za nadřazené DN v případě, kdy je DN bezprostředně nadřazeným záznamem adresáře jinému danému DN.

“Filtry certifikátů” na stránce 26
Filtr certifikátů definuje sadu podobných atributů certifikátu s rozlišujícím názvem pro skupinu uživatelských certifikátů ve zdrojovém registru uživatelů X.509. Dále můžete také využít filtr certifikátů jako základ pro přidružení zásad filtru certifikátů.

Související informace

Koncepce serveru adresářů

Nadřazené rozlišovací jméno

Nadřazené rozlišovací jméno (DN) je záznam v prostoru pro jména serveru adresářů LDAP (Lightweight Directory Access Protocol). Záznamy serveru LDAP jsou řazeny hierarchicky, a to ve struktuře, která může odrážet politické, geografické, organizační a doménové hranice. Rozlišovací jméno DN je označeno za nadřazené DN v případě, kdy je DN bezprostředně nadřazeným záznamem adresáře jinému danému DN.

Příkladem úplného rozlišovacího jména tak může být cn=Tim Jones, o=IBM, c=US. Každý záznam má minimálně jeden atribut, který je využíván k pojmenování tohoto záznamu. Tento atribut pojmenování se nazývá relativní rozlišovací jméno záznamu (RDN). Záznam, který je umístěn nad daným RDN, se nazývá nadřazené rozlišovací jméno. V tomto případě cn=Tim Jones pojmenovává záznam, je to tedy RDN. o=IBM, c=US jsou nadřazená DN pro cn=Tim Jones.

Produkt EIM (Enterprise Identity Mapping) používá server adresářů jako řadič domény pro ukládání dat pro doménu EIM. Nadřazené rozlišovací jméno DN v kombinaci se jménem domény EIM určuje umístění dat domény EIM v prostoru pro jména na serveru adresářů. Když použijete průvodce konfigurací EIM k vytvoření a vstupu do nové domény, můžete zadat toto nadřazené DN pro právě vytvářenou doménu. Použitím nadřazeného rozlišovacího jména zadáte, kde v prostoru pro jména LDAP budou uložena v paměti data EIM pro danou doménu. V případě, že nezadáte nadřazené DN, data EIM budou uložena v prostoru pro jména ve vlastní příponě a předvolené umístění dat domény EIM je ibm-eimDomainName=EIM.

Související pojmy

“Rozlišovací jméno” na stránce 46
Rozlišovací jméno (DN) je záznam v LDAP (Lightweight Directory Access Protocol), který poskytuje jedinečnou identifikaci a popisuje záznam na serveru adresářů (LDAP). Pomocí průvodce konfigurací EIM provedete konfiguraci serveru adresářů, aby bylo možné ukládat informace o doméně EIM. Jelikož produkt EIM používá server adresářů k ukládání dat EIM, můžete použít rozlišovací jména jako prostředek ověření k řadiči domény EIM.

Související informace

Koncepce serveru adresářů

Schéma LDAP a další pokyny týkající se EIM

Tyto informace použijte, chcete-li se dozvědět, co je třeba k tomu, aby server adresářů fungoval s produktem EIM (Enterprise Identity Mapping).

Produkt EIM vyžaduje, aby hostitelem řadiče domény byl server adresářů, který podporuje LDAP (Lightweight Directory Access Protocol), verze 3. Navíc produkt serveru adresářů musí být schopný přijmout schéma EIM a rozumět níže uvedeným atributům a objektovým třídám.

- Atribut ibm-entryUUID.
- Typy atributů IBM (ibmattributetypes):
  - acIEntry
  - acIPropagate
  - acISource
  - entryOwner
  - ownerPropagate
  - ownerSource
- Atributy EIM, včetně tří nových atributů pro podporu přidružení zásad:
  - 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

• Objektové třídy EIM, včetně tří nových tříd pro podporu přidružení zásad:
- ibm-eimApplicationRegistry
- ibm-eimDomain
- ibm-eimIdentifier
- ibm-eimRegistry
- ibm-eimRegistryUser
- ibm-eimSourceRelationship
- ibm-eimSystemRegsitry
- ibm-eimTargetRelationship
- ibm-eimFilterPolicy
- ibm-eimDefaultPolicy
- ibm-eimPolicyListAux

Související pojmy

"Řadič domény EIM" na stránce 6
Doména EIM je server LDAP (Lightweight Directory Access Protocol), který je konfigurován pro správu jedné nebo více domén EIM. Doména EIM obsahuje všechny EIM identifikátory, přidružení EIM a uživatelské registry, které jsou definovány v doméně. Systémy (klienti EIM) se účastní domény tím způsobem, že používají data domény pro vyhledávací operace EIM.

Koncepce EIM pro i5/OS

Produkt EIM můžete implementovat na jakékoliv platformě IBM eServer. Budete-li však implementovat produkt EIM v systému System i, měli byste znát určité informace, které jsou specifické pro implementaci v systému System i.

Chcete-li se dozvědět více o aplikacích i5/OS podporujících EIM, o pokynech týkajících se uživatelských profilů a o dalších tématech, která vám pomohou efektivně využívat EIM v systému System i, přečtěte si níže uvedené informace:

Související pojmy

"Koncepce produktu EIM" na stránce 4
Abyste byli schopni celkově porozumět využití produktu EIM (Enterprise Identity Mapping) v rámci vašeho podniku, je nezbytné, abyste pochopili koncepce jeho fungování. Ačkoli se konfigurace a implementace pro určitá rozhraní API EIM může na jednotlivých platformách serverů lišit, jsou koncepce produktu EIM společné pro platformy IBM eServer.

Pokyny pro EIM týkající se uživatelských profilů v systému i5/OS

Schopnost provádět úkoly v produktu EIM (Enterprise Identity Mapping) není založena na oprávnění vašeho uživatelského profilu i5/OS, ale spíše na oprávnění řízení přístupu EIM.

Avšak aby byl operační systém i5/OS připraven používat EIM, je nutné provést další úkoly. Tyto další úkoly vyžadují, abyste měli uživatelský profil i5/OS s odpovídajícími zvláštními oprávněními.

Chcete-li nastavit operační systém i5/OS tak, aby používal EIM, které bude používat produkt System i Navigator, váš uživatelský profil musí mít tato zvláštní oprávnění:

• Administrátor zabezpečení (*SECADM).

- Všechny objekty (*ALLOBJ).
- Konfigurace systému (*IOSYSCFG).

Rozšíření příkazů uživatelského profilu i5/OS pro identifikátory EIM

Jakmile jednou nakonfigurujete EIM pro váš systém, můžete využívat nového parametru EIMASSOC jak u příkazu CRTUSRPRF (Vytvoření uživatelského profilu), tak i u příkazu CHGUSRPRF (Změna uživatelského profilu). Tento parametr můžete používat k definování přidružení identifikátorů EIM pro uvedený uživatelský profil pro lokální registr.

Když použijete tento parametr, můžete zadat následující informace:

- Jméno identifikátoru EIM, což může být nové, nebo již existující jméno identifikátoru.
- Volba akce přidružení, která může přidat (*ADD), nahradit (*REPLACE) nebo odstranit (*REMOVE) přidružení, které určíte.

  Poznámka: K vytvoření nového přidružení použijte volbu *ADD. Volbu *REPLACE použijete například tehdy, když jste předtím definovali přidružení na špatný identifikátor. Volba *REPLACE odstraní všechna existující přidružení na jakékoliv jiné identifikátory zadaného typu pro lokální registr a pak přidá to přidružení, které je uvedené pro parametr. Volbu *REMOVE použijte k odstranění jakýchkoliv zadaných přidružení z uvedeného identifikátoru.
- Typ přidružení identifikátorů, jenž může být jak cílovým, tak i zdrojovým, nebo administračním přidružením.
- Zda se má vytvořit uvedený identifikátor EIM, jestliže již neexistuje.

Pro profil operačního systému i5/OS obvykle vytvoříte cílové přidružení, zvláště v prostředí jediného přihlášení. Poté, když použijete příkaz k vytvoření potřebného cílového přidružení (a identifikátoru EIM, je-li to nezbytné), můžete vytvořit odpovídající zdrojové přidružení. Chcete-li vytvořit zdrojové přidružení pro jinou totožnost uživatele, jako je například činitel Kerberos, kterou se uživatel přihlašuje do sítě, můžete použít produkt System i Navigator.

Když jste v systému nakonfigurovali EIM, zadali jste do systému totožnost a heslo uživatele, které budou používány při provádění operací EIM v zastoupení systému. Tato totožnost uživatele musí mít dostatečné oprávnění pro řízení přístupu k EIM pro vytváření identifikátorů a přidávání přidružení.

Hesla uživatelských profilů i5/OS a EIM

Vaším primárním cílem, jako administrátora systému, je při konfiguraci EIM jako části prostředí jediného přihlášení snížit náročnost správy uživatelských hesel, kterou musíte pro typického koncového uživatele v podniku provádět. Použijete-li mapování totožností, jež EIM umožňuje, v kombinaci s ověřením Kerberos, pak víte, že uživatelé budou muset provést méně přihlášení do systému a budou si muset pamatovat a spravovat méně hesel. Budete mít z toho prospěch, protože vás nebudou často volat kvůli problémům s totožnostmi uživatele a nebudou vás například volat kvůli nutnosti resetovat hesla, když uživatelé svá hesla zapomenou. Avšak vaše pravidla hesel a zásad zabezpečení ochrany dat stále platí a vy budete muset stále spravovat tyto uživatelské profily pro uživatele, kdykoli platnost hesla vyprší.

Chcete-li ještě lépe využívat výhody, které poskytuje prostředí jediného přihlášení do systému, můžete změnit nastavení hesel pro ty uživatelské profily, které jsou cílem mapování totožností. Jakožto cíl mapování totožnosti již uživatel nemusí zadávat heslo pro uživatelský profil, když přistupuje do systému System i nebo k prostředku operačního systému i5/OS aktivovanému pro EIM. Pro typického uživatele můžete nastavit heslo na *NONE, takže s uživatelským profilem se nemusí používat žádné heslo. Vlastník uživatelského profilu už nikdy nebude potřebovat heslo díky mapování totožností a jedinému přihlášení do systému. Nastavíte-li heslo na *NONE, budete mít další výhodu, protože se ani vy, ani vaši uživatelé nebudete muset starat o ukončení platnosti hesla. Navíc nikdo nebude moci využít tento profil k přímému přihlášení do systému System i nebo k přístupu k prostředkům EIM operačního systému i5/OS. Avšak můžete chtít, aby si administrátoři zachovali hesla pro své uživatelské profily v případě, že se někdy budou muset přímo přihlásit do systému System i. Jestliže například selže řadič domény EIM a mapování totožností nefunguje, administrátor může potřebovat schopnost přímého přihlášení do systému System i, dokud se problém s řadičem domény nevyřeší.

Související pojmy

“Kontrola přístupu k EIM” na stránce 38
Uživatel EIM je uživatel, který vlastní kontrolu přístupu k produktu EIM. Tato kontrola přístupu k EIM je založena na skutečnosti, že uživatel je členem předvolené skupiny uživatelů LDAP (Lightweight Directory Access Protocol) pro danou doménu.

Související informace

Příkaz CRTUSRPRF (Vytvoření uživatelského profilu)

Monitorování EIM v operačním systému i5/OS

Pro váš komplexní plán zabezpečení ochrany dat je důležité uvážit, jaké monitorování provádíte.

Při konfiguraci a používání produktu EIM (Enterprise Identity Mapping) možná budete chtít nakonfigurovat pro server adresářů podporu monitorování. Tím zajistíte odpovídající úroveň odpovědnosti, kterou vyžaduje vaše zásada zabezpečení ochrany dat. Podpora monitorování může být užitečná například tehdy, když potřebujete zjistit, který z uživatelů mapovaných přidružením zásad provedl ve vašem systému nějakou operaci nebo změnil objekt.

Související informace

Monitorování serveru adresářů

Aplikace operačního systému i5/OS podporující EIM

Produkt EIM umí používat různé aplikace i5/OS.

Níže uvedené aplikace i5/OS mohou být nakonfigurované tak, aby používaly produkt EIM (Enterprise Identity Mapping):

- Hostitelské servery i5/OS (v současné době používané System i Access for Windows
- a System i Navigator).
- Telnet Server (v současné době používaný PC5250 a IBM Websphere Host On Demand).
- QFileSrv.400 ODBC (umožňuje použití jediného přihlášení do systému prostřednictvím SQL).
- JDBC (umožňuje použití EIM prostřednictvím SQL).
- Distributed Relational Database Architecture (DRDA) (umožňuje použití EIM pomocí SQL).
- IBM WebSphere Host On-Demand verze 8, (funkce Web Express Logon).
- i5/OS NetServer
- QFileSvr.400

Scénáře: EIM (Enterprise Identity Mapping)

Tyto informace použijte, chcete-li se dozvědět více o tom, jak spravovat uživatelské totožnosti na více různých systémech v rámci prostředí jediného přihlášení.

Produkt EIM (Enterprise Identity Mapping) je technologií infrastruktury IBM, která vám umožní sledovat a spravovat totožnosti uživatele v rámci celého podniku. Obvykle se EIM používá spolu s technologií ověření, kterou je např. služba síťového ověření, k zavedení prostředí jediného přihlášení.

Související informace

Scénáře jediného přihlášení

Plánování EIM

Předtím než nastavíte EIM, měli byste vytvořit plán implementace EIM (Enterprise Identity Mapping) a zajistit úspěšnou konfiguraci EIM pro systém System i nebo platformu, kde je několik různých prostředí.

Plán implementace je nezbytnou podmínkou pro úspěšnou konfiguraci a používání produktu EIM (Enterprise Identity Mapping) v rámci vašeho podniku. Chcete-li vytvořit tento plán, budete muset shromáždit data o systému, o aplikacích a uživatelích, kteří budou EIM využívat. Shromážděné informace vám pak pomohou se správně rozhodnout, co bude nejlepší pro vlastní konfiguraci EIM ve vašem podniku.

Jelikož je EIM technologií infrastruktury IBM eServer dostupnou pro všechny platformy IBM, bude váš plán implementace záviset na tom, jaké platformy jsou ve vašem podniku. Ačkoli existuje značný počet plánovacích aktivit, jež jsou specifické zvlášť pro každou platformu, velký počet plánovacích aktivit EIM se může použít pro všechny platformy IBM. Při vytváření obecného plánu implementace byste měli pracovat se všeobecnými plánovacími aktivitami EIM. Informace o tom, jak naplánovat vaši implementaci EIM, naleznete pod následujícími odkazy:

Plánování EIM pro eServer

Chcete-li nakonfigurovat a úspěšně používat produkt EIM (Enterprise Identity Mapping) v podniku se smíšenými platformami, je nezbytné připravit plán implementace. Při přípravě plánu implementace budete potřebovat shromáždit data o systémech, aplikacích a uživatelích, kteří budou používat EIM. Shromážděné informace využijte při rozhodování o tom, jak nejlépe nakonfigurovat EIM ve smíšeném prostředí platforem.

Níže uvedený seznam poskytuje podrobný návod plánovacích úkolů, které byste měli provést před konfigurováním a používáním EIM ve smíšeném prostředí platforem. Přečtěte si informace na těchto stranách, chcete-li se dozvědět, jak úspěšně naplánovat konfigurační potřeby EIM včetně toho, jaké dovednosti potřebuje váš implementační tým, jaké informace potřebujete shromáždit a jaká rozhodnutí o konfiguraci musíte udělat. Možná vám pomůže, když si plánovací formuláře vytisknete (položka č. 8 v seznamu), takže si je budete moci v průběhu provádění plánovacího procesu vyplňovat.

Požadavky nastavení EIM (Enterprise Identity Mapping) pro eServer

Chcete-li produkt EIM (Enterprise Identity Mapping) úspěšně implementovat, musíte splnit tři oblasti požadavků: požadavky na úrovni podniku nebo sítě, systémové požadavky a aplikační požadavky.

požadavky na úrovni podniku nebo sítě

Ve vašem podniku nebo síti musíte nakonfigurovat jeden systém tak, aby fungoval jako řadič domény EIM. Je to zvlášť nakonfigurovaný server Lightweight Directory Access Protocol (LDAP), který ukládá a poskytuje data domény EIM. Existuje mnoho hledisek, která musí být vzata v úvahu při rozhodování o tom, jaký produkt adresářových služeb použít pro řadič domény, včetně faktu, že ne všechny produkty serveru LDAP podporují řadič domény EIM.

Dalším hlediskem je dostupnost nástrojů administrace. Jednou z voleb je možnost použít rozhraní API EIM ve vašich vlastních aplikacích k provádění administračních funkcí. Plánujete-li použít produkt IBM Tivoli Directory Server for i5/OS jako řadič domény EIM, můžete ke správě EIM použít produkt System i Navigator. Pokud plánujte použít produkt IBM Directory, můžete použít obslužný program eimadmin, který je součástí V1R4 LDAP SPE.

Informace uvedené níže poskytují základní informace o tom, které platformy IBM poskytují server adresářů, jenž podporuje EIM. Podrobnější informace o výběru serveru adresářů, který poskytuje podporu řadiče domény EIM, naleznete v Plánování řadiče domény EIM.

Systémové a aplikační požadavky

Každý systém, který se účastní v doméně EIM, musí splňovat následující požadavky:

- Mít nainstalovaný klientský software LDAP.
- Mít implementaci rozhraní API EIM.

Každá aplikace, která se bude účastnit v doméně EIM, musí být schopná používat rozhraní API EIM k vyhledávání mapování a k jiným operacím.

Poznámka: V případě distribuované aplikace nemusí být nutné, aby strany serveru i klienta byly schopné používat rozhraní API EIM. V běžných případech potřebuje používat rozhraní API EIM pouze strana serveru aplikace.

Níže uvedená tabulka ukazuje informace o podpoře EIM, kterou poskytují platformy eServer. Informace jsou uspořádány podle platformy a sloupce označují tyto údaje:

- Klient EIM nezbytný k tomu, aby platforma podporovala rozhraní API EIM.
- Typ konfiguračních a administračních nástrojů EIM, které jsou pro platformu k dispozici.
- Produkt serveru adresářů, který může být nainstalovaný, aby platforma sloužila jako řadič domény EIM.

Platforma nemusí sloužit jako řadič domény EIM, aby se mohla účastnit v doméně EIM.

Tabulka 9. Podpora EIM ze strany eServeru

Platforma	Klient EIM (podpora rozhraní API)	Řadič domény	Nástroje administrace EIM
AIX na systému System p	AIX R5.2	IBM Directory V5.1	Není k dispozici
Linux • SLES8 na PPC64 • Red Hat 7.3 na i386 • SLES7 na systému System z	Stáhněte si jeden z níže uvedených: • Klient IBM Directory V4.1. • Klient IBM Directory V5.1. • Klient Open LDAP v2.0.23	IBM Directory V5.1	Není k dispozici
i5/OS na systému System i	i5/OS V5R3 nebo pozdější	IBM Tivoli Directory Server for i5/OS	System i Navigator
Windows 2000 na systému System x	Stáhněte si jeden z níže uvedených: • Klient IBM Directory V4.1. • Klient IBM Directory V5.1.	Klient IBM Directory V5.1.	Není k dispozici
z/OS na systému System z	z/OS V1R4 LDAP SPE OW57137	z/OS V1R4 LDAP	V1R4 LDAP SPE OW57137

Pokud platforma poskytuje podporu klienta EIM (rozhraní API), pak se takový systém může účastnit v doméně EIM. Není nutné, aby platforma poskytovala podporu řadiče domény EIM, pokud nechcete ve svém podniku používat právě tuto platformu jako řadič domény EIM.

Související informace

IBM Tivoli Directory Server

Identifikace potřebných dovedností a rolí

Produkt EIM je navržen tak, že v malé organizaci může být za jeho konfiguraci a administraci snadno zodpovědná jediná osoba. Ve větší organizaci může být tato odpovědnost rozložena na více lidí.

Množství osob, které budete ve vašem týmu potřebovat, závisí na množství požadovaných dovedností, jež má každý člen týmu, na typech platforem zahrnutých do vaší implementace EIM a na tom, jak chce vaše organizace rozdělit úkoly zabezpečení ochrany dat a odpovědnost.

Úspěšná implementace EIM vyžaduje konfiguraci a vzájemnou součinnost několika softwarových produktů. Protože každý z těchto produktů vyžaduje specifické dovednosti a role, můžete sestavit implementační tým EIM, jenž by se skládal z odborníků z několika různých oborů, zvláště pracujete-li ve velké organizaci.

Níže uvedené informace popisují dovednosti a oprávnění nezbytná k úspěšné implementaci EIM. Tyto dovednosti se prezentují jako názvy pracovních pozic lidí, kteří jsou odborníky v dané oblasti. Například úkol vyžadující znalost protokolu LDAP (Lightweight Directory Access Protocol) je označován jako úkol pro administrátora serveru adresářů.

Členové týmu a jejich role

Níže uvedené informace popisují odpovědnosti a požadovaná oprávnění rolí, které jsou potřebné pro správu EIM. Tento seznam rolí můžete použít k určení členů týmu, kteří jsou nezbytní pro instalaci a konfiguraci předpokládaných produktů, konfiguraci EIM a jedné nebo více domén EIM.

Jedna z prvních sad rolí, kterou musíte definovat, je určení počtu a typu administrátorů pro doménu. Všichni pracovníci, kteří dostali administrační povinnosti a oprávnění EIM, musí být zapojeni do procesu plánování EIM jako členové implementačního týmu EIM.

Poznámka: Administrátoři EIM hrají ve vaší organizaci důležitou úlohu a mají stejné oprávnění jako jednotlivci, kteří mohou vytvářet v systému totožnosti uživatele. Když pro totožnosti uživatele vytvoří přidružení EIM, určují, kdo bude mít přístup do vašeho systému a jaká oprávnění při tom bude mít. Společnost IBM doporučuje, abyste toto oprávnění dali na základě zásad zabezpečení ochrany dat těm jednotlivcům, ke kterým máte důvěru.

Níže uvedená tabulka uvádí potenciální role členů týmu a úkoly a dovednosti potřebné ke konfiguraci a správě EIM.

Poznámka: Jestliže ve vaší organizaci bude za celou konfiguraci EIM a administrační úkoly zodpovědná jedna osoba, měla by mít roli a oprávnění administrátora EIM.

Tabulka 10. Role, úkoly a dovednosti pro konfiguraci EIM

Role	Oprávnění k úkolům	Požadované dovednosti
Administrátor EIM	• Koordinace operací domény • Přidání, odstranění a změna definic registru, identifikátorů EIM a přidružení totožností uživatele • Oprávnění řadiče k datům v rámci domény EIM	Znalost nástrojů administrace EIM
Administrátor identifikátorů EIM	• Vytváření a změna identifikátorů EIM • Přidání a odstranění administračních a zdrojových přidružení (není možné přidat nebo odstranit cílová přidružení)	Znalost nástrojů administrace EIM
Administrátor registrů EIM	Správa všech definic registru EIM • Přidání a odstranění cílových přidružení (není možné přidat nebo odstranit zdrojové a administrační přidružení) • Aktualizace definic registrů EIM	Znalost: • Všechny registry uživatelů definované v doméně EIM (jako jsou informace o totožnostech uživatele) • Nástroje administrace EIM
Administrátor registrů X EIM	Správa definice určitého registru EIM • Přidání a odstranění cílových přidružení pro určitý uživatelský registr (například registr X) • Aktualizace určité definice registru	Znalost: • Konkrétní registr uživatelů definovaný v doméně EIM (jako jsou informace o totožnostech uživatele) • Nástroje administrace EIM

Tabulka 10. Role, úkoly a dovednosti pro konfiguraci EIM (pokračování)

Role	Oprávnění k úkolům	Požadované dovednosti
Administrátor serveru adresářů (LDAP)	• Instalace a konfigurace serveru adresářů (jestliže to je nutné) • Přizpůsobení konfigurace serveru adresářů EIM • Vytvoření domény EIM (viz poznámka) • Definování uživatelů oprávněných přistupovat k řadiči domény EIM • Volitelné: definování prvního administrátora EIM **Poznámka:** Administrátor serveru adresářů může dělat všechno, co může dělat administrátor EIM.	Znalost: • Instalace serveru adresářů, konfigurace a přizpůsobení. • Nástroje administrace EIM
Administrátor registrů uživatelů	• Nastavování uživatelských profilů nebo totožností uživatele pro určitý registr uživatelů • Volitelné: slouží jako administrátor registrů EIM pro uvedený registr uživatelů	Znalost: • Nástroje pro administraci registru uživatelů • Nástroje administrace EIM
Systémový programátor nebo administrátor systému	Instalace potřebných softwarových produktů (může zahrnovat instalaci EIM)	Znalost: • Systémové programování nebo administrátorské dovednosti • Instalační procedury pro platformu
Aplikační programátor	Vytváření aplikací, jež používají rozhraní API EIM	Znalost: • Platforma • Programovací dovednosti • Kompilace programů

Související pojmy

"Kontrola přístupu k EIM" na stránce 38
Uživatel EIM je uživatel, který vlastní kontrolu přístupu k produktu EIM. Tato kontrola přístupu k EIM je založena na skutečnosti, že uživatel je členem předvolené skupiny uživatelů LDAP (Lightweight Directory Access Protocol) pro danou doménu.

Plánování domény EIM (Enterprise Identity Mapping)

Část výchozího implementačního plánovacího procesu produktu EIM (Enterprise Identity Mapping) vyžaduje, abyste definovali doménu EIM. Chcete-li získat maximální užitek z centralizované schránky mapovaných informací, je nutné naplánovat doménu tak, aby byla sdílena mnoha aplikacemi a systémy.

Když budete procházet celým tématem plánování EIM, budete shromažďovat informace, které potřebujete k definování domény a budete je zaznamenávat na plánovací formuláře. Vzorové sekce pracovních formulářů vám mohou pomoct shromáždit a zaznamenat tyto informace v každé etapě plánování.

Níže uvedená tabulka uvádí informace, které potřebujete shromáždit, když plánujte doménu a navrhujete role členů implementačního týmu EIM, kteří by mohli být zodpovědní za každou potřebnou informační položku.

Poznámka: I když tabulka uvádí daný úkol jako návrh přiřazení odpovědnosti za shromáždění popsaných informací, měli byste přiřadit role podle potřeb a zásady zabezpečení ochrany dat ve vaší organizaci. Například v menší organizaci můžete jako administrátora určit jednu osobu, která bude zodpovědná za všechny stránky plánování, konfigurace a správy EIM.

Tabulka 11. Informace potřebné ke plánování domény EIM

Potřebné informace	Role
1. Zda již existuje doména, která vyhovuje vašim potřebám, nebo zda byste ji měli vytvořit.	Administrátor EIM
2. Který server adresářů bude fungovat jako řadič domény EIM. (Podrobné informace o volbě řadiče domény najdete v tématu "Plánování řadiče domény EIM (Enterprise Identity Mapping)".)	Administrátor serveru adresářů (LDAP) nebo administrátor EIM
3. Jméno pro doménu. (Můžete také zadat volitelný popis.)	Administrátor EIM
4. Kde se v adresáři mají ukládat data domény EIM. **Poznámka:** V závislosti na tom, jaký systém si vyberete pro hostování serveru adresářů a jaký adresář pro ukládání dat domény EIM, může být nutné před vytvořením domény provést konfigurační úlohy adresářových služeb.	Jak administrátor serveru adresářů (LDAP), tak administrátor EIM
5. Aplikace a operační systémy, které se budou účastnit v doméně. Konfigurujete-li první doménu, tato výchozí nastavení se mohou skládat jenom z jednoho systému. (Podrobné informace najdete v tématu "Vytvoření plánu pojmenování definice registru EIM (Enterprise Identity Mapping)" na stránce 58.)	Tým EIM
6. Osoby a entity, které se budou v doméně účastnit. **Poznámka:** Chcete-li si zjednodušit výchozí testování, můžete omezit počet účastníků na jeden či dva.	Tým EIM

Plánování řadiče domény EIM (Enterprise Identity Mapping)

Když budete shromažďovat informace pro definování domény EIM (Enterprise Identity Mapping), budete se muset rozhodnout, který server adresářů bude sloužit jako řadič domény EIM.

Produkt EIM vyžaduje, aby hostitelem řadiče domény byl server adresářů, jenž podporuje Lightweight Directory Access Protocol (LDAP) verze 3. Navíc musí být produkt server adresářů schopný akceptovat schéma LDAP a jiné pokyny pro EIM a chápat určité atributy a objektové třídy.

Vlastní-li váš podnik více než jeden server adresářů, který může fungovat jako hostitel pro řadič domény EIM, měli byste uvažovat o použití sekundárních replikovaných řadičů domény. Očekáváte-li například velké množství operací vyhledávání mapování, repliky mohou vylepšit výkon vyhledávacích operací.

Také byste měli zvážit, zda by váš řadič domény měl být *lokální* nebo *vzdálený* ve vztahu k systému, od něhož očekáváte, že bude provádět nejvíce operací vyhledávání mapování. Bude-li řadič domény vůči vysoce zatíženému systému lokální, můžete tím u lokálního systému zlepšit výkon vyhledávacích operací. Chcete-li tato rozhodnutí zaznamenat, použijte plánovací formuláře stejně tak, jako si zaznamenáváte informace o své doméně a další informace o adresářích.

Poté, co určíte, který server adresářů v podniku bude fungovat jako hostitel pro váš řadič domény EIM, musíte učinit určitá rozhodnutí ohledně přístupu k řadiči domény.

Plánování přístupu k řadiči domény

Potřebujete si naplánovat, jak budou aplikace podporující EIM a operační systémy přistupovat k serveru adresářů, který funguje jako hostitel pro řadič domény EIM. Chcete-li přistupovat k doméně EIM, musíte:

1. být schopni se přiřadit k řadiči domény EIM
2. ujistit se, že přiřazený subjekt je členem skupiny kontroly přístupu k EIM nebo že je administrátorem LDAP. Další informace uvádí téma Správa kontroly přístupu k EIM.

Jak zvolit vazbu EIM

Rozhraní API EIM podporují několik různých mechanismů vytvoření připojení, známého také pod názvem vazba, s řadičem domény EIM. Každý typ mechanismu vazby poskytuje odlišnou úroveň ověření a šifrování spojení. Možné volby jsou:

Jednoduché vazby
Jednoduchá vazba je spojení LDAP, kde klient LDAP poskytuje serveru LDAP k ověření rozlišovací jméno vazby a heslo vazby. Rozlišovací jméno vazby a heslo poskytuje administrátor v adresáři LDAP. Toto je nejslabší forma ověření a nejméně zabezpečená, protože rozlišovací jméno vazby a heslo se posílají nezakódované a jsou odposlechnutelné. Chcete-li přidat další úroveň ochrany hesla vazby, použijte protokol CRAM-MD5. V případě použití protokolu CRAM-MD5 klient posílá serveru k ověření přepočtenou hodnotu klíče místo čistého textu.

Ověření serveru pomocí SSL (Secure Socket Layer) - ověření na straně serveru
Server LDAP může být nakonfigurován pro spojení SSL nebo TLS (Transport Layer Security). Server LDAP používá ke svému ověření na klienta LDAP digitální certifikát a vytváří zakódovanou komunikační relaci. Certifikátem je ověřován pouze server LDAP. Koncový uživatel je ověřován rozlišovacím jménem vazby a heslem. Síla ověření je stejná jako u jednoduché vazby, ale všechna data jsou zakódovaná kvůli soukromí (včetně rozlišovacího jména vazby a hesla).

Ověření klienta pomocí SSL
Server LDAP může být nakonfigurován tak, aby k ověření koncového uživatele pro zabezpečená spojení SSL nebo TLS na server LDAP požadoval místo rozlišovacího jména vazby a hesla digitální certifikát. Jak klient, tak server jsou ověřováni a relace je zakódovaná. Tato volba poskytuje vyšší úroveň ověření uživatele a chrání soukromí všech přenášených dat.

Ověření Kerberos
Klient LDAP se může být ověřen na serveru tiketem Kerberos, což je volitelná náhrada rozlišovacího jména vazby a hesla. (Kerberos), jenž je ověřený síťový ověřovací systém třetí strany, umožňuje v nezabezpečené síti činiteli (uživateli nebo službě) prokázat svou totožnost jiné službě. Centralizovaný server nazývaný centrum distribuce klíčů (KDC) zpracovává ověření činitelů. KDC ověřuje uživatele tiketem Kerberos. Tyto tikety prokazují totožnost činitele jiným službám v síti. Když se činitel prostřednictvím těchto tiketů ověřuje, může si s cílovou službou vyměňovat šifrovaná data. Tato volba poskytuje vyšší úroveň ověření uživatele a chrání soukromí ověřovacích informací.

Volba mechanismu vazby je založena na úrovni zabezpečení ochrany dat požadované aplikací schopnou pracovat s EIM a ověřovacími mechanismy podporovanými serverem LDAP, jenž funguje jako hostitel pro doménu EIM.

Také možná budete muset provést dodatečnou konfiguraci LDAP serveru, abyste povolili ověřovací mechanismus, který jste si vybrali. V dokumentaci serveru LDAP, jenž funguje jako hostitel pro váš řadič domény, si ověřte, které další konfigurační úlohy možná budete muset provést.

Vzorový plánovací formulář obsahující informace o řadiči domény

Když rozhodnete o řadiči domény EIM, použijte plánovací formuláře pro záznam informací o řadiči domény EIM, které potřebují vaše operační systémy a aplikace podporující EIM. Administrátor LDAP může použít informace shromážděné během tohoto procesu k definování totožnosti vazby aplikace nebo operačního systému na server adresářů LDAP, který funguje jako hostitel pro řadič domény EIM.

Níže uvedená vzorová část plánovacích formulářů ukazuje typ informací, které potřebujete shromáždit. Zahrnuje také ukázkové hodnoty, jež můžete použít při konfiguraci řadiče domény EIM.

Tabulka 12. Informace o doméně a řadiči domény pro plánovací formulář EIM

Informace potřebné ke konfiguraci domény EIM a řadiče domény	**Vzorové odpovědi**
Smysluplné jméno pro doménu. Může to být název firmy, oddělení nebo aplikace, která doménu používá.	MyDomain
Volitelné: Jestliže konfigurujete doménu EIM v již existujícím adresáři LDAP, uveďte nadřazené rozlišovací jméno domény. Je to rozlišovací jméno, které představuje záznam hned nad záznamem jména domény ve stromové hierarchii informací o adresáři, například o=ibm,c=us.	o=ibm,c=us
Výsledné plně kvalifikované rozlišovací jméno domény EIM. Je to plně definované jméno domény EIM, které popisuje umístění adresáře dat domény EIM. Plně kvalifikované rozlišovací jméno domény se skládá minimálně z DN pro doménu (ibm-eimDomainName=) a jména domény, které jste zadali. Jestliže se rozhodnete zadat nadřazené DN pro doménu, potom se plně kvalifikované DN domény skládá z relativního DN domény (ibm-eimDomainName=), jména domény (MyDomain) a nadřazeného DN (o=ibm,c=us). **Poznámka:**	Jedno z níže uvedeného v závislosti na tom, zda vyberete nadřazené DN: • ibm-eimDomainName=MyDomain • ibm-eimDomainName=MyDomain,o=ibm,c=us
Adresa připojení pro řadič domény. Skládá se z typu připojení (základní ldap nebo zabezpečený ldap, například ldap:// nebo ldaps://) a z následujících informací:	ldap://
• Volitelné: hostitelské jméno nebo IP adresa • Volitelné: číslo portu	• some.ldap.host • 389
Výsledná úplná adresa připojení pro řadič domény	ldap://some.ldap.host:389
Mechanismus vazby, který vyžadují aplikace nebo systémy. Volby zahrnují: • Jednoduchá vazba • CRAM MD5 • Ověření serveru • Ověření klienta • Kerberos	Kerberos

Jestliže se váš konfigurační a administrátorský tým skládá z několika členů, budete muset na základě jejich rolí určit totožnost vazby a mechanismus, který by každý člen týmu měl používat pro přístup k doméně EIM. Také potřebujete určit totožnost vazby a mechanismus pro koncové uživatele aplikací EIM. Při shromažďování těchto informací vám může posloužit jako příklad níže uvedený pracovní formulář.

