Systemy IBM - iSeries

Enterprise Identity Mapping

Wersja 5, Wydanie 4

Systemy IBM - iSeries

Enterprise Identity Mapping

Wersja 5, Wydanie 4

Uwaga

Przed korzystaniem z niniejszych informacji oraz z produktu, którego dotyczą, należy przeczytać informacje, które zawiera dodatek “Uwagi”, na stronie 123.

Wydanie piąte (luty 2006)

Niniejsze wydanie dotyczy wersji 5, wydania 4, modyfikacji 0 systemu operacyjnego IBM i5/OS (numer produktu 5722–SS1) oraz wszelkich kolejnych wersji i modyfikacji tego produktu, o ile nowe wydania nie wskazują inaczej. Wersja ta nie działa na wszystkich modelach komputerów z procesorem RISC ani na modelach z procesorem CISC.

Spis treści

Enterprise Identity Mapping

Produkt Enterprise Identity Mapping (EIM) for iSeries to implementacja w systemie i5/OS infrastruktury @server firmy IBM pozwalającej administratorom i programistom aplikacji na rozwiązanie problemu zarządzania wieloma rejestrami użytkowników w przedsiębiorstwie. Większość przedsiębiorstw korzystających z sieci staje przed problemem obsługi wielu rejestrów użytkowników, co wymaga, aby każda osoba lub jednostka w danym przedsiębiorstwie miała określoną tożsamość w każdym z rejestrów. Potrzeba obsługi wielu rejestrów użytkowników wiąże się z powstaniem w krótkim czasie poważnego problemu administracyjnego, który dotyczy użytkowników, administratorów i programistów aplikacji. Rozwiązaniem jest niedrogi mechanizm Enterprise Identity Mapping (EIM), który umożliwia proste zarządzanie wieloma rejestrami i tożsamościami użytkowników w przedsiębiorstwie.

Mechanizm EIM umożliwia tworzenie systemu odwzorowań tożsamości, nazywanego powiązaniami, między różnymi tożsamościami użytkownika w różnych rejestrach użytkowników dla danej osoby w przedsiębiorstwie. Ponadto EIM udostępnia zestaw funkcji API, które mogą być użyte niezależnie od platformy do tworzenia aplikacji wykorzystujących utworzone odwzorowania tożsamości do wyszukiwania relacji między tożsamościami użytkownika. Ponadto odwzorowywania EIM można używać razem z usługą uwierzytelniania sieciowego lub protokołem Kerberos zaimplementowanym w systemie i5/OS w celu udostępnienia środowiska pojedynczego wpisywania się.

Konfigurowanie i zarządzanie EIM można wykonać za pomocą graficznego interfejsu użytkownika systemu iSeries, programu iSeries Navigator. Serwer iSeries używa EIM, aby umożliwić interfejsom i5/OS uwierzytelnianie użytkowników za pomocą usługi uwierzytelniania sieciowego. Aplikacje i system i5/OS mogą akceptować bilety Kerberos i używać EIM do znalezienia profilu użytkownika reprezentującego tę samą osobę, co bilet Kerberos.

Więcej na temat działania EIM, pojęć związanych z EIM i informacje związane z wykorzystaniem EIM w przedsiębiorstwie zawierają następujące sekcje:

Co nowego w wersji V5R4

Poniższy temat opisuje zmiany w wersji V5R4 produktu Enterprise Identity Mapping (EIM) for iSeries.

Nowe lub rozszerzone funkcje związane z produktem EIM

- Definicje rejestrów grupowych Istnieje możliwość utworzenia definicji rejestrów grupowych, umożliwiających zmniejszenie ilości pracy niezbędnej do skonfigurowania odwzorowania EIM. Definicją rejestru grupowego można zarządzać tak, jak definicją pojedynczego rejestru.
- Dodawanie definicji rejestrów grupowych Aby utworzyć definicję rejestru grupowego i dodać ją do domeny EIM, należy wykonać opisane poniżej czynności.
- Dodawanie elementu do definicji rejestru grupowego Jeśli system jest połączony z domeną EIM, na której przechowywana jest definicja rejestru grupowego, można dodać do niej element, wykonując opisane poniżej czynności.

Rozszerzenie informacji o EIM

W bieżącej wersji wprowadzono wiele aktualizacji, wpływających na sposób implementowania definicji rejestrów grupowych w różnych sytuacjach związanych z produktem EIM.

- Powiązania strategii Poniższe informacje objaśniają, po co ustanawiać relację odwzorowania dla wszystkich identyfikatorów użytkowników w pojedynczym rejestrze i domenie.
- Operacje wyszukiwaniaInformacje objaśniające przepływ dla operacji wyszukiwania, która zwraca tożsamość użytkownika docelowego w rejestrze użytkowników będącym elementem definicji rejestru grupowego.
- Niejednoznaczne wyniki Operacje wyszukiwania mogą zwracać niejednoznaczne wyniki, jeśli w zapytaniu pojedyncza definicja rejestru użytkownika zostanie określona jako element wielu definicji rejestrów grupowych.

Ponadto aktualizowany został temat Pojedyncze logowanie Centrum informacyjnego; zawarto w nim dokumentację na temat implementacji EIM jako części środowiska pojedynczego logowania w celu zredukowania zarządzania hasłami. W temacie tym przedstawiono kilka szczegółowych scenariuszy najczęściej spotykanych sytuacji związanych z pojedynczym logowaniem ze szczegółową instrukcją konfiguracji pomocną przy ich implementacji.

Jak sprawdzić, co zostało dodane lub zmienione

Miejsca, w których zostały zmienione informacje, oznaczono:

- symbolem » początek dodanych lub zmienionych informacji,
- symbolem « koniec dodanych lub zmienionych informacji.

Więcej informacji o nowościach i zmianach w tym wydaniu zawiera dokument Informacje dla użytkowników systemu AS/400.

Drukowalne pliki PDF

Przeglądanie i drukowanie poniższych informacji w formacie PDF.

Aby wyświetlić albo pobrać dokument w formacie PDF, wybierz opcję Eterprise Identity Mapping (około 1820 kB).

Możesz przejrzeć lub pobrać następujące tematy pokrewne:

- Network authentication services (około 1398 kB) zawiera informacje na temat sposobu konfigurowania usług uwierzytelniania sieciowego wraz z EIM w celu utworzenia środowiska pojedynczego logowania.
- Serwer IBM Directory Server (LDAP) (około 1700 kB) zawiera informacje na temat sposobu konfigurowania serwera LDAP, którego można użyć jako kontrolera domeny EIM, oraz informacje dotyczące zaawansowanego konfigurowania LDAP.

Zapisywanie plików PDF

Aby zapisać plik w formacie PDF na stacji roboczej w celu jego przejrzenia lub wydrukowania:

1. Prawym przyciskiem myszy kliknij plik PDF w używanej przeglądarce (prawym przyciskiem myszy kliknij odsyłacz powyżej).
2. Kliknij opcję zapisania pliku PDF lokalnie.
3. Przejdź do katalogu, w którym chcesz zapisać plik PDF.
4. Kliknij **Zapisz**.

Pobieranie programu Adobe Reader

Do przeglądania lub drukowania plików PDF potrzebny jest program Adobe Reader. Darmową kopię można pobrać z serwisu WWW Adobe (www.adobe.com/products/acrobat/readstep.html) .

Przegląd EIM

Informacje opisujące, w rozwiązaniu których problemów EIM może pomóc, podające aktualnie stosowane rozwiązania tych problemów i informujące, dlaczego rozwiązanie z wykorzystaniem EIM jest lepsze.

Obecnie środowiska składają się ze złożonej grupy systemów i aplikacji, co sprawia, że konieczne jest zarządzanie wieloma rejestrami użytkowników. Potrzeba obsługi wielu rejestrów użytkowników wiąże się z powstaniem w krótkim czasie poważnego problemu administracyjnego, który dotyczy użytkowników, administratorów i programistów aplikacji. Wiele przedsiębiorstw usiłuje w bezpieczny sposób zarządzać uwierzytelnianiem i autoryzacją w systemach i aplikacjach. Produkt EIM jest opracowaną przez firmę IBM @server technologią infrastruktury umożliwiającą administratorom i programistom aplikacji rozwiązanie tego problemu w sposób prostszy i tańszy, niż to było możliwe do tej pory.

Poniżej opisano poszczególne problemy, przedstawiono obecnie stosowane rozwiązania i wyjaśniono, dlaczego metoda zastosowana w EIM jest lepsza.

Problem zarządzania wieloma rejestrami użytkowników

Sieciami zawierającymi różne systemy i serwery zarządza wielu administratorów. Każdy z nich stosuje własny sposób zarządzania użytkownikami wykorzystując przy tym różne rejestry użytkowników. W takich złożonych sieciach administratorzy są odpowiedzialni za zarządzanie tożsamościami i hasłami użytkowników stosowanymi w wielu systemach. Ponadto administratorzy często muszą synchronizować te tożsamości i hasła, a użytkownicy muszą pamiętać wiele tożsamości oraz haseł i odpowiednio z nich korzystać. Nakład pracy administratorów i użytkowników w takim środowisku jest zbyt duży. Wskutek tego administratorzy zamiast zajmować się zarządzaniem często poświęcają wiele czasu na rozwiązywanie problemów z nieudanymi próbami zalogowania się i na resetowanie haseł, których zapomnieli użytkownicy.