Tabulka 13. Příklad plánovacího formuláře totožností vazeb

Oprávnění EIM nebo role	**Totožnost vazby**	**Mechanismus vazby**	**Potřebný důvod**
Administrátor EIM	eimadmin@krbrealm1.com	Kerberos	Konfiguruje a spravuje EIM.
Administrátor LDAP	cn=administrator	Jednoduchá vazba	Konfiguruje řadič domény EIM.
Administrátor registrů X EIM	cn=admin2	CRAM MD5	Spravuje definice určitých registrů.
Vyhledávání mapování EIM	cn=MyApp,c=US	Jednoduchá vazba	Provádí operace vyhledávání mapování aplikací.

Vytvoření plánu pojmenování definice registru EIM (Enterprise Identity Mapping)

Chcete-li používat produkt EIM (Enterprise Identity Mapping) k mapování totožnosti uživatele v jednom registru uživatelů na stejnou totožnost uživatele v jiném registru uživatelů, pak oba registry musí být definované v produktu EIM.

Musíte vytvořit definici registru pro každou aplikaci nebo registr uživatelů operačního systému, který se bude zapojovat do domény EIM. Registry uživatelů mohou představovat registry operačních systémů, jako je Resource Access Control Facility (RACF) nebo i5/OS, distribuovaný registr (jako např. Kerberos) nebo podmnožina systémového registru, která je využívána výlučně aplikacemi.

Doména EIM může obsahovat definice registru pro registry uživatelů, které mohou existovat na jakékoliv platformě. Například doména, kterou spravuje řadič domény v operačním systému i5/OS, může obsahovat definice registru pro platformy jiné než i5/OS (jako například registr AIX). Ačkoli můžete definovat jakýkoliv registr uživatelů v doméně EIM, musíte také definovat registry uživatelů pro aplikace a operační systémy podporující EIM.

Definici registru EIM můžete pojmenovat jakkoli, jméno pouze musí být jedinečné v doméně EIM. Například můžete pojmenovat definici registru EIM na základě jména systému, který funguje jako hostitel pro registr uživatelů. Jestliže to nestačí k rozlišení definice registru od podobných definic, můžete použít tečku (.) nebo podtržítko (_) a přidat typ registru uživatelů, který definujete. Bez ohledu na kritérium, které si zvolíte, měli byste pro definice registru EIM zvážit vytvoření konvence pojmenování. Tímto zajistíte, že jména definic budou v celé doméně konzistentní a budou příslušně popisovat typ a instanci definovaného registru uživatelů a způsob jeho použití. Například jméno každé definice registru můžete zvolit tak, že použijete kombinaci jména aplikace nebo operačního systému, které registr používá, a fyzické umístění registru v podniku.

Aplikace, která je napsána pro použití EIM, může uvést buď jméno alias zdrojového registru, nebo jméno alias cílového registru, nebo obě jména alias. Při vytváření definic registru EIM musíte zkontrolovat dokumentaci pro aplikace, abyste určili, zda máte uvést jeden nebo více jmen alias pro definice registru. Přiřazujete-li tato jména alias odpovídajícím definicím registrů, aplikace mohou provádět vyhledávání jmen alias k nalezení definice nebo definic registrů, které odpovídají jménům alias v aplikaci.

Níže uvedená vzorová část plánovacího formuláře vám může posloužit jako návod pro zaznamenávání informací o podílejících se registrech uživatelů. Skutečný pracovní formulář můžete použít ke specifikaci jména definice registru pro každý registr uživatelů, ke specifikaci toho, zda používá jméno alias a k popisu umístění a použití registru uživatelů. Některé informace, které budete potřebovat pro pracovní formulář, získáte z instalační a konfigurační dokumentace aplikace.

Tabulka 14. Vzorový plánovací formulář informací definice registru EIM

Jméno definice registru	Typ registru uživatelů	Alias definice registru	Popis registru
Systém_C	Registr uživatelů operačního systému i5/OS	Viz dokumentace k aplikaci.	Registr uživatelů hlavního systému pro i5/OS v Systému C
Systém_A_WAS	WebSphere LTPA	app_23_alias_source	Registr uživatelů WebSphere LTPA v Systému A
Systém_B	Linux	Viz dokumentace k aplikaci.	Registr uživatelů Linux v Systému B
Systém_A	Registr uživatelů operačního systému i5/OS	app_23_alias_target app_xx_alias_target	Registr uživatelů hlavního systému pro i5/OS v Systému A
Systém_D	Registr uživatelů Kerberos	app_xx_alias_source	sféra Kerberos legal.mydomain.com
Systém_4	Registr uživatelů operačního systému Windows 2000	Viz dokumentace k aplikaci.	Registr uživatelů aplikace lidských zdrojů v Systému 4

Poznámka: Typy přidružení pro každý registr se určí později v procesu plánování.

Když dokončíte tuto sekci plánovacího formuláře, měli byste naplánovat mapování totožností. Zjistíte tak, zda ke tvorbě mapování, které potřebujete pro totožnosti uživatele v každém definovaném registru uživatelů, máte použít přidružení identifikátorů, přidružení zásad, nebo oba typy přidružení.

Vytvoření plánu mapování totožností

Kritická část plánovacího procesu zavádění produktu EIM (Enterprise Identity Mapping) vyžaduje, abyste si ve vašem podniku určili způsob použití mapování totožností.

Existují dva způsoby, jak v EIM mapovat totožnosti:

- **Přidružení identifikátorů** popisují vztahy mezi identifikátorem EIM a totožnostmi uživatele v registrech uživatelů, které představují danou osobu. Přidružení identifikátorů vytvoří mapování typu jeden-na-jeden mezi identifikátorem EIM a určitou totožností uživatele. Můžete použít přidružení identifikátorů k nepřímému definování vztahu mezi totožnostmi uživatele pomocí identifikátoru EIM.

  Jestliže vaše zásady zabezpečení ochrany dat vyžadují vysoký stupeň odpovědnosti, může být nutné téměř výhradně používat přidružení identifikátorů pro implementaci mapování totožností. Protože k vytvoření mapování typu jeden-na-jeden pro totožnosti uživatele, které uživatelé vlastní, používáte přidružení totožností, vždy můžete přesně určit, kdo na objektu nebo v systému provedl zásah.
- **Přidružení zásad** popisují vztah mezi několika totožnostmi uživatele a jedinou totožností uživatele v registru uživatelů. Přidružení zásad používá podporu zásad mapování EIM k vytvoření mapování typu mnoho-na-jeden mezi totožnostmi uživatele bez identifikátoru EIM.

  Přidružení zásad mohou být užitečná, máte-li v podniku jednu nebo více velkých skupin uživatelů, kteří potřebují přístup k systémům nebo aplikacím, a vy nechcete, aby měli specifické totožnosti uživatele k získávání tohoto přístupu. Provozujete například webovou aplikaci, která přistupuje k určité vnitřní aplikaci. Možná se vám nebude chtít nastavovat stovky nebo tisíce totožností uživatele a uživatele ověřovat pro tuto vnitřní aplikaci. V této situaci můžete nakonfigurovat mapování totožností tak, že všichni uživatelé této webové aplikace budou mapováni na jednu totožnost uživatele s minimální úrovní autorizace, která je nutná ke spuštění aplikace. Tohoto typu mapování totožností můžete dosáhnout použitím přidružení zásad.

Chcete-li mít v podniku nejlepší řízení totožností uživatele, můžete se rozhodnout používat přidružení identifikátorů a zároveň tak získat nejvyšší stupeň zjednodušené správy hesel. Tam, kde to je vhodné, se můžete rozhodnout používat kombinaci přidružení zásad a přidružení identifikátorů. Zachováte tak jediné přihlášení do systému a zároveň budete mít určitou kontrolu nad totožností uživatele pro administrátory. Bez ohledu na to, jaký typ mapování totožností nejlépe vyhovuje vašim podnikatelským potřebám a vhodně zapadá do vaší zásady zabezpečení ochrany dat, musíte si vytvořit plán mapování totožností a zajistit tak odpovídajícím způsobem implementaci mapování totožností.

Při tvorbě plánu mapování totožností postupujte takto:

Související pojmy

“Vytváření přidružení EIM” na stránce 98
Existují dva různé typy přidružení, které je možné vytvořit. Toto přidružení může být buď cílovým přidružením identifikátoru, nebo přidružením zásady.

“Vytvoření přidružení zásad” na stránce 99
Přidružení zásad umožňuje přímé definování vztahů mezi více totožnostmi uživatele v jednom či více registrech a jednotlivou totožností cílového uživatele v jiném registru.

Plánování přidružení EIM (Enterprise Identity Mapping):

Přidružení jsou záznamy, které vytváříte v doméně EIM a definujete jimi vztah mezi totožnostmi uživatele v různých registrech uživatelů.

V produktu EIM můžete vytvořit jeden ze dvou typů přidružení: k definování mapování typu jeden-na-jeden slouží přidružení identifikátorů a k definování mapování typu mnoho-na-jeden slouží přidružení zásad. Přidružení zásad můžete použít namísto přidružení identifikátorů nebo v kombinaci s ním.

Určitý typ přidružení, který se rozhodnete vytvořit, závisí na tom, jak uživatel používá danou totožnost uživatele a na vašem celkovém plánu mapování totožností.

Můžete vytvořit libovolný z níže uvedených typů přidružení identifikátorů:

- **Cílová přidružení**

  Cílová přidružení definujete pro ty uživatele, kteří obvykle přistupují do systému jako serveru z nějakého jiného klientského systému. Tento typ přidružení se používá, když aplikace provádí operace vyhledávání mapování.
- **Zdrojová přidružení**

  Zdrojová přidružení definujete tehdy, když totožnost uživatele je první, kterou uživatel zadá při přihlašování do systému nebo sítě. Tento typ přidružení se používá, když aplikace provádí operace vyhledávání mapování.
- **Administrační přidružení**

  Administrační přidružení definujete tehdy, když chcete být schopni sledovat skutečnost, že totožnost uživatele patří určitému uživateli, ale nechcete, aby totožnost uživatele byla k dispozici pro operace vyhledávání mapování. Tento typ přidružení můžete použít ke sledování všech totožností uživatele, které osoba v podniku používá.

Přidružení zásad vždy definuje cílové přidružení.

Je možné, aby jedna definice registru měla více než jeden typ přidružení v závislosti na tom, jak se používá registr uživatelů, ke kterému se vztahuje. I když počet nebo kombinace přidružení, které můžete definovat, nejsou omezené, udržujte jejich počet na minimu - zjednodušíte tak administraci své domény EIM.

Obvykle aplikace poskytne nápovědu, které definice registru očekává pro zdrojové a cílové registry, ale neurčí typy přidružení. Každý koncový uživatel aplikace musí být mapován na aplikaci alespoň jedním přidružením. Toto přidružení může být mapováním typu jeden-na-jeden mezi jejich jedinečným identifikátorem EIM a totožností uživatele v požadovaném cílovém registru nebo to může být mapování typu mnoho-na-jeden mezi zdrojovým registrem, kde je totožnost uživatele členem a požadovaným cílovým registrem. Jaký typ přidružení použijete, záleží na vašich požadavcích mapování totožností a kritériích, které aplikace poskytuje.

Již dříve jste v rámci plánovacího procesu doplnili informace o identifikátorech EIM a definicích registru EIM do dvou plánovacích formulářů pro totožnosti uživatele ve své organizaci. Teď potřebujete tyto informace spojit tím, že určíte typy přidružení, které chcete použít k mapování uživatelů v podniku. Potřebujete zjistit, zda definovat přidružení zásad pro určitou aplikaci a její registry uživatelů, nebo zda definovat určitá přidružení identifikátorů (zdrojové, cílové nebo administrační) pro každou totožnost uživatele v systému nebo v registru aplikace. Můžete to provést zaznamenáním informace o požadovaných typech přidružení jak v plánovacím formuláři definice registru, tak v odpovídajícím řádku pracovního formuláře přidružení.

Chcete-li dokončit plán mapování totožností, můžete použít níže uvedené pracovní formuláře jako vzory, které vám pomohou zaznamenat informace přidružení, jež potřebujete k popisu uceleného obrazu plánu implementace mapování totožností.

Tabulka 15. Vzorový plánovací formulář informací definice registru EIM

Jméno definice registru	Typ registru uživatelů	Alias definice registru	Popis registru	Typy přidružení
Systém_C	Registr uživatelů operačního systému i5/OS	Viz dokumentace k aplikaci.	Registr uživatelů hlavního systému pro i5/OS v Systému C	Cílové
Systém_A_WAS	WebSphere LTPA	app_23_alias_source	Registr uživatelů WebSphere LTPA v Systému A	Primárně zdrojové
Systém_B	Linux	Viz dokumentace k aplikaci.	Registr uživatelů Linux v Systému B	Zdrojové a cílové

Tabulka 15. Vzorový plánovací formulář informací definice registru EIM (pokračování)

Jméno definice registru	Typ registru uživatelů	Alias definice registru	Popis registru	Typy přidružení
Systém_A	Registr uživatelů operačního systému i5/OS	app_23_alias_target app_xx_alias_target	Registr uživatelů hlavního systému pro i5/OS v Systému A	Cílové
Systém_D	Registr uživatelů Kerberos	app_xx_alias_source	sféra Kerberos legal.mydomain.com	Zdrojové
Systém_4	Registr uživatelů operačního systému Windows 2000	Viz dokumentace k aplikaci.	Registr uživatelů aplikace lidských zdrojů v Systému 4	Administrační
order.mydomain.com	Registr uživatelů operačního systému Windows 2000		Hlavní registr přihlášení pro zaměstnance oddělení objednávek	Předvolené zásady registru (zdrojový registr)
Systém_A_order_app	Aplikace oddělení objednávek		Specifický registr aplikace pro aktualizace objednávek	Předvolené zásady registru (cílový registr)
Systém_C_order_app	Aplikace oddělení objednávek		Specifický registr aplikace pro aktualizace objednávek	Předvolené zásady registru (cílový registr)

Tabulka 16. Příklad plánovacího formuláře identifikátorů EIM

Jedinečné jméno identifikátoru	Popis identifikátoru nebo totožnosti uživatele	Alias identifikátoru
John S Day	Manažer personálního oddělení	app_23_admin
John J Day	Právní oddělení	app_xx_admin
Sharon A. Jones	Administrátor oddělení objednávek	

Tabulka 17. Příklad plánovacího formuláře přidružení identifikátor

Jedinečné jméno identifikátoru: _____John S Day_____		
Registr uživatelů	**Totožnost uživatele**	**Typy přidružení**
Systém A WAS v Systému A	johnday	Zdrojové
Registr uživatelů Linux v Systému B	jsd1	Zdrojové a cílové
i5/OS v Systému C	JOHND	Cílové
Registr 4 v systému personálního oddělení Windows 2000	JDAY	Administrační

Tabulka 18. Příklad plánovacího formuláře přidružení zásad

Typ přidružení zásad	Registr zdrojového uživatele	Registr cílového uživatele	Totožnost uživatele	Popis
Předvolený registr	order.mydomain.com	Systém_A_order_app	SYSUSERA	Uživatel oddělení objednávek Windows ověřený mapami na odpovídající totožnost uživatele aplikace

Tabulka 18. Příklad plánovacího formuláře přidružení zásad (pokračování)

Typ přidružení zásad	Registr zdrojového uživatele	Registr cílového uživatele	Totožnost uživatele	Popis
Předvolený registr	order.mydomain.com	Systém_C_order_app	SYSUSERB	Uživatel oddělení objednávek Windows ověřený mapami na odpovídající totožnost uživatele aplikace

Vytvoření plánu pojmenování identifikátoru EIM:

Při plánování potřeby mapování totožností EIM můžete vytvořit jedinečné identifikátory EIM pro uživatele aplikací podporující EIM a operační systémy ve vašem podniku, když pro uživatele chcete vytvořit mapování typu jeden-na-jeden mezi totožnostmi uživatele. Použitím přidružení identifikátorů k vytvoření mapování typu jeden-na-jeden maximalizujete výhody správy hesel, které EIM poskytuje.

Plán pojmenování, který vytvoříte, vychází z vašich podnikatelských potřeb a preferencí. Jediným požadavkem pro jména identifikátorů EIM je, aby byla jedinečná. Některé firmy mohou používat celé jméno každého zaměstnance; jiné mohou upřednostňovat jiný typ dat, například číslo zaměstnance. Chcete-li tvorbu jmen identifikátorů EIM založit na celém jméně, je možné, že dojde k duplikaci jmen. Jak vyřešíte potenciální duplikaci jmen identifikátorů, je věcí osobních preferencí. Možná budete pracovat s každým případem jednotlivě tak, že přidáte předem určený řetězec znaků ke každému jménu identifikátoru, a tak zajistíte jeho jedinečnost. Například můžete přidat ke každému jménu číslo oddělení.

Částí rozvoje plánu pojmenování identifikátorů EIM je rozhodnutí o vašem celkovém plánu mapování totožností. Pomůže vám rozhodnout, zda ve vašem podniku potřebujete pro mapování totožností použít identifikátory a přidružení identifikátorů, anebo přidružení zásad. Chcete-li vytvořit plán pojmenování identifikátorů EIM, můžete použít pracovní formulář, který je uveden níže a který vám pomůže se shromážděním informací týkajících se totožností uživatele ve vaší organizaci a s plánováním identifikátorů EIM pro totožnosti uživatele. Pracovní formulář představuje druh informací, které administrátor EIM potřebuje znát, když tvoří identifikátory EIM nebo přidružení zásad pro uživatele nebo aplikace.

Tabulka 19. Příklad plánovacího formuláře identifikátorů EIM

Jedinečné jméno identifikátoru	Popis identifikátoru nebo totožnosti uživatele	Alias identifikátoru
John S Day	Manažer personálního oddělení	app_23_admin
John J Day	Právní oddělení	app_xx_admin
Sharon A. Jones	Administrátor oddělení objednávek	

Aplikace napsána pro používání EIM může uvést jméno alias, které použije k nalezení odpovídajícího identifikátoru EIM pro aplikaci. Naopak aplikace jej může použít k určení toho, jakou specifickou totožnost uživatele použít. Musíte zkontrolovat dokumentaci pro aplikace, abyste určili, zda máte uvést jeden nebo více jmen alias pro identifikátor. Identifikátor EIM nebo pole s popisem totožnosti mají volný formát a lze je použít k zadání popisných informací o uživateli.

Nemusíte vytvořit identifikátory EIM pro všechny členy vašeho podniku najednou. Po vytvoření výchozího identifikátoru EIM a jeho použití k otestování konfigurace EIM, můžete vytvořit další identifikátory EIM založené na cílech vaší organizace a použití EIM. Můžete například přidávat identifikátory EIM podle oddělení nebo oblastí. Nebo můžete přidat identifikátory EIM, když budete nasazovat další aplikace EIM.

Poté, co shromáždíte informace potřebné k rozvoji plánu pojmenování identifikátorů EIM, můžete plánovat přidružení pro totožnosti uživatele.

Pracovní formuláře pro implementaci EIM (Enterprise Identity Mapping)

Když budete postupovat plánovacím procesem produktu EIM, mohou vám posloužit tyto pracovní formuláře ke shromažďování informací, které budete potřebovat vašem podniku ke konfiguraci a použití produktu EIM. Na plánovacích stránkách jsou k dispozici, je-li to vhodné, příklady dokončených sekcí pracovních formulářů.

Tyto pracovní formuláře slouží jako příklad typů pracovních formulářů, které budete potřebovat při tvorbě implementačního plánu EIM. Počet uvedených položek je menší než počet, který budete pravděpodobně potřebovat pro své informace EIM. Tyto pracovní formuláře můžete upravovat a přizpůsobit je tak své vlastní situaci.

Tabulka 20. Pracovní formulář domény a řadiče domény

Informace potřebné ke konfiguraci domény EIM a řadiče domény	**Odpovědi**
Smysluplné jméno pro doménu. Může to být název firmy, oddělení nebo aplikace, která doménu používá.	
Volitelně: nadřazené rozlišovací jméno pro doménu. Je to rozlišovací jméno, které představuje záznam hned nad záznamem jména domény ve stromové hierarchii informací o adresáři, například o=ibm,c=us.	
Výsledné plně kvalifikované rozlišovací jméno domény EIM. Je to plně definované jméno domény EIM, které popisuje umístění adresáře dat domény EIM. Plně kvalifikované rozlišovací jméno domény se skládá minimálně z DN pro doménu (ibm-eimDomainName=) a jména domény, které jste zadali. Jestliže se rozhodnete zadat nadřazené DN pro doménu, potom se plně kvalifikované DN domény skládá z relativního DN domény (ibm-eimDomainName=), jména domény (MyDomain) a nadřazeného DN (o=ibm,c=us).	
Adresa připojení pro řadič domény. Skládá se z typu připojení (základní ldap nebo zabezpečený ldap, například ldap:// nebo ldaps://) a z následujících informací:	
• Volitelné: hostitelské jméno nebo IP adresa • Volitelné: číslo portu	
Výsledná úplná adresa připojení pro řadič domény	
Mechanismus vazby, který vyžadují aplikace nebo systémy. Volby zahrnují: • Jednoduchá vazba • CRAM MD5 • Ověření serveru • Ověření klienta • Kerberos	

Příklad použití tohoto pracovního formuláře uvádí téma Plánování řadiče domény EIM.

Tabulka 21. Plánovací formulář totožností vazeb

Oprávnění nebo role EIM	**Totožnost vazby**	**Mechanismus vazby**	**Potřebný důvod**

Tabulka 21. Plánovací formulář totožností vazeb (pokračování)

Příklad použití tohoto pracovního formuláře uvádí téma Plánování řadiče domény EIM.

Tabulka 22. Plánovací formulář pro informace o definici registru EIM

Jméno definice registru	**Typ registru uživatelů**	**Alias definice registru**	**Popis registru**	**Typy přidružení**

Příklad použití tohoto pracovního formuláře uvádí téma Vytvoření plánu pojmenování definice registru EIM.

Tabulka 23. Plánovací formulář identifikátorů EIM

Jedinečné jméno identifikátoru	**Popis identifikátoru nebo totožnosti uživatele**	**Alias identifikátoru**

Příklad použití tohoto pracovního formuláře uvádí téma Vytvoření plánu pojmenování identifikátorů EIM.

Tabulka 24. Plánovací formulář přidružení identifikátorů

Jedinečné jméno identifikátoru: _____John S Day_____		
Registr uživatelů	Totožnost uživatele	Typy přidružení

Příklad použití tohoto pracovního formuláře uvádí téma Plánování přidružení EIM.

Tabulka 25. Plánovací formulář přidružení zásad

Typ přidružení zásad	Registr zdrojového uživatele	Registr cílového uživatele	Totožnost uživatele	Popis

Příklad použití tohoto pracovního formuláře uvádí téma Plánování přidružení EIM.

Plánování vývoje aplikací EIM (Enterprise Identity Mapping)

Aby aplikace mohla používat produkt EIM (Enterprise Identity Mapping) a účastnit se v doméně, musí být schopná používat rozhraní API EIM.

Měli byste si prohlédnout dokumentaci o rozhraní API EIM a dokumentaci EIM určenou dané platformě a zjistit, zda existují nějaké specifické pokyny ohledně plánování, kterým byste měli porozumět, píšete-li nebo přizpůsobujete-li aplikace pro rozhraní API EIM. Například mohou existovat pokyny týkající se kompilace či jiné pokyny pro aplikace v programovacím jazyce C nebo v C++, které volají rozhraní API EIM. V závislosti na platformě aplikace mohou existovat pokyny týkající se příkazů link-edit nebo i jiné pokyny.

Související úlohy

“Rozhraní API EIM” na stránce 120
Produkt EIM (Enterprise Identity Mapping) poskytuje mechanismy pro správu totožností uživatele mezi platformami. EIM má několik rozhraní API (application programming interface), která mohou aplikace používat při řízení operací EIM v zastoupení aplikace nebo uživatele aplikace.

Plánování EIM pro operační systém i5/OS

Existuje několik technologií a služeb, které produkt EIM (Enterprise Identity Mapping) vykonává v systému System i. Dříve než začnete na serveru konfigurovat EIM, měli byste se rozhodnout, jaké funkční vybavení chcete implementovat tím, že použijete EIM a jediné přihlášení do systému.

Před implementací EIM byste měli učinit rozhodnutí ohledně základních požadavků zabezpečení ochrany dat na vaší síti a tato bezpečnostní opatření aplikovat. V podniku EIM umožňuje administrátorům a uživatelům jednodušší správu totožností. Použijete-li zároveň službu síťového ověření, EIM umožní jediné přihlášení pro váš podnik.

Plánujte-li použít službu Kerberos k ověření uživatelů jako část implementace jediného přihlášení do systému, měli byste také nakonfigurovat službu síťového ověření.

Chcete-li se dozvědět o plánování konfigurace EIM ve vašem systému více, prostudujte si níže uvedené informace:

Související informace

Nezbytné předpoklady instalace EIM (Enterprise Identity Mapping) pro systém i5/OS

Následující plánovací formulář označuje služby, které byste měli nainstalovat před konfigurací produktu EIM.

Tabulka 26. Plánovací formulář pro nezbytné předchozí instalace pro produkt EIM

Plánovací formulář pro nezbytné předchozí instalace pro produkt EIM	**odpověď**
Je váš operační systém i5/OS verze V5R4 nebo pozdější?	
Jsou na systému nainstalovány následující volby a produkty? • i5/OS Host Servers (5761-SS1 volba 12). • System i Access for Windows (5761-XE1). • Qshell Interpreter (5761-SS1 volba 30) (nutný pro případ konfigurace služby síťového ověření a také pro EIM). **Poznámka:** 5722 je kód produktu pro volby a produkty operačního systému i5/OS, verzí, které předcházely verzi V6R1.	
Je produkt System i Navigator nainstalován na PC administrátora včetně následujících dílčích komponent? • Síť. • Zabezpečení (nutné při konfiguraci služby síťového ověření a také pro EIM).	
Nainstalovali jste nejnovější verzi servisního balíku System i Access for Windows? Nejnovější servisní balík najdete na webových stránkách System i Access	
Pokud je server adresářů, jako je například IBM Tivoli Directory Server for i5/OS , aktuálně nakonfigurován a vy si ho přejete používat jako řadič domény EIM, znáte rozlišovací jméno (DN) a heslo administrátora LDAP?	
Může být aktuálně nakonfigurovaný server adresářů dočasně zastaven? (Toto bude vyžadováno pro dokončení procesu konfigurace EIM.)	
Máte zvláštní oprávnění *SECADM, *ALLOBJ a *IOSYSCFG ?	
Použili jste nejnovější opravy PTF?	

Instalace požadovaných voleb produktu System i Navigator

Při povolení prostředí jediného přihlášení EIM a služby síťového ověření budete muset nainstalovat obě volby, jednak volbu **Síť**, a také volbu **Zabezpečení** produktu System i Navigator.

Produkt EIM se nachází ve volbě **Síť** a služba síťového ověření je součástí volby **Zabezpečení**. Pokud nemáte v plánu ve vaší síti používat službu síťového ověření, nebudete muset volbu **Zabezpečení** produktu System i Navigator instalovat.

Chcete-li instalovat volbu Síť produktu System i Navigator nebo ověřit, zda máte tuto volbu nainstalovanou, ujistěte se, že je na PC, který používáte,instalován produkt System i Access for Windows, prostřednictvím kterého lze spravovat systém System i.

Instalace volby **Síť**:

1. Klepněte na **Start > Programy > System i Access for Windows > Výběrová instalace**.
2. Postupujte podle instrukcí v dialogu. V dialogu **Výběr komponent** rozbalte **System i Navigator** a pak vyberte volbu **Síť**. Pokud budete také využívat službu ověření sítě, měli byste také vybrat volbu **Zabezpečení**.
3. Pokračujte zbývajícími kroky **Výběrové instalace**.

Související informace

Služby síťového ověření

Pokyny týkající se zálohování a obnovy EIM

Plán zálohování a obnovy dat produktu EIM je nezbytný k tomu, aby byla data chráněna a mohla být obnovena v případě, že nastane problém se serverem adresářů, který funguje jako hostitel řadiče domény EIM. K obnovení potřebujete také znát důležité konfigurační informace EIM.

Související informace

Replikace serveru adresářů

Úlohy replikace

Pokyny pro uložení a obnovu serveru adresářů

Zálohování a obnova dat domény EIM:

Způsob, jakým uložíte data EIM, záleží na tom, jak se rozhodnete spravovat tuto oblast serveru adresářů, který funguje jako řadič domény pro data EIM.

Jedním ze způsobů jak zálohovat data, zvláště v případě obnovy po zhroucení systému, je uložit knihovnu databáze. Standardně to je knihovna QUSRDIRDB. Jestliže je povolený i protokol changelog, měli byste uložit i knihovnu QUSRDIRCL. Server adresářů v systému, ve kterém chcete obnovit knihovnu, musí mít stejné schéma LDAP a konfiguraci jako původní server adresářů. Soubory, ve kterých jsou tyto informace uloženy, jsou v /QIBM/UserData/OS400/DirSrv. Další konfigurační data se nacházejí v QUSRSYS/QGLDCFG (*USRSPC object) a QUSRSYS/QGLDVLDL (objekt *VLDL). Chcete-li mít pro svůj server adresářů úplnou zálohu, musíte uložit obě knihovny, soubory integrovaného systému souborů a objekty QUSRSYS.

Můžete například použít soubor LDIF, kterým uložíte celý nebo částečný obsah serveru adresářů. Chcete-li zálohovat informace řadiče domény produktu IBM Tivoli Directory Server for i5/OS, postupujte takto:

1. V produktu System i Navigator rozbalte **Síť > Servery > TCP/IP**.
2. Klepněte pravým tlačítkem myši na **Server adresářů** , vyberte **Nástroje**, poté vyberte **Exportovat soubor**. Tímto zobrazíte stránku, která vám dovolí specifikovat, které části obsahu serveru adresářů se mají do souboru vyexportovat.
3. Přeneste vyexportovaný soubor na ten systém System i, který chcete používat jako váš záložní server adresářů.
4. V produktu System i Navigator na záložním serveru rozbalte **Síť > Servery > TCP/IP**.
5. Chcete-li nahrát obsah přeneseného souboru na nový server, klepněte pravým tlačítkem myši na **Server adresářů**, vyberte **Nástroje**, poté vyberte **Importovat**.

Jiný způsob, jak uložit data domény EIM, je nakonfigurovat a použít replikovaný server adresářů. Všechny změny dat domény EIM se automaticky posílají na replikovaný server adresářů, takže v případě, že server adresářů, který funguje jako hostitel pro řadič domény, selže nebo ztratí data EIM, lze data načíst z replikovaného serveru.

Na typu replikačního modelu, který si vyberete, záleží způsob konfigurace a použití replikovaného serveru adresářů.

Zálohování a obnova dat domény EIM:

Stane-li se, že dojde k selhání systému, může být nutné v tomto systému obnovit informace o konfiguraci EIM. Tyto informace nelze snadno uložit ani obnovit přenosem z jiného systému.

K uložení a obnově konfigurace EIM máte tyto možnosti:

- K uložení informací o konfiguraci EIM a k uložení dalších důležitých informací o konfiguraci použijte příkaz SAVSECDTA (Uložení dat zabezpečení). Poté v každém systému obnovte objekt QSYS uživatelského profilu.

  Poznámka: Musíte použít příkaz SAVSECDTA a jednotlivě obnovit objekt QSYS uživatelského profilu v každém systému s konfigurací EIM. Mohou nastat problémy, jestliže se pokusíte obnovit objekt QSYS uživatelského profilu na jiném systému, než ve kterém byl uložen.

- Buď znovu spusťte průvodce konfigurací EIM, nebo manuálně aktualizujte vlastnosti složky konfigurace EIM. Chcete-li si tento proces usnadnit, měli byste si uložit implementační plánovací formulář EIM nebo si u každého systému poznamenat informace o konfiguraci EIM.

Rovněž je možné naplánovat zálohu a obnovu dat služby síťového ověření v případě, že jste nakonfigurovali službu síťového ověření jako součást prostředí jediného přihlášení.

Konfigurace EIM

Průvodce konfigurací produktu EIM vám umožní snadno a rychle dokončit základní konfiguraci pro váš systém. Průvodce vám poskytne tři volby konfigurace systému EIM.

To, jak použijete průvodce konfigurace v určitém systému, záleží na vašem souhrnném plánu použití EIM v podniku a na potřebách konfigurace EIM. Například mnoho administrátorů chce používat EIM společně se službou síťového ověření kvůli vytvoření prostředí jediného přihlášení přes více systémů a platforem, aniž by bylo nutné měnit vlastní zásady zabezpečení. Průvodce konfigurací EIM vám tak umožňuje konfigurovat službu síťového ověření jako součást konfigurace EIM. Konfigurace a použití služby síťového ověření však není nezbytným předchozím požadavkem pro konfiguraci a použití EIM.

Před zahájením procesu konfigurace EIM pro jeden nebo více systémů proveďte plánování implementace EIM a získejte potřebné informace. Musíte například zvážit následující otázky:

- Který systém System i chcete konfigurovat jako řadič domény EIM pro doménu EIM? Použijte průvodce konfigurací EIM a vytvořte nejdříve v systému novou doménu. Potom použijte průvodce ke konfiguraci všech dalších systémů, které se mají připojit k této doméně.
- Chcete konfigurovat službu síťového ověření v každém systému, který konfigurujete pro EIM? Pokud ano, můžete použít průvodce konfigurací EIM a vytvořit základní konfiguraci služby síťového ověření na každém systému System i. K dokončení konfigurace služby síťového ověření však musíte provést další úlohy.

Když použijete průvodce konfigurací EIM a vytvoříte základní konfiguraci pro každý systém System i, bude před vámi ještě stále řada úloh konfigurace EIM, které musíte provést, abyste získali úplnou konfiguraci EIM. Přečtěte si téma Scénář: Povolení jediného přihlášení, kde najdete příklad ukazující, jak fiktivní společnost konfigurovala prostředí jediného přihlášení pomocí služby síťového ověření a EIM.

Chcete-li konfigurovat EIM, musíte mít všechna níže uvedená zvláštní oprávnění:

- Administrátor zabezpečení (*SECADM).
- Všechny objekty (*ALLOBJ).
- Konfigurace systému (*IOSYSCFG).

Před použitím průvodce konfigurací EIM musíte dokončit všechny kroky “Plánování EIM” na stránce 50, abyste přesně určili, jak budete EIM používat. Konfigurujete-li EIM jako součást vytváření prostředí jediného přihlášení, měli byste dokončit také všechny kroky plánování jediného přihlášení.

Chcete-li spustit průvodce konfigurací EIM, postupujte takto:

1. Spusťte produkt System i Navigator.
2. Přihlašte se k systému, pro který chcete konfigurovat EIM. Konfigurujete-li EIM pro více než jeden systém, začněte s tím systémem, na kterém chcete konfigurovat řadič domény pro EIM.
3. Rozbalte **Síť → EIM (Enterprise Identity Mapping)**.
4. Klepněte pravým tlačítkem myši na **Konfigurace** a vyberte **Konfigurovat**. Spustí se průvodce konfigurací EIM.
5. Vyberte volbu konfigurace EIM a postupujte podle pokynů průvodce až do dokončení průvodce.
6. V případě, že nevíte, jaké údaje máte v průvodci zadat, klepněte na volbu **Nápověda**.

Jakmile dokončíte plánování, můžete použít průvodce konfigurací EIM a vytvořit jednu ze tří základních konfigurací EIM. Průvodce můžete použít ke vstupu do stávající domény nebo k vytvoření nové domény a ke vstupu do ní. Když

použijete průvodce konfigurací EIM k vytvoření a ke vstupu do nové domény, můžete si zvolit, zda budete konfigurovat řadič domény EIM v lokálním nebo vzdáleném systému. Níže uvedené informace obsahují pokyny pro konfiguraci EIM podle požadovaného typu základní konfigurace EIM:

Související informace

Služby síťového ověření

Jediné přihlášení

Vytvoření a vstup do nové lokální domény

Když používáte průvodce konfigurací EIM k vytváření a ke vstupu do nové domény, můžete se rozhodnout, že nakonfigurujete řadič domény EIM v lokálním systému v rámci vytváření konfigurace EIM.

V případě nutnosti průvodce konfigurací EIM zajistí, abyste dodali základní konfigurační informace pro server adresářů. Také v případě, že na systému System i dosud není nakonfigurován produkt Kerberos, vyvolá průvodce program, který bude vaším průvodcem při vytváření služby síťového ověření.

Poté, co dokončíte všechny úlohy v rámci průvodce konfigurací EIM, můžete provést níže uvedené úlohy:

- Vytvoření nové domény EIM.
- Konfigurace lokálního serveru adresářů, který bude pracovat jako řadič domény EIM.
- Konfigurace služby síťového ověření v systému.
- Vytvoření definic registru pro lokální registr i5/OS a registr Kerberos.
- Konfigurace systému jako člena nové domény EIM.

Chcete-li konfigurovat systém za účelem vytvoření a vstupu do nové domény EIM, musíte mít všechna níže uvedená zvláštní oprávnění:

- Administrátor zabezpečení (*SECADM).
- Všechny objekty (*ALLOBJ).
- Konfigurace systému (*IOSYSCFG).

Chcete-li k vytvoření a vstupu do nové lokální domény použít průvodce konfigurací EIM, postupujte takto:

1. V prostředí produktu System i Navigator vyberte systém, pro který chcete konfigurovat EIM. Pak rozbalte položku **Síť > EIM (Enterprise Identity Mapping)**.
2. Pravým tlačítkem myši klepněte na **Konfigurace** a vyberte volbu **Konfigurovat**. Tím spustíte průvodce konfigurací produktu EIM.

   Poznámka: V případě, že už jste v systému měli dříve nakonfigurován produkt EIM, bude tato volba znít **Překonfigurovat**.
3. Na **uvítací stránce** průvodce vyberte volbu **Vytvořit a vstoupit do nové domény**. Pak klepněte na **Další**.
4. Na stránce **Zadat umístění domény EIM** vyberte volbu **Na lokálním serveru adresářů**. Pak klepněte na **Další**.

   Poznámka: Tato volba nakonfiguruje lokální server adresářů, aby pracoval jako řadič domény EIM. Vzhledem k tomu, že tento server adresářů uchovává všechna data EIM pro doménu, musí být aktivní a musí zůstat aktivní, aby podporoval operace vyhledávání mapování EIM a další operace.

   Pokud na systému System i není aktuálně nakonfigurována služba síťového ověření nebo jsou nezbytné dodatečné informace o konfiguraci služby síťového ověření za účelem konfigurování prostředí jediného přihlášení, zobrazí se stránka **Konfigurace služby síťového ověření**. Tato stránka vám umožňuje spustit průvodce konfigurací služby síťového ověření, v jehož rámci pak nakonfigurujete službu síťového ověření. Rovněž můžete službu síťového ověření nakonfigurovat později, prostřednictvím průvodce konfigurací pro tuto službu, kterého poskytuje produkt System i Navigator. Poté, co dokončíte konfiguraci služby síťového ověření, bude průvodce konfigurací EIM pokračovat.
5. Chcete-li nakonfigurovat službu síťového ověření, postupujte takto:

a. Na stránce **Konfigurace služby síťového ověření** spusťte výběrem volby **Ano** průvodce konfigurací služby síťového ověření. S pomocí tohoto průvodce můžete nakonfigurovat několik rozhraní a služeb operačního systému i5/OS, které budou ve sféře Kerberos. Rovněž můžete nakonfigurovat prostředí jediného přihlášení, které bude využívat jak EIM, tak služba síťového ověření.

b. Na stránce **Zadání informací o sféře** zadejte do pole **Předvolená sféra** jméno předvolené sféry. Pokud k ověření Kerberos používáte produkt Microsoft Active Directory, vyberte volbu **Použít Microsoft Active Directory k ověření Kerberos** a klepněte na **Další**.

c. Na stránce **Zadání informací o KDC** zadejte do pole **KDC** plně kvalifikované jméno serveru Kerberos pro tuto sféru. Dále zadejte 88 do pole **Port**. Pak klepněte na **Další**.

d. Na stránce **Zadání informací o serveru hesel** vyberte buď **Ano**, nebo **Ne** za účelem nastavení serveru hesel. Server hesel umožňuje změnit hesla na serveru Kerberos. Pokud vyberete volbu **Ano**, zadejte do pole **Server hesel** jméno serveru hesel. V poli **Port** ponechte předvolenou hodnotu 464 a klepněte na Další.

e. Na stránce **Výběr položek souboru tabulky klíčů** zvolte **Ověření i5/OS Kerberos** a klepněte na **Další**.

   Poznámka: Kromě toho můžete vytvářet záznamy souboru tabulky klíčů pro produkt IBM Tivoli Directory Server for i5/OS, i5/OS NetServer a pro produkt IBM HTTP Server for i5/OS, pokud chcete, aby tyto služby rovněž používaly ověření Kerberos. Dříve než budete moci používat ověření Kerberos, možná budete muset provést dodatečnou konfiguraci těchto služeb.

f. Na stránce **Vytvoření záznamu souboru tabulky klíčů i5/OS** zadejte a potvrďte heslo a poté klepněte na **Další**. Musí to být stejné heslo, které budete používat při přidávání činitelů i5/OS na server Kerberos.

g. Volitelné: Na stránce **Vytvoření dávkového souboru** vyberte volbu **Ano**, zadejte níže uvedené informace a pak klepněte na **Další**:

   - V poli **Dávkový soubor** proveďte aktualizaci cesty k adresáři. Klepněte na **Procházet** a vyhledejte příslušnou cestu k adresáři nebo změňte cestu, která je uvedena v poli **Dávkový soubor**.
   - V poli **Zahrnout heslo** vyberte **Ano**. Tím zajistíte, aby všechna hesla přiřazená k činiteli i5/OS byla zahrnuta do dávkového souboru. Povšimněte si, že hesla se zobrazí jako čistý text a může si je přečíst kdokoliv, kdo má přístupová práva ke čtení dávkového souboru. Proto je velmi důležité, abyste vymazali dávkový soubor ze serveru Kerberos a z PC okamžitě poté, co jej použijete. Pokud nezahrnete heslo, budete vyzváni k zadání hesla při spuštění dávkového souboru.

     Poznámka: Činitele, kteří jsou generováni průvodcem produktu Microsoft Active Directory, můžete také přidat manuálně. Chcete-li zjistit, jak to provést, prostudujte si téma Přidání činitelů i5/OS na server Kerberos.
   - Na stránce **Shrnutí** zkontrolujte konfigurační informace týkající se služby síťového ověření. Klepnutím na **Dokončit** se vrátíte do průvodce konfigurací EIM.

6. Pokud není server adresářů nakonfigurován, zobrazí se po obnově průvodce konfigurací EIM stránka **Konfigurace serveru adresářů**. Zadáním níže uvedených informací nakonfigurujte lokální server adresářů:

   Poznámka: Pokud nakonfigurujete lokální server adresářů dříve, než použijete průvodce konfigurací EIM, zobrazí se namísto toho stránka **Zadání uživatele pro připojení**. Tuto stránku použijte k zadání rozlišovacího jména a hesla pro administrátora LDAP, abyste zajistili, že průvodce bude mít dostatečná oprávnění k administraci domény EIM a k administraci objektů, které jsou v doméně EIM. Pak pokračujte dalším krokem této procedury. V případě, že nevíte, jaké údaje máte zadat pro tuto stránku, klepněte na volbu **Nápověda**.

   a. V poli **Port** ponechte předvolené číslo portu 389 nebo zadejte jiné číslo portu, které má být použito pro nezabezpečené komunikace EIM se serverem adresářů.

   b. Do pole **Rozlišovací jméno** zadejte rozlišovací jméno (DN) serveru LDAP, které bude identifikovat administrátora LDAP pro server adresářů. Průvodce konfigurací EIM vytvoří toto rozlišovací jméno administrátora LDAP a použije je k nakonfigurování serveru adresářů jako řadiče domény pro novou doménu, kterou vytváříte.

   c. Do pole **Heslo** zadejte heslo administrátora LDAP.

   d. Do pole **Potvrdit heslo** zadejte vaše heslo pro kontrolu ještě jednou.

e. Klepněte na **Další**.

7. Na stránce **Zadání domény** zadejte níže uvedené informace:
   a. Do pole **Doména** napište jméno domény EIM, kterou chcete vytvořit. Ponechte předvolené jméno EIM nebo použijte libovolný řetězec znaků, který pro vás bude mít smysl. Nesmíte však používat zvláštní znaky, jako je **= + < > , # ;** \ and *****.
   b. Do pole **Popis** zadejte text, který bude novou doménu popisovat.
   c. Klepněte na **Další**.
8. Na stránce **Zadání nadřazeného DN pro doménu** vyberte **Ano**, abyste zadali nadřazené rozlišovací jméno pro doménu, kterou vytváříte, nebo zadejte **Ne**, což bude mít za následek, že data EIM budou ukládána do adresáře s příponou, jejíž jméno bude odvozeno ze jména domény EIM.

   Poznámka: V případě, že vytváříte doménu na lokálním serveru adresářů, je nadřazené DN volitelné. Zadáním nadřazeného DN určujete, kde v prostoru lokálního serveru LDAP mají být uložena data pro doménu. Pokud nezadáte žádné nadřazené DN, produkt EIM umístí data do své vlastní přípony v prostoru pro jména. Pokud vyberete volbu **Ano**, použijte posuvný seznam k výběru přípony lokálního LDAP, která se má použít jako nadřazené DN, nebo zadejte text za účelem vytvoření a pojmenování nového nadřazeného DN. Zadání jména pro novou doménu není povinné. Pokud chcete získat další informace o používání nadřazeného DN, klepněte na **Nápověda**.
9. Na stránce **Informace o registrech** zadejte, zda si přejete přidat lokální registry uživatelů k doméně EIM jako definice registrů. Vyberte jeden nebo oba níže uvedené typy registrů uživatelů:

   Poznámka: V tomto okamžiku nemusíte vytvářet definice registru. Pokud se rozhodnete vytvořit definice registru později, musíte přidat definice systémového registru a aktualizovat vlastnosti konfigurace EIM.
   a. Výběrem volby **Lokální i5/OS** přidáte definici registru pro lokální registr. V příslušném poli ponechte předvolenou hodnotu pro jméno definice registru anebo pro ně zadejte nějakou jinou hodnotu. Jméno registru EIM je libovolný řetězec, který reprezentuje typ registru a specifickou instanci daného registru.
   b. Výběrem volby **Kerberos** přidáte definici registru pro registr Kerberos. V příslušném poli ponechte předvolenou hodnotu pro jméno definice registru nebo pro ně zadejte nějakou jinou hodnotu. Předvolené jméno definice registru je stejné jako jméno sféry. Ponecháním předvoleného jména a použitím stejného jména registru Kerberos, jako je jméno sféry, můžete zvýšit výkon při vyhledávání informací z registru. V případě potřeby vyberte volbu **Totožnosti uživatele Kerberos jsou citlivé na velká písmena**.
   c. Klepněte na **Další**.
10. Na stránce **Zadání uživatele systému EIM** vyberte **Typ uživatele**, který má být systémem používán při provádění operací EIM v zastoupení funkcí operačního systému. Tyto operace zahrnují operace vyhledávání mapování a výmaz přidružení v případě vymazávání lokálního uživatelského profilu i5/OS. Můžete si vybrat z následujících typů uživatelů: **Rozlišovací jméno a heslo**, **Soubor tabulky klíčů a činitel Kerberos** nebo **Činitel a heslo Kerberos**. Které typy uživatele budete moci zvolit, závisí především na stávající konfiguraci systému. Pokud je například pro systém nakonfigurována služba síťového ověření, typy uživatelů Kerberos nemusí být dostupné pro účely výběru. K typu uživatele, který vyberete, se váží další informace, jež musíte na stránce zadat:

    Poznámka: Musíte zadat uživatele, který je aktuálně definován na serveru adresářů, jenž funguje jako hostitel pro řadič domény EIM. Uživatel, kterého zadáte, musí mít oprávnění k provádění operací mapování a administrace registru, a to minimálně pro lokální registr uživatelů. Pokud zadávaný uživatel tato oprávnění nemá, mohou selhat některé funkce operačního systému spojené s použitím jediného přihlášení a s vymazáním uživatelských profilů.

    Pokud jste nenakonfigurovali server adresářů před spuštěním tohoto průvodce, bude jediným typem uživatele, který můžete vybrat, typ **Rozlišovací jméno a heslo**, a jediné rozlišovací jméno, které můžete zadat, bude DN administrátora serveru LDAP.

    - Jestliže vyberete volbu **Rozlišovací jméno a heslo**, musíte zadat tyto informace:
      – Do pole **Rozlišovací jméno** zadejte rozlišovací jméno LDAP, které bude identifikovat uživatele v systému při provádění operací EIM.

- Do pole **Heslo** zadejte heslo pro rozlišovací jméno.
- Do pole **Potvrdit heslo** zadejte pro kontrolu vaše heslo ještě jednou.

• Pokud vyberete volbu **Činitel a heslo Kerberos**, musíte zadat tyto informace:
- Do pole **Činitel** zadejte jméno činitele Kerberos, které má systém použít při provádění operací EIM.
- Do pole **Sféra** zadejte plně kvalifikované jméno sféry Kerberos, jejímž členem je činitel. Jméno činitele a jméno sféry jednoznačně identifikují uživatele Kerberos v souboru tabulky klíčů. Například činitel jsmith ve sféře ordept.myco.com je reprezentována v souboru tabulky klíčů jako jsmith@ordept.myco.com.
- Do pole **Heslo** zadejte heslo pro uživatele.
- Do pole **Potvrdit heslo** zadejte pro kontrolu vaše heslo ještě jednou.

• Pokud vyberete volbu **Soubor tabulky klíčů a činitel Kerberos**, zadejte následující údaje:
- Do pole **Soubor tabulky klíčů** zadejte plně kvalifikované jméno cesty a souboru tabulky klíčů, které obsahuje činitele Kerberos a které má systém použít při provádění operací EIM. Nebo klepněte na **Procházet**, projděte adresáře v integrovaném systému souborů systému System i a vyberte příslušný soubor tabulky klíčů.
- Do pole **Činitel** zadejte jméno činitele Kerberos, které má systém používat při provádění operací EIM.
- Do pole **Sféra** zadejte plně kvalifikované jméno sféry Kerberos, jejímž členem je činitel. Jméno činitele a jméno sféry jednoznačně identifikují uživatele Kerberos v souboru tabulky klíčů. Například činitel jsmith ve sféře ordept.myco.com je reprezentována v souboru tabulky klíčů jako jsmith@ordept.myco.com.

• Klepněte na **Ověřit připojení**, abyste se ujistili, že průvodce může použít zadané informace o uživateli k úspěšnému vytvoření připojení k řadiči domény EIM.
• Klepněte na **Další**.

11. V okně **Shrnutí** zkontrolujte konfigurační informace, které jste zadali. Pokud jsou všechny informace správné, klepněte na **Dokončit**.

Dokončení konfigurace EIM pro doménu

Po dokončení přidá průvodce novou doménu do složky **Správa domén**. To znamená, že jste vytvořili základní konfiguraci EIM pro tento server. Musíte však provést ještě níže uvedené úlohy, kterými dokončíte vaši konfiguraci EIM pro doménu:

1. Použijte průvodce konfigurací EIM na každém dodatečném serveru, který chcete připojit k doméně.
2. V případě nutnosti přidejte definice registru EIM do domény EIM i pro další platformy a aplikace (jiné než System i), které mají být členy domény EIM. Tyto definice registrů se vztahují ke skutečným registrům uživatelů, kteří musí být součástí domény. Můžete buď přidat definice systémového registru, nebo přidat definice aplikačního registru, v závislosti na vašich potřebách implementace EIM.
3. Na základě vašich potřeb vztahujících se k implementaci EIM určete, zda je potřeba:
   • Vytvořit identifikátory EIM pro každého jedinečného uživatele nebo entitu v doméně a pro ně vytvořit přidružení identifikátorů.
   • Vytvořit přidružení zásad za účelem mapování skupiny uživatelů na totožnost jediného cílového uživatele.
   • Vytvořit kombinaci těchto možností.
4. Použijte funkci produktu EIM testování mapování k otestování mapování totožnosti pro vaši konfiguraci EIM.
5. Pokud je jediným uživatelem EIM, kterého jste definovali, rozlišovací jméno administrátora LDAP, pak má váš uživatel EIM vysokou úroveň oprávnění ke všem datům na serveru adresářů. Proto byste měli vzít v úvahu možnost vytvoření jednoho nebo více rozlišovacích jmen jako dodatečných uživatelů, kteří budou mít omezenější kontrolu přístupu k datům EIM. Další informace o vytváření rozlišovacích jmen pro server adresářů uvádí téma Rozlišovací jména pod heslem i5/OS. Počet dodatečných uživatelů EIM, které budete definovat, je závislý na tom, nakolik vaše zásada zabezpečení klade důraz na oddělení povinností a odpovědností v oblasti zabezpečení ochrany dat. Obvykle je možné vytvořit alespoň dva následující typy rozlišovacích jmen (DN):
   • **Uživatel, který má kontrolu přístupu na úrovni administrátora EIM.**

     Toto DN administrátora EIM zajišťuje odpovídající úroveň oprávnění pro administrátora, který je odpovědný za správu domény EIM. Toto DN administrátora EIM je možné použít k připojení k řadiči domény za účelem správy všech aspektů domény EIM prostřednictvím produktu System i Navigator.

- **Alespoň jeden uživatel, který bude mít všechny níže uvedené kontroly přístupu**:
  - Administrátor identifikátorů.
  - Administrátor registrů.
  - Operace mapování EIM.

  Tento uživatel poskytuje odpovídající úroveň kontroly přístupu vyžadovanou pro uživatele systému, který provádí operace EIM v zastoupení operačního systému.

Poznámka: Chcete-li pro uživatele systému použít toto nové rozlišovací jméno namísto rozlišovacího jména administrátora LDAP, musíte změnit vlastnosti konfigurace EIM pro systém System i. Další informace o změně rozlišovacího jména uživatele systému uvádí téma Správa vlastností konfigurace EIM.

Kromě toho možná budete chtít použít SSL (Secure Sockets Layer) nebo TLS (Transport Layer Security) ke konfiguraci bezpečného připojení k řadiči domény EIM za účelem ochrany přenosu dat EIM. V případě, že povolíte SSL pro server adresářů, musíte aktualizovat vlastnosti konfigurace EIM a zadat, že systém System i používá připojení zabezpečené prostřednictvím SSL. Navíc musíte aktualizovat vlastnosti domény a zadat, že EIM používá připojení SSL ke správě domény prostřednictvím produktu System i Navigator.

Poznámka: Jestliže jste vytvořili základní konfiguraci služby síťového ověření, možná budete muset provést dodatečné úlohy, zejména v případě, že jste implementovali prostředí jediného přihlášení. Informace o těchto dodatečných krocích získáte, když si prostudujete kompletní postup konfigurace, který je uveden ve scénáři Povolení prostředí jediného přihlášení pro operační systém i5/OS.

Vytvoření a vstup do nové vzdálené domény

Když používáte průvodce konfigurací EIM k vytváření a vstupu do nové domény, můžete se rozhodnout, že v rámci vytváření vaší konfigurace EIM nakonfigurujete server adresářů ve vzdáleném systému tak, aby pracoval jako řadič domény EIM.

Musíte zadat příslušné informace pro připojení ke vzdálenému serveru adresářů, abyste umožnili konfiguraci EIM. Také v případě, že na systému System i dosud není nakonfigurován produkt Kerberos, vyvolá průvodce program, který bude vaším průvodcem při vytváření služby síťového ověření.

Poznámka: Server adresářů ve vzdáleném systému musí podporovat produkt EIM. EIM vyžaduje server adresářů, který podporuje LDAP (Lightweight Directory Access Protocol) verze 3, fungoval jako hostitel pro řadič domény. Kromě tohoto musí být na serveru adresářů nakonfigurováno schéma EIM. Tuto podporu poskytuje například produkt IBM Directory Server V5.1. Podrobnější informace o požadavcích na řadič domény EIM najdete v tématu “Plánování řadiče domény EIM (Enterprise Identity Mapping)” na stránce 55.

Poté, co dokončíte všechny úlohy v rámci průvodce konfigurací EIM, můžete provést níže uvedené úlohy:

- Vytvoření nové domény EIM.
- Konfigurace vzdáleného serveru adresářů, který bude pracovat jako řadič domény EIM.
- Konfigurace služby síťového ověření v systému.
- Vytvoření definic registru pro lokální registr i5/OS a registr Kerberos.
- Konfigurace systému jako člena nové domény EIM.

Chcete-li konfigurovat systém za účelem vytvoření a vstupu do nové domény EIM, musíte mít všechna níže uvedená zvláštní oprávnění:

- Administrátor zabezpečení (*SECADM).
- Všechny objekty (*ALLOBJ).
- Konfigurace systému (*IOSYSCFG).

Chcete-li k vytvoření a k vstupu do domény ve vzdáleném systému použít průvodce konfigurací EIM, postupujte takto:

1. Ověřte si, zda-li je server adresářů ve vzdáleném systému aktivní.
2. V prostředí produktu System i Navigator vyberte systém, pro který chcete konfigurovat EIM. Pak rozbalte položku **Síť > EIM (Enterprise Identity Mapping)**.
3. Pravým tlačítkem myši klepněte na **Konfigurace** a vyberte volbu **Konfigurovat**. Tím spustíte průvodce konfigurací produktu EIM.

   Poznámka: V případě, že už jste v systému měli dříve nakonfigurován produkt EIM, bude tato volba znít **Překonfigurovat**.
4. Na **uvítací stránce** průvodce vyberte volbu **Vytvořit a vstoupit do nové domény**. Pak klepněte na **Další**.
5. Na stránce **Zadat umístění domény EIM** vyberte volbu **Na lokálním serveru adresářů**. Pak klepněte na **Další**.

   Poznámka: Tato volba nakonfiguruje lokální server adresářů, aby pracoval jako řadič domény EIM. Vzhledem k tomu, že tento server adresářů uchovává všechna data EIM pro doménu, musí být aktivní a musí zůstat aktivní, aby podporoval operace vyhledávání mapování EIM a další operace.

   Pokud na systému System i není aktuálně nakonfigurována služba síťového ověření nebo jsou nezbytné dodatečné informace o konfiguraci služby síťového ověření za účelem konfigurování prostředí jediného přihlášení, zobrazí se stránka **Konfigurace služby síťového ověření**. Tato stránka vám umožňuje spustit průvodce konfigurací služby síťového ověření, v jehož rámci pak nakonfigurujete službu síťového ověření. Rovněž můžete službu síťového ověření nakonfigurovat později, prostřednictvím průvodce konfigurací pro tuto službu, kterého poskytuje produkt System i Navigator. Poté, co dokončíte konfiguraci služby síťového ověření, bude průvodce konfigurací EIM pokračovat.
6. Chcete-li nakonfigurovat službu síťového ověření, postupujte takto:
   a. Na stránce **Konfigurace služby síťového ověření** spusťte výběrem volby **Ano** průvodce konfigurací služby síťového ověření. S pomocí tohoto průvodce můžete nakonfigurovat několik rozhraní a služeb operačního systému i5/OS, které budou ve sféře Kerberos. Rovněž můžete nakonfigurovat prostředí jediného přihlášení, které bude využívat jak EIM, tak služba síťového ověření.
   b. Na stránce **Zadání informací o sféře** zadejte do pole **Předvolená sféra** jméno předvolené sféry. Pokud k ověření Kerberos používáte produkt Microsoft Active Directory, vyberte volbu **Použít Microsoft Active Directory k ověření Kerberos** a klepněte na **Další**.
   c. Na stránce **Zadání informací o KDC** zadejte do pole **KDC** plně kvalifikované jméno serveru Kerberos pro tuto sféru. Dále zadejte 88 do pole **Port**. Pak klepněte na **Další**.
   d. Na stránce **Zadání informací o serveru hesel** vyberte buď **Ano**, nebo **Ne** za účelem nastavení serveru hesel. Server hesel umožňuje změnit hesla na serveru Kerberos. Pokud vyberete volbu **Ano**, zadejte do pole **Server hesel** jméno serveru hesel. V poli **Port** ponechte předvolenou hodnotu 464 a klepněte na Další.
   e. Na stránce **Výběr položek souboru tabulky klíčů** zvolte **Ověření i5/OS Kerberos** a klepněte na **Další**.

      Poznámka: Kromě toho můžete vytvářet záznamy souboru tabulky klíčů pro produkt IBM Tivoli Directory Server for i5/OS, i5/OS NetServer a pro produkt IBM HTTP Server for i5/OS, pokud chcete, aby tyto služby rovněž používaly ověření Kerberos. Dříve než budete moci používat ověření Kerberos, možná budete muset provést dodatečnou konfiguraci těchto služeb.
   f. Na stránce **Vytvoření záznamu souboru tabulky klíčů i5/OS** zadejte a potvrďte heslo a poté klepněte na **Další**. Musí to být stejné heslo, které budete používat při přidávání činitelů i5/OS na server Kerberos.
   g. Volitelné: Na stránce **Vytvoření dávkového souboru** vyberte volbu **Ano**, zadejte níže uvedené informace a pak klepněte na **Další**:
      - V poli **Dávkový soubor** proveďte aktualizaci cesty k adresáři. Klepněte na **Procházet** a vyhledejte příslušnou cestu k adresáři nebo změňte cestu, která je uvedena v poli **Dávkový soubor**.
      - V poli **Zahrnout heslo** vyberte **Ano**. Tím zajistíte, aby všechna hesla přiřazená k činiteli i5/OS byla zahrnuta do dávkového souboru. Povšimněte si, že hesla se zobrazí jako čistý text a může si je přečíst kdokoliv, kdo má přístupová práva ke čtení dávkového souboru. Proto je velmi důležité, abyste vymazali dávkový soubor ze serveru Kerberos a z PC okamžitě poté, co jej použijete. Pokud nezahrnete heslo, budete vyzváni k zadání hesla při spuštění dávkového souboru.

Poznámka: Činitele, kteří jsou generováni průvodcem produktu Microsoft Active Directory, můžete také přidat manuálně. Chcete-li zjistit, jak to provést, prostudujte si téma Přidání činitelů i5/OS na server Kerberos.

- Na stránce **Shrnutí** zkontrolujte konfigurační informace týkající se služby síťového ověření. Klepnutím na **Dokončit** se vrátíte do průvodce konfigurací EIM.

7. Použijte stránku **Zadání řadiče domény EIM** k zadání informací o připojení pro vzdálený řadič domény EIM, který chcete nakonfigurovat:
   a. Do pole **Jméno řadiče domény** zadejte jméno vzdáleného serveru adresářů, který chcete konfigurovat jako řadič domény pro vytvářenou doménu. Jméno řadiče domény může být hostitelským v zastoupení TCP/IP a v zastoupení domény serveru adresářů nebo adresou serveru adresářů.
   b. Zadejte níže uvedené informace o připojení pro připojení k řadiči domény:
      - Vyberte volbu **Použít zabezpečené připojení (SSL nebo TLS)**, abyste zajistili používání zabezpečeného připojení k řadiči domény EIM. Po výběru této volby bude proces připojování používat buď SSL (Secure Sockets Layer), nebo TSL (Transport Layer Security) k vytvoření zabezpečeného připojení a ochrany přenosu dat EIM přes nedůvěryhodnou síť, jako je Internet.

        Poznámka: Musíte ověřit, zda je řadič domény EIM nakonfigurován pro používání zabezpečeného připojení. Jinak může připojení k řadiči domény selhat.
      - Do pole **Port** zadejte port TCP/IP, na kterém server adresářů naslouchá. Pokud je vybrána volba **Použít zabezpečené připojení**, předvolený port bude 636. Jinak bude předvolený port nastaven na hodnotu 389.
   c. Klepněte na **Ověřit připojení**, abyste otestovali, zda může průvodce použít zadané informace k úspěšnému vytvoření připojení ke vzdálenému řadiči domény EIM.
   d. Klepněte na **Další**.
8. Na stránce **Zadání uživatele pro připojení** vyberte **Typ uživatele** pro připojení. Je možné zvolit jeden z následujících typů uživatele: **Rozlišovací jméno a heslo**, **Soubor tabulky klíčů a činitel Kerberos** , **Činitel a heslo Kerberos** nebo **Uživatelský profil a heslo**. Dva uvedené typy uživatelů Kerberos jsou dostupné pouze v případě, že je pro lokální systém System i nakonfigurována služba síťového ověření. Výběr jednotlivého typu uživatele bude mít vliv na údaje, které budete muset pro úspěšné dokončení dialogu zadat:

   Poznámka: Chcete-li zajistit, aby průvodce měl dostatečná oprávnění k vytváření nezbytných objektů EIM v adresáři, vyberte jako typ uživatele volbu **Rozlišovací jméno a heslo** a jako uživatele zadejte rozlišovací jméno a heslo administrátora LDAP.

   Pro připojení můžete zadat také jiného uživatele. Avšak uživatel, kterého zadáte, musí mít oprávnění, která budou ekvivalentní oprávněním administrátora LDAP pro vzdálený server adresářů.
   a. Jestliže vyberete volbu **Rozlišovací jméno a heslo**, musíte zadat tyto informace:
      - Do pole **Rozlišovací jméno** zadejte rozlišovací jméno (DN) a heslo administrátora LDAP, abyste zajistili, že průvodce bude mít dostatečná oprávnění k administraci domény EIM a objektů v doméně EIM.
      - Do pole **Heslo** zadejte heslo pro rozlišovací jméno.
      - Do pole **Potvrdit heslo** zadejte vaše heslo pro kontrolu ještě jednou.
   b. Pokud vyberete volbu **Soubor tabulky klíčů a činitel Kerberos**, zadejte následující údaje:
      - Do pole **Soubor tabulky klíčů** zadejte plně kvalifikované jméno cesty a souboru tabulky klíčů, které obsahuje činitele Kerberos a které má průvodce použít při připojování k doméně EIM. Nebo klepněte na **Procházet**, projděte adresáře v integrovaném systému souborů systému i5/OS a vyberte příslušný soubor tabulky klíčů.
      - Do pole **Činitel** zadejte jméno činitele Kerberos, které má být použito k identifikaci uživatele.
      - Do pole **Sféra** zadejte plně kvalifikované jméno sféry Kerberos, jejímž členem je činitel. Jméno činitele a jméno sféry jednoznačně identifikují uživatele Kerberos v souboru tabulky klíčů. Například činitel jsmith ve sféře ordept.myco.com je reprezentována v souboru tabulky klíčů jako jsmith@ordept.myco.com.
   c. Pokud vyberete volbu **Činitel a heslo Kerberos**, musíte zadat tyto informace:
      - Do pole **Činitel** zadejte jméno činitele Kerberos, které má průvodce použít při připojování k doméně EIM.

- Do pole **Sféra** zadejte plně kvalifikované jméno sféry Kerberos, jejímž členem je činitel. Jméno činitele a jméno sféry jednoznačně identifikují uživatele Kerberos v souboru tabulky klíčů. Například činitel jsmith ve sféře ordept.myco.com je reprezentována v souboru tabulky klíčů jako jsmith@ordept.myco.com.
- Do pole **Heslo** zadejte heslo pro činitele Kerberos.
- Do pole **Potvrdit heslo** zadejte vaše heslo pro kontrolu ještě jednou.

d. Jestliže vyberete volbu **Uživatelský profil a heslo**, musíte zadat tyto informace:
   - Do pole **Uživatelský profil** zadejte jméno uživatelského profilu, které má průvodce použít při připojování k doméně EIM.
   - Do pole **Heslo** zadejte heslo pro uživatelský profil.
   - Do pole **Potvrdit heslo** zadejte vaše heslo pro kontrolu ještě jednou.

e. Klepnutím na **Ověřit připojení** otestujte, zda průvodce může použít zadané informace o uživateli k úspěšnému vytvoření připojení k řadiči domény EIM.

f. Klepněte na **Další**.

9. Na stránce **Zadání domény** zadejte níže uvedené informace:
   a. Do pole **Doména** napište jméno domény EIM, kterou chcete vytvořit. Ponechte předvolené jméno EIM nebo použijte libovolný řetězec znaků, který pro vás bude mít smysl. Nesmíte však používat zvláštní znaky, jako je **= + < > ,** # **;** \ and *****.
   b. Do pole **Popis** zadejte text, který bude novou doménu popisovat.
   c. Klepněte na **Další**.
10. V dialogu **Zadání nadřazeného DN pro doménu** vyberte volbu **Ano**, abyste určili nadřazené DN, které má průvodce použít k umístění domény EIM, kterou vytváříte. Je to rozlišovací jméno, které představuje záznam hned nad záznamem jména domény ve stromové hierarchii informací o adresáři. Nebo zadejte **Ne**, což bude mít za následek, že data EIM budou ukládána do adresáře, jehož jméno přípony bude odvozeno ze jména domény EIM.

    Poznámka: Pokud použijete průvodce k nakonfigurování domény na vzdáleném řadiči domény, musíte zadat příslušné nadřazené DN pro doménu. Vzhledem k tomu, že všechny nezbytné konfigurační objekty pro nadřazené DN již musí existovat (jinak konfigurace EIM selže), měli byste namísto ručního zadávání informací o DN použít volbu procházení a vyhledat příslušné nadřazené DN. Pokud chcete získat další informace o používání nadřazeného DN, klepněte na **Nápověda**.
11. Na stránce **Informace o registrech** zadejte, zda si přejete přidat lokální registry uživatelů k doméně EIM jako definice registrů. Vyberte jeden nebo oba níže uvedené typy registrů uživatelů:

    Poznámka: V tomto okamžiku nemusíte vytvářet definice registru. Pokud se rozhodnete vytvořit definice registru později, musíte přidat definici systémového registru a aktualizovat vlastnosti konfigurace EIM.
    a. Výběrem volby **Lokální i5/OS** přidáte definici registru pro lokální registr. V příslušném poli ponechte předvolenou hodnotu pro jméno definice registru anebo pro ně zadejte nějakou jinou hodnotu. Jméno registru EIM je libovolný řetězec, který reprezentuje typ registru a specifickou instanci daného registru.
    b. Výběrem volby **Kerberos** přidáte definici registru pro registr Kerberos. V příslušném poli ponechte předvolenou hodnotu pro jméno definice registru nebo pro ně zadejte nějakou jinou hodnotu. Předvolené jméno definice registru je stejné jako jméno sféry. Ponecháním předvoleného jména a použitím stejného jména registru Kerberos, jako je jméno sféry, můžete zvýšit výkon při vyhledávání informací z registru. V případě potřeby vyberte volbu **Totožnosti uživatele Kerberos jsou citlivé na velká písmena**.
    c. Klepněte na **Další**.
12. Na stránce **Zadání uživatele systému EIM** vyberte **Typ uživatele**, který má být systémem používán při provádění operací EIM v zastoupení funkcí operačního systému. Tyto operace zahrnují operace vyhledávání mapování a výmaz přidružení v případě vymazávání lokálního uživatelského profilu i5/OS. Můžete si vybrat z následujících typů uživatelů: **Rozlišovací jméno a heslo**, **Soubor tabulky klíčů a činitel Kerberos** nebo **Činitel a heslo Kerberos**. Které typy uživatele budete moci zvolit, závisí především na stávající konfiguraci systému. Pokud je například pro systém nakonfigurována služba síťového ověření, typy uživatelů Kerberos nemusí být dostupné pro účely výběru. K typu uživatele, který vyberete, se váží další informace, jež musíte na stránce zadat:

Poznámka: Musíte zadat uživatele, který je aktuálně definován na serveru adresářů, jenž funguje jako hostitel pro řadič domény EIM. Uživatel, kterého zadáte, musí mít oprávnění k provádění operací mapování a administrace registru, a to minimálně pro lokální registr uživatelů. Pokud zadávaný uživatel tato oprávnění nemá, mohou selhat některé funkce operačního systému spojené s použitím jediného přihlášení a s vymazáním uživatelských profilů.