Problem zarządzania wieloma rejestrami użytkowników dotyczy także programistów aplikacji, którzy mają za zadanie utworzenie aplikacji wielowarstwowych lub heterogenicznych. Rozumieją oni, że klienci dysponują ważnymi danymi biznesowymi rozproszonymi po różnego typu systemach, przy czym każdy z tych systemów przetwarza własne rejestry użytkowników. Muszą więc utworzyć rejestry użytkowników dotyczące praw własności i powiązaną z nimi semantykę ochrony dla aplikacji. Chociaż rozwiązuje to problem z punktu widzenia programisty, zwiększa jednak nakład pracy użytkowników i administratorów.

Rozwiązania stosowane obecnie (Current)

Aby uporać się z problemem zarządzania wieloma rejestrami użytkowników wykorzystuje się różne metody, ale oferowane przez nie rozwiązania są niepełne. Na przykład protokół LDAP udostępnia rozproszony rejestr użytkowników. Użycie protokołu LDAP (lub innych popularnych rozwiązań, takich jak Microsoft Passport) oznacza jednak, że administratorzy muszą zarządzać dodatkowym rejestrem użytkowników i semantyką ochrony albo powinni zastąpić istniejące aplikacje, które zaprojektowano pod kątem korzystania z tych rejestrów.

Stosując to rozwiązanie administratorzy muszą zarządzać wieloma mechanizmami ochrony i pojedynczymi zasobami, co wymaga dodatkowego nakładu pracy i potencjalnie zwiększa ryzyko naruszenia ochrony. Jeśli wiele mechanizmów obsługuje pojedynczy zasób, znacznie wzrasta prawdopodobieństwo, że po zmianie uprawnienia dla jednego mechanizmu, nie zostanie zmienione uprawnienie dla innego. Ryzyko naruszenia ochrony dotyczy na przykład sytuacji, kiedy użytkownik nie może uzyskać dostępu do zasobów za pomocą jednego interfejsu, ale może go uzyskać za pomocą innych interfejsów.

Po wykonaniu pracy przez administratorów okazuje się, że problem nie został całkowicie rozwiązany. Ogólnie można stwierdzić, że przedsiębiorstwa zainwestowały zbyt dużo pieniędzy w obecnie stosowane rejestry użytkowników i powiązane z nimi semantyki ochrony, a wszystko po to, by ułatwić sobie zadanie. Utworzenie kolejnego rejestru użytkowników i powiązanej z nim semantyki ochrony rozwiązuje problem z punktu widzenia dostawcy aplikacji, ale nie rozwiązuje problemów, z którymi muszą się borykać użytkownicy i administratorzy.

Innym stosowanym rozwiązaniem jest użycie pojedynczego logowania. Na rynku dostępne są produkty umożliwiające administratorom zarządzanie plikami zawierającymi wszystkie tożsamości i hasła użytkowników. Rozwiązanie to ma jednak kilka słabych punktów, które wymieniono poniżej.

- Rozwiązuje ono tylko jeden z problemów, przed którymi stają użytkownicy. Co prawda umożliwia ono użytkownikom wpisanie się do wielu systemów za pomocą jednej tożsamości i hasła, ale nie eliminuje konieczności używania haseł użytkowników w innych systemach, ani potrzeby zarządzania tymi hasłami.
- Powstaje dodatkowy problem związany z ryzykiem naruszenia ochrony, biorącym się stąd, że w plikach tych przechowywane są hasła w postaci jawnej lub możliwej do deszyfrowania. Hasła nigdy nie powinny być ani przechowywane w plikach z jawnym tekstem, ani łatwo dostępne dla kogokolwiek, w tym także administratorów.
- Nierozwiązane pozostają problemy dotyczące programistów aplikacji z innych firm, którzy dostarczają heterogeniczne lub wielowarstwowe aplikacje. W dalszym ciągu muszą oni dla tworzonych aplikacji dostarczać rejestry użytkowników dotyczące praw własności.

Pomimo tych wszystkich słabych punktów, niektóre przedsiębiorstwa wybrały tego typu rozwiązania, ponieważ w jakiś sposób rozwiązują one problemy związane ze stosowaniem wielu rejestrów użytkowników.

Rozwiązanie zastosowane w EIM

Produkt EIM umożliwia zbudowanie nowatorskiego i niedrogiego rozwiązania do łatwiejszego zarządzania wieloma rejestrami i tożsamościami użytkowników w wielowarstwowym, heterogenicznym środowisku aplikacji. EIM jest architekturą umożliwiającą opisanie relacji między poszczególnymi osobami lub jednostkami (takimi jak serwery plików i serwery wydruków) w przedsiębiorstwie a wieloma jednostkami, które je w nim reprezentują. Ponadto EIM udostępnia funkcje API, które umożliwiają aplikacjom zadawanie pytań dotyczących tych relacji.

Na przykład dysponując tożsamością użytkownika danej osoby w jednym rejestrze użytkowników można określić, która tożsamość użytkownika w innym rejestrze użytkowników reprezentuje tę samą osobę. Jeśli użytkownik został uwierzytelniony za pomocą jednej tożsamości użytkownika i można odwzorować tę tożsamość na odpowiednią tożsamość w innym rejestrze użytkowników, nie musi on być ponownie uwierzytelniany. Wiadomo, kim jest ten użytkownik i potrzebna jest tylko informacja, która tożsamość użytkownika reprezentuje go w drugim rejestrze użytkowników. Z tego względu EIM udostępnia przedsiębiorstwu ogólną funkcję odwzorowywania tożsamości.

EIM dopuszcza odwzorowania jeden-do-wielu (w jednym rejestrze użytkowników dopuszczalne jest istnienie pojedynczego użytkownika z więcej niż jedną tożsamością). Administrator nie musi jednak tworzyć pojedynczo odwzorowań dla wszystkich tożsamości użytkowników w rejestrze użytkowników. EIM dopuszcza także odwzorowania wiele-do-jednego (wielu użytkowników odwzorowanych na jedną tożsamość użytkownika w jednym rejestrze użytkowników).

Możliwość odwzorowywania tożsamości użytkowników między różnymi rejestrami użytkowników przynosi wiele korzyści. Przede wszystkim aplikacje mogą elastycznie używać jednego rejestru użytkowników do uwierzytelniania, a innego do autoryzacji. Administrator może na przykład odwzorować tożsamość użytkownika systemu Windows w rejestrze Kerberos na profil użytkownika systemu i5/OS w innym rejestrze użytkowników, aby użytkownik miał dostęp do zasobów i5/OS, do których jest autoryzowany jego profil użytkownika i5/OS.

EIM jest otwartą architekturą, której administratorzy mogą używać do reprezentowania w dowolnym rejestrze relacji odwzorowań tożsamości. Nie wymaga się kopiowania istniejących danych do nowego repozytorium i zachowania między nimi synchronizacji. Jedynymi nowymi wprowadzanymi danymi są informacje o relacjach. Produkt EIM przechowuje dane w katalogu LDAP, co umożliwia elastyczne zarządzanie danymi w jednym miejscu i dysponowanie replikami, tam gdzie są potrzebne. EIM zapewnia także przedsiębiorstwom i programistom aplikacji łatwiejszą pracę w szerszym zakresie środowisk przy jednocześnie niższych kosztach. Osiągnięcie tego byłoby niemożliwe bez zastosowania EIM.

Produkt EIM, używany w połączeniu z usługą uwierzytelniania sieciowego i z implementacją protokołu Kerberos systemu i5/OS udostępnia rozwiązanie pojedynczego logowania. Można napisać aplikacje używające funkcji API GSS i EIM do akceptowania biletu Kerberos i odwzorowania go na inną, powiązaną tożsamość użytkownika w innym rejestrze użytkowników. Powiązanie między tożsamością użytkownika, które udostępnia to odwzorowanie tożsamości, może być zrealizowane przez utworzenie powiązań identyfikatorów, które za pośrednictwem identyfikatora EIM wiążą jedną tożsamość użytkownika z inną lub przez utworzenie powiązań strategii, które tworzą bezpośrednie powiązanie tożsamości użytkownika w grupie z pojedynczą, określoną tożsamością użytkownika.

Aby używać odwzorowywania tożsamości, administratorzy muszą:

1. Skonfigurować w sieci domenę EIM. Do utworzenia kontrolera domeny dla domeny i skonfigurowania dostępu do tej domeny można użyć kreatora konfigurowania EIM serwera iSeries. Korzystając z kreatora można wybrać utworzenie nowej domeny EIM i kontrolera domeny w systemie lokalnym lub zdalnym. Lub, jeśli domena EIM już istnieje, można się do niej przyłączyć.
2. Określić, którzy użytkownicy zdefiniowani na serwerze katalogów, który udostępnia kontroler domeny EIM, mają prawo do zarządzania lub dostępu do określonych informacji w domenie EIM, i przypisać im odpowiednie grupy praw kontroli dostępu EIM.

3. Utworzyć definicje rejestrów EIM dla tych rejestrów użytkowników, które będą należeć do domeny EIM. Dla domeny EIM można zdefiniować dowolny rejestr użytkowników, ale konieczne jest zdefiniowanie rejestrów użytkowników dla tych aplikacji i systemów operacyjnych, które obsługują odwzorowania EIM.
4. W zależności od wymagań implementacji EIM, określić, które z poniższych zadań należy wykonać, aby zakończyć konfigurowanie EIM:
   - Utworzenie identyfikatorów EIM dla każdego użytkownika w domenie i utworzenie dla nich powiązań identyfikatorów.
   - Utworzenie powiązań strategii.
   - Utworzenie kombinacji powyższych elementów.