Pokud jste nenakonfigurovali server adresářů před spuštěním tohoto průvodce, bude jediným typem uživatele, který můžete vybrat, typ **Rozlišovací jméno a heslo**, a jediné rozlišovací jméno, které můžete zadat, bude DN administrátora serveru LDAP.

a. Jestliže vyberete volbu **Rozlišovací jméno a heslo**, musíte zadat tyto informace:
   - Do pole **Rozlišovací jméno** zadejte rozlišovací jméno LDAP, které bude identifikovat uživatele v systému při provádění operací EIM.
   - Do pole **Heslo** zadejte heslo pro rozlišovací jméno.
   - Do pole **Potvrdit heslo** zadejte pro kontrolu vaše heslo ještě jednou.

b. Pokud vyberete volbu **Činitel a heslo Kerberos**, musíte zadat tyto informace:
   - Do pole **Činitel** zadejte jméno činitele Kerberos, které má systém použít při provádění operací EIM.
   - Do pole **Sféra** zadejte plně kvalifikované jméno sféry Kerberos, jejímž členem je činitel. Jméno činitele a jméno sféry jednoznačně identifikují uživatele Kerberos v souboru tabulky klíčů. Například činitel jsmith ve sféře ordept.myco.com je reprezentována v souboru tabulky klíčů jako jsmith@ordept.myco.com.
   - Do pole **Heslo** zadejte heslo pro uživatele.
   - Do pole **Potvrdit heslo** zadejte pro kontrolu vaše heslo ještě jednou.

c. Pokud vyberete volbu **Soubor tabulky klíčů a činitel Kerberos**, zadejte následující údaje:
   - Do pole **Soubor tabulky klíčů** zadejte plně kvalifikované jméno cesty a souboru tabulky klíčů, které obsahuje činitele Kerberos a které má systém použít při provádění operací EIM. Nebo klepněte na **Procházet**, projděte adresáře v integrovaném systému souborů systému System i a vyberte příslušný soubor tabulky klíčů.
   - Do pole **Činitel** zadejte jméno činitele Kerberos, které má systém používat při provádění operací EIM.
   - Do pole **Sféra** zadejte plně kvalifikované jméno sféry Kerberos, jejímž členem je činitel. Jméno činitele a jméno sféry jednoznačně identifikují uživatele Kerberos v souboru tabulky klíčů. Například činitel jsmith ve sféře ordept.myco.com je reprezentována v souboru tabulky klíčů jako jsmith@ordept.myco.com.

d. Klepněte na **Ověřit připojení**, abyste se ujistili, že průvodce může použít zadané informace o uživateli k úspěšnému vytvoření připojení k řadiči domény EIM.

e. Klepněte na **Další**.

13. V okně **Shrnutí** zkontrolujte konfigurační informace, které jste zadali. Pokud jsou všechny informace správné, klepněte na **Dokončit**.

Dokončení konfigurace EIM pro doménu

Po dokončení přidá průvodce novou doménu do složky **Správa domén**. To znamená, že jste vytvořili základní konfiguraci EIM pro tento server. Musíte však provést ještě níže uvedené úlohy, kterými dokončíte vaši konfiguraci EIM pro doménu:

1. Použijte průvodce konfigurací EIM na každém dodatečném serveru, který chcete připojit k existující doméně. Další informace naleznete v tématu “Vstup do existující domény” na stránce 78.
2. V případě nutnosti přidejte definice registru EIM do domény EIM i pro další platformy a aplikace (jiné než System i), které mají být členy domény EIM.Tyto definice registrů se vztahují ke skutečným registrům uživatelů, kteří musí být součástí domény. V závislosti na vaší implementaci EIM si prohlédněte buď téma “Přidání definice systémového registru” na stránce 89 nebo téma “Přidání definice aplikačního registru” na stránce 89.
3. Na základě vašich potřeb vztahujících se k implementaci EIM určete, zda je potřeba:
   a. “Vytvoření identifikátoru EIM” na stránce 95 pro každého jedinečného uživatele nebo entitu v doméně a pro ně “Vytvoření přidružení identifikátorů EIM” na stránce 98.
   b. “Vytvoření přidružení zásad” na stránce 99 za účelem mapování skupiny uživatelů na totožnost jediného cílového uživatele..

c. Vytvoření kombinace těchto možností.

4. Použijte funkci produktu EIM “Testování mapování EIM” na stránce 85 k otestování mapování totožnosti pro vaši konfiguraci EIM.
5. Pokud je jediným uživatelem EIM, kterého jste definovali, rozlišovací jméno administrátora LDAP, pak má váš uživatel EIM vysokou úroveň oprávnění ke všem datům na serveru adresářů. Proto byste měli vzít v úvahu možnost vytvoření jednoho nebo více rozlišovacích jmen jako dodatečných uživatelů, kteří budou mít omezenější kontrolu přístupu k datům EIM. Další informace o vytváření rozlišovacích jmen pro server adresářů uvádí téma Rozlišovací jména pod heslem i5/OS. Počet dodatečných uživatelů EIM, které budete definovat, je závislý na tom, nakolik vaše zásada zabezpečení klade důraz na oddělení povinností a odpovědností v oblasti zabezpečení ochrany dat. Obvykle je možné vytvořit alespoň dva následující typy rozlišovacích jmen (DN):
   - **Uživatel, který má kontrolu přístupu na úrovni administrátora EIM.**

     Toto DN administrátora EIM zajišťuje odpovídající úroveň oprávnění pro administrátora, který je odpovědný za správu domény EIM. Toto DN administrátora EIM je možné použít k připojení k řadiči domény za účelem správy všech aspektů domény EIM prostřednictvím produktu System i Navigator.
   - **Alespoň jeden uživatel, který bude mít všechny níže uvedené kontroly přístupu**:
     - Administrátor identifikátorů.
     - Administrátor registrů.
     - Operace mapování EIM.

     Tento uživatel poskytuje odpovídající úroveň kontroly přístupu vyžadovanou pro uživatele systému, který provádí operace EIM v zastoupení operačního systému.

   Poznámka: Chcete-li pro uživatele systému použít toto nové rozlišovací jméno namísto rozlišovacího jména administrátora LDAP, musíte změnit vlastnosti konfigurace EIM pro systém System i. Další informace o změně DN uživatele systému uvádí téma “Správa konfiguračních vlastností EIM” na stránce 113.

Jestliže jste vytvořili základní konfiguraci služby síťového ověření, možná budete muset provést dodatečné úlohy, zejména v případě, že jste implementovali prostředí jediného přihlášení. Informace o těchto dodatečných krocích získáte, když si prostudujete kompletní postup konfigurace, který je uveden ve scénáři Povolení prostředí jediného přihlášení pro operační systém i5/OS.

Vstup do existující domény

Tyto informace popisují, jak lze v systému System i použít průvodce konfigurací EIM pro konfiguraci řadiče domény, vytvořit doménu EIM a poté použít průvodce ke konfiguraci ostatních systémů tak, aby se účastnily domény.

Po vytvoření domény EIM a konfiguraci řadiče domény v jednom systému můžete za účelem vstupu do existující domény EIM nakonfigurovat všechny další systémy System i. Při práci s průvodcem musíte dodávat informace o doméně spolu s informacemi o připojení k řadiči domény EIM. Když použijete průvodce konfigurací EIM pro vstup do existující domény a pokud v systému zvolíte konfiguraci produktu Kerberos jako součást konfigurace EIM, průvodce vám také nabídne volbu spuštění průvodce pro konfiguraci služby síťového ověření.

Po ukončení práce s průvodcem konfigurace EIM pro vstup do existující domény můžete přejít k následujícím úkolům:

- Konfigurace služby síťového ověření v systému.
- Vytvoření definic registru pro lokální registr i5/OS a registr Kerberos.
- Konfigurace systému pro účast v existující doméně EIM.

V případě konfigurace vašeho systému za účelem vstupu do existující domény EIM musíte mít všechna následující zvláštní oprávnění.

- Administrátor zabezpečení (*SECADM).
- Všechny objekty (*ALLOBJ).

Chcete-li začít pracovat s průvodcem konfigurací EIM pro vstup do existující domény, můžete přejít k následujícím úkolům:

1. Ověřte si, zda-li je server adresářů ve vzdáleném systému aktivní.
2. V prostředí produktu System i Navigator vyberte systém, pro který chcete konfigurovat EIM. Pak rozbalte položku **Síť > EIM (Enterprise Identity Mapping)**.
3. Pravým tlačítkem myši klepněte na **Konfigurace** a vyberte volbu **Konfigurovat...**. Tím spustíte průvodce konfigurací produktu EIM.

   Poznámka: V případě, že už jste v systému měli dříve nakonfigurován produkt EIM, bude tato volba znít **Překonfigurovat...**.
4. Na **Uvítací** stránce průvodce zvolte **Vstoupit do existující domény** a klepněte na **Další**.

   Poznámka: Pokud na systému System i není aktuálně nakonfigurována služba síťového ověření nebo jsou nezbytné dodatečné informace o konfiguraci služby síťového ověření za účelem konfigurování prostředí jediného přihlášení, zobrazí se stránka **Konfigurace služby síťového ověření**. Tato stránka vám umožňuje spustit průvodce konfigurací služby síťového ověření, v jehož rámci pak nakonfigurujete službu síťového ověření. Rovněž můžete službu síťového ověření nakonfigurovat později, prostřednictvím průvodce konfigurací pro tuto službu, kterého poskytuje produkt System i Navigator. Poté, co dokončíte konfiguraci služby síťového ověření, bude průvodce konfigurací EIM pokračovat.
5. Chcete-li nakonfigurovat službu síťového ověření, postupujte takto:
   a. Na stránce **Konfigurace služby síťového ověření** spusťte výběrem volby **Ano** průvodce konfigurací služby síťového ověření. S pomocí tohoto průvodce můžete nakonfigurovat několik rozhraní a služeb operačního systému i5/OS, které budou ve sféře Kerberos. Rovněž můžete nakonfigurovat prostředí jediného přihlášení, které bude využívat jak EIM, tak služba síťového ověření.
   b. Na stránce **Zadání informací o sféře** zadejte do pole **Předvolená sféra** jméno předvolené sféry. Pokud k ověření Kerberos používáte produkt Microsoft Active Directory, vyberte volbu **Použít Microsoft Active Directory k ověření Kerberos** a klepněte na **Další**.
   c. Na stránce **Zadání informací o KDC** zadejte do pole **KDC** plně kvalifikované jméno serveru Kerberos pro tuto sféru. Dále zadejte 88 do pole **Port**. Pak klepněte na **Další**.
   d. Na stránce **Zadání informací o serveru hesel** vyberte buď **Ano**, nebo **Ne** za účelem nastavení serveru hesel. Server hesel umožňuje změnit hesla na serveru Kerberos. Pokud vyberete volbu **Ano**, zadejte do pole **Server hesel** jméno serveru hesel. V poli **Port** ponechte předvolenou hodnotu 464 a klepněte na Další.
   e. Na stránce **Výběr položek souboru tabulky klíčů** zvolte **Ověření i5/OS Kerberos** a klepněte na **Další**.

      Poznámka: Kromě toho můžete vytvářet záznamy souboru tabulky klíčů pro produkt IBM Tivoli Directory Server for i5/OS, i5/OS NetServer a pro produkt IBM HTTP Server for i5/OS, pokud chcete, aby tyto služby rovněž používaly ověření Kerberos. Dříve než budete moci používat ověření Kerberos, možná budete muset provést dodatečnou konfiguraci těchto služeb.
   f. Na stránce **Vytvoření záznamu souboru tabulky klíčů i5/OS** zadejte a potvrďte heslo a poté klepněte na **Další**. Musí to být stejné heslo, které budete používat při přidávání činitelů i5/OS na server Kerberos.
   g. Volitelné: Na stránce **Vytvoření dávkového souboru** vyberte volbu **Ano**, zadejte níže uvedené informace a pak klepněte na **Další**:
      - V poli **Dávkový soubor** proveďte aktualizaci cesty k adresáři. Klepněte na **Procházet** a vyhledejte příslušnou cestu k adresáři nebo změňte cestu, která je uvedena v poli **Dávkový soubor**.
      - V poli **Zahrnout heslo** vyberte **Ano**. Tím zajistíte, aby všechna hesla přiřazená k činiteli i5/OS byla zahrnuta do dávkového souboru. Povšimněte si, že hesla se zobrazí jako čistý text a může si je přečíst kdokoliv, kdo má přístupová práva ke čtení dávkového souboru. Proto je velmi důležité, abyste vymazali dávkový soubor ze serveru Kerberos a z PC okamžitě poté, co jej použijete. Pokud nezahrnete heslo, budete vyzváni k zadání hesla při spuštění dávkového souboru.

Poznámka: Činitele, kteří jsou generováni průvodcem produktu Microsoft Active Directory, můžete také přidat manuálně. Chcete-li zjistit, jak to provést, prostudujte si téma Přidání činitelů i5/OS na server Kerberos.

- Na stránce **Shrnutí** zkontrolujte konfigurační informace týkající se služby síťového ověření. Klepnutím na **Dokončit** se vrátíte do průvodce konfigurací EIM.

6. Na stránce **Zadání řadiče domény** zkontrolujte následující informace:

   Poznámka: Server adresářů, který slouží jako řadič domény, musí být pro úspěšné provedení konfigurace EIM aktivní.

   a. Do pole **Jméno řadiče domény** zadejte jméno systému, který slouží jako řadič domény pro doménu EIM, jež má být připojena k systému System i.
   b. V případě, že si přejete využívat zabezpečené připojení s řadičem domény EIM, klepněte na **Použít zabezpečené připojení (SSL nebo TLS)**. Po výběru této volby bude proces připojování používat buď SSL (Secure Sockets Layer), nebo TSL (Transport Layer Security) k vytvoření zabezpečeného připojení a ochrany přenosu dat EIM přes nedůvěryhodnou síť, jako je Internet.

      Poznámka: Musíte ověřit, zda je řadič domény EIM nakonfigurován pro používání zabezpečeného připojení. Jinak může připojení k řadiči domény selhat.

   c. Do pole **Port** zadejte port TCP/IP, na kterém server adresářů naslouchá. Pokud je vybrána volba **Použít zabezpečené připojení**, předvolený port bude 636. Jinak bude předvolený port nastaven na hodnotu 389.
   d. Chcete-li ověřit, zda průvodce může použít zadané informace ke spojení s řadičem domény EIM, klepněte na **Ověřit připojení**.
   e. Klepněte na **Další**.

7. Na stránce **Zadání uživatele pro připojení** vyberte **Typ uživatele** pro připojení. Můžete vybrat jeden z těchto typů uživatele: **Rozlišovací jméno a heslo**, **Soubor tabulky klíčů a činitel Kerberos**, **Činitel a heslo Kerberos** nebo **Uživatelský profil a heslo**. Dva uvedené typy uživatelů Kerberos jsou dostupné pouze v případě, že je pro lokální systém System i nakonfigurována služba síťového ověření. Výběr jednotlivého typu uživatele bude mít vliv na údaje, které budete muset pro úspěšné dokončení dialogu zadat:

   Poznámka: Chcete-li zajistit, aby průvodce měl dostatečná oprávnění k vytváření nezbytných objektů EIM v adresáři, vyberte jako typ uživatele volbu **Rozlišovací jméno a heslo** a jako uživatele zadejte rozlišovací jméno a heslo administrátora LDAP.

   Pro připojení můžete zadat také jiného uživatele. Avšak uživatel, kterého zadáte, musí mít oprávnění, která budou ekvivalentní oprávněním administrátora LDAP pro vzdálený server adresářů.

   - Jestliže vyberete volbu **Rozlišovací jméno a heslo**, musíte zadat tyto informace:
     - Do pole **Rozlišovací jméno** zadejte rozlišovací jméno (DN) LDAP. Toto jméno bude identifikovat uživatele, který má oprávnění vytvářet objekty v lokálním prostoru pro jména serveru LDAP. Pokud jste již dříve používali tohoto průvodce pro konfiguraci serveru LDAP, rozlišovací jméno administrátora serveru LDAP by mělo zůstat stejné.
     - Do pole **Heslo** zadejte heslo pro rozlišovací jméno.
     - Do pole **Potvrdit heslo** zadejte vaše heslo pro kontrolu ještě jednou.
   - Pokud vyberete volbu **Soubor tabulky klíčů a činitel Kerberos**, zadejte následující údaje:
     - Do pole **Soubor tabulky klíčů** zadejte plně kvalifikované jméno cesty a souboru tabulky klíčů, které obsahuje činitele Kerberos a které má průvodce použít při připojování k doméně EIM. Nebo klepněte na **Procházet**, projděte adresáře v integrovaném systému souborů systému System i a vyberte příslušný soubor tabulky klíčů.
     - Do pole **Činitel** zadejte jméno činitele Kerberos, které má být použito k identifikaci uživatele.
     - Do pole **Sféra** zadejte plně kvalifikované jméno sféry Kerberos, jejímž členem je činitel. Jméno činitele a jméno sféry jednoznačně identifikují uživatele Kerberos v souboru tabulky klíčů. Například činitel jsmith ve sféře ordept.myco.com je reprezentována v souboru tabulky klíčů jako jsmith@ordept.myco.com.
   - Pokud vyberete volbu **Činitel a heslo Kerberos**, musíte zadat tyto informace:

- Do pole **Činitel** zadejte jméno činitele Kerberos, které má průvodce použít při připojování k doméně EIM.
- Do pole **Sféra** zadejte plně kvalifikované jméno sféry Kerberos, jejímž členem je činitel. Jméno činitele a jméno sféry jednoznačně identifikují uživatele Kerberos v souboru tabulky klíčů. Například činitel jsmith ve sféře ordept.myco.com je reprezentována v souboru tabulky klíčů jako jsmith@ordept.myco.com.
- Do pole **Heslo** zadejte heslo pro činitele Kerberos.
- Do pole **Potvrdit heslo** zadejte vaše heslo pro kontrolu ještě jednou.

• Jestliže vyberete volbu **Uživatelský profil a heslo**, musíte zadat tyto informace:
- Do pole **Uživatelský profil** zadejte jméno uživatelského profilu, které má průvodce použít při připojování k doméně EIM.
- Do pole **Heslo** zadejte heslo pro uživatelský profil.
- Do pole **Potvrdit heslo** zadejte vaše heslo pro kontrolu ještě jednou.

• Klepnutím na **Ověřit připojení** otestujte, zda průvodce může použít zadané informace o uživateli k úspěšnému vytvoření připojení k řadiči domény EIM.
• Klepněte na **Další**.

8. Na stránce **Zadání domény** zvolte jméno domény, kterou si přejete připojit, a klepněte na **Další**.
9. Na stránce **Informace o registrech** zadejte, zda si přejete přidat lokální registry uživatelů k doméně EIM jako definice registrů. Vyberte jeden nebo oba níže uvedené typy registrů uživatelů:
   • Výběrem volby **Lokální i5/OS** přidáte definici registru pro lokální registr. V příslušném poli ponechte předvolenou hodnotu pro jméno definice registru anebo pro ně zadejte nějakou jinou hodnotu. Jméno registru EIM je libovolný řetězec, který reprezentuje typ registru a specifickou instanci daného registru.

     Poznámka: V tomto případě nemusíte lokální definici registru i5/OS vytvářet. Pokud se rozhodnete vytvořit definici registru operačního systému i5/OS později musíte přidat definici systémového registru a aktualizovat vlastnosti konfigurace EIM.

   • Výběrem volby **Kerberos** přidáte definici registru pro registr Kerberos. V příslušném poli ponechte předvolenou hodnotu pro jméno definice registru nebo pro ně zadejte nějakou jinou hodnotu. Předvolené jméno definice registru je stejné jako jméno sféry. Ponecháním předvoleného jména a použitím stejného jména registru Kerberos, jako je jméno sféry, můžete zvýšit výkon při vyhledávání informací z registru. V případě potřeby vyberte volbu **Totožnosti uživatele Kerberos jsou citlivé na velká písmena**.

     Poznámka: Pokud jste použili průvodce konfigurací EIM v jiném systému pro přidání definice registru pro registr Kerberos tam, kde systém System i vykonává službu činitele, nebudete muset při této konfiguraci definici registru Kerberos přidávat. Avšak po ukončení práce s průvodcem bude nutné zadat pro tento systém v konfiguračních vlastnostech jméno daného registru Kerberos.

   • Klepněte na **Další**.
10. Na stránce **Zadání uživatele systému EIM** vyberte **Typ uživatele**, který má být systémem používán při provádění operací EIM v zastoupení funkcí operačního systému. Tyto operace zahrnují operace vyhledávání mapování a výmaz přidružení v případě vymazávání lokálního uživatelského profilu i5/OS. Můžete si vybrat z následujících typů uživatelů: **Rozlišovací jméno a heslo**, **Soubor tabulky klíčů a činitel Kerberos** nebo **Činitel a heslo Kerberos**. Které typy uživatele budete moci zvolit, závisí především na stávající konfiguraci systému. Pokud je například pro systém nakonfigurována služba síťového ověření, typy uživatelů Kerberos nemusí být dostupné pro účely výběru. K typu uživatele, který vyberete, se váží další informace, jež musíte na stránce zadat:

    Poznámka: Musíte zadat uživatele, který je aktuálně definován na serveru adresářů, jenž funguje jako hostitel pro řadič domény EIM. Uživatel, kterého zadáte, musí mít oprávnění k provádění operací mapování a administrace registru, a to minimálně pro lokální registr uživatelů. Pokud zadávaný uživatel tato oprávnění nemá, mohou selhat některé funkce operačního systému spojené s použitím jediného přihlášení a s vymazáním uživatelských profilů.

    • Jestliže vyberete volbu **Rozlišovací jméno a heslo**, musíte zadat tyto informace:
    - Do pole **Rozlišovací jméno** zadejte rozlišovací jméno LDAP, které bude identifikovat uživatele v systému při provádění operací EIM.

- Do pole **Heslo** zadejte heslo pro rozlišovací jméno.
- Do pole **Potvrdit heslo** zadejte pro kontrolu vaše heslo ještě jednou.

- Pokud vyberete volbu **Činitel a heslo Kerberos**, musíte zadat tyto informace:
  - Do pole **Činitel** zadejte jméno činitele Kerberos, které má systém použít při provádění operací EIM.
  - Do pole **Sféra** zadejte plně kvalifikované jméno sféry Kerberos, jejímž členem je činitel. Jméno činitele a jméno sféry jednoznačně identifikují uživatele Kerberos v souboru tabulky klíčů. Například činitel jsmith ve sféře ordept.myco.com je reprezentována v souboru tabulky klíčů jako jsmith@ordept.myco.com.
  - Do pole **Heslo** zadejte heslo pro uživatele.
  - Do pole **Potvrdit heslo** zadejte pro kontrolu vaše heslo ještě jednou.
- Pokud vyberete volbu **Soubor tabulky klíčů a činitel Kerberos**, zadejte následující údaje:
  - Do pole **Soubor tabulky klíčů** zadejte plně kvalifikované jméno cesty a souboru tabulky klíčů, které obsahuje činitele Kerberos a které má systém použít při provádění operací EIM. Nebo klepněte na **Procházet**, projděte adresáře v integrovaném systému souborů systému System i a vyberte příslušný soubor tabulky klíčů.
  - Do pole **Činitel** zadejte jméno činitele Kerberos, které má systém používat při provádění operací EIM.
  - Do pole **Sféra** zadejte plně kvalifikované jméno sféry Kerberos, jejímž členem je činitel. Jméno činitele a jméno sféry jednoznačně identifikují uživatele Kerberos v souboru tabulky klíčů. Například činitel jsmith ve sféře ordept.myco.com je reprezentována v souboru tabulky klíčů jako jsmith@ordept.myco.com.
- Klepněte na **Ověřit připojení**, abyste se ujistili, že průvodce může použít zadané informace o uživateli k úspěšnému vytvoření připojení k řadiči domény EIM.
- Klepněte na **Další**.

11. Na stránce **Shrnutí** zkontrolujte informace o konfiguraci, které byly zadány. Pokud jsou všechny informace správné, klepněte na **Dokončit**.

Dokončení konfigurace EIM pro doménu

Po ukončení práce s průvodcem bude doména přidána ke složce **Správa domén** , a tímto vytvoříte základní konfiguraci EIM na tomto serveru. Chcete-li dokončit konfiguraci EIM pro doménu, postupujte takto:

1. V případě nutnosti přidejte definice registru EIM do domény EIM i pro další systémy a aplikace (jiné než systém i5/OS), které mají být členy domény EIM. Tyto definice registrů se vztahují ke skutečným registrům uživatelů, kteří musí být součástí domény. V závislosti na vašich potřebách vztahujících se k implementaci EIM se můžete rozhodnout pro volbu Přidat definice systémových registrů, nebo pro volbu Přidat definice aplikačních registrů.
2. Na základě vašich potřeb vztahujících se k implementaci EIM určete, zda je potřeba:
   - Vytvořit identifikátory EIM pro každého jedinečného uživatele nebo entitu v doméně a pro ně vytvořit přidružení identifikátorů.
   - Vytvořit přidružení zásad za účelem mapování skupiny uživatelů na totožnost jediného cílového uživatele.
   - Vytvořit kombinaci těchto možností.
3. Použijte funkci produktu EIM testování mapování k otestování mapování totožnosti pro vaši konfiguraci EIM.
4. Pokud je jediným uživatelem EIM, kterého jste definovali, rozlišovací jméno administrátora LDAP, pak má váš uživatel EIM vysokou úroveň oprávnění ke všem datům na serveru adresářů. Proto byste měli vzít v úvahu možnost vytvoření jednoho nebo více rozlišovacích jmen jako dodatečných uživatelů, kteří budou mít omezenější kontrolu přístupu k datům EIM. Další informace o vytváření rozlišovacích jmen pro server adresářů uvádí téma Rozlišovací jména pod heslem i5/OS. Počet dodatečných uživatelů EIM, které budete definovat, je závislý na tom, nakolik vaše zásada zabezpečení klade důraz na oddělení povinností a odpovědností v oblasti zabezpečení ochrany dat. Obvykle je možné vytvořit alespoň dva následující typy rozlišovacích jmen (DN):
   - **Uživatel, který má kontrolu přístupu na úrovni administrátora EIM.**

     Toto DN administrátora EIM zajišťuje odpovídající úroveň oprávnění pro administrátora, který je odpovědný za správu domény EIM. Toto DN administrátora EIM je možné použít k připojení k řadiči domény za účelem správy všech aspektů domény EIM prostřednictvím produktu System i Navigator.
   - **Alespoň jeden uživatel, který bude mít všechny níže uvedené kontroly přístupu**:
     - Administrátor identifikátorů.

– Administrátor registrů.
– Operace mapování EIM.

Tento uživatel poskytuje odpovídající úroveň kontroly přístupu vyžadovanou pro uživatele systému, který provádí operace EIM v zastoupení operačního systému.

Poznámka: Chcete-li pro uživatele systému použít toto nové rozlišovací jméno namísto rozlišovacího jména administrátora LDAP, musíte změnit vlastnosti konfigurace EIM pro systém System i. Další informace o změně rozlišovacího jména uživatele systému uvádí téma Správa vlastností konfigurace EIM.

Jestliže jste vytvořili základní konfiguraci služby síťového ověření, možná budete muset provést dodatečné úlohy, zejména v případě, že jste implementovali prostředí jediného přihlášení. Informace o těchto dodatečných krocích získáte, když si prostudujete kompletní postup konfigurace, který je uveden ve scénáři Povolení prostředí jediného přihlášení pro operační systém i5/OS.

Konfigurace zabezpečeného připojení k řadiči domény EIM

Za účelem ochrany přenosu dat EIM a pro vytvoření zabezpečeného připojení k řadiči domény EIM můžete použít SSL (Secure Sockets Layer) nebo TSL (Transport Layer Security Protocol).

Chcete-li nakonfigurovat SSL nebo TLS pro produkt EIM, postupujte takto:

1. Je-li to nutné, použijte produkt DCM (Digital Certificate Manager) k vytvoření certifikátu pro server adresářů.
2. Povolte SSL pro lokální server adresářů, který je hostitelem pro řadič domény EIM.
3. Aktualizujte konfigurační vlastnosti EIM tak, aby systém System i používal zabezpečené připojení SSL. Při aktualizaci konfiguračních vlastností EIM postupujte takto:
   a. V produktu System i Navigator, vyberte systém, ve kterém jste nakonfigurovali EIM, a rozbalte **Síť → EIM (Enterprise Identity Mapping)**.
   b. Klepněte pravým tlačítkem myši na **Konfigurace** a vyberte **Vlastnosti**.
   c. Na stránce **Domény** vyberte **Použít zabezpečené připojení (SSL nebo TLS)** a do pole **Port** zadejte zabezpečený port, na kterém váš server adresářů bude naslouchat, nebo přijměte předvolenou hodnotu 636 a klepněte na **OK**.
4. Aktualizujte vlastnosti domény EIM u každé domény EIM tak, aby produkt EIM používal při správě domény prostřednictvím produktu System i Navigator připojení SSL. Chcete-li aktualizovat vlastnosti domény EIM, postupujte takto:
   a. V produktu System i Navigator, vyberte systém, ve kterém jste nakonfigurovali EIM, a rozbalte **Síť → EIM(Enterprise Identity Mapping) → Správa domén**.
   b. Vyberte doménu EIM, ve které chcete pracovat.
      - V případě, že se tato doména nenachází na seznamu **Správa domén**, prozkoumejte téma Přidání domény EIM do Správy domén.
      - Pokud nejste aktuálně připojeni k doméně EIM, ve které chcete pracovat, prostudujte si téma Připojení k řadiči domény EIM.
   c. Klepněte pravým tlačítkem myši na doménu EIM, k níž jste připojeni, a vyberte **Vlastnosti**.
   d. Na stránce **Domény** vyberte **Použít zabezpečené připojení (SSL nebo TLS)** a do pole **Port** zadejte zabezpečený port, na kterém váš server adresářů bude naslouchat, nebo přijměte předvolenou hodnotu 636 a klepněte na **OK**.

Správa EIM

Poté, co nakonfigurujete produkt EIM (Enterprise Identity Mapping) na systému System i , budete muset postupně provést mnoho administračních úloh souvisejících se správou domény EIM a dat pro doménu.

Chcete-li získat více informací o správě EIM ve vašem podniku, prostudujte si níže uvedené stránky.

Správa domén EIM

Ke správě všech domén EIM můžete použít produkt System i Navigator.

Chcete-li spravovat libovolnou doménu EIM, musí být doména uvedena ve složce **Správa domén** (nebo ji tam musíte přidat) pod složkou **Síť** v produktu System i Navigator. Když při vytváření a konfiguraci domény EIM použijete průvodce konfigurací EIM, bude doména přidána do složky **Správa domén** automaticky, abyste mohli spravovat doménu a informace v doméně.

Ke správě domény EIM, která je umístěna kdekoli v téže síti, můžete použít libovolné připojení systému System i, dokonce i když používaný systém není účasten v doméně.

Pro doménu můžete použít následující úlohy správy:

Přidání domény EIM do složky Správa domén

Chcete-li přidat doménu EIM do složky Správa domén, musíte mít zvláštní oprávnění *SECADM a přidávaná doména musí existovat před přidáním do složky Správa domén.

Chcete-li přidat doménu EIM do složky **Správa domén**, postupujte takto:

1. Rozbalte **Síť > EIM (Enterprise Identity Mapping)**.
2. Klepněte pravým tlačítkem myši na **Správa domén** a vyberte **Přidání domény**.
3. V dialogu **Přidání domény** zadejte požadovanou doménu a informace o připojení. Nebo klepněte na **Procházet** a prohlédněte si seznam domén, které spravuje zadaný řadič domény.

   Poznámka: Pokud klepnete na **Procházet**, zobrazí se dialog **Připojení k řadiči domény EIM**. Chcete-li si prohlédnout seznam domén, musíte se připojit k řadiči domény buď pomocí řízení přístupu administrátora LDAP, nebo řízení přístupu administrátora EIM. Obsah seznamu domén se liší podle vaší kontroly přístupu k EIM. Máte-li kontrolu přístupu administrátora LDAP, můžete si prohlížet seznam všech domén, které spravuje řadič domény. V opačném případě seznam zobrazí pouze ty domény, pro které máte kontrolu přístupu administrátora EIM.
4. V případě, že nevíte, jaké údaje máte zadat pro jednotlivá pole, klepněte na volbu **Nápověda**.
5. Klepnutím na **OK** doménu přidáte.

Připojení k doméně EIM

Dříve než můžete začít pracovat s doménou EIM, musíte se nejdříve připojit k řadiči domény EIM pro danou doménu. K doméně EIM se můžete připojit i v případě, že systém System i není aktuálně konfigurován pro účast v této doméně.

Pokud se chcete připojit k řadiči domény EIM, musí být uživatel, pomocí kterého se připojujete, členem skupiny řízení přístupu EIM. Členství ve skupině kontroly přístupu k EIM určuje, jaké úkoly můžete v doméně provádět a jaká data EIM můžete zobrazovat a měnit.

Chcete-li se připojit k doméně EIM, postupujte takto:

1. Rozbalte **Síť > EIM (Enterprise Identity Mapping) > Správa domén**.
2. Klepněte prvým tlačítkem myši na doménu, ke které se chcete připojit.

   Poznámka: Není-li doména, se kterou chcete pracovat, uvedena v seznamu pod **Správou domén** , musíte přidat EIM doménu do složky správy domén.
3. Klepněte pravým tlačítkem myši na doménu EIM, ke které se chcete připojit, a vyberte **Připojit**.
4. V dialogu **Připojení k řadiči domény EIM** uveďte **Typ uživatele**, zadejte požadované identifikační informace pro uživatele a vyberte volbu hesla pro připojení k řadiči domény.
5. V případě potřeby klepněte na volbu **Nápověda** a určete, jaké informace máte použít v jednotlivých polích dialogu.
6. Klepnutím na **OK** se připojíte k řadiči domény.

Povolení přidružení zásad pro doménu

Přidružení zásad umožňuje různé způsoby vytváření mapování typu mnoho-na-jeden v situaci, kdy neexistuje přidružení mezi totožnostmi uživatele a identifikátorem EIM.

Přidružení zásad můžete použít pro mapování zdrojové sady více totožností uživatele (spíše než jedné totožnosti uživatele) k jedné totožnosti cílového uživatele v daném cílovém registru uživatelů. Dříve než bude možné používat přidružení zásad, musíte se nejdříve ujistit, zda jste povolili v doméně používat přidružení zásad pro operace vyhledávání mapování.

Chcete-li povolit podporu zásady mapování na používání přidružení zásad pro doménu, musíte být připojeni k doméně EIM, ve které si přejete pracovat, a musíte mít řízení přístupu administrátora EIM.

Chcete-li umožnit podporu vyhledávání mapování pro používání přidružení zásad pro doménu, postupujte takto:

1. Rozbalte **Síť > EIM (Enterprise Identity Mapping) > Správa domén**.
2. Klepněte pravým tlačítkem myši na doménu EIM, ve které chcete pracovat, a vyberte volbu **Zásada mapování**.
   - Není-li doména, se kterou chcete pracovat, uvedena v seznamu pod **Správou domén**, musíte přidat EIM doménu do složky správy domén.
   - Pokud nejste aktuálně připojeni k doméně EIM, ve které chcete pracovat, musíte se připojit k řadiči domény EIM. (Volba **Zásada mapování** nebude k dispozici dokud se nepřipojíte k doméně.)
3. Na stránce **Obecné** vyberte **Povolit vyhledávaní mapování pomocí přidružení zásad pro doménu**.
4. Klepněte na **OK**.

Poznámka: Je nutné povolit vyhledávání mapování a používání přidružení zásad pro každou definici cílového registru, pro který jsou přidružení zásad definována. Pokud nepovolíte vyhledávání mapování pro definici cílového registru, tento registr nebude součástí operace vyhledávání mapování EIM. A pokud nezadáte, že tento cílový registr může používat přidružení zásad, pak jakékoliv definované přidružení zásad pro tento registr bude operacemi vyhledávání mapování EIM ignorováno.

Související pojmy

"Podpora a povolení zásad mapování EIM" na stránce 37
Podpora zásad mapování produktu EIM (Enterprise Identity Mapping) vám umožní použít přidružení zásad stejně jako určitá přidružení identifikátorů v doméně EIM. Přidružení zásad můžete používat namísto přidružení identifikátorů nebo v kombinaci s ním.

Testování mapování EIM

Testování mapování EIM vám umožňuje ve vaší konfiguraci provádět operace vyhledávání mapování EIM. Test kontroluje, zda se daná totožnost zdrojového uživatele správně mapuje na odpovídající totožnost cílového uživatele. Provedením takového testu se ujistíte, jestli operace vyhledávání mapování EIM vrátí správnou totožnost cílového uživatele, který odpovídá zadaným informacím.

K tomu, aby bylo možné použít funkce mapování k otestování vaší konfigurace EIM, musíte být připojeni k doméně EIM, ve které si přejete pracovat, a dále musí být vaše řízení přístupu EIM na jedné z níže uvedených úrovní:

- Administrátor EIM.
- Administrátor identifikátorů.
- Administrátor registrů.
- Operace vyhledávání mapování EIM.

Chcete-li využít podpory testování mapování, postupujte takto:

1. Rozbalte **Síť > EIM (Enterprise Identity Mapping) > Správa domén**.
2. Vyberte doménu EIM, ve které chcete pracovat.
   - V případě, že se tato doména nenachází na seznamu **Správa domén**, prozkoumejte téma Přidání domény EIM do Správy domén.

- Pokud nejste aktuálně připojeni k doméně EIM, ve které chcete pracovat, prostudujte si téma Připojení k řadiči domény EIM.

3. Klepněte pravým tlačítkem myši na doménu EIM, ke které jste připojeni, a vyberte **Testovat mapování**.
4. V dialogu **Testovat mapování** zadejte následující informace:
   a. Do pole **Zdrojový registr** zadejte jméno definice registru, jež bude odkazovat na registr uživatelů, který chcete využívat jako zdroj operace vyhledávání mapování.
   b. Do pole **Zdrojový uživatel** zadejte jméno totožnosti uživatele, které chcete využívat jako zdroj pro testování operace vyhledávání mapování.
   c. Do pole **Cílový registr** zadejte jméno definice registru, které odkazuje na registr uživatelů, jenž si přejete využívat jako cíl pro testování operace vyhledávání mapování.
   d. Volitelně: Do pole **Vyhledávací informace** můžete zadat vyhledávací informaci definovanou pro cílového uživatele.
5. Další informace týkající se jednotlivých polí tohoto dialogu naleznete po klepnutí na **Nápověda**.
6. Klepněte na **Test** a následně si prohlédněte zobrazené výsledky operace vyhledávání mapování.

   Poznámka: Pokud operace vyhledávání mapování vrátí nejednoznačné výsledky, zobrazí se dialogové okno Testování mapování - výsledky. Toto okno indikuje chybovou zprávu a uvádí seznam cílových uživatelů, které najde operace vyhledávání.
   a. Chcete-li odstranit problémy s nejednoznačnými výsledky, vyberte cílového uživatele a klepněte na **Vlastnosti**.
   b. Zobrazí se dialogové okno Testování a mapování - Podrobnosti, které indikuje informace o operaci vyhledávání mapování pro určitého cílového uživatele. Klepněte na Nápovědu, chcete-li podrobnější informace o výsledcích operace vyhledávání mapování.
   c. Klepněte na **Zavřít**, chcete-li ukončit dialogové okno **Testování mapování - výsledky** .
7. Pokračujte v testování vaší konfigurace nebo klepněte na **Zavřít** pro ukončení testování.

Související pojmy

“Odstraňování problémů s mapováním EIM” na stránce 117
Existuje množství běžných problémů, které mohou způsobit, že mapování EIM nebude fungovat tak, jak se očekává, anebo vůbec. Níže uvedenou tabulku použijte k tomu, abyste nalezli informace o tom, jaké problémy mohou být příčinou nefunkčnosti mapování EIM, a jejich možná řešení. Jestliže mapování EIM nefunguje, budete možná muset procházet každým řešením v tabulce a zajistit tak nalezení a vyřešení problémů, které způsobují nefunkčnost mapování.

Práce s výsledky testování a řešení problémů:

V průběhu testu bude totožnost cílového uživatele vrácena v případě, že bylo při testu nalezeno přidružení mezi totožností zdrojového uživatele a cílovým registrem uživatelů tak, jak je administrátor zadal. Test také určí typ přidružení, který byl nalezen mezi dvěma totožnostmi uživatele. V případě, že během testu nebude nalezeno žádné přidružení odpovídající zadaným informacím, test bude ukončen vrácením totožnosti uživatele - žádný.

Tento test, jako každá operace vyhledávání mapování EIM, vyhledá a vrátí první odpovídající totožnost cílového uživatele. Vyhledávání probíhá v následujícím pořadí:

1. Specifické přidružení identifikátorů.
2. Přidružení zásad filtru certifikátů.
3. Předvolené přidružení zásad registru.
4. Předvolené přidružení zásad domény.

V některých případech test nevrátí žádnou totožnost cílového uživatele, i když byla pro doménu přidružení nakonfigurována. V tomto případě si ověřte, zda jste do testu zadali správné informace. Pokud jsou zadané informace správné a test stále nevrací žádné výsledky, může být problém způsoben jedním z následujících bodů:

- Na úrovni domény nebyla povolena podpora přidružení zásad. Budete muset povolit přidružení zásad pro doménu.

- Na úrovni jednotlivého registru nebyla povolena podpora přidružení zásad nebo podpora vyhledávání mapování. Budete muset povolit podporu vyhledávání mapování a použití přidružení zásad pro cílový registr.
- Cílové nebo zdrojové přidružení pro identifikátor EIM není správně nakonfigurováno. Například neexistuje zdrojové přidružení pro činitele Kerberos (nebo pro uživatele Windows) nebo toto přidružení není správné. Nebo také může cílové přidružení uvádět nesprávnou totožnost uživatele. Chcete-li ověřit přidružení určitého identifikátoru, zobrazte všechna přidružení identifikátorů EIM.
- Přidružení zásad není správně nakonfigurováno. Chcete-li ověřit zdrojové a cílové informace pro všechna přidružení zásad definovaných v doméně, zobrazte všechna přidružení zásad pro doménu.
- Kvůli rozlišování velkých a malých písmen definice registru neodpovídá totožnostem uživatele. Můžete tedy vymazat a znovu vytvořit registr nebo také můžete vymazat a znovu vytvořit přidružení se správným rozlišováním písmen.

Vrací-li test stále nejednoznačné výsledky, zobrazí se chybová správa. Test bude vracet nejednoznačné výsledky v případě, když bude zadaným kritériím pro daný test odpovídat více než jedna totožnost cílového uživatele. Operace vyhledávání mapování vrací více totožností cílového uživatele, nastane-li jedna nebo více z následujících situací:

- Identifikátor EIM má více jednotlivých cílových přidružení ke stejnému cílovému registru.
- Více než jeden identifikátor EIM má tutéž totožnost uživatele specifikovanou ve zdrojovém přidružení a každý z těchto identifikátorů má cílové přidružení k témuž cílovému registru, ačkoliv totožnost uživatele specifikovaná pro každé cílové přidružení může být odlišná.
- Více než jedno předvolené přidružení zásad domény uvádí stejný cílový registr.
- Více než jedno předvolené přidružení zásad registru uvádí stejný zdrojový registr a stejný cílový registr.
- Více než jedno přidružení zásad filtru certifikátů uvádí stejný zdrojový registr X.509, filtr certifikátů a cílový registr.

Operace vyhledávání mapování, která vrací více než jednu totožnost cílového uživatele, může způsobovat problémy aplikacím podporujícím EIM, včetně aplikací a produktů i5/OS. Proto je důležité, abyste určili příčinu nejednoznačných výsledků a nalezli způsob, jak tuto situaci vyřešit. Na základě příčiny problému pak můžete postupovat podle jednoho z následujících bodů:

- Test vrací více nežádoucích cílových totožností. To znamená, že konfigurace přidružení pro doménu není správná, vinou jedné z níže uvedených příčin:
  - Cílové nebo zdrojové přidružení pro identifikátor EIM není správně nakonfigurováno. Například neexistuje zdrojové přidružení pro činitele Kerberos (nebo pro uživatele Windows) nebo toto přidružení není správné. Nebo také může cílové přidružení uvádět nesprávnou totožnost uživatele. Chcete-li ověřit přidružení určitého identifikátoru, zobrazte všechna přidružení identifikátorů EIM.
  - Přidružení zásad není správně nakonfigurováno. Chcete-li ověřit zdrojové a cílové informace pro všechna přidružení zásad definovaných v doméně, zobrazte všechna přidružení zásad pro doménu.
- Test vrací vícenásobné totožnosti uživatele a tyto výsledky odpovídají způsobu, jakým jste provedli konfiguraci přidružení. Pak budete muset pro každou totožnost cílového uživatele zadat vyhledávací informace. Budete muset definovat jednotlivé vyhledávací informace pro všechny totožnosti cílového uživatele, které mají stejný zdroj (buď identifikátor EIM pro přidružení identifikátorů, nebo zdrojový registr uživatelů pro přidružení zásad). Definováním vyhledávací informace pro každou totožnost cílového uživatele zajistíte, že vyhledávací operace vrátí jedinou totožnost cílového uživatele namísto všech možných totožností uživatele. Další informace uvádí téma Přidání vyhledávací informace k totožnosti cílového uživatele. Tyto vyhledávací informace musíte zadat i pro operaci vyhledávání mapování.

  Poznámka: Tento přístup funguje pouze tehdy, má-li aplikace povoleno používat vyhledávací informace. Avšak základní aplikace i5/OS, jako například System i Access for Windows, nemohou využívat vyhledávací informace k rozlišování mezi více totožnostmi cílových uživatelů, které vrátila vyhledávací operace. Tudíž můžete zvážit nová definování přidružení pro doménu a zajistit tak, že operace vyhledávání mapování bude vracet jedinou totožnost cílového uživatele. Tak také zajistíte, že základní aplikace i5/OS budou moci úspěšně provádět vyhledávací operace a mapovat totožnosti.

Odstranění domény EIM ze složky Správa domén

Doménu EIM, kterou již nechcete spravovat, můžete ze složky **Správa domén** odstranit. Odstranění domény ze složky **Správa domén** však **není** totéž jako výmaz domény - nevymažete data domény z řadiče domény.

K odstranění domény není nutné žádné řízení přístupu EIM.

Chcete-li ze složky **Správa domén** odstranit doménu EIM, kterou již nechcete spravovat, proveďte tyto kroky:

1. Rozbalte **Síť > EIM (Enterprise Identity Mapping)**.
2. Klepněte pravým tlačítkem myši na **Správa domén** a vyberte **Odstranit doménu**.
3. Vyberte doménu EIM, kterou chcete odstranit ze složky **Správa domén**.
4. Klepnutím na **OK** odstraníte doménu.

Související úlohy

"Výmaz domény EIM a všech objektů konfigurace"
Dříve než vymažete doménu EIM, musíte vymazat všechny definice registrů a všechny identifikátory EIM v doméně. Pokud doménu a všechna data v doméně vymazat nechcete, ale zároveň již nechcete doménu spravovat, můžete místo toho doménu odstranit.

Výmaz domény EIM a všech objektů konfigurace

Dříve než vymažete doménu EIM, musíte vymazat všechny definice registrů a všechny identifikátory EIM v doméně. Pokud doménu a všechna data v doméně vymazat nechcete, ale zároveň již nechcete doménu spravovat, můžete místo toho doménu odstranit.

Chcete-li vymazat doménu EIM, musí být vaše řízení přístupu EIM na jedné z těchto úrovní:

- Administrátor LDAP.
- Administrátor EIM.

1. Rozbalte **Síť > EIM (Enterprise Identity Mapping) > Správa domén**.
2. Pokud je to nutné, vymažte všechny definice registrů z domény EIM.
3. Jestliže je to nutné, vymažte všechny identifikátory EIM z domény EIM.
4. Klepněte pravým tlačítkem myši na doménu, kterou chcete vymazat a vyberte volbu **Vymazat**.
5. V dialogu **Potvrzení výmazu** klepněte na **Ano**.

Poznámka: Zobrazí se dialogové okno s průběhem vymazávání, které bude zobrazovat stav vymazávání domény, až do okamžiku, kdy bude proces dokončen.

Související úlohy

"Odstranění domény EIM ze složky Správa domén"
Doménu EIM, kterou již nechcete spravovat, můžete ze složky **Správa domén** odstranit. Odstranění domény ze složky **Správa domén** však **není** totéž jako výmaz domény - nevymažete data domény z řadiče domény.

Správa definic registrů EIM

K tomu, aby se registry uživatelů a totožnosti uživatele, které registry obsahují, účastnily v produktu EIM, musíte pro ně vytvořit definice registrů. Potom můžete pomocí těchto definic registrů EIM spravovat to, jak se registry uživatelů a jejich totožnosti uživatele mohou účastnit v produktu EIM.

V oblasti správy definic registrů můžete provádět následující úlohy:

Související pojmy

"Vytvoření přidružení zásad" na stránce 99
Přidružení zásad umožňuje přímé definování vztahů mezi více totožnostmi uživatele v jednom či více registrech a jednotlivou totožností cílového uživatele v jiném registru.

Související úlohy

"Výmaz přidružení zásad" na stránce 111
Chcete-li vymazat přidružení zásad, musíte být připojeni k doméně EIM, ve které chcete pracovat, a musíte mít řízení přístupu buď jako administrátor EIM nebo jako administrátor registrů.

Přidání definice systémového registru

Chcete-li vytvořit definici systémového registru, musíte být připojeni k doméně EIM, ve které chcete pracovat, a musíte mít řízení přístupu administrátora EIM.

Chcete-li přidat definici systémového registru do domény EIM, postupujte takto.

1. Rozbalte **Síť > EIM (Enterprise Identity Mapping) > Správa domén**.
2. Vyberte doménu EIM, ve které chcete pracovat.
   - Pokud doména EIM, ve které chcete pracovat, není uvedena na seznamu Správa domén, prostudujte si téma "Přidání domény EIM do složky Správa domén" na stránce 84.
   - Pokud nejste aktuálně připojeni k doméně EIM, ve které chcete pracovat, prostudujte si téma "Připojení k doméně EIM" na stránce 84.
3. Rozbalte doménu EIM, k níž jste právě připojeni.
4. Pravým tlačítkem myši klepněte na **Registry uživatelů**, vyberte **Přidat registr** a nakonec vyberte **Systém**.
5. V dialogu **Přidání systémového registru** zadejte informace o definici systémového registru. Musíte zadat tyto informace:
   a. Jméno definice systémového registru.
   b. Typ definice registru.
   c. Popis definice systémového registru.
   d. (Volitelné.) Adresu URL registru uživatelů.
   e. Jedno nebo více jmen alias pro definici systémového registru (je-li to nezbytné).
6. Klepnutím na **OK** uložíte informace a přidáte definici registru do domény EIM.

Přidání definice aplikačního registru

Chcete-li vytvořit definici aplikačního registru, musíte být připojeni k doméně EIM, ve které chcete pracovat, a musíte mít řízení přístupu administrátora EIM.

Chcete-li přidat definici aplikačního registru do domény EIM, postupujte takto:

1. Rozbalte **Síť > EIM (Enterprise Identity Mapping) > Správa domén**.
2. Vyberte doménu EIM, ve které chcete pracovat.
   - Pokud doména EIM, ve které chcete pracovat, není uvedena na seznamu Správa domén, prostudujte si téma "Přidání domény EIM do složky Správa domén" na stránce 84.
   - Pokud nejste aktuálně připojeni k doméně EIM, ve které chcete pracovat, prostudujte si téma "Připojení k doméně EIM" na stránce 84.
3. Rozbalte doménu EIM, k níž jste právě připojeni.
4. Pravým tlačítkem myši klepněte na **Registry uživatelů**, vyberte **Přidat registr** a poté vyberte **Aplikace**.
5. V dialogu **Přidání aplikačního registru** zadejte informace pro definici aplikačního registru. Musíte zadat tyto informace:
   a. Jméno definice aplikačního registru.
   b. Jméno definice systémového registru, jehož podmnožinou je aplikační registr uživatelů, který právě definujete. Definice systémového registru, kterou zadáte, již musí existovat v EIM, jinak proces vytváření definice aplikačního registru selže.
   c. Typ definice registru.
   d. Popis definice aplikačního registru.
   e. Jedno nebo více jmen alias pro definici aplikačního registru (je-li to nezbytné).
6. V případě, že nevíte, jaké údaje máte zadat pro jednotlivá pole, klepněte na volbu **Nápověda**.

7. Klepnutím na **OK** uložíte informace a přidáte definici registru do domény EIM.

Související pojmy

"Definice systémových registrů" na stránce 13
Definice systémového registru je záznam vytvořený v produktu EIM za účelem reprezentace a popisu zvláštního registru uživatelů v rámci pracovní stanice nebo serveru.

Přidání definice skupinového registru

Chcete-li vytvořit definici skupinového registru, musíte být připojeni k doméně EIM, ve které chcete pracovat, a musíte mít řízení přístupu na úrovni administrátora EIM.

Chcete-li přidat definici skupinového registru do domény EIM, postupujte takto:

1. Rozbalte **Síť → EIM (Enterprise Identity Mapping) → Správa domény.**
2. Vyberte doménu EIM, ve které chcete pracovat.
   a. V případě, že se tato doména nenachází ve Správě domén, prohlédněte si téma Přidání domény EIM do Správy domén.
   b. Pokud nejste aktuálně připojeni k doméně EIM, ve které chcete pracovat, prostudujte si téma Připojení k řadiči domény EIM.
3. Rozbalte doménu EIM, k níž jste připojeni.
4. Pravým tlačítkem myši klepněte na **Registry uživatelů**, vyberte **Přidat registr** a pak vyberte **Skupina.**
5. V dialogovém okně Přidání skupinového registru zadejte informace o definici skupinového registru tímto způsobem:
   a. Jméno definice skupinového registru.
   b. Vyberte **Členové skupinového jsou citliví na velikost písmen**, pokud jsou členové definice skupinového registru citliví na velikost písmen.
   c. Popis definice skupinového registru.
   d. Jedno nebo více jmen alias pro definici skupinového registru (je-li to nezbytné).
6. V případě, že nevíte, jaké údaje máte zadat pro jednotlivá pole, klepněte na volbu **Nápověda**.
7. Klepnutím na **OK** uložíte informace a přidáte definici registru do domény EIM.

Přidání jména alias do definice registrů

Může se stát, že vy nebo vývojář aplikací budete chtít specifikovat dodatečné rozlišovací informace pro definici registru. To můžete učinit prostřednictvím vytvoření jména alias pro definici registru. Vy nebo jiné osoby pak můžete používat jméno alias pro definici registru, abyste lépe odlišili jeden registr uživatelů od jiného.

Tato podpora jmen alias umožňuje programátorům psát aplikace, aniž by museli předem znát přesné jméno definice registru EIM, které vybral administrátor, jenž má na starosti distribuci aplikace. Administrátor EIM může v dokumentaci k aplikaci vyhledat jméno alias, které aplikace používá. Pomocí těchto informací může administrátor EIM přiřadit toto jméno alias k definici registru EIM, která reprezentuje aktuální registr uživatelů, jenž má být aplikací používán.

Chcete-li do definice registru přidat jméno alias, musíte být připojeni k doméně EIM, ve které chcete pracovat, a vaše řízení přístupu EIM musí být na jedné z níže uvedených úrovní:

- Administrátor registrů.
- Administrátor vybraných registrů (pro registr, který modifikujete).
- Administrátor EIM.

Chcete-li do definice registru EIM přidat jméno alias, postupujte takto:

1. Rozbalte **Síť > EIM (Enterprise Identity Mapping) > Správa domén**.
2. Vyberte doménu EIM, ve které chcete pracovat.
   - Pokud doména EIM, ve které chcete pracovat, není uvedena na seznamu Správa domén, prostudujte si téma "Přidání domény EIM do složky Správa domén" na stránce 84.

- Pokud nejste aktuálně připojeni k doméně EIM, ve které chcete pracovat, prostudujte si téma “Připojení k doméně EIM” na stránce 84.

3. Rozbalte doménu EIM, k níž jste právě připojeni.
4. Klepněte na **Registry uživatelů**, čímž zobrazíte seznam definic registrů v rámci domény.

   Poznámka: Pokud máte kontrolu přístupu administrátora pro vybrané registry, bude seznam obsahovat pouze ty definice registrů, k nimž jste výslovně oprávněni.
5. Pravým tlačítkem myši klepněte na definici registru, pro kterou chcete přidat jméno alias. Pak vyberte **Vlastnosti**.
6. Vyberte stránku **Aliasy** a zadejte jméno a typ jména alias, které chcete přidat.

   Poznámka: Můžete určit typ jména alias, který není na seznamu typů.
7. V případě, že nevíte, jaké údaje máte zadat pro jednotlivá pole, klepněte na volbu **Nápověda**.
8. Klepněte na **Přidat**.
9. Klepnutím na **OK** uložíte změny, které jste provedli v definici registru.

Definice typu registru soukromého uživatele v EIM

Při vytváření definice registru EIM můžete zadat jeden z předdefinovaných typů registru uživatelů, aby představoval skutečný registr uživatelů, který existuje v systému v rámci podniku.

Ačkoli předdefinované definice typu registru pokrývají většinu registrů uživatelů v operačním systému, budete možná muset vytvořit definici registru, pro kterou EIM nezahrnuje předem definovaný typ registru. Máte dvě možnosti, jak tuto situaci vyřešit. Můžete buď použít stávající definici registru, která odpovídá charakteristice registru uživatelů, nebo můžete definovat soukromý typ registru uživatelů.

Chcete-li definovat typ registru uživatelů, který není v rámci EIM předdefinovaný k rozpoznávání, musíte použít totožnost objektu, neboli OID (object identity), a zadat typ registru ve formě **ObjectIdentifier-normalization**, kde **ObjectIdentifier** je identifikátor objektu ve tvaru dekadických čísel s tečkami, např. 1.2.3.4.5.6.7, a **normalization** je buď hodnota **caseExact**, nebo hodnota **caseIgnore**. Například OID pro operační systém System i je 1.3.18.0.2.33.2-caseIgnore.

Měli byste získat všechny potřebné OID od legitimních registračních autorit, abyste zajistili, že budete vytvářet a používat jedinečné OID. Jedinečné OID vám pomohou vyvarovat se možných konfliktů s OID vytvořenými jinými organizacemi nebo aplikacemi.

Existují dva způsoby, jak získat OID:

- **Registrace objektů pomocí autorit**. Tento způsob je vhodný v případě, když potřebujete malý počet pevných OID pro reprezentaci informace. Tyto OID by mohly představovat zásady certifikátů pro uživatele ve vašem podniku.
- **Získání přiřazení ″arc″ od registrační autority a přiřazení vlastních OID podle potřeby**. Tento způsob, který je přiřazením rozsahu identifikátorů objektu s dekadickými čísly a tečkami, je dobrou volbou v případě, jestliže potřebujete velký počet OID nebo jestliže jsou přiřazení OID závislá na změnách. Přiřazení ″arc″ se skládá z počátečních dekadických čísel s tečkou, na kterých musíte založit **ObjectIdentifier**. Přiřazení arc by mohlo být například 1.2.3.4.5.. OID byste pak mohli vytvořit přidáváním k tomuto základnímu arc. Mohli byste například vytvořit OID ve formě 1.2.3.4.5.x.x.x).

Další informace o registraci OID u registrační autority najdete na Internetu v těchto zdrojích:

- Organizace ANSI (American National Standards Institute) je registrační autoritou ve Spojených státech pro názvy organizací, které spadají pod globální registrační proces zavedený organizacemi ISO (International Standards Organization) a ITU (International Telecommunication Union). Dokument ve formátu Microsoft Word se žádostí o indikátor RID (Registered Application Provider Identifier) je umístěn na webových stránkách ANSI Public Document Library http://public.ansi.org/ansionline/Documents/ . Dokument najdete pomocí výběru **Jiné služby > Registrační programy**. Hodnota ANSI OID arc pro organizace je 2.16.840.1. Organizace ANSI si účtuje poplatek za přiřazení OID arc. Přiřazené OID arc obdržíte od organizace ANSI přibližně za dva týdny. ANSI přiřadí pro vytvoření nového arc OID číslo (NEWNUM), například 2.16.840.1.NEWNUM.

- Ve většině zemí je registr OID udržován asociací pro národní standardy. Stejně jako u ANSI arc se většinou jedná o hodnoty arc přiřazené pod OID 2.16. Je možné, že při hledání registrační autority OID v dané zemi budete muset vyvinout určité úsilí. Adresy národních orgánů ISO můžete najít na webové stránce

  http://www.wssn.net/WSSN/listings/links_national.html . Informace obsahují poštovní adresu a e-mail. V mnoha případech je uvedena také Web stanice.
- Organizace IANA (Internet Assigned Numbers Authority) přiřazuje čísla soukromých podniků, kterými jsou OID, do hodnoty arc 1.3.6.1.4.1. Organizace IANA do dnešního dne přiřadila hodnoty arc více než 7500 společnostem.

  Aplikační stránka je umístěna na adrese http://www.iana.org/cgi-bin/enterprise.pl , pod heslem Private Enterprise Numbers. Vyřízení u organizace IANA obvykle trvá asi jeden týden. OID od organizace IANA je zdarma. Organizace IANA přiřadí číslo (NEWNUM), takže nová hodnota OID arc bude 1.3.6.1.4.1.NEWNUM.
- Federální vláda U.S.A. udržuje registr CSOR (Computer Security Objects Registry). CSOR je registrační autoritou pro hodnoty arc 2.16.840.1.101.3 a v současné době registruje objekty pro jmenovky zabezpečení, šifrovací algoritmy a zásady certifikátů. OID zásad certifikátů jsou definovány pod hodnotou arc 2.16.840.1.101.3.2.1. Registr CSOR poskytuje OID zásad pro agentury federální vlády U.S.A. Další informace o CSOR najdete na adrese

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

  Související pojmy

  “Definice registru EIM” na stránce 11
  Definice registru EIM je záznam v rámci produktu EIM, který můžete vytvořit za účelem reprezentace aktuálního registru uživatelů, jenž se nachází v systému daného podniku. Registr uživatelů funguje jako adresář a obsahuje seznam platných totožností uživatele pro určitý systém nebo aplikaci.

Povolení podpory vyhledávání mapování a použití přidružení zásad pro cílový registr

Podpora zásad mapování EIM (Enterprise Identity Mapping) vám umožňuje používat přidružení zásad jako prostředek k vytvoření mapování typu mnoho-na-jeden tam, kde neexistuje přidružení mezi totožnostmi uživatele a identifikátorem EIM. Přidružení zásad můžete použít pro mapování zdrojové sady více totožností uživatele (spíše než jedné totožnosti uživatele) k jedné totožnosti cílového uživatele v daném cílovém registru uživatelů.

Dříve než však budete moci používat přidružení zásad, se budete muset nejdříve ujistit, zda jste v doméně povolili používání přidružení zásad pro operace vyhledávání mapování. Také musíte dále povolit jedno nebo obě dvě nastavení pro každý registr:

- **Povolit vyhledávání mapování pro registr.** Tuto volbu vyberte, abyste se ujistili, zda bude registr součástí operací vyhledávání mapování EIM, bez ohledu na to, má-li tento registr jakékoliv definované přidružení zásad.
- **Použít přidružení zásad.** Tuto volbu vyberte k tomu, aby daný registr mohl být cílovým registrem přidružení zásad, a ujistěte se, zda je registr součástí operací vyhledávání mapování EIM.

Pokud nepovolíte vyhledávání mapování pro registr, tento registr nebude v žádném případě součástí operací vyhledávání mapování EIM. A pokud nezadáte, že registr může používat přidružení zásad, budou rovněž operace vyhledávání mapování ignorovat jakákoliv přidružení zásad pro tento registr, který by měl být cílem operace.

Chcete-li umožnit, aby vyhledávání mapování používalo přidružení zásad pro cílový registr, musíte být připojeni k doméně, ve které si přejete pracovat, a vaše kontrola přístupu k EIM (viz téma“Kontrola přístupu k EIM” na stránce 38) musí mít jednu z následujících úrovní:

- Administrátor EIM.
- Administrátor registrů.
- Administrátor pro vybrané registry (tedy pro registr, který chcete povolit).

Chcete-li obecně povolit podporu vyhledávání mapování a umožnit použití přidružení zásad specificky pro cílový registr, postupujte takto:

1. Rozbalte **Síť > EIM (Enterprise Identity Mapping) > Správa domén**.
2. Vyberte doménu EIM, ve které chcete pracovat.

- Pokud doména EIM, ve které chcete pracovat, není uvedena na seznamu **Správa domén**, prostudujte si téma "Přidání domény EIM do složky Správa domén" na stránce 84.
- Pokud nejste aktuálně připojeni k doméně EIM, ve které chcete pracovat, prostudujte si téma Připojení k řadiči domény EIM.

3. Chcete-li zobrazit seznam definic registrů pro doménu, vyberte **Registry uživatelů**.

   Poznámka: Pokud máte kontrolu přístupu administrátora pro vybrané registry, bude seznam obsahovat pouze ty definice registrů, k nimž jste výslovně oprávněni.
4. Klepněte pravým tlačítkem myši na definici registru, pro kterou si přejete povolit podporu zásad mapování pro daná přidružení zásad a vyberte **Zásada mapování**
5. Na stránce **Obecné** vyberte **Povolit vyhledávání mapování pro registr**. Vybráním této volby umožníte registru, aby byl součástí operace vyhledávání mapování EIM. Pokud tato volba nebude vybrána, vyhledávací operace nebude moci vrátit data pro registr, bez ohledu na to, je-li tento registr ve vyhledávací operaci registrem zdrojovým nebo cílovým.
6. Vyberte **Použít přidružení zásad**. Vybráním této volby umožníte vyhledávací operaci používat přidružení zásad, jako základ vrácených dat, v případě, že daný registr je cílem vyhledávací operace.
7. Klepnutím na **OK** uložte provedené změny.

Poznámka: Dříve než bude jakýkoliv registr schopen používat přidružení zásad, se musíte také ujistit, že jste také povolili přidružení zásad pro doménu.

Související pojmy

"Podpora a povolení zásad mapování EIM" na stránce 37
Podpora zásad mapování produktu EIM (Enterprise Identity Mapping) vám umožní použít přidružení zásad stejně jako určitá přidružení identifikátorů v doméně EIM. Přidružení zásad můžete používat namísto přidružení identifikátorů nebo v kombinaci s ním.

Výmaz definice registru

Když vymažete definici registru domény EIM (Enterprise Identity Mapping), neovlivníte tím registr uživatelů, na který se definice registru odkazuje. Tento registr uživatelů se však již nebude moci účastnit v doméně EIM.

Při výmazu definice registru musíte zvážit níže uvedené okolnosti:

- Když vymažete definici registru, ztratíte všechna přidružení pro tento registr uživatelů. Pokud znovu definujete registr na doménu, musíte znovu vytvořit potřebná přidružení.
- Když vymažete definici registru X.509, ztratíte také všechny filtry certifikátů definované pro tento registr. Jestliže znovu definujete registr X.509 na doménu, musíte znovu vytvořit všechny potřebné filtry certifikátů.
- Pokud existují definice aplikačních registrů, které specifikují definici systémového registru jako nadřazený registr, nemůžete vymazat definici systémového registru.

Chcete-li vymazat definici registru, musíte být připojeni k doméně EIM, ve které chcete pracovat, a musíte mít řízení přístupu na úrovni administrátora EIM.

Chcete-li vymazat definici registru EIM, postupujte takto:

1. Rozbalte **Síť > EIM (Enterprise Identity Mapping) > Správa domén**.
2. Vyberte doménu EIM, ve které chcete pracovat.
   - Pokud doména EIM, ve které chcete pracovat, není uvedena na seznamu **Správa domén**, prostudujte si téma "Přidání domény EIM do složky Správa domén" na stránce 84.
   - Pokud nejste aktuálně připojeni k doméně EIM, ve které chcete pracovat, prostudujte si téma Připojení k řadiči domény EIM.
3. Rozbalte doménu EIM, k níž jste připojeni.
4. Klepnutím na **Registry uživatelů** zobrazte seznam definic registrů pro doménu.

Poznámka: Pokud máte kontrolu přístupu administrátora pro vybrané registry, bude seznam obsahovat pouze ty definice registrů, k nimž jste výslovně oprávněni.

5. Klepněte pravým tlačítkem myši na registr uživatelů, který chcete vymazat, vyberte volbu **Vymazat**.
6. Klepnutím na **Ano** v dialogu **Potvrzení** vymažte definici registru.

Odstranění jména alias z definice registru

Chcete-li odstranit jméno alias z identifikátoru EIM, musíte být připojeni k doméně EIM, ve které chcete pracovat, a vaše řízení přístupu EIM musí být na úrovni administrátor registrů pro vybrané registry nebo na úrovni administrátor EIM.

Chcete-li odstranit jméno alias z definice registru, postupujte takto:

1. Rozbalte **Síť > EIM (Enterprise Identity Mapping) > Správa domén**.
2. Vyberte doménu EIM, ve které chcete pracovat.
   - Pokud doména EIM, ve které chcete pracovat, není uvedena na seznamu **Správa domén**, prostudujte si téma “Přidání domény EIM do složky Správa domén” na stránce 84.
   - Pokud nejste aktuálně připojeni k doméně EIM, ve které chcete pracovat, prostudujte si téma Připojení k řadiči domény EIM.
3. Rozbalte doménu EIM, k níž jste připojeni.
4. Klepnutím na **Registry uživatelů** zobrazte seznam definic registrů pro doménu.

   Poznámka: Pokud máte kontrolu přístupu administrátora pro vybrané registry, bude seznam obsahovat pouze ty definice registrů, k nimž jste výslovně oprávněni.
5. Klepněte pravým tlačítkem myši na definici registru a vyberte **Vlastnosti**.
6. Vyberte stránku **Alias**.
7. Vyberte jméno alias, které chcete odstranit, a klepněte na **Odstranit**.
8. Klepnutím na **OK** uložte změny.

Přidání člena do definice skupinového registru

Chcete-li přidat člena do definice skupinového registru, musíte být připojeni k doméně EIM, ve které chcete pracovat. Kromě toho musíte mít musíte mít řízení přístupu na úrovni administrátora EIM, administrátora registru a administrátora pro zvolené registry (pro definici skupinového registru, do kterého chcete přidat člena a rovněž pro jednotlivého člena, kterého chcete přidat).

Chcete-li přidat člena do definice skupinového registru, postupujte takto:

1. **Rozbalte síť → EIM (Enterprise Identity Mapping) → Správa domény.**
2. Vyberte doménu EIM, ve které chcete pracovat.
   a. V případě, že se tato doména nenachází ve Správě domén, prohlédněte si téma Přidání domény EIM do Správy domén.
   b. Pokud nejste aktuálně připojeni k doméně EIM, ve které chcete pracovat, prostudujte si téma Připojení k řadiči domény EIM.
3. Rozbalte doménu EIM, k níž jste připojeni.
4. 4. Klepněte na **Registry uživatelů**, čímž zobrazíte seznam definic registrů v rámci domény.
5. 5. Pravým tlačítkem myši klepněte na definici skupinového registru, do které chcete přidat člena, a vyberte **Vlastnosti.**
6. 6. Vyberte stránku **Členové** a klepněte na **Přidat**.
7. 7. V dialogovém okně **Přidat skupinový registr EIM** vyberte jeden nebo více definic registru a klepněte na **OK**. Obsah tohoto seznamu se liší v souvislosti s vaším typem kontroly přístupu k EIM a je vyhrazený pro definice registru se stejnou citlivostí na velká/malá písmena jako ostatní členové skupiny.
8. 8. Klepnutím na **OK** ukončíte práci.

Správa identifikátorů EIM

Tyto informace použijte, chcete-li se dozvědět, jak vytvářet a spravovat identifikátory EIM pro doménu.

Vytváření a používání identifikátorů EIM, které představují uživatele v síti, může být velmi užitečné při sledování, která osoba vlastní totožnost určitého uživatele. Uživatelé v rámci podniku se téměř vždy mění. Někteří odcházejí, jiní přicházejí a další se přesunují mezi oblastmi. Tyto změny přispívají k vyvíjejícímu se problému se sledováním totožností uživatele a hesel pro systémy a aplikace v síti. Kromě toho zaberou úlohy pro správu hesel v podniku značný čas. Pomocí vytvoření identifikátorů EIM a jejich přidružení k totožnostem pro každého uživatele můžete vytvořit proces sledování toho, kdo vlastní určitou totožnost uživatele. Můžete tak také mnohem zjednodušit správu hesel.

Implementace prostředí jediného přihlášení rovněž zjednoduší proces správy totožností uživatelů, především tehdy, když se přemísťují do jiného oddělení nebo oblasti v rámci podniku. Povolení jediného přihlášení může eliminovat potřebu, aby si tito uživatelé pamatovali nová uživatelská jména a hesla pro nové systémy.