   Informacje pokrewne

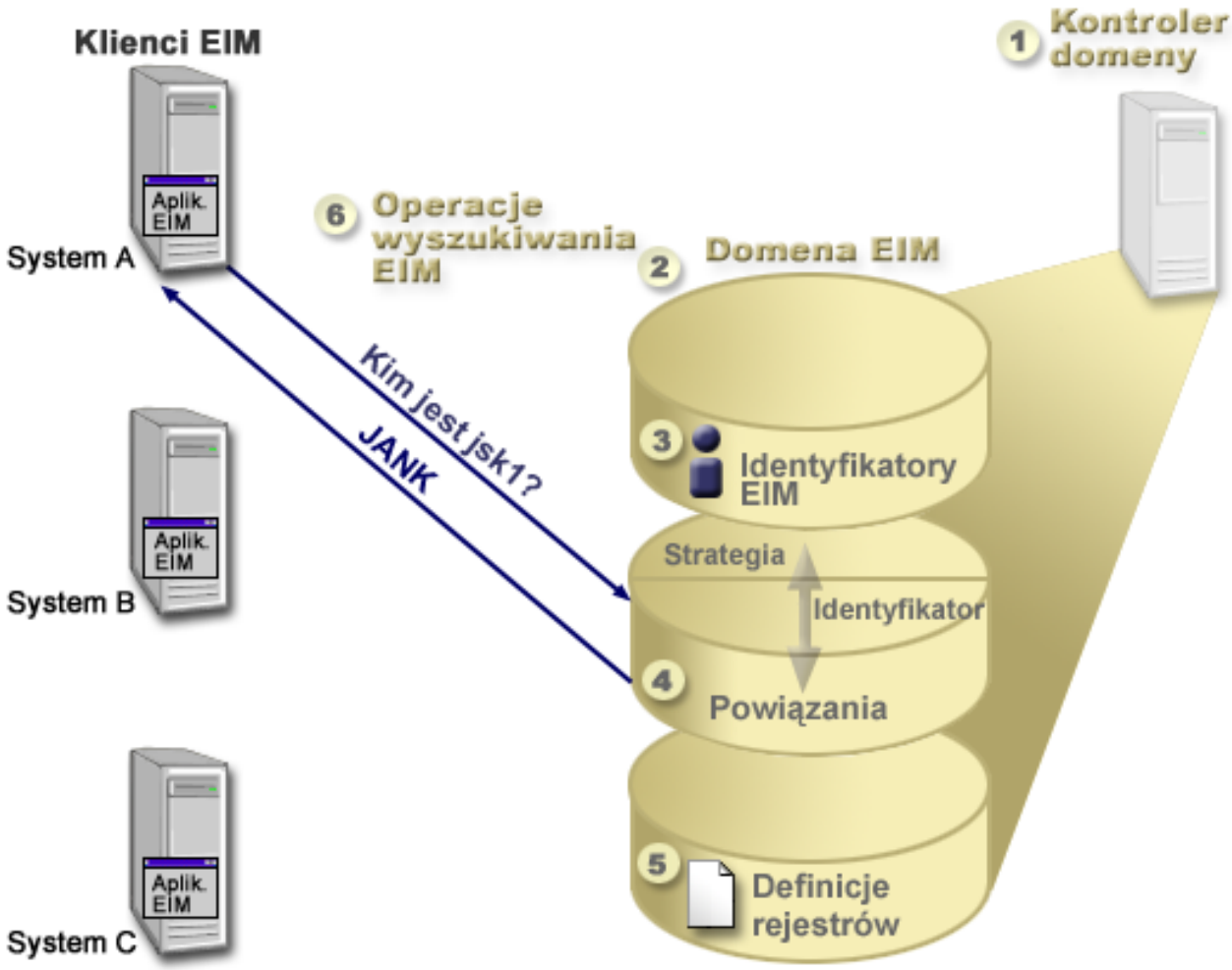
   Temat Pojedyncze wpisanie się (SSO) w Centrum informacyjnym

Pojęcia związane z EIM

Ważne pojęcia związane z EIM i niezbędne do pomyślnej implementacji.

Do świadomego wykorzystania EIM w przedsiębiorstwie konieczne jest zrozumienie koncepcji dotyczących sposobu działania EIM. Mimo że konfiguracja i implementacja funkcji API EIM różni się w zależności od platform serwerów, koncepcje dotyczące EIM są wspólne dla platform IBM @server .

Rysunek 1 przedstawia przykład implementacji EIM w przedsiębiorstwie. Trzy serwery funkcjonują jako klienci produktu EIM i zawierają aplikacje obsługujące EIM, które wysyłają żądania danych EIM poprzez operacje wyszukiwania EIM 6 . Kontroler domeny 1 przechowuje informacje na temat domeny EIM 2 zawierające identyfikator EIM 3 , powiązania 4 między tymi identyfikatorami EIM a tożsamościami użytkowników i definicje rejestrów EIM 5 .



Rysunek 1. Przykład implementacji EIM

Więcej informacji na temat pojęć związanych z EIM i serwerem @server można uzyskać w następujących tematach:

Pojęcia pokrewne

"Koncepcje dotyczące LDAP w kontekście EIM" na stronie 46
Informacje objaśniające, jak używać protokołu LDAP z produktem EIM.

"Pojęcia związane z serwerem iSeries i EIM" na stronie 49
Poniższe informacje zawierają listę aplikacji produktu Enterprise Identity Mapping (EIM).

Kontroler domeny EIM

Informacje objaśniające korzyści z użycia kontrolera domeny EIM.

Kontroler domeny EIM jest serwerem LDAP, który został skonfigurowany do obsługi co najmniej jednej domeny EIM. *Domena EIM* jest katalogiem LDAP, który składa się z wszystkich identyfikatorów EIM, powiązań EIM i rejestrów użytkowników, które zostały zdefiniowane w tej domenie. Systemy (klienci EIM) należące do domeny EIM używają danych domeny do operacji wyszukiwania EIM.

Obecnie można skonfigurować serwer IBM Directory Server na niektórych platformach IBM @server tak, aby działał jako kontroler domeny EIM. W systemie jako klient do domeny może należeć dowolny system obsługujący funkcje API EIM. Systemy klientów używają funkcji API EIM do kontaktowania się z kontrolerem domeny EIM w celu wykonania zadań opisanych w sekcji "Operacje wyszukiwania EIM" na stronie 27. Położenie klienta EIM określa,

czy kontroler domeny EIM jest systemem lokalnym, czy też zdalnym. Kontroler domeny jest *lokalny*, jeśli klient EIM działa w tym samym systemie, co kontroler domeny. Kontroler domeny jest *zdalny*, jeśli klient EIM działa w systemie innym niż kontroler domeny.

Uwaga: Jeśli planujesz skonfigurować serwer katalogów w systemie zdalnym, musi on udostępniać obsługę EIM. Odwzorowania EIM wymagają, aby kontroler domeny był udostępniany przez serwer katalogów obsługujący protokół LDAP w wersji 3. Ponadto serwer katalogów musi mieć skonfigurowane akceptowanie schematu EIM. Obsługę tę udostępniają produkty IBM Directory Server for iSeries i IBM Directory Server V5.1.

Domena EIM

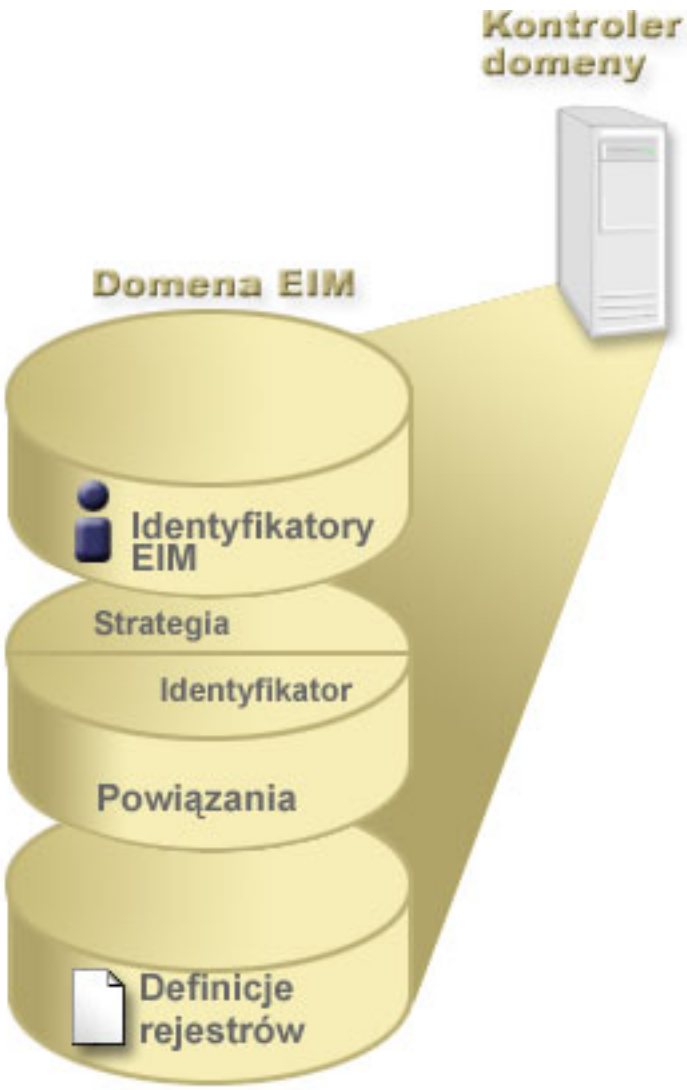
Informacje objaśniające sposób użycia domeny do składowania wszystkich identyfikatorów.

Domena EIM jest katalogiem na serwerze LDAP, który zawiera dane EIM dla przedsiębiorstwa. Domena EIM jest kolekcją wszystkich identyfikatorów i powiązań EIM oraz rejestrów użytkowników zdefiniowanych w tej domenie; jest to także forma kontroli dostępu dla danych. Systemy (klienci EIM) należące do domeny używają danych domeny do operacji wyszukiwania EIM.

Domena EIM jest czym innym niż rejestr użytkowników. Rejestr użytkowników definiuje zbiór tożsamości użytkowników znany i określony jako zaufany przez konkretną instancję systemu operacyjnego lub aplikacji. Rejestr użytkownika zawiera także informacje potrzebne do uwierzytelnienia użytkownika danej tożsamości. Ponadto rejestr użytkowników często zawiera inne atrybuty, takie jak preferencje użytkowników, uprawnienia w systemie lub dane osobowe danej tożsamości.

Domena EIM *odnosi* się do tożsamości użytkowników zdefiniowanych w rejestrach użytkowników. Domena EIM zawiera informacje dotyczące *relacji* między tożsamościami w różnych rejestrach użytkowników (nazwa użytkownika, typ rejestru i instancja rejestru) a rzeczywistymi ludźmi lub jednostkami reprezentowanymi przez te tożsamości.

Rysunek 2 przedstawia dane przechowywane w domenie EIM. Dane te zawierają identyfikatory EIM, definicje rejestrów EIM i powiązania EIM. Dane EIM definiują relacje między tożsamościami użytkowników a osobami lub jednostkami reprezentowanymi w przedsiębiorstwie przez te tożsamości.



Rysunek 2. Domena EIM i dane w niej przechowywane

Do danych EIM należą:

Definicje rejestrów EIM

Każda tworzona definicja rejestru EIM reprezentuje rzeczywisty rejestr użytkowników (i zawarte w nim informacje o tożsamości użytkowników), który istnieje w systemie przedsiębiorstwa. Po zdefiniowaniu w EIM konkretnego rejestru użytkowników, rejestr ten może należeć do domeny EIM. Można utworzyć dwa rodzaje definicji rejestru, jeden rodzaj odnosi się do rejestrów użytkowników systemu, drugi do rejestrów użytkowników aplikacji.

Identyfikatory EIM

Każdy tworzony identyfikator EIM jednoznacznie reprezentuje w przedsiębiorstwie osobę lub jednostkę (taką jak serwer wydruków lub serwer plików). Identyfikator EIM można utworzyć, jeśli chcemy mieć odwzorowanie typu jeden-do-jednego między tożsamościami użytkownika należącymi do osoby lub jednostki, którym odpowiada identyfikator EIM.

Powiązania EIM

Tworzone powiązania EIM reprezentują relacje między tożsamościami użytkownika. Należy zdefiniować powiązania, aby klienci EIM mogli używać funkcji API EIM do pomyślnego wykonywania operacji wyszukiwania EIM. Operacje te przeszukują domenę EIM pod kątem zdefiniowanych powiązań. Istnieją dwa różne rodzaje powiązań, które można utworzyć:

Powiązania identyfikatorów

Powiązania identyfikatora umożliwiają zdefiniowanie relacji typu jeden-do-jednego między tożsamościami użytkownika za pomocą identyfikatora EIM zdefiniowanego dla pojedynczej tożsamości. Każde tworzone powiązanie identyfikatora EIM reprezentuje pojedynczą, określoną relację między identyfikatorem EIM i powiązaną tożsamością użytkownika w przedsiębiorstwie. Powiązania identyfikatorów udostępniają informacje wiążące identyfikator EIM z określoną tożsamością użytkownika w określonym rejestrze użytkowników i umożliwiają utworzenie odwzorowania tożsamości typu jeden-do-jednego dla użytkownika. Powiązania identyfikatorów są przydatne szczególnie wtedy, gdy pojedyncze osoby mają tożsamości użytkownika z uprawnieniami specjalnymi i innymi uprawnieniami, które chcemy kontrolować przez utworzenie odwzorowań typu jeden-do-jednego między ich tożsamościami użytkownika.

Powiązania strategii

Powiązania strategii umożliwiają zdefiniowanie relacji między grupą tożsamości użytkownika w jednym lub większej liczbie rejestrów użytkowników a pojedynczą tożsamością użytkownika w innym rejestrze użytkowników. Każde utworzone powiązanie strategii powoduje powstanie odwzorowań typu wiele-do-jednego między źródłową grupą tożsamości użytkownika w jednym rejestrze użytkowników a pojedynczą tożsamością użytkownika docelowego. Zazwyczaj tworzone są powiązania strategii w celu odwzorowania grupy użytkowników, którzy potrzebują takiego samego poziomu autoryzacji, na pojedynczą tożsamość użytkownika z tym poziomem autoryzacji.

Pojęcia pokrewne

"Definicje rejestrów EIM" na stronie 12
Informacje opisujące sposób tworzenia definicji rejestru, zawierającej wszystkie rejestry użytkowników w systemie.

"Identyfikator EIM"
Informacje opisujące sposób tworzenia identyfikatorów użytkownika lub jednostki w przedsiębiorstwie.

"Operacje wyszukiwania EIM" na stronie 27
Informacje objaśniające proces odwzorowania EIM i wyświetlania przykładów.

Identyfikator EIM

Informacje opisujące sposób tworzenia identyfikatorów użytkownika lub jednostki w przedsiębiorstwie.

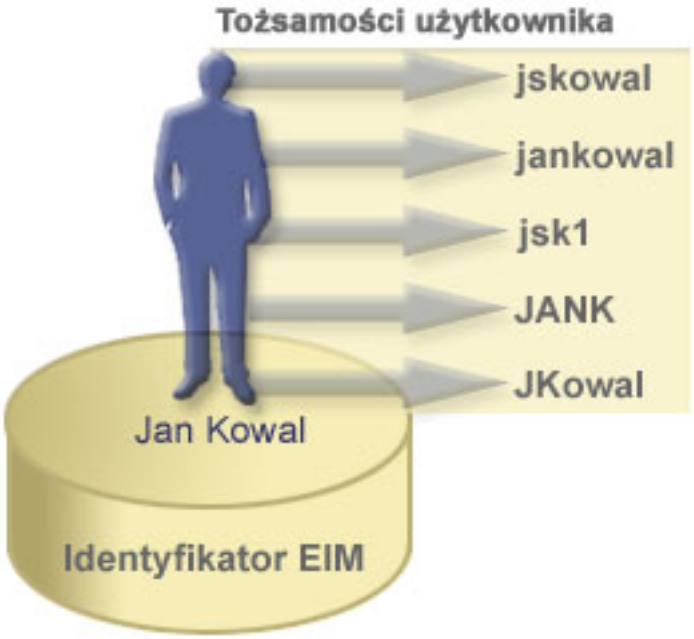
Identyfikator EIM reprezentuje osobę lub jednostkę w przedsiębiorstwie. Typowa sieć składa się z różnych platform sprzętowych oraz aplikacji i powiązanych z nimi rejestrów użytkowników. W większości platform i w wielu aplikacjach używane są rejestry użytkowników specyficzne dla danej platformy lub aplikacji. Rejestry te zawierają wszystkie informacje identyfikujące użytkowników, którzy pracują z danymi serwerami lub aplikacjami.

Odwzorowań EIM można użyć do utworzenia unikalnych identyfikatorów EIM dla ludzi lub jednostek w przedsiębiorstwie. Następnie można utworzyć powiązania identyfikatorów lub odwzorowania tożsamości jeden-do-jednego między identyfikatorem EIM a różnymi tożsamościami użytkownika dla danej osoby lub jednostki reprezentowanej przez ten identyfikator EIM. Proces ten ułatwia tworzenie heterogenicznych, wielowarstwowych aplikacji. Ponadto łatwiej jest wtedy tworzyć narzędzia i używać ich po to, aby uprościć administrowanie związane z zarządzaniem wszystkimi tożsamościami użytkownika, które dana osoba lub jednostka ma w przedsiębiorstwie.

Identyfikator EIM reprezentujący osobę

Rysunek 3 przedstawia przykładowy identyfikator EIM reprezentujący osobę *Jan Kowalski* i jego różne tożsamości w przedsiębiorstwie. W tym przykładzie *Jan Kowalski* ma pięć tożsamości: jankowalski, jsk1, JANK, jskowalski i JKowalski.