Poznámka: Způsob vytváření a použití identifikátorů EIM závisí na potřebách vaší organizace. Chcete-li se získat další informace, prostudujte si téma “Vytvoření plánu pojmenování identifikátoru EIM” na stránce 62.

Můžete spravovat identifikátory EIM pro libovolnou doménu EIM, která je dostupná ve složce **Správa domén**. Při správě identifikátorů EIM v doméně EIM můžete provádět kteroukoliv z níže uvedených úloh:

Související informace

Jediné přihlášení

Vytvoření identifikátoru EIM

Chcete-li vytvořit definici EIM identifikátoru, musíte být připojeni k doméně EIM, ve které chcete pracovat, a musíte mít řízení přístupu jako buď jako administrátor EIM nebo jako administrátor identifikátoru.

Pokud chcete vytvořit identifikátor EIM pro osobu nebo entitu v podniku, postupujte takto:

1. Rozbalte **Síť > EIM (Enterprise Identity Mapping) > Správa domén**.
2. Vyberte doménu EIM, ve které chcete pracovat.
   - Pokud doména EIM, ve které chcete pracovat, není uvedena na seznamu **Správa domén**, prostudujte si téma “Přidání domény EIM do složky Správa domén” na stránce 84.
   - Pokud nejste aktuálně připojeni k doméně EIM, ve které chcete pracovat, prostudujte si téma “Připojení k doméně EIM” na stránce 84.
3. Rozbalte doménu EIM, k níž jste připojeni.
4. Klepněte pravým tlačítkem myši na **Identifikátory** a vyberte **Nový identifikátor**.
5. V dialogu **Nový identifikátor EIM** zadejte níže uvedené informace o identifikátoru EIM:
   a. Jméno identifikátoru.
   b. Zda má systém vygenerovat jedinečné jméno, je-li to nutné.
   c. Popis identifikátoru.
   d. Jeden nebo více jmen alias identifikátoru, je-li to nutné.
6. V případě, že nevíte, jaké údaje máte zadat pro jednotlivá pole, klepněte na volbu **Nápověda**.
7. Jakmile zadáte požadované informace, klepněte na **OK** a vytvořte identifikátor EIM.

Poznámka: Pokud vytváříte velký počet identifikátorů EIM, trvá někdy dlouhou dobu, než se při rozbalování složky **Identifikátory** zobrazí seznam identifikátorů. Chcete-li dosáhnout vyššího výkonu v případech, kdy máte velký počet identifikátorů EIM v doméně, prohlédněte si téma “Přizpůsobení zobrazení identifikátorů EIM” na stránce 97.

Přidání jména alias do identifikátoru EIM

Možná budete chtít vytvořit jméno alias, abyste poskytli další rozlišovací informace pro identifikátor EIM. Aliasy mohou pomoci při vyhledávání určitých identifikátorů EIM, když provádíte operaci vyhledávání EIM. Jména alias mohou být užitečná například v situacích, kdy něčí legální jméno je odlišné od jména, pod kterým je osoba známa.

Jména identifikátorů EIM musí být v rámci domény EIM jedinečná. Aliasy mohou být nápomocny tam, kde by používání jedinečných jmen mohlo být komplikované. Někdy mohou mít v podniku některé osoby stejné jméno, což může být v případě využívání vlastních jmen jako identifikátorů EIM matoucí. Pokud máte například dva uživatele se jménem John J. Johnson, mohli byste vytvořit jméno alias John Joseph Johnson pro jednoho uživatele a jméno alias John Jeffrey Johnson pro druhého uživatele, a usnadnit tak rozlišení totožnosti každého uživatele. Další jména alias by mohla obsahovat zaměstnanecké číslo každého uživatele, číslo oddělení, titul nebo jiné rozlišovací znaky.

Chcete-li přidat jméno alias k identifikátoru EIM, musíte být připojeni k doméně EIM, ve které chcete pracovat, a vaše “Kontrola přístupu k EIM” na stránce 38 musí být na jedné z těchto úrovní:

- Administrátor EIM.
- Administrátor identifikátorů.

Chcete-li přidat jméno alias identifikátoru EIM, postupujte takto.

1. Rozbalte **Síť > EIM (Enterprise Identity Mapping) > Správa domén**.
2. Vyberte doménu EIM, ve které chcete pracovat.
   - Pokud doména EIM, ve které chcete pracovat, není uvedena na seznamu **Správa domén**, prostudujte si téma “Přidání domény EIM do složky Správa domén” na stránce 84.
   - Pokud nejste aktuálně připojeni k doméně EIM, ve které chcete pracovat, prostudujte si téma “Připojení k doméně EIM” na stránce 84.
3. Rozbalte doménu EIM, k níž jste připojeni.
4. Klepnutím na **Identifikátory** zobrazíte v pravém podokně seznam identifikátorů EIM, které jsou v doméně k dispozici.

   Poznámka: Někdy se může stát, že poté, co se pokusíte rozbalit složku **Identifikátory**, může trvat delší dobu, než se seznam identifikátorů zobrazí. Chcete-li dosáhnout vyššího výkonu v případech, kdy máte velký počet identifikátorů EIM v doméně, prohlédněte si téma “Přizpůsobení zobrazení identifikátorů EIM” na stránce 97.
5. Klepněte pravým tlačítkem myši na identifikátor EIM, pro který chcete přidat jméno alias, a vyberte **Vlastnosti**.
6. V poli **Alias** zadejte jméno alias, které chcete přidat tomuto identifikátoru EIM, a klepněte na **Přidat**.
7. Klepnutím na **OK** uložíte změny identifikátoru EIM.

Odstranění jména alias z identifikátoru EIM

Chcete-li odstranit jméno alias z identifikátoru EIM, musíte být připojeni k doméně EIM, ve které chcete pracovat, a vaše řízení přístupu EIM musí být na úrovni administrátor identifikátorů nebo administrátor EIM.

Chcete-li odstranit jméno alias z identifikátoru EIM, postupujte takto:

1. Rozbalte **Síť > EIM (Enterprise Identity Mapping) > Správa domén**.
2. Vyberte doménu EIM, ve které chcete pracovat.
   - Pokud doména EIM, ve které chcete pracovat, není uvedena na seznamu **Správa domén**, prostudujte si téma “Přidání domény EIM do složky Správa domén” na stránce 84.
   - Pokud nejste aktuálně připojeni k doméně EIM, ve které chcete pracovat, prostudujte si téma “Připojení k doméně EIM” na stránce 84.
3. Rozbalte doménu EIM, k níž jste připojeni.
4. Klepnutím na **Identifikátory** zobrazíte v pravém podokně seznam identifikátorů EIM, které jsou v doméně k dispozici.

   Poznámka: Někdy se může stát, že poté, co se pokusíte rozbalit složku **Identifikátory**, může trvat delší dobu, než se seznam identifikátorů zobrazí. Chcete-li dosáhnout vyššího výkonu v případech, kdy máte velký počet identifikátorů EIM v doméně, prohlédněte si téma “Přizpůsobení zobrazení identifikátorů EIM” na stránce 97.
5. Klepněte pravým tlačítkem myši na identifikátor EIM, pro který chcete přidat jméno alias, a vyberte **Vlastnosti**.

6. Vyberte jméno alias, které chcete odstranit, a klepněte na **Odstranit**.
7. Klepnutím na **OK** uložte provedené změny.

Výmaz identifikátoru EIM

Chcete-li vymazat identifikátor EIM, musíte být připojeni k doméně EIM, ve které chcete pracovat, a musíte mít řízení přístupu administrátora EIM.

Pokud chcete vymazat identifikátor EIM, postupujte takto:

1. Rozbalte **Síť > EIM (Enterprise Identity Mapping) > Správa domén**.
2. Vyberte doménu EIM, ve které chcete pracovat.
   - Pokud doména EIM, ve které chcete pracovat, není uvedena na seznamu **Správa domén**, prostudujte si téma "Přidání domény EIM do složky Správa domén" na stránce 84.
   - Pokud nejste aktuálně připojeni k doméně EIM, ve které chcete pracovat, prostudujte si téma Připojení k řadiči domény EIM.
3. Rozbalte doménu EIM, k níž jste právě připojeni.
4. Klepněte na **Identifikátory**.

   Poznámka: Někdy se může stát, že poté, co se pokusíte rozbalit složku **Identifikátory**, může trvat delší dobu, než se seznam identifikátorů zobrazí. Chcete-li dosáhnout vyššího výkonu v případech, kdy máte velký počet identifikátorů EIM v doméně, můžete provést "Přizpůsobení zobrazení identifikátorů EIM".
5. Vyberte identifikátor EIM, který chcete vymazat. Chcete-li vymazat více identifikátorů, tiskněte při výběru identifikátorů EIM klávesu **Ctrl**.
6. Klepněte pravým tlačítkem myši na vybrané identifikátory EIM a vyberte **Vymazat**.
7. V dialogu **Potvrzení výmazu** klepněte na **Ano** a vymažte vybrané identifikátory EIM.

Přizpůsobení zobrazení identifikátorů EIM

Někdy se může stát, že poté, co se pokusíte rozbalit složku Identifikátory, může trvat delší dobu, než se seznam identifikátorů zobrazí. Pokud chcete dosáhnout vyššího výkonu v případech, kdy máte velký počet identifikátorů EIM v doméně, můžete přizpůsobit zobrazení složky Identifikátory.

Chcete-li přizpůsobit zobrazení složky **Identifikátory**, postupujte takto:

1. Rozbalte **Síť —> EIM (Enterprise Identity Mapping) —> Správa domén**.
2. Vyberte doménu EIM, ve které chcete pracovat.
   - Pokud doména EIM, ve které chcete pracovat, není uvedena na seznamu **Správa domén**, prostudujte si téma "Přidání domény EIM do složky Správa domén" na stránce 84.
   - Pokud nejste aktuálně připojeni k doméně EIM, ve které chcete pracovat, prostudujte si téma "Připojení k doméně EIM" na stránce 84.
3. Pravým tlačítkem myši klepněte na složku **Identifikátory** a vyberte volbu **Přizpůsobit zobrazení**.
4. Zadejte kritéria, která se mají použít k zobrazení identifikátorů EIM v doméně. Chcete-li zúžit počet zobrazených identifikátorů EIM, zadejte znaky, které mají být použity pro třídění identifikátorů. Do jména identifikátoru můžete zadat jeden nebo více zástupných znaků (*). Například můžete jako třídicí kritérium zadat *JOHNSON* do pole **Identifikátory**. Výsledky vrátí všechny identifikátory EIM, kde je znakový řetězec JOHNSON definován jako součást jména identifikátoru EIM. Kromě toho vrátí také identifikátory EIM, kde je znakový řetězec JOHNSON definován jako součást jména alias pro identifikátor EIM.
5. Klepnutím na **OK** uložte provedené změny.

Správa přidružení EIM

Produkt EIM vám umožňuje vytvářet a spravovat dva druhy přidružení, které definují přímé nebo nepřímé vztahy mezi totožnostmi uživatele: přidružení identifikátorů a přidružení zásad. Produkt EIM umožňuje vytvářet a spravovat přidružení identifikátorů mezi identifikátory EIM a příslušnými totožnostmi uživatele, což vám umožňuje definovat nepřímé, avšak specifické individuální vztahy mezi totožnostmi uživatele.

Produkt EIM rovněž umožňuje vytvářet přidružení zásad za účelem popsání vztahu mezi více totožnostmi uživatele v rámci jednoho nebo více registrů totožností individuálního uživatele v jiném registru. Přidružení zásad používá podporu zásad mapování EIM k vytvoření mapování typu mnoho-na-jeden mezi totožnostmi uživatele bez identifikátoru EIM. Vzhledem k tomu, že oba typy přidružení definují vztahy mezi totožnostmi uživatele v podniku, představuje správa přidružení významný faktor v oblasti správy EIM.

Správa přidružení v rámci domény je klíčem ke zjednodušení administračních úloh, které jsou nezbytné za účelem sledování informací o tom, kteří uživatelé mají účty v různých systémech v síti. Když implementujete bezpečnou síť s prostředím jediného přihlášení, musíte udržovat přidružení identifikátorů a přidružení zásad aktuální.

Máte možnost provádět níže uvedené úlohy správy přidružení:

Vytváření přidružení EIM

Existují dva různé typy přidružení, které je možné vytvořit. Toto přidružení může být buď cílovým přidružením identifikátoru, nebo přidružením zásady.

Můžete vytvořit přidružení identifikátorů za účelem nepřímého definování vztahu mezi dvěma totožnostmi, které používá jeden jedinec. Přidružení identifikátorů popisuje vztah mezi identifikátorem EIM a totožností uživatele v registru uživatelů. Přidružení identifikátorů umožňuje vytvářet mapování typu jeden-na-jeden mezi identifikátorem EIM a každou z různých totožností, které se vztahují k uživateli, kterého reprezentuje daný identifikátor EIM.

Můžete vytvořit přidružení zásad za účelem přímého definování vztahu mezi více totožnostmi uživatele v jednom nebo více registrech a totožností individuálního cílového uživatele v jiném registru. Přidružení zásad používá podporu zásad mapování EIM k vytvoření mapování typu mnoho-na-jeden mezi totožnostmi uživatele bez identifikátoru EIM. Přidružení zásad umožňují rychle vytvářet velké množství mapování mezi souvisejícími totožnostmi uživatele v různých registrech uživatelů.

To, zda zvolíte vytvoření přidružení identifikátorů, vytvoření přidružení zásad nebo budete společně používat obě metody, záleží čistě na vašich potřebách implementace.

Související pojmy

“Vytvoření plánu mapování totožností” na stránce 59
Kritická část plánovacího procesu zavádění produktu EIM (Enterprise Identity Mapping) vyžaduje, abyste si ve vašem podniku určili způsob použití mapování totožností.

“Vytvoření přidružení zásad” na stránce 99
Přidružení zásad umožňuje přímé definování vztahů mezi více totožnostmi uživatele v jednom či více registrech a jednotlivou totožností cílového uživatele v jiném registru.

Související úlohy

“Vytvoření přidružení identifikátorů EIM”
Přidružení identifikátorů definuje v rámci vašeho podniku pro osoby či entity vztahy mezi identifikátory EIM a totožností uživatele, na které se identifikátory EIM odkazují.

Vytvoření přidružení identifikátorů EIM:

Přidružení identifikátorů definuje v rámci vašeho podniku pro osoby či entity vztahy mezi identifikátory EIM a totožností uživatele, na které se identifikátory EIM odkazují.

Je možné vytvořit až tři typy přidružení identifikátorů: cílové, zdrojové a administrační. Chcete-li předejít možným problémům s přidruženími a problémům se způsobem, jakým tato přidružení mapují jednotlivé totožnosti, prohlédněte si téma “Vytvoření plánu mapování totožností” na stránce 59.

Chcete-li vytvořit přidružení identifikátorů, musíte být připojeni k doméně EIM, ve které si přejete pracovat, a vaše řízení přístupu musí odpovídat danému typu přidružení, které si přejete vytvořit.

Chcete-li vytvořit zdrojové nebo administrační přidružení, musí být vaše kontrola přístupu k EIM na jedné z těchto úrovní:

- Administrátor identifikátorů.
- Administrátor EIM.

Chcete-li vytvořit cílové přidružení, musí být vaše kontrola přístupu k EIM na jedné z následujících úrovní:

- Administrátor registrů.
- Administrátor pro vybrané registry (pro definici registru, která se vztahuje k registru uživatelů obsahujícímu totožnost cílového uživatele).
- Administrátor EIM.

Chcete-li vytvořit přidružení identifikátorů, postupujte takto:

1. Rozbalte **Síť > EIM (Enterprise Identity Mapping) > Správa domén**.
2. Vyberte doménu EIM, ve které chcete pracovat.
   - Pokud doména EIM, ve které chcete pracovat, není uvedena na seznamu **Správa domén**, prostudujte si téma “Přidání domény EIM do složky Správa domén” na stránce 84.
   - Pokud nejste aktuálně připojeni k doméně EIM, ve které chcete pracovat, prostudujte si téma “Připojení k doméně EIM” na stránce 84.
3. Rozbalte doménu EIM, k níž jste právě připojeni.
4. Klepněte na **Identifikátory**, čímž zobrazíte seznam identifikátorů EIM pro doménu.

   Poznámka: Někdy se může stát, že poté, co se pokusíte rozbalit složku **Identifikátory**, může trvat delší dobu, než se seznam identifikátorů zobrazí. Chcete-li dosáhnout vyššího výkonu v případech, kdy máte velký počet identifikátorů EIM v doméně, prohlédněte si téma “Přizpůsobení zobrazení identifikátorů EIM” na stránce 97.
5. Klepněte pravým tlačítkem myši na identifikátor EIM, pro který si přejete vytvořit přidružení, a vyberte volbu **Vlastnosti...**.
6. Zvolte stránku **Přidružení** a klepněte na **Přidat...**.
7. Chcete-li definovat přidružení, zadejte v dialogu **Přidání přidružení** následující informace:
   - Jméno registru, který obsahuje totožnost uživatele, kterou si přejete přidružit k identifikátoru EIM. Zadejte přesné jméno existující definice registru nebo vyberte volbu procházení, pokud chcete jméno definice vybrat.
   - Jméno totožnosti uživatele, které si přejete přiřadit k identifikátoru EIM.
   - Typ přidružení. Můžete zvolit jedno ze tří typů těchto přidružení:
     - Administrační
     - Zdrojové
     - Cílové
8. V případě, že nevíte, jaké údaje máte zadat pro jednotlivá pole, klepněte na volbu **Nápověda**.
9. Volitelné: Pro cílové přidružení klepněte za účelem zobrazení dialogu **Přidat přidružení - rozšířené** na **Rozšířené...**. Zadejte vyhledávací informace pro totožnost cílového uživatele a dále pro návrat k dialogu **Přidat přidružení**, klepněte na **OK**.
10. Jakmile zadáte požadované informace, vytvořte přidružení klepnutím na **OK**.

Související pojmy

“Vytváření přidružení EIM” na stránce 98
Existují dva různé typy přidružení, které je možné vytvořit. Toto přidružení může být buď cílovým přidružením identifikátoru, nebo přidružením zásady.

Vytvoření přidružení zásad:

Přidružení zásad umožňuje přímé definování vztahů mezi více totožnostmi uživatele v jednom či více registrech a jednotlivou totožností cílového uživatele v jiném registru.

Přidružení zásad používá podporu zásad mapování EIM k vytvoření mapování typu mnoho-na-jeden mezi totožnostmi uživatele bez identifikátoru EIM. Protože lze použít přidružení zásad mnoha způsoby, které se překrývají, měli byste důkladně porozumět, jak funguje podpora zásad mapování EIM a vyhledávací operace předtím, než vytvoříte a použijete přidružení zásad. Rovněž kvůli tomu, aby se zabránilo možným problémům souvisejícími s přidruženími a problémům se způsobem, jakým tato přidružení mapují jednotlivé totožnosti, budete muset pro váš podnik před zahájením definice jednotlivých přidružení vyvinout souhrnný plán mapování totožností.

To, zda zvolíte vytvoření přidružení identifikátorů, vytvoření přidružení zásad nebo budete společně používat obě metody, záleží čistě na vašich potřebách implementace.

Rovněž se bude lišit způsob vytváření přidružení zásad v návaznosti na určitý typ daného přidružení zásad. Informace jak postupovat při vytváření přidružení zásad najdete v následujících tématech:

Související pojmy

"Správa definic registrů EIM" na stránce 88
K tomu, aby se registry uživatelů a totožnosti uživatele, které registry obsahují, účastnily v produktu EIM, musíte pro ně vytvořit definice registrů. Potom můžete pomocí těchto definic registrů EIM spravovat to, jak se registry uživatelů a jejich totožnosti uživatele mohou účastnit v produktu EIM.

"Vytváření přidružení EIM" na stránce 98
Existují dva různé typy přidružení, které je možné vytvořit. Toto přidružení může být buď cílovým přidružením identifikátoru, nebo přidružením zásady.

"Podpora a povolení zásad mapování EIM" na stránce 37
Podpora zásad mapování produktu EIM (Enterprise Identity Mapping) vám umožní použít přidružení zásad stejně jako určitá přidružení identifikátorů v doméně EIM. Přidružení zásad můžete používat namísto přidružení identifikátorů nebo v kombinaci s ním.

"Vytvoření plánu mapování totožností" na stránce 59
Kritická část plánovacího procesu zavádění produktu EIM (Enterprise Identity Mapping) vyžaduje, abyste si ve vašem podniku určili způsob použití mapování totožností.

Vytvoření předvoleného přidružení zásad domény:

Chcete-li vytvořit předvolené přidružení zásad domény, musíte být připojeni k doméně EIM, ve které chcete pracovat, a musíte mít EIM řízení přístupu buď jako administrátor EIM nebo jako administrátor registrů.

Přidružení zásad popisuje vztahy mezi více totožnostmi uživatele a jedinou totožností uživatele v cílovém registru uživatelů. Přidružení zásad můžete také použít pro popis vztahů mezi zdrojovou sadou totožností více uživatelů a jedinou totožností cílového uživatele v daném cílovém registru uživatelů. Přidružení zásad používá podporu zásad mapování EIM k vytvoření mapování typu mnoho-na-jeden mezi totožnostmi uživatele bez identifikátoru EIM.

Poznámka: Vzhledem k tomu, že přidružení zásad je možno využívat mnoha navzájem se překrývajícími způsoby, je nutné, abyste se před vytvořením a používáním přidružení zásad důkladně obeznámili s tématem Podpora zásad mapování. Rovněž kvůli tomu, aby se zabránilo možným problémům souvisejícími s přidruženími a problémům se způsobem, jakým tato přidružení mapují jednotlivé totožnosti, budete muset pro váš podnik před zahájením definice jednotlivých přidružení vyvinout souhrnný plán mapování totožností.

V předvoleném přidružení zásad domény jsou všichni uživatelé v doméně zároveň zdrojem pro přidružení zásad a jsou tak mapováni k jednomu cílovému registru a cílovému uživateli. Pro každý registr v doméně můžete definovat předvolené přidružení zásad domény. Pokud se dvě nebo více přidružení zásad domény vztahují ke stejnému cílovému registru, můžete samostatně definovat vyhledávací informaci pro každé jednotlivé přidružení zásad, abyste zajistili, že operace vyhledávání mapování budou moci rozlišovat mezi cílovými registry. Jinak mohou operace vyhledávání mapování vrátit více totožností cílového uživatele. Důsledkem těchto nejednoznačných výsledků pro aplikace spoléhající na EIM by mohlo být, že tyto aplikace nebudou schopny určit přesnou cílovou totožnost.

Chcete-li vytvořit předvolené přidružení zásad domény, postupujte takto:

1. Rozbalte **Síť > EIM (Enterprise Identity Mapping) > Správa domén**.

2. Klepněte pravým tlačítkem myši na doménu EIM, ve které chcete pracovat, a vyberte volbu **Zásada mapování**
   - Pokud doména EIM, ve které chcete pracovat, není uvedena na seznamu **Správa domén**, prostudujte si téma “Přidání domény EIM do složky Správa domén” na stránce 84.
   - Pokud nejste aktuálně připojeni k doméně EIM, ve které chcete pracovat, prostudujte si téma Připojení k řadiči domény EIM.
3. Na stránce Obecné vyberte **Povolit vyhledávání mapování pomocí přidružení zásad pro doménu**.
4. Vyberte stránku **Domény** a klepněte na **Přidat**.
5. V dialogu **Přidaní předvoleného přidružení zásad domény** zadejte následující požadované informace:
   - Jméno definice registru pro **Cílový registr** pro přidružení zásad.
   - Jméno totožnosti uživatele pro **Cílového uživatele** pro přidružení zásad.
6. Další informace týkající se dokončení práce s tímto dialogem a také s následujícím dialogem uvádí **Nápověda**.
7. Volitelné: Chcete-li zobrazit dialog **Přidat přidružení - rozšířené**, klepněte na **Rozšířené**. Zadejte **Vyhledávací informaci** pro přidružení zásad a dále pro návrat k dialogu **Přidání předvoleného přidružení zásad domény** klepněte na **OK**.

   Poznámka: Pokud se dvě nebo více předvolená přidružení zásad domény vztahují ke stejnému cílovému registru, bude nutné samostatně definovat vyhledávací informaci pro všechny totožnosti cílového uživatele v těchto přidruženích zásad. Definováním vyhledávací informace pro každou totožnost cílového uživatele se v tomto případě ujistíte, že operace vyhledávání mapování budou moci rozlišovat mezi jednotlivými totožnostmi. Jinak mohou operace vyhledávání mapování vrátit více totožností cílového uživatele. Důsledkem těchto nejednoznačných výsledků pro aplikace spoléhající na EIM by mohlo být, že tyto aplikace nebudou schopny určit přesnou cílovou totožnost.
8. Chcete-li vytvořit nové přidružení zásad a vrátit se na stránku **Domény**, klepněte na **OK**. Nové přidružení zásad se nyní zobrazí v tabulce **Předvolené přidružení zásad domény**.
9. Ověřte si, zda je toto nové přidružení zásad povoleno pro cílový registr.
10. Chcete-li uložit změny a opustit dialog **Zásada mapování**, klepněte na **OK**.

Poznámka: Ověřte si, zda jsou podpora zásad mapování a používání přidružení zásad pro cílový registr uživatelů správně aktivovány. Pokud tomu tak není, přidružení zásad nebude fungovat.

Vytvoření předvoleného přidružení zásad registru:

Chcete-li vytvořit předvolené přidružení zásad registru, musíte být připojeni k doméně EIM, ve které chcete pracovat, a musíte mít řízení přístupu buď jako administrátor EIM nebo jako administrátor registrů.

Přidružení zásad popisuje vztahy mezi více totožnostmi uživatele a jedinou totožností uživatele v cílovém registru uživatelů. Přidružení zásad můžete také použít pro popis vztahů mezi zdrojovou sadou totožností více uživatelů a jedinou totožností cílového uživatele v daném cílovém registru uživatelů. Přidružení zásad používá podporu zásad mapování EIM k vytvoření mapování typu mnoho-na-jeden mezi totožnostmi uživatele bez identifikátoru EIM.

Poznámka: Vzhledem k tomu, že přidružení zásad je možno využívat mnoha navzájem se překrývajícími způsoby, je nutné, abyste se před vytvořením a používáním přidružení zásad důkladně obeznámili s tématem Podpora zásad mapování. Rovněž kvůli tomu, aby se zabránilo možným problémům souvisejícími s přidruženími a problémům se způsobem, jakým tato přidružení mapují jednotlivé totožnosti, budete muset pro váš podnik před zahájením definice jednotlivých přidružení vyvinout souhrnný plán mapování totožností.

V předvoleném přidružení zásad registru jsou všichni uživatelé jednoho registru zdrojem přidružení zásad a mapují se na jediný cílový registr a cílového uživatele. Když aktivujete předvolené přidružení zásad registru pro cílový registr, přidružení zásad se ujistí, zda mohou být veškeré totožnosti zdrojového uživatele mapovány na jeden určitý cílový registr a na jednoho určitého cílového uživatele.

Chcete-li vytvořit předvolené přidružení zásad registru, postupujte takto:

1. Rozbalte **Síť > EIM (Enterprise Identity Mapping) > Správa domén**.

2. Vyberte doménu EIM, ve které chcete pracovat.
   - Pokud doména EIM, ve které chcete pracovat, není uvedena na seznamu **Správa domén**, prostudujte si téma "Přidání domény EIM do složky Správa domén" na stránce 84.
   - Pokud nejste aktuálně připojeni k doméně EIM, ve které chcete pracovat, prostudujte si téma Připojení k řadiči domény EIM.
3. Na stránce Obecné vyberte **Povolit vyhledávání mapování pomocí přidružení zásad pro doménu**.
4. Na stránce Obecné vyberte **Povolit vyhledávání mapování pomocí přidružení zásad pro doménu**.
5. V dialogu **Přidání předvoleného přidružení zásad registru** zadejte následující požadované informace:
   - Jméno definice registru pro **Zdrojový registr** pro přidružení zásad.
   - Jméno definice registru pro **Cílový registr** pro přidružení zásad.
   - Jméno totožnosti uživatele pro **Cílového uživatele** pro přidružení zásad.
6. Další informace týkající se dokončení práce s tímto dialogem a také s následujícím dialogem uvádí **Nápověda**.
7. Volitelné: Chcete-li zobrazit dialog **Přidat přidružení - rozšířené**, klepněte na **Rozšířené**. Zadejte **Vyhledávací informaci** pro přidružení zásad a dále pro návrat k dialogu **Přidání předvoleného přidružení zásad registru** klepněte na **OK**. Pokud se dvě nebo více přidružení zásad se stejnými zdrojovými registry odkazují na stejný cílový registr, bude nutné samostatně definovat vyhledávací informace pro všechny totožnosti cílového uživatele v těchto přidruženích zásad. Definováním vyhledávací informace pro každou totožnost cílového uživatele se v tomto případě ujistíte, že operace vyhledávání mapování budou moci rozlišovat mezi jednotlivými totožnostmi. Jinak mohou operace vyhledávání mapování vrátit více totožností cílového uživatele. Důsledkem těchto nejednoznačných výsledků pro aplikace spoléhající na EIM by mohlo být, že tyto aplikace nebudou schopny určit přesnou cílovou totožnost.
8. Chcete-li vytvořit nové přidružení zásad a vrátit se na stránku **Registry**, klepněte na **OK**. Nové předvolené přidružení zásad registru se nyní zobrazí v tabulce **Předvolené přidružení zásad**.
9. Ověřte si, zda je toto nové přidružení zásad povoleno pro cílový registr.
10. Chcete-li uložit změny a opustit dialog **Zásada mapování**, klepněte na **OK**.

Poznámka: Ověřte si, zda jsou podpora zásad mapování a používání přidružení zásad pro cílový registr uživatelů správně aktivovány. Pokud tomu tak není, přidružení zásad nebude fungovat.

Vytvoření přidružení zásad filtru certifikátů:

Chcete-li vytvořit přidružení zásad filtru certifikátů, musíte být připojeni k doméně EIM, ve které chcete pracovat, a musíte mít řízení přístupu buď jako administrátor EIM nebo jako administrátor registrů.

Přidružení zásad popisuje vztahy mezi zdrojovou sadou totožností více uživatelů a jedinou totožností cílového uživatele v daném cílovém registru uživatelů. Přidružení zásad používá podporu zásad mapování EIM k vytvoření mapování typu mnoho-na-jeden mezi totožnostmi uživatele bez identifikátoru EIM.

Poznámka: Vzhledem k tomu, že přidružení zásad je možno využívat mnoha navzájem se překrývajícími způsoby, je nutné, abyste se před vytvořením a používáním přidružení zásad důkladně obeznámili s tématem Podpora zásad mapování. Rovněž kvůli tomu, aby se zabránilo možným problémům souvisejícími s přidruženími a problémům se způsobem, jakým tato přidružení mapují jednotlivé totožnosti, budete muset pro váš podnik před zahájením definice jednotlivých přidružení vyvinout souhrnný plán mapování totožností.

V přidružení zásad filtru certifikátů uvedete sadu certifikátů v jediném registru X.509 jako zdroj přidružení zásad. Tyto certifikáty se mapují na jediný cílový registr a cílového uživatele, které zadáte. Na rozdíl od předvoleného přidružení zásad registru, kde jsou všichni uživatele v jediném registru také zdrojem přidružení zásad, rozsah přidružení zásad filtru certifikátů je mnohem flexibilnější. Jako zdroj v registru můžete uvést podmnožinu certifikátů. Právě filtr certifikátů, který zadáte pro přidružení zásad bude určovat jeho rozsah.

Poznámka: Předvolené přidružení zásad vytvořte a použijte v případě, že chcete mapovat všechny certifikáty v registru uživatelů X.509 na jedinou totožnost cílového uživatele.

Filtr certifikátů kontroluje, jak přidružení zásad filtru certifikátů mapuje jednu zdrojovou sadu totožností uživatele, v tomto případě digitálního certifikátu, k určité totožnosti cílového uživatele. A proto tedy filtr certifikátů, který chcete používat, musí existovat dříve, než budete moci vytvořit přidružení zásad filtru certifikátů.

Předtím tedy, než vytvoříte přidružení zásad filtru certifikátů, budete nejdříve muset jako základ přidružení zásad vytvořit filtr certifikátů.

Chcete-li vytvořit přidružení zásad filtru certifikátů postupujte takto:

1. Rozbalte **Síť > EIM (Enterprise Identity Mapping) > Správa domén**.
2. Klepněte pravým tlačítkem myši na doménu EIM, ve které chcete pracovat, a vyberte volbu **Zásada mapování**
   - Pokud doména EIM, ve které chcete pracovat, není uvedena na seznamu **Správa domén**, prostudujte si téma “Přidání domény EIM do složky Správa domén” na stránce 84.
   - Pokud nejste aktuálně připojeni k doméně EIM, ve které chcete pracovat, prostudujte si téma Připojení k řadiči domény EIM.
3. Na stránce Obecné vyberte **Povolit vyhledávání mapování pomocí přidružení zásad pro doménu**.
4. Vyberte stránku **Filtr certifikátů**. Pokud chcete zobrazit dialog **Přidat přidružení zásad filtru certifikátů**, klepněte na **Přidat**.
5. Další informace týkající se dokončení práce s tímto dialogem a také s následujícím dialogem uvádí **Nápověda**.
6. Chcete-li definovat přidružení zásad, zadejte následující informace:
   a. Chcete-li používat **Zdrojový registr X.509** pro přidružení zásad, zadejte jméno definice registru uživatelů X.509. Chcete-li vybrat jméno ze seznamu definic registru pro doménu, klepněte na **Procházet**.
   b. Chcete-li zobrazit dialog **Výběr filtru certifikátů**, klepněte na **Vybrat** a vyberte tak existující filtr certifikátů jako základ pro nové přidružení zásad filtru certifikátů.

      Poznámka: Rozhodně **musíte** použít existující filtr certifikátů. Pokud se filtr certifikátů, který chcete použít, nenachází na seznamu, klepněte na **Přidat** pro vytvoření nového filtru certifikátů.
   c. Zadejte jméno definice registru pro **Cílový registr** nebo pro výběr definice ze seznamu existujících definic registru pro doménu klepněte na **Procházet**.
   d. Zadejte jméno **Cílového uživatele**, na nějž budou mapovány veškeré certifikáty ve **Zdrojovém registru X.509**, který odpovídá filtru certifikátů. Chcete-li vybrat uživatele ze seznamu uživatelů, kteří jsou doméně známi, klepněte na **Procházet**.
   e. Volitelné: Chcete-li zobrazit dialog **Přidat přidružení - rozšířené**, klepněte na **Rozšířené**. Pro totožnost cílového uživatele zadejte **Vyhledávací informace**. Chcete-li se vrátit na dialog **Přidat přidružení zásad filtru certifikátů**, klepněte na **OK**.

      Poznámka: Pokud se dvě nebo více přidružení zásad se stejným zdrojovým registrem X.509 a stejnými kritérii filtru certifikátů vztahují ke stejnému cílovému registru, budete muset pro totožnosti cílového uživatele v každé z těchto přidružení zásad definovat vyhledávací informace. Definováním vyhledávací informace pro každou totožnost cílového uživatele se v tomto případě ujistíte, že operace vyhledávání mapování budou moci rozlišovat mezi jednotlivými totožnostmi. Jinak mohou operace vyhledávání mapování vrátit více totožností cílového uživatele. Důsledkem těchto nejednoznačných výsledků pro aplikace spoléhající na EIM by mohlo být, že tyto aplikace nebudou schopny určit přesnou cílovou totožnost.
7. Chcete-li vytvořit přidružení zásad filtru certifikátů a vrátit se na stránku **Filtr certifikátů**, klepněte na **OK**. Nové přidružení zásad se zobrazí na seznamu.
8. Ověřte si, zda je toto nové přidružení zásad povoleno pro cílový registr.
9. Chcete-li uložit změny a opustit dialog **Zásada mapování**, klepněte na **OK**.

Poznámka: Ověřte si, zda jsou podpora zásad mapování a používání přidružení zásad pro cílový registr uživatelů správně aktivovány. Pokud tomu tak není, přidružení zásad nebude fungovat.

Vytvoření filtru certifikátů:

Filtr certifikátů definuje sadu podobných atributů certifikátu s rozlišujícím názvem pro skupinu uživatelských certifikátů ve zdrojovém registru uživatelů X.509. Dále můžete také využít filtr certifikátů jako základ pro přidružení zásad filtru certifikátů.