Rysunek 3: Relacja między identyfikatorem EIM użytkownika *Jan Kowalski* a jego różnymi tożsamościami

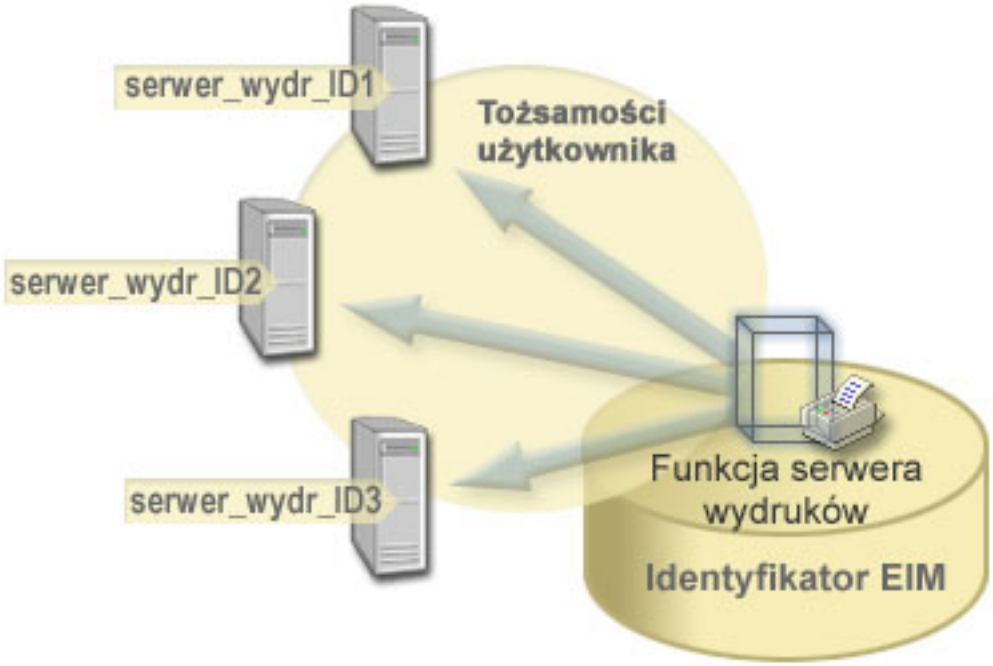


W EIM można tworzyć powiązania definiujące relacje między identyfikatorem Jan Kowalski a każdą z jego różnych tożsamości. Tworząc takie powiązania w celu zdefiniowania relacji, użytkownicy mogą pisać aplikacje używające funkcji API EIM do wyszukania potrzebnej, ale nieznanej tożsamości użytkownika w oparciu o jego znaną tożsamość.

Identyfikator EIM reprezentujący jednostkę

Oprócz reprezentowania osób identyfikatory EIM mogą także reprezentować jednostki w przedsiębiorstwie, co ilustruje rysunek 4. Na przykład w przedsiębiorstwie funkcja serwera wydruków jest często uruchamiana w wielu systemach. Na rysunku 4 funkcja serwera wydruków w przedsiębiorstwie jest uruchamiana pod trzema różnymi tożsamościami: serwer_wydr_ID1, serwer_wydr_ID2 i serwer_wydr_ID3.

Rysunek 4: Relacja między identyfikatorem EIM reprezentującym funkcję serwera wydruków a różnymi tożsamościami użytkowników dla tej funkcji



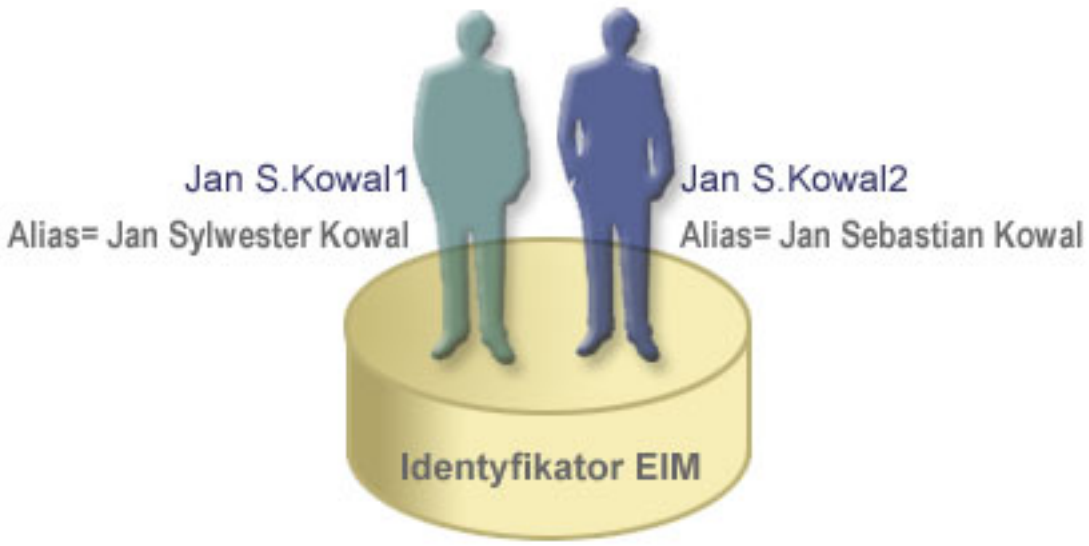
Za pomocą EIM można utworzyć jeden identyfikator reprezentujący funkcję serwera wydruków w całym przedsiębiorstwie. W pokazanym przykładzie identyfikator EIM Funkcja serwera wydruków reprezentuje rzeczywisty serwer wydruków w przedsiębiorstwie. Powiązania tworzy się w celu zdefiniowania relacji między identyfikatorem EIM (Funkcja serwera wydruków) a poszczególnymi tożsamościami użytkowników dla tej funkcji (serwer_wydr_ID1, serwer_wydr_ID2 i serwer_wydr_ID3). Powiązania te umożliwiają programistom aplikacji używanie operacji wyszukiwania EIM w celu znalezienia konkretnej funkcji serwera wydruków. Dostawcy aplikacji mogą tworzyć rozproszone aplikacje w prostszy sposób zarządzające funkcją serwera wydruków w przedsiębiorstwie.

Identyfikatory EIM a używanie aliasów

Nazwy identyfikatorów EIM muszą być unikalne w domenie EIM. Stosowanie aliasów bywa pomocne w sytuacji, gdy używanie unikalnych nazw identyfikatorów może być utrudnione. Identyfikatory EIM mogą być na przykład pomocne w sytuacji, gdy czyjaś nazwa formalna jest inna niż nazwa, pod jaką dana osoba jest znana. Na przykład różne osoby w przedsiębiorstwie mogą współużytkować tę samą nazwę, co może być mylące, jeśli jako identyfikatorów EIM używa się nazw własnych.

Rysunek 5 ilustruje sytuację, gdy w przedsiębiorstwie znajdują się dwaj użytkownicy *Jan S.Kowalski*. Administrator EIM tworzy dwa różne identyfikatory, aby można było ich rozróżnić: Jan S.Kowalski1 i Jan S.Kowalski2. Jednak stwierdzenie, który użytkownik *Jan S.Kowalski* jest reprezentowany przez który z tych identyfikatorów nie jest wcale oczywiste.

Rysunek 5: Aliasy dla dwóch identyfikatorów EIM w oparciu o współużytkowaną nazwę własną *Jan S.Kowalski*



Używając aliasów, administrator EIM może dostarczyć dla każdego identyfikatora EIM dodatkowe informacje na temat poszczególnych osób. Każdy identyfikator EIM może mieć wiele aliasów służących do określenia, którego użytkownika *Jan S. Kowalski* ten identyfikator reprezentuje. Dodatkowe aliasy mogą na przykład zawierać numery pracowników przypisane poszczególnym użytkownikom, numer wydziału, stanowisko lub inny wyróżniający atrybut. W tym przykładzie alias dla użytkownika Jan S.Kowalski1 może mieć postać Jan Sebastian Kowalski, a alias dla użytkownika Jan S.Kowalski2 może mieć postać Jan Sylwester Kowalski.

Informacje aliasu mogą być pomocne przy znajdowaniu określonego identyfikatora EIM. Na przykład aplikacja używająca EIM może określić alias używany do znajdowania odpowiedniego identyfikatora EIM dla aplikacji. Administrator może dodać ten alias do identyfikatora EIM, aby aplikacja mogła używać aliasu zamiast unikalnej nazwy identyfikatora do operacji EIM. Aplikacja może podać te dane, gdy korzysta z funkcji API Get EIM Target Identities from the Identifier (eimGetTargetFromIdentifier()) do wykonania operacji wyszukania EIM przy znajdowaniu potrzebnej tożsamości użytkownika.

Pojęcia pokrewne

"Domena EIM" na stronie 7
Informacje objaśniające sposób użycia domeny do składowania wszystkich identyfikatorów.

Definicje rejestrów EIM

Informacje opisujące sposób tworzenia definicji rejestru, zawierającej wszystkie rejestry użytkowników w systemie.

Definicja rejestru produktu EIM po pozycja w EIM utworzona do reprezentowania rzeczywistego rejestru użytkowników istniejącego w systemie w przedsiębiorstwie. Rejestr użytkowników działa jako katalog i zawiera listę poprawnych tożsamości użytkowników dla konkretnego systemu lub aplikacji. Podstawowy rejestr użytkowników zawiera tożsamości użytkowników i hasła. Przykładem rejestru użytkowników jest rejestr z/OS Security Server Resource Access Control Facility (RACF). Rejestry użytkowników mogą także zawierać inne informacje. Na przykład katalog LDAP zawiera nazwy wyróżniające powiązań, hasła i prawa dostępu do danych przechowywanych w katalogu LDAP. Innym przykładem często stosowanych rejestrów są nazwy użytkowników w domenie Kerberos lub tożsamości użytkowników w domenie Windows Active Directory a także rejestr profili użytkowników systemu i5/OS.

Można także zdefiniować rejestry użytkowników istniejące w innych rejestrach użytkowników. Niektóre aplikacje używają podzbioru tożsamości użytkownika w jednej instancji rejestru użytkowników. Na przykład rejestr z/OS Security Server (RACF) może zawierać konkretne rejestry użytkowników będące podzbiorem użytkowników w ogólnym rejestrze użytkowników the overall RACF.

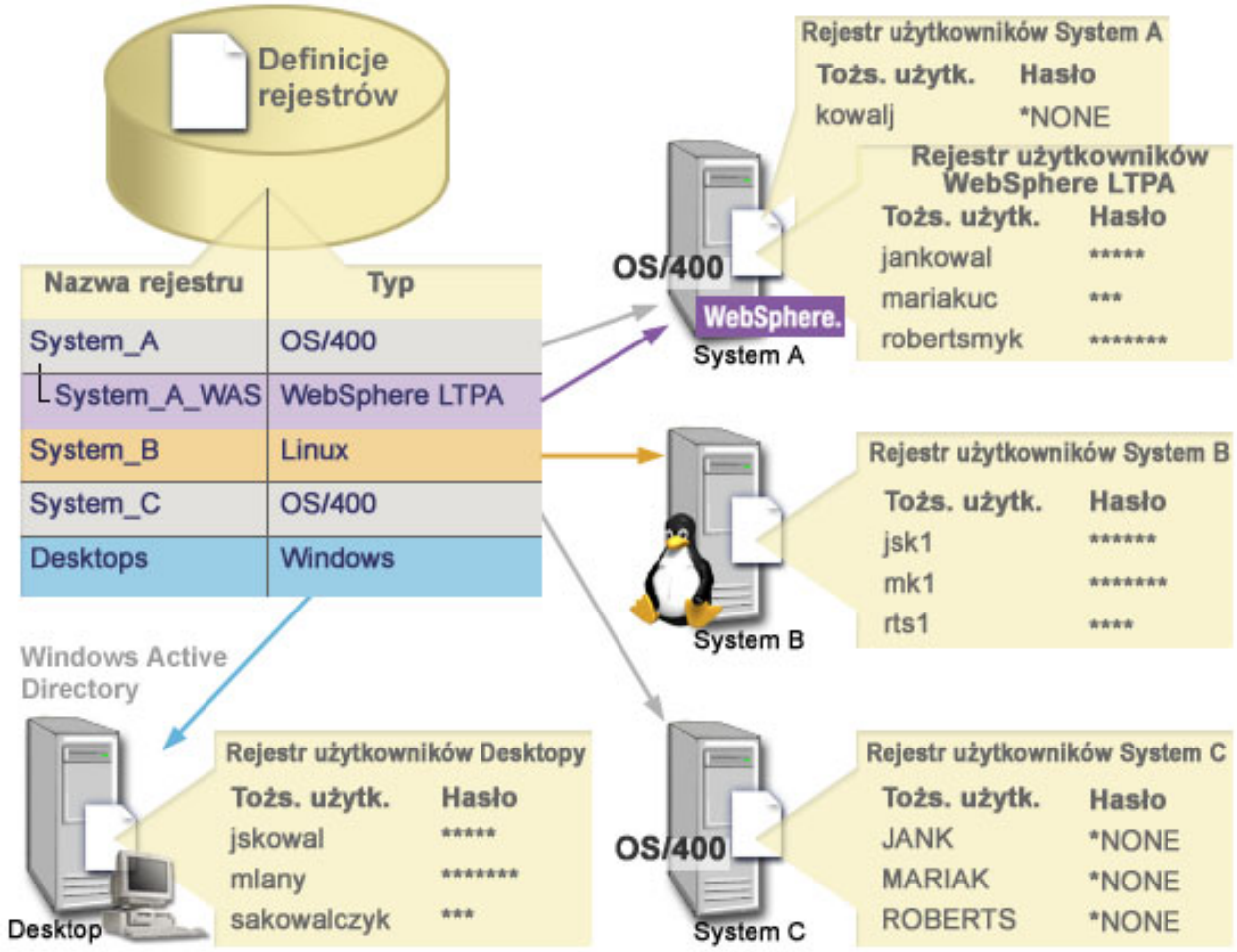
Definicje rejestrów EIM zawierają informacje dotyczące rejestrów użytkowników w przedsiębiorstwie. Administrator definiuje te rejestry w EIM, dostarczając następujące informacje:

- Unikalna, arbitralna nazwa rejestru EIM. Każda definicja rejestru reprezentuje konkretną instancję rejestru użytkowników. Dlatego należy wybrać nazwę definicji rejestru EIM, która będzie pomocna podczas identyfikowania konkretnej instancji rejestru użytkowników. Na przykład jako nazwę rejestru użytkowników można wybrać nazwę hosta TCP/IP lub nazwę hosta połączoną z nazwą aplikacji w przypadku rejestru użytkowników aplikacji. Podczas tworzenia unikalnych nazw definicji rejestrów EIM można używać dowolnej kombinacji znaków alfanumerycznych, liter o dowolnej wielkości oraz spacji.
- Typ rejestru użytkowników. Istnieje wiele predefiniowanych typów rejestrów użytkowników udostępnianych przez EIM dla większości rejestrów użytkowników systemów operacyjnych. Obejmują one:
  - System AIX
  - Domino - długie nazwy
  - Domino - krótkie nazwy
  - Kerberos
  - Kerberos - rozróżnianie wielkości liter
  - LDAP
  - - LDAP - krótka nazwa
  - Linux
  - Novell Directory Server
  - - Inny
  - - Inny - rozróżnianie wielkości liter
  - i5/OS (lub OS/400)
  - Tivoli Access Manager
  - RACF
  - Windows - lokalny
  - Domena Windows (Kerberos) (w tym typie rozróżniana jest wielkość liter.)
  - X.509

Uwaga: Wprawdzie udostępnione są predefiniowane typy definicji rejestrów dla większości rejestrów użytkowników systemu operacyjnego, jednak może zaistnieć potrzeba utworzenia definicji rejestru, dla którego EIM nie zawiera takiego typu definicji. W takim przypadku są dwie możliwości. Można użyć istniejącej definicji rejestru, która jest zgodna z charakterystyką danego rejestru użytkowników lub zdefiniować prywatny typ rejestru użytkowników. W przykładzie przedstawionym na rysunku 6 administrator zdefiniował typ rejestru jako WebSphere LTPA dla definicji rejestru System_A_WAS.

Na rysunku 6 administrator utworzył definicje rejestrów systemu EIM dla rejestrów użytkowników reprezentujących system A, system B, system C i Windows Active Directory, zawierający nazwy użytkowników Kerberos, których używają użytkownicy przy logowaniu na swoich stacjach roboczych. Dodatkowo administrator utworzył definicję rejestru aplikacji dla uwierzytelniania WebSphere (R) Lightweight Third-Party Authentication (LTPA), działającego w systemie A. Nazwa definicji rejestru używana przez administratora pomaga zidentyfikować konkretny rejestr użytkowników. Na przykład adres IP lub nazwa hosta często całkowicie wystarczają wielu typom rejestrów użytkowników. W przykładzie tym administrator użył System_A_WAS jako nazwy definicji rejestru aplikacji do identyfikowania tej specyficznej instancji aplikacji WebSphere LTPA. Określił również, że nadrzędnym rejestrem systemu dla definicji rejestru aplikacji jest rejestr System_A.

Rysunek 6: Definicje rejestrów EIM dla pięciu rejestrów użytkowników w przedsiębiorstwie



Uwaga: Aby ograniczyć zarządzanie hasłami użytkowników, administrator na rysunku 6 ustawił hasła profili użytkowników systemu i5/OS w systemach A i C na *NONE. W tym przypadku administrator konfiguruje środowisko pojedynczego logowania i jedyną aplikacją, z którą pracują użytkownicy jest aplikacja z obsługą EIM, taka jak program iSeries Navigator. Dlatego administrator chce usunąć hasła ze swoich profili użytkowników i5/OS, aby zarówno użytkownicy, jak i administrator, mieli mniej haseł, którymi trzeba zarządzać.

Pojęcia pokrewne

"Domena EIM" na stronie 7
Informacje objaśniające sposób użycia domeny do składowania wszystkich identyfikatorów.

Definicje rejestrów systemu

Inne zasoby i informacje związane z używaniem produktu EIM.

Definicja rejestru systemu to pozycja tworzona w EIM do reprezentowania i opisania różnych rejestrów użytkowników stacji roboczej lub serwera. Definicję rejestru systemu EIM można utworzyć dla rejestru użytkowników, jeśli rejestry w przedsiębiorstwie mają następujące cechy:

- Rejestr jest dostarczany przez system operacyjny, taki jak AIX lub i5/OS albo produkt zarządzania ochroną, taki jak z/OS Security Server Resource Access Control Facility (RACF).
- Rejestr zawiera tożsamości użytkowników, które są unikalne dla konkretnej aplikacji, takiej jak Lotus Notes.
- Rejestr zawiera rozproszone tożsamości użytkowników, takie jak nazwy użytkowników protokołu Kerberos lub nazwy wyróżniające LDAP.

Operacje wyszukiwania EIM są wykonywane poprawnie bez względu na to, czy administrator EIM zdefiniuje rejestr jako rejestr systemu czy też aplikacji. Jednak oddzielne definicje rejestrów umożliwiają zarządzanie danymi odwzorowywania w oparciu o aplikację. Za zarządzanie odwzorowaniami specyficznymi dla aplikacji może być odpowiedzialny administrator danego rejestru.

Definicje rejestrów aplikacji

Informacje ułatwiające tworzenie rejestrów użytkowników dla niektórych aplikacji.