Filtr certifikátů v přidružení zásad určuje, které certifikáty v uvedeném zdrojovém registru X.509 se mapují na určitého cílového uživatele. Certifikáty, jejichž informace o DN subjektu a DN vyhovují kritériím filtru, se mapují na zadaného cílového uživatele během vyhledávacích operací mapování EIM (Enterprise Identity Mapping).

Chcete-li vytvořit filtry certifikátů, musíte být připojeni k doméně EIM, ve které si přejete pracovat, a dále musí být vaše “Kontrola přístupu k EIM” na stránce 38 na jedné z následujících úrovní:

- Administrátor EIM.
- Administrátor registrů.
- Administrátor pro vybrané registry (pro definici registru, jež se vztahuje k registru uživatelů X.509, pro který chcete vytvořit filtr certifikátů).

Filtr certifikátů založený na určitém rozlišovacím jméně (DN) vytvoříte z digitálního certifikátu. Údaje o DN, které zadáváte, mohou být buď rozlišovací jméno subjektu, které označuje majitele certifikátu, nebo rozlišovací jméno vydávajícího, které označuje certifikační autoritu. Toto DN pro filtr certifikátů můžete také zadat buď jako celé DN, nebo částečné DN.

Když přidáte filtr certifikátů do přidružení zásad filtru certifikátů, filtr certifikátů určí, které z certifikátů v registru X.509 budou mapovány na totožnost cílového uživatele specifikovanou prostřednictvím přidružení zásad. V případě, kdy je digitální certifikát totožností zdrojového uživatele v operaci vyhledávání mapování EIM (poté, co vyhledávací aplikace použije rozhraní API eimFormatUserIdentity() EIM za účelem naformátování jména totožnosti uživatele), a v případě, kdy je použito přidružení zásad filtru certifikátů, porovná EIM údaje DN v certifikátu s údaji celého DN, nebo částečného DN zadaných ve filtru. Pokud údaje DN v certifikátu odpovídají filtru, EIM vrátí totožnost cílového uživatele, který byl zadán přidružením zásad filtru certifikátů.

Když vytvoříte filtr certifikátů, můžete zadat požadované informace o rozlišovacím jméně jedním ze tří možných způsobu:

- Můžete zadat plné, nebo částečné DN certifikátu pro **DN subjektu**, pro **DN vydávajícího** a nebo pro oba zároveň.
- Je možné zkopírovat informace z daného certifikátu do vaší schránky a použít je tak k vygenerování seznamu kandidátů na filtr certifikátů, který bude založen na informaci o rozlišovacím jméně v certifikátu. Pak se můžete rozhodnout, která jména DN budou využívána pro filtr certifikátů.

  Poznámka: Pokud si přejete vygenerovat za účelem vytvoření filtru certifikátů požadované informace o rozlišovacím jméně, je nutné předtím nejdříve zkopírovat informace o certifikátu do vaší schránky. Dále je nutné, aby certifikát byl v kódovaném formátu base64. Podrobnější informace o metodách získání certifikátu ve správném formátu uvádí téma Filtr certifikátů.
- Z digitálního certifikátu, pro který existuje zdrojové přidružení s identifikátorem EIM, můžete vygenerovat seznam kandidátů na filtr certifikátů na základě informací o rozlišovacím jméně. Pak se můžete rozhodnout, která jména DN budou využívána pro filtr certifikátů.

Chcete-li vytvořený filtr certifikátů používat jako základ pro přidružení zásad, postupujte takto:

1. Rozbalte **Síť > EIM (Enterprise Identity Mapping) > Správa domén**.
2. Klepněte pravým tlačítkem myši na doménu EIM, ve které chcete pracovat, a vyberte volbu **Zásada mapování**
   - Pokud doména EIM, ve které chcete pracovat, není uvedena na seznamu **Správa domén**, prostudujte si téma “Přidání domény EIM do složky Správa domén” na stránce 84.
   - Pokud nejste aktuálně připojeni k doméně EIM, ve které chcete pracovat, prostudujte si téma Připojení k řadiči domény EIM.
3. Vyberte stránku **Filtr certifikátů** a pro zobrazení dialogu **Filtry certifikátů** klepněte na **Filtry certifikátů**.

Poznámka: Pokud klepnete na **Filtry certifikátů** bez toho, aniž byste vybrali přidružení zásad, zobrazí se dialog **Procházet registry EIM**. Tento dialog vám umožní v doméně, pro kterou si přejete prohlížet filtry certifikátů, vybrat registr X.509 ze seznamu definic X.509. Obsah tohoto seznamu se liší v souvislosti s vaším typem kontroly přístupu k EIM.

4. Klepněte na **Přidat**, chcete-li zobrazit dialog **Přidat filtr certifikátů**.
5. V dialogu **Přidat filtr certifikátů** vyberte, zda chcete přidat jeden filtr certifikátů nebo zda chcete vygenerovat filtr certifikátů na základě daného digitálního certifikátu. Další informace týkající se dokončení práce s tímto dialogem a také s následujícím dialogem uvádí **Nápověda**.
   a. Pokud vyberete volbu **Přidat jeden filtr certifikátů**, můžete se rozhodnout pro úplné nebo částečné informace o **DN subjektu**, nebo o úplné či částečné informace o **DN vydávajícího** (nebo obojí). Chcete-li vytvořit filtr certifikátů a vrátit se do dialogu **Filtr certifikátů**, klepněte na **OK**. Filtr se nyní objeví v seznamu.
   b. Pokud vyberete volbu **Generovat filtr certifikátů z digitálního certifikátu**, můžete klepnutím na **OK** zobrazit dialog **Generovat filtry certifikátů**.
      1) Do pole **Informace o certifikátu** vložte kódovanou verzi informace o certifikátu base64, kterou jste předtím zkopírovali do vaší schránky.
      2) Chcete-li vygenerovat seznam potencionálních filtrů certifikátů na bázi **DN subjektu** pro certifikát a **DN vydávajícího**, klepněte na **OK**.
      3) Z dialogu **Procházet filtry certifikátů** vyberte jeden nebo více těchto filtrů certifikátů. Chcete-li se vrátit na dialog **Vybrat filtry certifikátů**, kde budou nyní vybrané filtry certifikátů zobrazeny, klepněte na **OK**.
   c. Pokud vyberete volbu **Generovat filtr certifikátů ze zdrojového přidružení pro uživatele X.509**, můžete klepnutím na **OK** zobrazit dialog **Generovat filtry certifikátů**. Tento dialog zobrazí totožnost uživatele X.509, jenž má v doméně zdrojové přidružení s identifikátorem EIM.
      1) Vyberte totožnost uživatele X.509, jehož digitální certifikát si přejete používat pro vygenerování jednoho nebo více kandidátů filtru certifikátů a klepněte na **OK**.
      2) Chcete-li vygenerovat seznam potencionálních filtrů certifikátů na bázi **DN subjektu** pro certifikát a **DN vydávajícího**, klepněte na **OK**.
      3) Z dialogu **Procházet litry certifikátů** vyberte jeden nebo více těchto potencionálních filtrů certifikátů. Chcete-li se vrátit na dialog **Vybrat filtry certifikátů**, kde budou nyní vybrané filtry certifikátů zobrazeny, klepněte na **OK**.

Nyní můžete použít nový filtr certifikátů jako základ pro Vytvoření přidružení zásad filtru certifikátů.

Přidání vyhledávací informace k totožnosti cílového uživatele

Vyhledávací informace jsou volitelná jedinečná identifikační data pro totožnost cílového uživatele definovaného v přidružení. Toto přidružení může být buď cílovým přidružením identifikátoru, nebo přidružením zásady.

Vyhledávací informace jsou nezbytné pouze v případě, kdy operace vyhledávání mapování může vrátit více než jednu totožnost cílového uživatele. V takové situaci mohou vzniknout problémy pro aplikace podporující EIM, včetně aplikací a produktů operačního systému i5/OS, které nejsou určeny ke zpracování takového množství výsledků.

V případě potřeby můžete přidat jedinečné vyhledávací informace po každou totožnost cílového uživatele za účelem poskytnutí podrobnějších identifikačních informací a dalšího popsání totožnosti každého cílového uživatele. Jestliže definujete vyhledávací informace pro totožnost cílového uživatele, musí být tyto vyhledávací informace poskytnuty operaci vyhledávání mapování, aby bylo zajištěno, že operace vrátí jedinečnou totožnost cílového uživatele. Jinak aplikace, které se spoléhají na EIM, nemusí být schopny určit přesnou totožnost cílového uživatele, kterou mají použít.

Poznámka: Pokud chcete, aby vyhledávací operace EIM byla schopna vrátit více než jednu totožnost cílového uživatele, měli byste za účelem vyřešení této situace opravit konfiguraci přidružení EIM namísto použití vyhledávacích informací. Další informace naleznete v tématu “Odstraňování problémů s mapováním EIM” na stránce 117.

Způsob přidání vyhledávacích informací za účelem dalšího definování totožnosti cílového uživatele se liší v závislosti na tom, zda byla totožnost cílového uživatele definována jako přidružení identifikátorů nebo jako cílové přidružení.

Bez ohledu na metodu, kterou použijete k přidání vyhledávacích informací, budou informace, které zadáte, zaměřeny na totožnost cílového uživatele, nikoli na přidružení identifikátorů nebo na přidružení zásad, v němž se daná totožnost uživatele nachází.

Přidání vyhledávacích informací do totožnosti cílového uživatele v přidružení identifikátorů:

Chcete-li přidat vyhledávací informace do totožnosti cílového uživatele v některém přidružení identifikátorů, musíte být připojeni k doméně EIM, ve které chcete pracovat, a musíte mít oprávnění pro "Kontrola přístupu k EIM" na stránce 38 na jedné z níže uvedených úrovní:

- Administrátor registrů.
- Administrátor pro vybrané registry (pro definici registru, která se vztahuje k registru uživatelů obsahujícímu totožnost cílového uživatele).
- Administrátor EIM.

Chcete-li přidat vyhledávací informace do totožnosti cílového uživatele v některém přidružení identifikátorů, postupujte takto:

1. Rozbalte **Síť > EIM (Enterprise Identity Mapping) > Správa domén**.
2. Vyberte doménu EIM, ve které chcete pracovat.
   - Pokud doména EIM, ve které chcete pracovat, není uvedena na seznamu **Správa domén**, prostudujte si téma "Přidání domény EIM do složky Správa domén" na stránce 84.
   - Pokud nejste aktuálně připojeni k doméně EIM, ve které chcete pracovat, prostudujte si téma Připojení k řadiči domény EIM.
3. Rozbalte doménu EIM, k níž jste připojeni.
4. Klepněte na **Identifikátory**, čímž zobrazíte seznam identifikátorů EIM pro doménu.

   Poznámka: Někdy se může stát, že poté, co se pokusíte rozbalit složku **Identifikátory**, může trvat delší dobu, než se seznam identifikátorů zobrazí. Chcete-li dosáhnout vyššího výkonu v případech, kdy máte velký počet identifikátorů EIM v doméně, můžete přizpůsobit složku **Identifikátory** tím, že omezíte vyhledávací hodnotu použitou pro zobrazování identifikátorů. Pravým tlačítkem myši klepněte na **Identifikátory**, vyberte volbu **Přizpůsobit toto zobrazení > Zahrnout**a zadejte kritéria pro zobrazení, která mají být použita ke generování seznamu identifikátorů EIM, které mají být zahrnuty do seznamu.
5. Pravým tlačítkem myši klepněte na identifikátor EIM a vyberte volbu **Vlastnosti**.
6. Vyberte stránku **Přidružení** , vyberte cílové přidružení, do kterého chcete přidat vyhledávací informace, a klepněte na **Podrobnosti**. V případě, že nevíte, jaké údaje máte zadat pro jednotlivá pole, klepněte na volbu **Nápověda**.
7. V dialogu **Přidružení - podrobnosti** zadejte **vyhledávací informace** , které chcete použít k další identifikaci totožnosti cílového uživatele v tomto přidružení. Pak klepněte na **Přidat**.
8. Zopakujte tento krok pro každý záznam vyhledávacích informací, který chcete přidat do přidružení.
9. Klepnutím na **OK** uložte provedené změny a vraťte se do dialogu **Přidružení - podrobnosti**.
10. Klepnutím na **OK** ukončíte práci.

Přidání vyhledávacích informací do totožnosti cílového uživatele v přidružení zásad:

Chcete-li přidat vyhledávací informace do totožnosti cílového uživatele v některém přidružení zásad, musíte být připojeni k doméně EIM, ve které chcete pracovat, a musíte mít oprávnění pro "Kontrola přístupu k EIM" na stránce 38 na jedné z níže uvedených úrovní:

- Administrátor registrů.
- Administrátor pro vybrané registry (pro definici registru, který se vztahuje k registru uživatelů obsahujícímu totožnost cílového uživatele).
- Administrátor EIM.

Chcete-li přidat vyhledávací informace do totožnosti cílového uživatele v přidružení zásad, postupujte takto:

1. Rozbalte **Síť > EIM (Enterprise Identity Mapping) > Správa domén**.
2. Vyberte doménu EIM, ve které chcete pracovat.
   - Pokud doména EIM, ve které chcete pracovat, není uvedena na seznamu **Správa domén**, prostudujte si téma "Přidání domény EIM do složky Správa domén" na stránce 84.
   - Pokud nejste aktuálně připojeni k doméně EIM, ve které chcete pracovat, prostudujte si téma Připojení k řadiči domény EIM.
3. V dialogu **Zásada mapování** použijte stránky k zobrazení přidružení zásad pro danou doménu.
4. Vyhledejte a vyberte přidružení zásad pro cílový registr, který obsahuje totožnost cílového uživatele, pro něhož chcete přidat vyhledávací informace.
5. Klepnutím na **Podrobnosti** zobrazte příslušný dialog **Přidružení zásad - podrobnosti** pro typ přidružení zásad, který jste vybrali. V případě, že nevíte, jaké údaje máte zadat pro jednotlivá pole, klepněte na volbu **Nápověda**.
6. Zadejte **vyhledávací informace**, které chcete použít k další identifikaci totožnosti cílové ho uživatele v daném přidružení zásad. Pak klepněte na **Přidat**. Zopakujte tento krok pro každý záznam vyhledávacích informací, který chcete přidat do přidružení.
7. Klepnutím na **OK** uložte provedené změny a vraťte se na původní dialog **Přidružení zásad - podrobnosti**.
8. Klepnutím na **OK** ukončíte práci.

Odstranění vyhledávací informace z totožnosti cílového uživatele

Vyhledávací informace jsou volitelná jedinečná identifikační data pro totožnost cílového uživatele definovaného v přidružení. Toto přidružení může být buď cílovým přidružením identifikátoru, nebo přidružením zásady.

Vyhledávací informace jsou nezbytné pouze v případě, kdy operace vyhledávání mapování může vrátit více než jednu totožnost cílového uživatele. V takové situaci mohou vzniknout problémy pro aplikace podporující EIM, včetně aplikací a produktů operačního systému i5/OS, které nejsou určeny ke zpracování takového množství výsledků.

Vyhledávací informace musí být zadána pro operace vyhledávání mapování tak, aby tato operace mohla vrátit jedinečnou totožnost cílového uživatele. Pokud ovšem dříve definované vyhledávací informace nejsou nadále potřebné, je možné tyto informace odstranit, takže tyto informace již nebudou operacím vyhledávání mapování poskytovány.

Způsob, jakým lze vyhledávací informace odstranit, závisí na skutečnosti, jsou-li tyto informace definovány pro přidružení identifikátorů nebo pro cílové přidružení. Vyhledávací informace je vázána na totožnost cílového uživatele, ne na přidružení identifikátorů nebo na přidružení zásad, kde se tato totožnost uživatele nachází. Pokud tedy vymažete poslední přidružení identifikátorů nebo přidružení zásad, které danou totožnost cílového uživatele definují, bude z domény EIM vymazána i totožnost uživatele spolu s vyhledávací informací.

Odstranění vyhledávací informace pro totožnost cílového uživatele v přidružení identifikátorů:

Chcete-li odstranit vyhledávací informace pro totožnost cílového uživatele v přidružení identifikátorů, musíte být připojeni k doméně EIM, ve které si přejete pracovat, a vaše "Kontrola přístupu k EIM" na stránce 38 musí mít jednu z následujících úrovní:

- Administrátor registrů.
- Administrátor pro vybrané registry (pro definici registru, která se vztahuje k registru uživatelů obsahujícímu totožnost cílového uživatele).
- Administrátor EIM.

Chcete-li odstranit vyhledávací informace pro totožnost cílového uživatele v přidružení identifikátorů, postupujte takto:

1. Rozbalte **Síť > EIM (Enterprise Identity Mapping) > Správa domén**.
2. Vyberte doménu EIM, ve které chcete pracovat.
   - Pokud doména EIM, ve které chcete pracovat, není uvedena na seznamu **Správa domén**, prostudujte si téma "Přidání domény EIM do složky Správa domén" na stránce 84.

- Pokud nejste aktuálně připojeni k doméně EIM, ve které chcete pracovat, prostudujte si téma Připojení k řadiči domény EIM.

3. Rozbalte doménu EIM, k níž jste připojeni.
4. Klepněte na **Identifikátory**, čímž zobrazíte seznam identifikátorů EIM pro doménu.

   Poznámka: Někdy se může stát, že poté, co se pokusíte rozbalit složku **Identifikátory**, může trvat delší dobu, než se seznam identifikátorů zobrazí. Chcete-li dosáhnout vyššího výkonu v případech, kdy máte velký počet identifikátorů EIM v doméně, můžete přizpůsobit složku **Identifikátory** tím, že omezíte vyhledávací hodnotu použitou pro zobrazování identifikátorů. Pravým tlačítkem myši klepněte na **Identifikátory**, vyberte volbu **Přizpůsobit toto zobrazení > Zahrnout**a zadejte kritéria pro zobrazení, která mají být použita ke generování seznamu identifikátorů EIM, které mají být zahrnuty do seznamu.
5. Pravým tlačítkem myši klepněte na identifikátor EIM a vyberte volbu **Vlastnosti**.
6. Vyberte stránku **Přidružení**, vyberte cílové přidružení totožnosti uživatele, pro které chcete odstranit vyhledávací informace, a klepněte na **Podrobnosti**.
7. V dialogu **Přidružení - podrobnosti** vyberte vyhledávací informace, které si přejete z totožnosti uživatele odstranit, a klepněte na **Odstranit**.

   Poznámka: Po klepnutí na **Odstranit** se nezobrazí žádná výzva k potvrzení operace výmazu.
8. Klepnutím na **OK** uložte provedené změny a vraťte se do dialogu **Přidružení - podrobnosti**.
9. Klepnutím na **OK** ukončíte práci.

Odstranění vyhledávací informace pro totožnost cílového uživatele v přidružení zásad:

Chcete-li odstranit vyhledávací informace pro totožnost cílového uživatele v přidružení zásad, musíte být připojeni k doméně EIM, ve které si přejete pracovat, a vaše “Kontrola přístupu k EIM” na stránce 38 musí mít jednu z následujících úrovní:

- Administrátor registrů.
- Administrátor pro vybrané registry (pro definici registru, který se vztahuje k registru uživatelů obsahujícímu totožnost cílového uživatele).
- Administrátor EIM.

Chcete-li odstranit vyhledávací informace pro totožnost cílového uživatele v přidružení zásad, postupujte takto:

1. Rozbalte **Síť > EIM (Enterprise Identity Mapping) > Správa domén**.
2. Vyberte doménu EIM, ve které chcete pracovat.
   - Pokud doména EIM, ve které chcete pracovat, není uvedena na seznamu **Správa domén**, prostudujte si téma “Přidání domény EIM do složky Správa domén” na stránce 84.
   - Pokud nejste aktuálně připojeni k doméně EIM, ve které chcete pracovat, prostudujte si téma Připojení k řadiči domény EIM.
3. V dialogu **Zásada mapování** použijte stránky k zobrazení přidružení zásad pro danou doménu.
4. Najděte a vyberte přidružení zásad pro cílový registr, který obsahuje totožnost cílového uživatele, pro kterou má být vyhledávací informace odstraněna.
5. Klepnutím na **Podrobnosti** zobrazte příslušný dialog **Přidružení zásad - podrobnosti** pro typ přidružení zásad, který jste vybrali.
6. Vyberte vyhledávací informace, které si přejete z totožnosti cílového uživatele odstranit, a klepněte na **Odstranit**.

   Poznámka: Po klepnutí na **Odstranit** se nezobrazí žádná výzva k potvrzení operace výmazu.
7. Klepnutím na **OK** uložte provedené změny a vraťte se na původní dialog **Přidružení zásad - podrobnosti**.
8. Klepnutím na **OK** ukončíte práci.

Zobrazení všech přidružení identifikátorů pro identifikátor EIM

Chcete-li zobrazit všechna přidružení pro identifikátor EIM, musíte být připojeni k doméně EIM, ve které si přejete pracovat, a k provedení tohoto úkolu je nutné, abyste měli nějakou úroveň řízení přístupu EIM.

Prohlížet je možné všechna přidružení s jakoukoliv kontrolou přístupu, mimo kontrolu přístupu administrátora pro vybrané registry. Tyto úrovně kontroly přístupu vám umožní vypisovat a prohlížet pouze taková přidružení k registrům, pro která máte jednoznačné oprávnění. Ostatní přidružení k registrům budete moci prohlížet v případě, máte-li kontrolu přístupu k operacím vyhledávání mapování EIM.

Chcete-li zobrazit všechna přidružení mezi identifikátorem EIM a totožnostmi uživatele (ID), pro která byla definována přidružení pro identifikátory EIM, postupujte takto:

Chcete-li zobrazit přidružení pro identifikátory, postupujte takto:

1. Rozbalte **Síť > EIM (Enterprise Identity Mapping) > Správa domén**.
2. Vyberte doménu EIM, ve které chcete pracovat.
   - Pokud doména EIM, ve které chcete pracovat, není uvedena na seznamu **Správa domén**, prostudujte si téma “Přidání domény EIM do složky Správa domén” na stránce 84.
   - Pokud nejste aktuálně připojeni k doméně EIM, ve které chcete pracovat, prostudujte si téma Připojení k řadiči domény EIM.
3. Rozbalte doménu EIM, k níž jste připojeni.
4. Klepněte na **Identifikátory**, čímž zobrazíte seznam identifikátorů EIM pro doménu.

   Poznámka: Někdy se může stát, že poté, co se pokusíte rozbalit složku **Identifikátory**, může trvat delší dobu, než se seznam identifikátorů zobrazí. Chcete-li dosáhnout vyššího výkonu v případech, kdy máte velký počet identifikátorů EIM v doméně, můžete přizpůsobit složku **Identifikátory** tím, že omezíte vyhledávací hodnotu použitou pro zobrazování identifikátorů. Pravým tlačítkem myši klepněte na **Identifikátory**, vyberte volbu **Přizpůsobit toto zobrazení > Zahrnout**a zadejte kritéria pro zobrazení, která mají být použita ke generování seznamu identifikátorů EIM, které mají být zahrnuty do seznamu.
5. Vyberte identifikátor EIM, klepněte pravým tlačítkem myši na identifikátor a vyberte **Vlastnosti**.
6. Za účelem zobrazení seznamu přidružených identifikátorů pro vybrané identifikátory EIM vyberte stránku **Přidružení**.
7. Proces dokončíte klepnutím na **OK**.

Zobrazení všech přidružení zásad pro doménu

Chcete-li zobrazit všechna přidružení zásad definovaných pro doménu, musíte být připojeni k doméně EIM, ve které si přejete pracovat, a k provedení tohoto úkolu je také nutné, abyste měli nějakou úroveň řízení přístupu EIM.

Prohlížet je možné všechna přidružení zásad s jakoukoliv kontrolou přístupu, mimo kontrolu přístupu administrátora pro vybrané registry. Tato úroveň kontroly přístupu vám umožní vypisovat a prohlížet pouze taková přidružení k registrům, pro která máte jednoznačné oprávnění. Proto nemůžete s touto kontrolou přístupu vypisovat ani prohlížet žádná předvolená přidružení zásad domény, ledaže byste měli kontrolu přístupu k operacím vyhledávání mapování EIM.

Chcete-li zobrazit všechna přidružení zásad pro doménu, postupujte takto:

1. Rozbalte **Síť > EIM (Enterprise Identity Mapping) > Správa domén**.
2. Klepněte pravým tlačítkem myši na doménu EIM, ve které chcete pracovat, a vyberte volbu **Zásada mapování**
   - Pokud doména EIM, ve které chcete pracovat, není uvedena na seznamu **Správa domén**, prostudujte si téma “Přidání domény EIM do složky Správa domén” na stránce 84.
   - Pokud nejste aktuálně připojeni k doméně EIM, ve které chcete pracovat, prostudujte si téma Připojení k řadiči domény EIM.
3. Chcete-li zobrazit přidružení zásad definovaná pro doménu, vyberte následující stránky:

a. Chcete-li zobrazit předvolená přidružení zásad domény definovaná pro doménu, vyberte stránku **Domény** a zkontrolujte, zda je přidružení zásad povoleno na úrovni registru.
b. Chcete-li zobrazit předvolená přidružení zásad registrů definovaná pro doménu, vyberte stránku **Registry**. Můžete si také prohlédnout, jaké zdrojové a cílové registry ovlivňují přidružení zásad.
c. Chcete-li zobrazit přidružení zásad filtru certifikátů definovaná a povolená na úrovni registru, vyberte stránku **Filtr certifikátů**.

4. Proces dokončíte klepnutím na **OK**.

Zobrazení všech přidružení zásad pro definici registru

Chcete-li zobrazit všechna přidružení zásad definovaných pro určitý registr, musíte být připojeni k doméně EIM, ve které si přejete pracovat, a k provedení tohoto úkolu je také nutné, abyste měli nějakou úroveň řízení přístupu EIM.

Prohlížet je možné všechna přidružení zásad s jakoukoliv kontrolou přístupu, mimo kontrolu přístupu administrátora pro vybrané registry. Tato úroveň kontroly přístupu vám umožní vypisovat a prohlížet pouze taková přidružení k registrům, pro která máte jednoznačné oprávnění. Proto nemůžete s touto kontrolou přístupu vypisovat ani prohlížet žádná předvolená přidružení zásad domény, ledaže byste měli kontrolu přístupu k operacím vyhledávání mapování EIM.

Chcete-li zobrazit všechna přidružení zásad pro definici registru, postupujte takto:

1. Rozbalte **Síť > EIM (Enterprise Identity Mapping) > Správa domén**.
2. Vyberte doménu EIM, ve které chcete pracovat.
   - Pokud doména EIM, ve které chcete pracovat, není uvedena na seznamu **Správa domén**, prostudujte si téma “Přidání domény EIM do složky Správa domén” na stránce 84.
   - Pokud nejste aktuálně připojeni k doméně EIM, ve které chcete pracovat, prostudujte si téma Připojení k řadiči domény EIM.
3. Klepněte pravým tlačítkem myši na definici registru, se kterou chcete pracovat, a vyberte **Zásada mapování**.
4. Chcete-li zobrazit přidružení zásad definovaná pro určitou definici registru, vyberte následující stránky:
   - Chcete-li zobrazit předvolená přidružení zásad domény definovaná pro registr, vyberte stránku **Domény**.
   - Chcete-li zobrazit předvolená přidružení zásad registrů definovaná a povolená pro registr, vyberte stránku **Registry**.
   - Chcete-li zobrazit přidružení zásad filtru certifikátů definovaná a povolená pro registr, vyberte stránku **Filtr certifikátů**.
5. Proces dokončíte klepnutím na **OK**.

Výmaz přidružení identifikátorů

Chcete-li vymazat některé přidružení identifikátorů, musíte být připojeni k doméně EIM, ve které chcete pracovat, a vaše řízení přístupu k EIM musí splňovat požadavky pro typ přidružení, který chcete vymazat.

Chcete-li vymazat zdrojové nebo administrační přidružení, musíte mít kontrolu přístupu k EIM na jedné z těchto úrovní:

- Administrátor identifikátorů.
- Administrátor EIM.

Chcete-li vymazat cílové přidružení, musíte mít kontrolu přístupu k EIM na jedné z těchto úrovní:

- Administrátor registrů.
- Administrátor pro vybrané registry (pro definici registru, která se vztahuje k registru uživatelů obsahujícímu totožnost cílového uživatele).
- Administrátor EIM.

Chcete-li vymazat přidružení identifikátorů, postupujte takto:

1. Rozbalte **Síť > EIM (Enterprise Identity Mapping) > Správa domén**.

2. Vyberte doménu EIM, ve které chcete pracovat.
   - Pokud doména EIM, ve které chcete pracovat, není uvedena na seznamu **Správa domén**, prostudujte si téma “Přidání domény EIM do složky Správa domén” na stránce 84.
   - Pokud nejste aktuálně připojeni k doméně EIM, ve které chcete pracovat, prostudujte si téma Připojení k řadiči domény EIM.
3. Rozbalte doménu EIM, k níž jste připojeni.
4. Klepněte na **Identifikátory**, čímž zobrazíte seznam identifikátorů EIM pro doménu.

   Poznámka: Někdy se může stát, že poté, co se pokusíte rozbalit složku **Identifikátory**, může trvat delší dobu, než se seznam identifikátorů zobrazí. Chcete-li dosáhnout vyššího výkonu v případech, kdy máte velký počet identifikátorů EIM v doméně, můžete přizpůsobit složku **Identifikátory** tím, že omezíte vyhledávací kritéria použitá pro zobrazování identifikátorů. Pravým tlačítkem myši klepněte na **Identifikátory**, vyberte volbu **Přizpůsobit toto zobrazení > Zahrnout**a zadejte kritéria pro zobrazení, která mají být použita ke generování seznamu identifikátorů EIM, které mají být zahrnuty do seznamu.
5. Vyberte identifikátor EIM, klepněte pravým tlačítkem myši na identifikátor a vyberte **Vlastnosti**.
6. Za účelem zobrazení seznamu přidružených identifikátorů pro vybrané identifikátory EIM vyberte stránku **Přidružení**.
7. Vyberte přidružení, které chcete vymazat, a klepnutím na **Odstranit** jej vymažte.

   Poznámka: Po klepnutí na **Odstranit** se nezobrazí žádná výzva k potvrzení operace výmazu.
8. Klepnutím na **OK** uložte provedené změny.

Poznámka: Poté, co odstraníte cílové přidružení, mohou některé operace vyhledávání mapování v cílovém registru, které se spoléhají na použití vymazaného přidružení, selhat (v případě, že pro dotčený cílový registr neexistuje jiné přidružení (ať už přidružení zásad nebo přidružení identifikátorů)).

Jediným způsobem, jak definovat totožnost uživatele vůči EIM, je zadat totožnost uživatele během vytváření přidružení, buď přidružení identifikátorů, nebo přidružení zásad. Když pak vymažete poslední cílové přidružení pro totožnost uživatele (ať již odstraněním jednotlivého cílového přidružení nebo odstraněním přidružení zásad), totožnost daného uživatele již nebude v EIM nadále definována. Jméno totožnosti uživatele a veškeré vyhledávací informace pro totožnost daného uživatele tak budou ztraceny.

Výmaz přidružení zásad

Chcete-li vymazat přidružení zásad, musíte být připojeni k doméně EIM, ve které chcete pracovat, a musíte mít řízení přístupu buď jako administrátor EIM nebo jako administrátor registrů.

Chcete-li vymazat přidružení zásad, postupujte takto:

1. Rozbalte **Síť > EIM (Enterprise Identity Mapping) > Správa domén**.
2. Vyberte doménu EIM, ve které chcete pracovat.
   - Pokud doména EIM, ve které chcete pracovat, není uvedena na seznamu **Správa domén**, prostudujte si téma “Přidání domény EIM do složky Správa domén” na stránce 84.
   - Pokud nejste aktuálně připojeni k doméně EIM, ve které chcete pracovat, prostudujte si téma Připojení k řadiči domény EIM.
3. Vyberte odpovídající stránku typu domény, kterou si přejete vymazat.
4. Na této stránce vyberte odpovídající přidružení zásad a klepněte na **Odstranit**.

   Poznámka: Po klepnutí na **Odstranit** se nezobrazí žádná výzva k potvrzení operace výmazu.
5. Chcete-li opustit dialog **Zásada mapování** a uložit změny, klepněte na **OK**.

Poznámka: V případě, že odstraníte cílové přidružení zásad, a v případě, když pro daný cílový registr neexistují žádná jiná přidružení (ať už přidružení zásad nebo přidružení identifikátorů), pak jakékoliv operace vyhledávání mapování směrem k cílovému registru, jenž spoléhá na používání vymazaného přidružení zásad, mohou selhat.

Jediným způsobem, jak definovat totožnost uživatele vůči EIM, je zadat totožnost uživatele během vytváření přidružení, buď přidružení identifikátorů, nebo přidružení zásad. Když pak vymažete poslední cílové přidružení pro totožnost uživatele (ať již odstraněním jednotlivého cílového přidružení nebo odstraněním přidružení zásad), totožnost daného uživatele již nebude v EIM nadále definována. Jméno totožnosti uživatele a veškeré vyhledávací informace pro totožnost daného uživatele tak budou ztraceny.

Související pojmy

"Správa definic registrů EIM" na stránce 88
K tomu, aby se registry uživatelů a totožnosti uživatele, které registry obsahují, účastnily v produktu EIM, musíte pro ně vytvořit definice registrů. Potom můžete pomocí těchto definic registrů EIM spravovat to, jak se registry uživatelů a jejich totožnosti uživatele mohou účastnit v produktu EIM.

Správa řízení přístupu uživatelů k EIM

Uživatel EIM je uživatel, který vlastní oprávnění řízení přístupu EIM na základě členství v předdefinovaných skupinách uživatelů LDAP (Lightweight Directory Access Protocol). Uvedení kontroly přístupu k EIM pro uživatele přidá uživatele do určité skupiny uživatelů LDAP.

Každá skupina LDAP má oprávnění provádět různé administrační úlohy EIM v doméně. Jak a jaké typy administračních úloh, včetně vyhledávacích operací, může uživatel provádět, určuje skupina pro kontrolu přístupu, do níž uživatel EIM náleží.

Pouze uživatelé s kontrolou přístupu administrátora LDAP nebo administrátora EIM mohou přidávat další uživatele do skupiny pro kontrolu přístupu k EIM nebo měnit nastavení kontroly přístupu pro ostatní uživatele. Dříve než se uživatel může stát členem skupiny kontroly přístupu k EIM, musí mít přístup k serveru adresářů, jenž vystupuje jako řadič domény EIM. Musíte vzít na vědomí, že pouze určité typy uživatelů se mohou stát členy skupiny pro kontrolu přístupu k EIM: činitelé Kerberos, rozlišovací jména a uživatelské profily operačního systému i5/OS.

Poznámka: Chcete-li zpřístupnit typ uživatele činitele Kerberos v EIM, musíte v systému konfigurovat službu síťového ověření. Aby byl k dispozici pro EIM uživatelský profil i5/OS, musíte na serveru adresářů nakonfigurovat systémovou příponu objektu. To umožní serveru adresářů odkazovat se na systémové objekty i5/OS, jako jsou uživatelské profily i5/OS.

Chcete-li spravovat kontrolu přístupu pro stávajícího uživatele serveru adresářů nebo chcete-li přidat stávajícího uživatele serveru adresářů do skupiny pro kontrolu přístupu k EIM, postupujte takto:

1. Rozbalte **Síť > EIM (Enterprise Identity Mapping) > Správa domén**.
2. Vyberte doménu EIM, ve které chcete pracovat.
   - Pokud doména EIM, ve které chcete pracovat, není uvedena na seznamu **Správa domén**, prostudujte si téma "Přidání domény EIM do složky Správa domén" na stránce 84.
   - Pokud nejste aktuálně připojeni k doméně EIM, ve které chcete pracovat, prostudujte si téma Připojení k řadiči domény EIM.
3. Klepněte pravým tlačítkem myši na doménu EIM, ke které jste připojeni, a vyberte **Řízení přístupu**
4. V dialogu **Editovat kontrolu přístupu k EIM** vyberte **Typ uživatele**. Zobrazí se pole požadovaná pro zadání identifikačních informací o uživateli.
5. Zadejte požadované informace o uživateli, abyste označili uživatele, kterého chcete přidat do jedné nebo více skupin pro kontrolu přístupu k EIM. Klepnutím na **OK** zobrazíte panel **Editovat kontrolu přístupu k EIM**. V případě, že nevíte, jaké údaje máte zadat pro jednotlivá pole, klepněte na volbu **Nápověda**.
6. Vyberte jednu nebo více skupin pro **Kontrolu přístupu** uživatele. Klepnutím na **OK** přidáte uživatele do vybraných skupin. Klepnutím na volbu **Nápověda** získáte další podrobné informace o tom, jaká oprávnění má každá skupina, zjistíte další požadavky.