Definicja rejestrów aplikacji jest pozycją w produkcie EIM utworzoną, aby opisywać i reprezentować podzbiór identyfikatorów użytkowników zdefiniowanych w rejestrze systemowym. Tożsamości te współużytkują wspólny zbiór atrybutów lub cech, które umożliwiają im korzystanie z konkretnej aplikacji lub zbioru aplikacji. Definicje rejestrów aplikacji reprezentują rejestry użytkowników istniejące w innych rejestrach użytkowników. Na przykład rejestr z/OS Security Server (RACF) może zawierać konkretne rejestry użytkowników będące podzbiorem użytkowników w ogólnym rejestrze użytkowników the overall RACF. Z uwagi na tę relację należy podać nazwę nadrzędnego rejestru systemu dla każdej tworzonej definicji rejestru aplikacji.

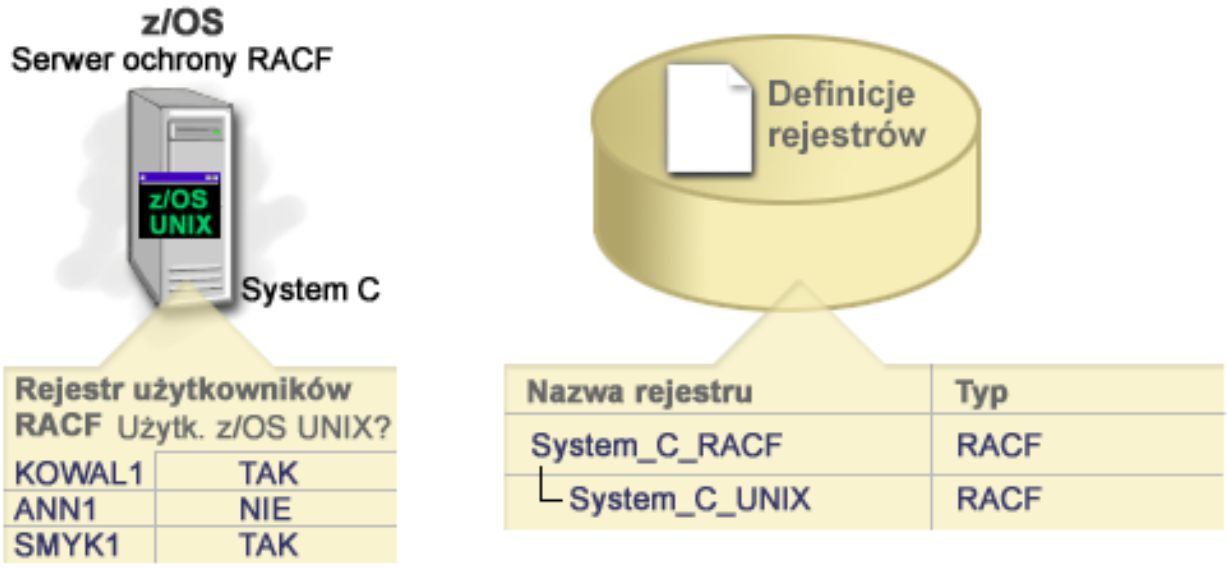
Definicję rejestru aplikacji EIM dla rejestru użytkowników można utworzyć wtedy, gdy tożsamości użytkowników w rejestrze mają następujące cechy:

- tożsamości użytkowników dla aplikacji nie są przechowywane w rejestrze użytkowników specyficznym dla aplikacji,
- tożsamości użytkowników dla aplikacji są przechowywane w rejestrze systemu zawierającym tożsamości użytkowników dla innych aplikacji.

Operacje wyszukiwania EIM są wykonywane poprawnie bez względu na to, czy administrator EIM utworzy definicje rejestru aplikacji lub systemu dla rejestru użytkowników. Jednak oddzielne definicje rejestrów umożliwiają zarządzanie danymi odwzorowywania w oparciu o aplikację. Za zarządzanie odwzorowaniami specyficznymi dla aplikacji może być odpowiedzialny administrator danego rejestru.

Na przykład rysunek 7 przedstawia, w jaki sposób administrator EIM utworzył definicję rejestru systemu do reprezentowania rejestru z/OS Security Server RACF. Administrator utworzył także definicję rejestru aplikacji do reprezentowania tożsamości użytkowników w rejestrze RACF, który używa oprogramowania z/OS(TM) UNIX System Services (z/OS UNIX). System C zawiera rejestr użytkowników RACF, w którym znajdują się informacje dotyczące trzech tożsamości użytkowników: KOWALSKI1, ANN1 i SMYK1. Dwie z tych tożsamości (KOWALSKI1 i SMYK1) uzyskują dostęp do oprogramowania z/OS UNIX w systemie C. Tożsamości te są w rzeczywistości użytkownikami RACF z unikalnymi atrybutami, które identyfikują ich jako użytkowników z/OS UNIX. W definicjach rejestrów EIM administrator EIM zdefiniował System_C_RACF do reprezentowania ogólnego rejestru użytkowników RACF. Administrator ten ponadto zdefiniował System_C_UNIX do reprezentowania tożsamości użytkowników, które mają atrybuty z/OS UNIX.

Rysunek 7: Definicje rejestrów EIM dla rejestru użytkowników RACF i użytkowników systemu z/OS UNIX



Definicje rejestrów grupowych

Informacje związane z tworzeniem w domenach EIM definicji rejestrów grupowych, opisujących i reprezentujących grupę definicji rejestrów.

Logiczne pogrupowanie definicji rejestrów umożliwia zmniejszenie ilości pracy niezbędnej do skonfigurowania odwzorowania EIM. Definicją rejestru grupowego można zarządzać tak, jak definicją pojedynczego rejestru.

Wszystkie elementy definicji rejestru grupowego zawierają zazwyczaj jedną lub wiele wspólnych tożsamości, z którą można utworzyć powiązanie docelowe lub źródłowe. Pogrupowanie elementów umożliwia utworzenie jednego, zamiast wielu, powiązań między definicja rejestru grupowego, tożsamością użytkownika.

Na przykład Jan Kowalski loguje się w swoim podstawowym systemie przy użyciu tożsamości użytkownika jkowalski i używa tej samej tożsamości, JANK, w wielu systemach. Rejestry użytkowników we wszystkich tych systemach zawierają więc tożsamość użytkownika JANK. Z reguły Jan Kowalski musiałby utworzyć osobne docelowe powiązania między identyfikatorem EIM Jan Kowalski, a każdym z rejestrów użytkowników zawierających tożsamość JANK. Aby zmniejszyć ilość pracy potrzebnej do skonfigurowania odwzorowania EIM, może on utworzyć jedną definicję rejestru grupowego, zawierającą wszystkie rejestry użytkowników, których elementem jest tożsamość JANK. Może następnie utworzyć jedno docelowe powiązanie między identyfikatorem EIM Jan Kowalski, a definicją rejestru grupowego, zamiast wielu powiązań między identyfikatorem EIM, a poszczególnymi definicjami rejestrów. Powiązanie docelowe definicji rejestru grupowego umożliwia mu używanie tożsamości użytkownika jkowalski do odwzorowania tożsamości użytkownika JANK.

Należy zapoznać się z następującymi informacjami:

- Wszystkie elementy (definicje poszczególnych rejestrów) definicji rejestru grupowego muszą mieć ten sam status rozróżniania wielkości znaków.
- Wszystkie elementy (definicje poszczególnych rejestrów) definicji rejestru grupowego muszą być zdefiniowane w domenie EIM, zanim możliwe będzie dodanie ich do definicji rejestru grupowego.
- Definicja rejestru może być elementem jednej lub wielu grup, ale należy unikać określania pojedynczego rejestru użytkowników jako elementu wielu definicji rejestrów grupowych, ponieważ może to skutkować niejednoznacznymi wynikami operacji wyszukiwania. Definicja rejestru grupowego nie może być elementem innej definicji rejestru grupowego.

Powiązania EIM

Informacje objaśniające sposób użycia powiązanych tożsamości w różnych rejestrach użytkowników.

Powiązanie EIM jest pozycją utworzoną w domenie EIM w celu zdefiniowania relacji między tożsamościami użytkowników w różnych rejestrach użytkowników. Rodzaj utworzonego powiązania określa, czy zdefiniowana relacja jest bezpośrednia, czy pośrednia. W odwzorowaniach EIM można utworzyć jeden z dwóch rodzajów powiązań: powiązania identyfikatorów i powiązania strategii. Powiązań strategii można używać zamiast powiązań identyfikatorów lub w połączeniu z nimi. Sposób wykorzystania powiązań zależy od ogólnego planu implementacji EIM.

Aby uzyskać więcej informacji na temat pracy z powiązaniami, przejrzyj następujące sekcje:

Dane wyszukiwania

Informacje o tym, jak używać tych danych opcjonalnych do identyfikacji tożsamości użytkownika docelowego; funkcje API EIM mogą ich używać podczas operacji wyszukiwania odwzorowań do dopracowania wyszukiwania tożsamości użytkownika docelowego, będącego obiektem działania.

Można podać *opcjonalne* dane zwane danymi wyszukiwania, aby precyzyjniej zidentyfikować użytkownika docelowego. Tożsamość użytkownika docelowego może być podana albo w powiązaniu identyfikatora, albo w powiązaniu strategii. Dane wyszukiwania to unikalny łańcuch znaków, którego funkcja API EIM eimGetTargetFromSource lub eimGetTargetFromIdentifier może używać podczas wykonywania operacji wyszukiwania do dokładniejszego wyszukania tożsamości użytkownika docelowego, która jest obiektem operacji. Dane podane dla operacji wyszukiwania odpowiadają parametrowi informacji dodatkowych użytkowników w rejestrze dla tych funkcji API EIM.