7. Jakmile zadáte požadované informace, uložte změny klepnutím na **OK**.

Související pojmy

"Kontrola přístupu k EIM" na stránce 38
Uživatel EIM je uživatel, který vlastní kontrolu přístupu k produktu EIM. Tato kontrola přístupu k EIM je založena na skutečnosti, že uživatel je členem předvolené skupiny uživatelů LDAP (Lightweight Directory Access Protocol) pro danou doménu.

Související informace

Služby síťového ověření

Správa konfiguračních vlastností EIM

Na vašem serveru můžete spravovat několik různých konfiguračních vlastností produktu EIM. Tyto činnosti se obvykle neprovádí moc často,

avšak existuje několik situací, které vyžadují provedení drobných úprav konfiguračních vlastností. Pokud se například zhroutí systém a vy budete potřebovat znovu vytvořit konfiguraci vlastností EIM, můžete buď znovu spustit průvodce konfigurací EIM, nebo zde tyto vlastnosti změnit. Nebo se můžete rozhodnout, že nebudete při práci s průvodcem konfigurací EIM vytvářet definice registrů pro lokální registry. Aktualizaci informací o definici registru lze rovněž provést zde.

Vlastnosti, které můžete měnit, jsou:

- Doména EIM, ve které je účasten server.
- Informace o připojení pro řadič domény EIM.
- Totožnost uživatele, kterou systém používá k provádění operací EIM v zastoupení funkcí operačního systému.
- Jména definic registrů, která se vztahují ke skutečným registrům uživatelů, jež systém využívá během provádění operací EIM v zastoupení funkcí operačního systému. Tato jména definic registrů se vztahují k lokálním registrům uživatelů, které můžete vytvořit v průběhu práce s průvodcem konfigurací EIM.

  Poznámka: Pokud se rozhodnete, že nebudete při práci s průvodcem konfigurací EIM vytvářet jména definic lokálních registrů (mohou být již vytvořena nebo jste se rozhodli tato jména pro doménu definovat později), budete aktualizovat systém prostřednictvím těchto jmen definic registrů. Systém vyžaduje informace o definicích registrů k provádění operací EIM v zastoupení funkcí operačního systému.

Chcete-li změnit konfigurační vlastnosti EIM, musíte mít následující zvláštní oprávnění:

- Administrátor zabezpečení (*SECADM).
- Všechny objekty (*ALLOBJ).

Chcete-li provést změnu konfiguračních vlastností EIM ve vašem systému System i, postupujte takto:

1. Rozbalte **Síť > EIM (Enterprise Identity Mapping)**.
2. Klepněte pravým tlačítkem myši na **Konfigurace** a vyberte **Vlastnosti**.
3. Proveďte změny informací o konfiguraci EIM.
4. Chcete-li získat informace o tom, jaké údaje je nutné zadat do každého pole v dialogu, klepněte na **Nápověda**.
5. Chcete-li se ujistit, že všechny zadané informace umožní systému úspěšně se přihlásit k řadiči domény EIM, klepněte na **Ověření konfigurace**.
6. Klepnutím na **OK** uložte provedené změny.

Poznámka: Pokud jste pro vytvoření domény nebo pro vstup do domény nepoužili průvodce konfigurací EIM, nepokoušejte se vytvořit konfiguraci EIM manuálním zadáním konfiguračních vlastností. Použitím průvodce pro vytvoření vaší základní konfigurace EIM můžete předejít možným problémům s konfigurací, protože průvodce zvládá rozhodně více než pouhé nastavení těchto vlastností.

Odstraňování problémů s EIM

Použijte tyto metody odstraňování problémů k řešení některých základních problémů se kterými se můžete setkat při konfiguraci a používání produktu EIM (Enterprise Identity Mapping).

Produkt EIM je tvořen několika technologiemi a mnoha aplikacemi a funkcemi. V důsledku toho se mohou problémy objevovat v různých oblastech. Následující informace vám zde nastíní některé běžné problémy a chyby, na které byste mohli narazit během práce s EIM, a zároveň vám poskytnou několik návrhů, jak je možné jednotlivé problémy řešit.

Související informace

Odstraňování problémů s konfigurací jediného přihlášení

Odstraňování problémů s připojením k řadiči domény

Existuje značné množství faktorů, které mohou přispět ke vzniku problémů s připojením k řadiči domény EIM. Při řešení možných problémů vám pomůže následující tabulka.

Tabulka 27. Běžné problémy s připojením k řadiči domény EIM a jejich řešení

Možný problém	Možná řešení
Nemůžete se připojit k řadiči domény během práce s produktem System i Navigator za účelem správy EIM.	Informace o připojení k řadiči domény mohou být pro doménu, kterou si přejete spravovat, nesprávně zadány. Chcete-li ověřit informace o připojení k řadiči domény, postupujte takto: • Rozbalte **Síť-->EIM (Enterprise Identity Mapping)-->Síť->Správa domén**. Klepněte pravým tlačítkem myši na doménu, kterou chcete spravovat, a vyberte **Vlastnosti**. • Ověřte si, zda je **Jméno řadiče domény** zadáno správně a také jestli **Nadřazené DN**, pokud je zadáno, souhlasí. • Ověřte si, zda jsou informace o **Připojení** pro řadič domény správné. Zajistěte, aby bylo správně zadáno číslo **Portu**. Pokud je vybráno **Použít zabezpečené připojení (SSL nebo TLS)**, musí být server adresářů nakonfigurován na používání SSL. Chcete-li si ověřit, zda můžete zadané informace úspěšně použít k vytvoření připojení k řadiči domény, klepněte na **Ověřit připojení**. • Ověřte si, zda jsou informace v panelu **Připojení k řadiči domény** zadány správně.

Tabulka 27. Běžné problémy s připojením k řadiči domény EIM a jejich řešení (pokračování)

Možný problém	Možná řešení
Operační systém nebo aplikace nemůže za účelem vstupu do dat EIM navázat spojení s řadičem domény. Například operace vyhledávání mapování prováděné v zastoupení systému nefungují. Může k tomu docházet v případě, že konfigurace EIM v systému nebo systémech je chybná.	Ověřte si konfiguraci EIM. Rozbalte **Síť-->EIM (Enterprise Identity Mapping)-->Konfigurace** v systému, ve kterém se chcete ověřit. Klepněte pravým tlačítkem na složku **Konfigurace**, vyberte **Vlastnosti** a ověřte následující: • Stránka **Domény** : – Jméno řadiče domény a čísla portu jsou správná. – Chcete-li ověřit, že řadič domény je aktivní, klepněte na **Ověřit konfiguraci**. – Jméno lokálního registru je zadáno správně. – Jméno registru Kerberos je zadáno správně. – Ověřte, zda je vybráno **Povolit operace EIM v tomto systému**. • Stránka **Uživatel systému**: – Zadaný uživatel má pro vyhledávání mapování dostatečnou kontrolu přístupu k EIM a jeho heslo je platné. Další informace o různých typech pověření pro uživatele uvádí online nápověda. **Poznámka:** Pokud jste na serveru adresářů změnili heslo pro daného uživatele systému, musíte toto heslo změnit i zde. Jestliže se tato hesla neshodují, pak uživatel systému nemůže provádět funkce EIM operačního systému a operace vyhledávání mapování nebudou fungovat. – Chcete-li potvrdit, že zadané uživatelské informace jsou správné, klepněte na **Ověřit připojení**.
Informace o konfiguraci se zdají být správné, ale stále se nemůžete připojit k řadiči domény.	• Zajistěte, aby byl server adresářů, fungující jako řadič domény, aktivní. Pokud je řadičem domény systém System i, můžete použít produkt System i Navigator a postupovat takto: 1. Rozbalte **Síť > Servery > TCP/IP**. 2. Ověřte si, že server adresářů je ve stavu **Spuštěn**. Pokud je server zastaven, klepněte pravým tlačítkem myši na **Server adresářů** a vyberte **Start**

Poté, co ověříte informace o připojení a zajistíte, aby byl server adresářů aktivní, pokuste se o opětovné připojení k řadiči domény podle následujících kroků:

1. Rozbalte **Síť > EIM (Enterprise Identity Mapping) > Správa domén**.
2. Klepněte pravým tlačítkem myši na doménu EIM, ke které se chcete připojit, a vyberte **Připojit**.
3. Zadejte typ uživatele a požadované informace o uživateli, které by měly být použity při připojení k řadiči domény EIM.
4. Klepněte na **OK**.

Odstraňování všeobecných problémů s konfigurací a doménou EIM

Existuje množství všeobecných problémů, na které můžete narazit buď při konfiguraci produktu EIM ve vašem systému, nebo při přístupu k doméně EIM. V následující tabulce najdete více informací o některých běžných problémech a o jejich řešeních, která je možno využít.

Tabulka 28. Běžné problémy a jejich řešení při konfigurací EIM a práci s doménou EIM.

Možný problém	Možná řešení
Průvodce konfigurací EIM se po zadání volby **Dokončit** během procesu zastavil.	Průvodce možná čeká na spuštění řadiče domény. Ověřte si, že nedošlo k žádným chybám při spouštění serveru adresářů. V případě systému System i zkontrolujte protokol úlohy pro úlohu QDIRSRV v subsystému QSYSWRK. Chcete-li provést kontrolu protokolu úlohy, postupujte takto: 1. V produktu System i Navigator rozbalte **Řízení prací > Subsystémy > Qsyswrk**. 2. Klepněte pravým tlačítkem myši na **Qdirsrv** a vyberte **Protokol úlohy**.
Během práce s průvodcem konfigurací EIM při vytváření domény na vzdáleném systému jste obdrželi tuto chybovou zprávu: ″Zadali jste neplatné nadřazené rozlišovací jméno (DN).″ DN musí existovat na vzdáleném serveru adresářů. Zadejte nebo zvolte nové, či existující nadřazené DN.	Nadřazené DN zadané pro vzdálenou doménu neexistuje. Další informace o použití průvodce konfigurací EIM uvádí téma “Vytvoření a vstup do nové vzdálené domény” na stránce 73. Prohlédněte si také on-line nápovědu o zadání nadřazeného DN při vytváření domény.
Obdrželi jste zprávu, která hlásí, že doména EIM neexistuje.	Pokud jste ještě nevytvořili doménu EIM, použijte průvodce konfigurací EIM. Tento průvodce vám pomůže vytvořit doménu EIM, nebo vám umožní konfigurovat existující doménu EIM. Pokud jste již vytvořili doménu EIM, ověřte si, zda zadaný uživatel je členem skupiny, jak uvádí téma “Kontrola přístupu k EIM” na stránce 38, a zda má odpovídající oprávnění pro přístup do domény EIM.
Obdrželi jste zprávu, která hlásí, že objekt EIM (identifikátor, registr, přidružení, přidružení zásad nebo filtr certifikátů) nebyl nalezen nebo že nejste oprávněni pro přístup do dat EIM.	Ověřte si, zda tento objekt EIM existuje a jestli zadaný uživatel je členem skupiny, jak uvádí téma “Kontrola přístupu k EIM” na stránce 38, a zda má odpovídající oprávnění pro přístup do domény EIM.
Rozbalujete složku **Identifikátory** a zobrazení seznamu těchto identifikátorů trvá příliš dlouho.	Toto se může stát v případě velkého počtu jednotlivých identifikátorů definovaných v doméně. Chcete-li tento problém vyřešit, můžete přizpůsobit zobrazení složky **Identifikátory** tím, že omezíte vyhledávací kritéria pro zobrazení identifikátorů. Chcete-li přizpůsobit zobrazení identifikátorů, postupujte takto: 1. V produktu System i Navigator rozbalte **Síť > EIM (Enterprise Identity Mapping) > Správa domén**. 2. Rozbalte doménu, ve které si přejete zobrazit identifikátory EIM. 3. Pravým tlačítkem myši klepněte na **Identifikátory** a vyberte **Přizpůsobit toto zobrazení > Zahrnout**. 4. Zadejte kritéria zobrazení, která mají být použita při generování seznamu identifikátorů EIM, jež mají být zahrnuty do zobrazení. **Poznámka:** Je možné použít hvězdičku (*) jako zástupný znak. 5. Klepněte na **OK**. Když příště klepnete na **Identifikátory**, zobrazí se pouze identifikátory EIM, které odpovídají zadaným kritériím.

Tabulka 28. Běžné problémy a jejich řešení při konfigurací EIM a práci s doménou EIM. (pokračování)

Možný problém	Možná řešení
Při správě EIM pomocí produktu System i Navigator jste obdrželi chybovou zprávu, která hlásí, že ovladač EIM již není platný.	Připojení k řadiči domény bylo ztraceno. Chcete-li se opětovně připojit k řadiči domény, postupujte takto: 1. V produktu System i Navigator rozbalte **Síť > EIM (Enterprise Identity Mapping) > Správa domén**. 2. Klepněte pravým tlačítkem myši na doménu se kterou chcete pracovat, a vyberte **Znovu připojit**. 3. Zadejte informace o připojení. 4. Klepněte na **OK**.
Když používáte protokol Kerberos pro ověření EIM, do protokolu úlohy je napsána diagnostická zpráva CPD3E3F.	Tato zpráva bude vygenerována, kdykoliv dojde k selhání ověření nebo operací mapování totožností. Diagnostická zpráva obsahuje hlavní i vedlejší stavové kódy pro indikaci toho, kde se problém objevil. Nejběžnější chyby, které se objevují, jsou dokumentovány společně s jejich obnovou. Dokumentace pak odkazuje na přidružené informace s diagnostickou zprávou, která může pomoci při řešení daných problémů. Můžete si také prohlédnout téma Řešení problému při konfiguraci jediného přihlášení.

Odstraňování problémů s mapováním EIM

Existuje množství běžných problémů, které mohou způsobit, že mapování EIM nebude fungovat tak, jak se očekává, anebo vůbec. Níže uvedenou tabulku použijte k tomu, abyste nalezli informace o tom, jaké problémy mohou být příčinou nefunkčnosti mapování EIM, a jejich možná řešení. Jestliže mapování EIM nefunguje, budete možná muset procházet každým řešením v tabulce a zajistit tak nalezení a vyřešení problémů, které způsobují nefunkčnost mapování.

Tabulka 29. Běžné problémy s mapováním EIM a jejich řešení

Možný problém	Možná řešení
Informace o připojení řadiče domény mohou být nesprávné nebo řadič domény nemusí být aktivní.	Chcete-li se dozvědět, jak lze ověřit informace o připojení řadiče domény a jak lze ověřit, že řadič domény je aktivní, prostudujte si téma Problémy s připojením řadiče domény.

Tabulka 29. Běžné problémy s mapováním EIM a jejich řešení (pokračování)

Možný problém	Možná řešení
Operace vyhledávání mapování EIM prováděné prostřednictvím systému nefungují. Může k tomu docházet v případě, že konfigurace EIM v systému nebo systémech je chybná.	Ověřte si konfiguraci EIM. Rozbalte **Síť-->EIM (Enterprise Identity Mapping)-->Konfigurace** v systému, ve kterém se chcete ověřit. Klepněte pravým tlačítkem na složku **Konfigurace**, vyberte **Vlastnosti** a ověřte následující: • Stránka **Domény** : – Jméno řadiče domény a čísla portu jsou správná. – Chcete-li ověřit, že řadič domény je aktivní, klepněte na **Ověřit konfiguraci**. – Jméno lokálního registru je zadáno správně. – Jméno registru Kerberos je zadáno správně. – Ověřte, zda je vybráno **Povolit operace EIM v tomto systému**. • Stránka **Uživatel systému**: – Uvedený uživatel má dostatečnou kontrolu přístupu k EIM k tomu, aby mohl provést vyhledávání mapování a heslo je pro uživatele platné. Chcete-li se dozvědět více o různých typech pověření uživatelů, informace najdete v online nápovědě. **Poznámka:** Pokud jste na serveru adresářů změnili heslo pro daného uživatele systému, musíte toto heslo změnit i zde. Jestliže se tato hesla neshodují, pak uživatel systému nemůže provádět funkce EIM operačního systému a operace vyhledávání mapování nebudou fungovat. – Chcete-li potvrdit, že zadané uživatelské informace jsou správné, klepněte na **Ověřit připojení**.

Tabulka 29. Běžné problémy s mapováním EIM a jejich řešení (pokračování)

Možný problém	Možná řešení
Operace vyhledávání mapování může vrátit více totožností cílových uživatelů. K tomu může dojít, když nastane jedna nebo více z následujících situací: • Identifikátor EIM má více jednotlivých cílových přidružení ke stejnému cílovému registru. • Více než jeden identifikátor EIM má tutéž totožnost uživatele specifikovanou ve zdrojovém přidružení a každý z těchto identifikátorů má cílové přidružení k témuž cílovému registru, ačkoliv totožnost uživatele specifikovaná pro každé cílové přidružení může být odlišná. • Více než jedno předvolené přidružení zásad domény uvádí stejný cílový registr. • Více než jedno předvolené přidružení zásad registru uvádí stejný zdrojový registr a stejný cílový registr. • Více než jedno přidružení zásad filtru certifikátů uvádí stejný zdrojový registr X.509, filtr certifikátů a cílový registr.	Pomocí funkce Testování mapování EIM ověřte, že se určitá totožnost zdrojového uživatele mapuje správně na odpovídající totožnost cílového uživatele. V závislosti na výsledcích testu opravte problém následujícím způsobem: • Test vrací více nežádoucích cílových totožností. Důvodem je jedna z níže uvedených možností: – To by mohlo znamenat, že konfigurace přidružení pro doménu není správná, vinou jedné z níže uvedených příčin: - Cílové nebo zdrojové přidružení pro identifikátor EIM není správně nakonfigurováno. Například neexistuje zdrojové přidružení pro činitele Kerberos (nebo pro uživatele Windows) nebo toto přidružení není správné. Nebo také může cílové přidružení uvádět nesprávnou totožnost uživatele. Chcete-li ověřit přidružení určitého identifikátoru, zobrazte všechna přidružení identifikátorů EIM. - Přidružení zásad není správně nakonfigurováno. Chcete-li ověřit zdrojové a cílové informace pro všechna přidružení zásad definovaných v doméně, zobrazte všechna přidružení zásad pro doménu. – To by mohlo znamenat, že definice skupinového registru obsahující běžné členy představují zdrojové nebo cílové registry pro přidružení identifikátoru EIM nebo pro přidružení zásad. Podrobné informace, které vám poskytne operace vyhledávání testování mapování, použijte k určení toho, zda jsou zdrojové nebo cílové registry definicemi skupinového registru. Pokud ano, zkontrolujte vlastnosti definice skupinového registru a zjistěte, zda definice skupinového registru obsahují běžné členy. – Test vrací více cílových totožností a tyto výsledky odpovídají tomu, jak jste nakonfigurovali přidružení. Jestliže tato situace nastane, potřebujete určit vyhledávací informace pro každou totožnost cílového uživatele a tak zajistit, že vyhledávací operace vrátí jednu totožnost cílového uživatele spíše než všechny možné totožnosti cílových uživatelů. Další informace uvádí téma Přidání vyhledávací informace k totožnosti cílového uživatele. **Poznámka:** Tento přístup funguje pouze tehdy, má-li aplikace povoleno používat vyhledávací informace. Avšak základní aplikace i5/OS, jako například System i Access for Windows, nemohou využívat vyhledávací informace k rozlišování mezi více totožnostmi cílových uživatelů, které vrátila vyhledávací operace. Tudíž můžete zvážit nová definování přidružení pro doménu a zajistit tak, že operace vyhledávání mapování bude vracet jedinou totožnost cílového uživatele. Tak také zajistíte, že základní aplikace i5/OS budou moci úspěšně provádět vyhledávací operace a mapovat totožnosti.

Tabulka 29. Běžné problémy s mapováním EIM a jejich řešení (pokračování)

Možný problém	Možná řešení
Vyhledávací operace EIM nevracejí žádné výsledky a pro doménu jsou nakonfigurována přidružení.	Pomocí funkce Testování mapování EIM ověřte, že se určitá totožnost zdrojového uživatele mapuje správně na odpovídající totožnost cílového uživatele. V tomto případě si ověřte, zda jste do testu zadali správné informace. Pokud jsou zadané informace správné a test stále nevrací žádné výsledky, může být problém způsoben jedním z následujících bodů: • Konfigurace přidružení je nesprávná. Ověřte si konfiguraci přidružení pomocí informací týkajících se řešení problémů, které byly uvedeny v předchozí části. • Na úrovni domény nebyla povolena podpora přidružení zásad. Budete muset povolit přidružení zásad pro doménu. • Na úrovni jednotlivého registru nebyla povolena podpora přidružení zásad nebo podpora vyhledávání mapování. Budete muset povolit podporu vyhledávání mapování a použití přidružení zásad pro cílový registr. • Kvůli rozlišování velkých a malých písmen definice registru neodpovídá totožnostem uživatele. Můžete tedy vymazat a znovu vytvořit registr nebo také můžete vymazat a znovu vytvořit přidružení se správným rozlišováním písmen.

Související úlohy

"Testování mapování EIM" na stránce 85
Testování mapování EIM vám umožňuje ve vaší konfiguraci provádět operace vyhledávání mapování EIM. Test kontroluje, zda se daná totožnost zdrojového uživatele správně mapuje na odpovídající totožnost cílového uživatele. Provedením takového testu se ujistíte, jestli operace vyhledávání mapování EIM vrátí správnou totožnost cílového uživatele, který odpovídá zadaným informacím.

Rozhraní API EIM

Produkt EIM (Enterprise Identity Mapping) poskytuje mechanismy pro správu totožností uživatele mezi platformami. EIM má několik rozhraní API (application programming interface), která mohou aplikace používat při řízení operací EIM v zastoupení aplikace nebo uživatele aplikace.

Tato rozhraní API lze použít při provádění vyhledávacích operací mapování totožností, pro různé funkce správy a konfigurace EIM i při provádění změn informací a zadávání dotazů. Všechna tato rozhraní API jsou podporována na různých platformách IBM.

Rozhraní API EIM patří do několika níže uvedených kategorií:

- Operace pro obsluhu EIM a připojení.
- Administrace domény EIM.
- Operace registrů.
- Operace identifikátorů EIM.
- Správa přidružení EIM.
- Operace vyhledávání mapování EIM.
- Správa autorizace EIM.

Aplikace, které používají tato rozhraní API ke správě nebo využití informací EIM v doméně EIM, obvykle dodržují následující programovací model:

1. Získání ovladače EIM.
2. Připojení k doméně EIM.

3. Normální zpracování aplikací.
4. Použití rozhraní API administrace EIM nebo operace vyhledávání mapování totožností EIM.
5. Normální zpracování aplikací.
6. Zničení ovladače EIM před ukončením.

Související pojmy

"Plánování vývoje aplikací EIM (Enterprise Identity Mapping)" na stránce 65
Aby aplikace mohla používat produkt EIM (Enterprise Identity Mapping) a účastnit se v doméně, musí být schopná používat rozhraní API EIM.

Související informace

Rozhraní API k EIM (Enterprise Identity Mapping)

Informace související s EIM

Publikace typu IBM Redbook a ostatní kolekce témat v aplikaci Informační centrum, které se vztahují ke kolekci témat EIM (Enterprise Identity Mapping). Kterýkoli z těchto dokumentů ve formátu PDF si můžete zobrazit a vytisknout.

Červené knihy IBM

- Windows-based Single Signon and the EIM Framework on the IBM eServer iSeries Server
- iSeries Access for Windows V5R2 Hot Topics: Tailored Images, Application Administration, SSL, and Kerberos

Další informace

- Jediné přihlášení
- Služby síťového ověření
- IBM Tivoli Directory Server for i5/OS (LDAP)

Ustanovení a podmínky

Oprávnění k užívání těchto publikací je uděleno na základě následujících ustanovení a podmínek.

Osobní použití: Pokud zachováte všechny výhrady týkající se vlastnických práv, můžete tyto publikace kopírovat pro své osobní nekomerční použití. Tyto publikace ani jakékoliv jejich části nesmíte bez výslovného souhlasu IBM distribuovat, prezentovat ani z nich vytvářet odvozená díla.

Komerční použití: Pokud zachováte všechny výhrady týkající se vlastnických práv, můžete tyto publikace kopírovat, distribuovat a prezentovat výhradně uvnitř svého podniku. Bez výslovného souhlasu IBM nesmíte z těchto publikací vytvářet odvozená díla ani je (nebo jejich části) nesmíte kopírovat, distribuovat či prezentovat mimo rámec svého podniku.

Kromě oprávnění, která jsou zde výslovně udělena, se na publikace nebo jakékoliv informace, data, software a další duševní vlastnictví obsažené v těchto publikacích nevztahují žádná další vyjádřená ani odvozená oprávnění, povolení či práva.

IBM si vyhrazuje právo odvolat oprávnění zde udělená, kdykoli usoudí, že používání publikací poškozuje jeho zájmy nebo že výše uvedené pokyny nejsou řádně dodržovány.

Tyto informace můžete stahovat, exportovat či reexportovat pouze při dodržení všech příslušných zákonů a nařízení včetně veškerých vývozních zákonů a nařízení USA.

IBM NEPOSKYTUJE ŽÁDNOU ZÁRUKU, POKUD JDE O OBSAH TĚCHTO PUBLIKACÍ. TYTO PUBLIKACE JSOU POSKYTOVÁNY NA BÁZI ″JAK JSOU″ (AS-IS), BEZ JAKÝCHKOLIV ZÁRUK, VYJÁDŘENÝCH

VÝSLOVNĚ NEBO VYPLÝVAJÍCÍCH Z OKOLNOSTÍ VČETNĚ, A TO ZEJMÉNA, ZÁRUK PRODEJNOSTI, NEPORUŠENÍ PRÁV TŘETÍCH STRAN A VHODNOSTI PRO URČITÝ ÚČEL VYPLÝVAJÍCÍCH Z OKOLNOSTÍ.

Dodatek. Poznámky

Tyto informace platí pro produkty a služby nabízené v USA.

IBM nemusí v ostatních zemích nabízet produkty, služby a funkce popsané v tomto dokumentu. Informace o produktech a službách, které jsou momentálně dostupné ve vašem regionu, můžete získat od místního zástupce IBM. Žádný odkaz na produkt, program nebo službu IBM neznamená a ani z něj nelze vyvozovat, že smí být použit pouze uvedený produkt, program či služba IBM. Použít lze jakýkoliv funkčně ekvivalentní produkt, program či službu neporušující práva IBM na duševní vlastnictví. Za vyhodnocení a ověření činnosti libovolného produktu, programu či služby jiného výrobce než IBM však odpovídá uživatel.

IBM může mít patenty nebo podané žádosti o patent, které zahrnují předmět tohoto dokumentu. Získání tohoto dokumentu uživateli neposkytuje licenci na tyto patenty. Písemné dotazy ohledně licencí můžete zaslat na adresu:

IBM Director of Licensing
IBM Česká republika, spol. s r.o.
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Pokud máte zájem o licenci v zemi s dvoubajtovou znakovou sadou (DBCS), kontaktujte zastoupení IBM ve vaší zemi, nebo písemně zastoupení IBM na adrese:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

Následující odstavec se netýká Velké Británie nebo kterékoliv jiné země, kde taková opatření odporují místním zákonům: SPOLEČNOST INTERNATIONAL BUSINESS MACHINES CORPORATION POSKYTUJE PŘÍRUČKU “JAK JE”, BEZ ZÁRUK JAKÉHOKOLIV DRUHU, VÝSLOVNĚ VYJÁDŘENÝCH NEBO VYPLÝVAJÍCÍCH Z OKOLNOSTÍ, VČETNĚ, A TO ZEJMÉNA, ZÁRUK ČI PODMÍNEK PRODEJNOSTI NEBO VHODNOSTI PRO URČITÝ ÚČEL VYPLÝVAJÍCÍCH Z OKOLNOSTÍ. Právní řády některých zemí nepřipouštějí vyloučení záruk výslovně vyjádřených nebo vyplývajících z okolností, takže se na vás výše uvedené vyloučení nemusí vztahovat.

Tato publikace může obsahovat technické nepřesnosti nebo typografické chyby. Informace zde uváděné jsou pravidelně aktualizovány a v příštích vydáních této publikace již budou tyto změny zahrnuty. IBM má právo kdykoliv bez upozornění zdokonalovat nebo měnit produkty a programy popsané v této publikaci.

Jakékoliv odkazy v této publikaci na webové stránky jiných společností než IBM jsou poskytovány pouze pro pohodlí uživatele a nemohou být žádným způsobem vykládány jako doporučení těchto webových stránek ze strany IBM. Materiály obsažené na takovýchto webových stránkách nejsou součástí materiálů k tomuto produktu IBM a tyto webové stránky mohou být používány pouze na vlastní nebezpečí.

IBM může použít nebo distribuovat jakékoliv informace, které jí sdělíte, libovolným způsobem, který považuje za odpovídající, aniž by tím vznikl jakýkoliv závazek IBM vůči Vám.

Držitelé licence na tento program, kteří si přejí mít přístup i k informacím o programu za účelem (i) výměny informací mezi nezávisle vytvořenými programy a jinými programy (včetně tohoto) a (ii) vzájemného použití sdílených informací, mohou kontaktovat:

IBM Česká republika, spol. s r.o.
Software Interoperability Coordinator, Department 49XA
Česká republika

Rochester, MN 55901
U.S.A.

Informace tohoto typu mohou být dostupné za odpovídajících podmínek. V některých případech připadá v úvahu zaplacení poplatku.

IBM poskytuje licencovaný program popsaný v tomto dokumentu a veškeré dostupné licencované materiály na základě podmínek uvedených ve smlouvě IBM Customer Agreement, v Mezinárodní licenční smlouvě IBM na programy, v Licenční smlouvě IBM na strojový kód nebo v jiné ekvivalentní smlouvě.

Všechna zde obsažená data týkající se výkonu byla zjištěna v řízeném prostředí. Výsledky získané v jiných provozních prostředích se proto mohou významně lišit. Některá měření mohla být prováděna v systémech na úrovni vývoje a nelze tedy zaručit, že tato měření budou ve všeobecně dostupných systémech stejná. Některá měření mohla být navíc odhadnuta pomocí extrapolace. Skutečné výsledky se mohou lišit. Uživatelé tohoto dokumentu by měli verifikovat použitelná data pro své specifické prostředí.

Informace týkající se produktů jiných firem než IBM byly získány od dodavatelů těchto produktů, z jejich publikovaných sdělení, nebo z jiných veřejně dostupných zdrojů. IBM nezkoumala tyto produkty a nemůže tudíž potvrdit spolehlivost, kompatibilitu a další prohlášení vztahující se k těmto produktům. Dotazy, které se týkají vlastností produktů jiných firem než IBM, musí být adresovány jejich dodavatelům.

Veškerá prohlášení, týkající budoucích trendů nebo strategií IBM, podléhají změnám bez předchozího upozornění a představují pouze cíle a záměry.

Všechny uváděné ceny IBM jsou maloobchodní ceny navržené společností IBM, jsou nyní platné a mohou se bez upozornění změnit. Ceny u prodejců se mohou lišit.

Tyto informace slouží pouze pro účely plánování. Informace v tomto dokumentu mohou být změněny, než se produkty popsané v tomto dokumentu stanou obecně dostupnými.

Tyto publikace obsahují příklady údajů a sestav, používaných v každodenních obchodních činnostech. Abyste si udělali co neúplnější představu, obsahují příklady názvy konkrétních podniků, firemních značek a produktů. Všechny tyto názvy jsou fiktivní a jakákoliv podobnost se jmény a adresami používanými ve skutečných obchodních firmách je čistě náhodná.

COPYRIGHT

Tyto informace obsahují vzorové aplikační programy ve zdrojovém jazyce, které demonstrují techniku programování na různých operačních systémech. Vzorové programy smíte kopírovat, modifikovat a distribuovat v jakékoliv formě, aniž by Vám vznikl jakýkoliv finanční závazek vůči IBM, pro účely vývoje, použití, marketingu nebo distribuce aplikačních programů, které vyhovují rozhraní API pro provozní platformu, pro kterou byly vzorové programy napsány. Tyto příklady nebyly přísně testovány za všech podmínek. IBM proto nemůže zaručit nebo potvrdit spolehlivost, obsluhovatelnost nebo funkčnost těchto produktů.

Každá kopie nebo oblast těchto vzorových programů nebo odvozených prací musí zahrnovat níže uvedenou copyrightovou výhradu:

© (jméno Vaší společnosti) (rok). Části tohoto kódu jsou odvozeny ze vzorových programů IBM Corp. © Copyright IBM Corp. _zadejte rok nebo roky_. Všechna práva vyhrazena.

Jestliže si prohlížíte tyto informace ve formě softcopy, nemusí se zobrazit fotografie a barevné ilustrace.

Ochranné známky

Následující výrazy jsou ochranné známky společnosti International Business Machines Corporation ve Spojených státech a případně v dalších jiných zemích:

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 jsou registrované ochranné známky nebo ochranné známky společnosti Adobe Systems Incorporated ve Spojených státech a případně v dalších jiných zemích.

Linux je registrovaná ochranná známka Linuse Torvaldse ve Spojených státech a případně v dalších jiných zemích.

Microsoft, Windows, Windows NT a logo Windows jsou registrované ochranné známky společnosti Microsoft Corporation ve Spojených státech a případně v dalších jiných zemích.

UNIX je registrovaná ochranná známka skupiny The Open Group ve Spojených státech a jiných zemích.

Názvy jiných společností, produktů nebo služeb mohou být ochrannými nebo servisními známkami jiných společností.

Ustanovení a podmínky

Oprávnění k užívání těchto publikací je uděleno na základě následujících ustanovení a podmínek.

Osobní použití: Pokud zachováte všechny výhrady týkající se vlastnických práv, můžete tyto publikace kopírovat pro své osobní nekomerční použití. Tyto publikace ani jakékoliv jejich části nesmíte bez výslovného souhlasu IBM distribuovat, prezentovat ani z nich vytvářet odvozená díla.

Komerční použití: Pokud zachováte všechny výhrady týkající se vlastnických práv, můžete tyto publikace kopírovat, distribuovat a prezentovat výhradně uvnitř svého podniku. Bez výslovného souhlasu IBM nesmíte z těchto publikací vytvářet odvozená díla ani je (nebo jejich části) nesmíte kopírovat, distribuovat či prezentovat mimo rámec svého podniku.

Kromě oprávnění, která jsou zde výslovně udělena, se na publikace nebo jakékoliv informace, data, software a další duševní vlastnictví obsažené v těchto publikacích nevztahují žádná další vyjádřená ani odvozená oprávnění, povolení či práva.

IBM si vyhrazuje právo odvolat oprávnění zde udělená, kdykoli usoudí, že používání publikací poškozuje jeho zájmy nebo že výše uvedené pokyny nejsou řádně dodržovány.

Tyto informace můžete stahovat, exportovat či reexportovat pouze při dodržení všech příslušných zákonů a nařízení včetně veškerých vývozních zákonů a nařízení USA.

IBM NEPOSKYTUJE ŽÁDNOU ZÁRUKU, POKUD JDE O OBSAH TĚCHTO PUBLIKACÍ. TYTO PUBLIKACE JSOU POSKYTOVÁNY NA BÁZI ″JAK JSOU″ (AS-IS), BEZ JAKÝCHKOLIV ZÁRUK, VYJÁDŘENÝCH VÝSLOVNĚ NEBO VYPLÝVAJÍCÍCH Z OKOLNOSTÍ VČETNĚ, A TO ZEJMÉNA, ZÁRUK PRODEJNOSTI, NEPORUŠENÍ PRÁV TŘETÍCH STRAN A VHODNOSTI PRO URČITÝ ÚČEL VYPLÝVAJÍCÍCH Z OKOLNOSTÍ.

Vytištěno v Dánsku společností IBM Danmark A/S.