Dane wyszukiwania są potrzebne tylko jeśli operacja wyszukiwania odwzorowania może zwrócić więcej niż jedną tożsamość użytkownika docelowego. Zdarza się tak, gdy wystąpi któraś z poniżej wymienionych sytuacji:

- Identyfikator EIM ma wiele pojedynczych powiązań docelowych do tego samego rejestru docelowego.
- Więcej niż jeden identyfikator EIM ma pewną tożsamość użytkownika podaną w powiązaniu źródłowym i każdy z tych identyfikatorów EIM ma powiązanie docelowe do tego samego rejestru docelowego, jednak tożsamości użytkowników podane dla każdego powiązania docelowego mogą być różne.
- Więcej niż jedno powiązanie strategii domeny domyślnej określa dany rejestr docelowy.
- Więcej niż jedno powiązanie strategii rejestru domyślnego określa dany rejestr źródłowy i rejestr docelowy.
- Więcej niż jedno powiązanie strategii filtrów certyfikatów określa dany rejestr źródłowy X.509, filtr certyfikatu i rejestr docelowy.

Uwaga: Sytuacja taka może stanowić problem dla aplikacji z obsługą EIM, w tym aplikacji i produktów systemu i5/OS, które nie potrafią obsłużyć takich wyników. Jednakże podstawowe aplikacje systemu i5/OS, takie jak iSeries Access for Windows, nie używają danych wyszukiwania do rozróżnienia między wieloma tożsamościami użytkowników docelowych zwracanych przez operację wyszukiwania. Dlatego też należy rozważyć ponowne zdefiniowanie powiązań dla domeny, aby zapewnić, że operacja wyszukiwania odwzorowań będzie mogła zwrócić pojedynczą tożsamość użytkownika docelowego i że podstawowe aplikacje systemu i5/OS będą mogły pomyślnie wykonywać operacje wyszukiwania i odwzorować tożsamości.

Danych wyszukiwania można użyć, aby uniknąć sytuacji, w których może się zdarzyć, że operacja wyszukiwania odwzorowania zwróci więcej niż jedną tożsamość użytkownika docelowego. Aby temu zapobiec, należy zdefiniować unikalne dane wyszukiwania dla każdej tożsamości użytkownika docelowego w każdym powiązaniu. Dane te muszą być udostępnione operacji wyszukiwania odwzorowań, aby zapewnić, że zwróci ona tylko jedną unikalną tożsamość użytkownika docelowego. W przeciwnym przypadku aplikacje polegające na odwzorowaniu EIM nie będą mogły określić, której dokładnie tożsamości docelowej mają użyć.

Na przykład weźmy identyfikator EIM o nazwie Jan Kowalski, który ma dwa profile użytkownika w systemie A. Jednym z tych profili użytkownika jest UŻYTKOWNIKJK, a drugim ADMINOCHRONYJK, który ma uprawnienia

specjalne administratora ochrony. Dla identyfikatora Jan Kowalski są dwa powiązania docelowe. Jedno z tych powiązań docelowych jest dla tożsamości użytkownika UŻYTKOWNIKJK w rejestrze docelowym System_A i z podanymi danymi wyszukiwania uprawnienia użytkownika. Drugie powiązanie jest dla tożsamości użytkownika ADMINOCHRONYJK w rejestrze docelowym System_A i z podanymi danymi wyszukiwania szef ochrony.

Jeśli w operacji wyszukiwania odwzorowania nie zostaną podane żadne dane wyszukiwania, zwróci ona obie tożsamości użytkownika, UŻYTKOWNIKJK i ADMINOCHRONYJK. Jeśli zostaną podane dane wyszukiwania uprawnienia użytkownika, operacja wyszukiwania zwróci tylko tożsamość UŻYTKOWNIKJK. Jeśli zostaną podane dane wyszukiwania szef ochrony, zwrócona zostanie tylko tożsamość użytkownika ADMINOCHRONYJK.

Uwaga: Jeśli zostanie usunięte ostatnie powiązanie docelowe dla tożsamości użytkownika (niezależnie, czy jest to powiązanie identyfikatora czy powiązanie strategii), tożsamość użytkownika docelowego i wszystkie dane wyszukiwania są usuwane z domeny.

Ponieważ powiązań strategii certyfikatu i innych powiązań można używać na wiele sposobów, często łącząc je ze sobą, przed utworzeniem powiązań strategii certyfikatu i korzystaniem z nich należy gruntownie zapoznać się z obsługą strategii odwzorowania EIM i działaniem operacji wyszukiwania.

Powiązania identyfikatorów

Informacje o tym, jak używać powiązań identyfikatorów do opisania relacji między identyfikatorem produktu EIM a tożsamościami użytkownika w rejestrach użytkowników reprezentującymi daną osobę. Powiązanie identyfikatora tworzy bezpośrednie odwzorowanie typu jeden-do-jednego między identyfikatorem EIM a daną tożsamością użytkownika. Powiązań identyfikatorów można użyć również do pośredniego zdefiniowania relacji między tożsamościami użytkowników za pomocą identyfikatora EIM.

Identyfikator EIM reprezentuje określoną osobę lub jednostkę w przedsiębiorstwie. Powiązanie identyfikatora EIM opisuje relację między identyfikatorem EIM i pojedynczą tożsamością użytkownika w rejestrze użytkowników, również reprezentującą tę osobę. Tworząc powiązania między identyfikatorem EIM i wszystkimi tożsamościami użytkownika danej osoby lub jednostki, w sposób jednoznaczny określa się, jak dana osoba lub jednostka będzie korzystała z zasobów w przedsiębiorstwie.

Tożsamości użytkownika mogą być używane do uwierzytelniania, autoryzacji lub obu tych operacji. *Uwierzytelnianie* jest procesem sprawdzania, czy jednostka lub osoba dostarczająca dowodu tożsamości użytkownika ma uprawnienie do korzystania z niej. Weryfikacji tej często dokonuje się poprzez zmuszenie osoby wysyłającej daną tożsamość użytkownika do podania tajnych lub prywatnych informacji powiązanych z tą tożsamością, takich jak na przykład hasło. *Autoryzacja* jest procesem upewniania się, że poprawnie uwierzytelniona tożsamość użytkownika może wykonywać tylko te funkcje lub uzyskiwać dostęp tylko do tych zasobów, do których danej tożsamości nadano uprawnienia. Dawniej prawie wszystkie aplikacje były zmuszone do używania tożsamości w pojedynczym rejestrze użytkowników zarówno dla uwierzytelniania, jak i dla autoryzacji. Obecnie wykorzystując operacje wyszukiwania EIM aplikacje mogą używać do uwierzytelniania tożsamości zebranych w jednym rejestrze, podczas gdy do autoryzacji mogą używać powiązanych tożsamości użytkowników z innego rejestru użytkowników.

Identyfikator EIM udostępnia pośrednie powiązanie między tymi tożsamościami użytkowników, co umożliwia aplikacjom wyszukanie innej tożsamości użytkownika dla identyfikatora EIM na podstawie znanej tożsamości użytkownika. EIM udostępnia funkcje API umożliwiające aplikacjom wyszukiwanie nieznanej tożsamości użytkownika w konkretnym (docelowym) rejestrze użytkowników poprzez dostarczenie znanej tożsamości użytkownika z innego (źródłowego) rejestru użytkowników. Proces ten jest nazywany odwzorowywaniem tożsamości.

W EIM administrator może zdefiniować trzy różne typy powiązań, aby opisać relacje między identyfikatorem EIM a tożsamością użytkownika. Powiązania identyfikatorów mogą należeć do jednego z następujących typów: źródłowe, docelowe lub administracyjne. W zależności od tego, jak używana jest tożsamość użytkownika, utworzony zostaje odpowiedni typ powiązania. Tworzymy na przykład powiązania źródłowe i docelowe dla tych tożsamości użytkowników, które mają brać udział w operacjach wyszukiwania odwzorowań. Zazwyczaj jeśli tożsamość użytkownika jest używana do uwierzytelniania, tworzone dla niej jest powiązanie źródłowe. Dla tożsamości użytkowników używanych do autoryzacji tworzone są powiązania docelowe.

Przed utworzeniem powiązania identyfikatora należy utworzyć odpowiedni identyfikator EIM i odpowiednią definicję rejestru EIM dla rejestru użytkowników zawierającego powiązaną tożsamość użytkownika. Powiązanie definiuje relację między identyfikatorem EIM a tożsamością użytkownika, przy czym wykorzystywane są następujące informacje:

- Nazwa identyfikatora EIM
- Nazwa tożsamości użytkownika
- Nazwa definicji rejestru EIM
- Typ powiązania
- Opcjonalnie: informacje wyszukiwania dla dalszego utożsamiania tożsamości użytkownika docelowego w powiązaniu docelowym.

Powiązanie źródłowe

Powiązanie źródłowe umożliwia użycie tożsamości użytkownika jako źródła w operacji wyszukiwania EIM w celu znalezienia innej tożsamości użytkownika, która jest powiązana z tym samym identyfikatorem EIM.

Jeśli tożsamość użytkownika jest używana do *uwierzytelniania*, powinna mieć powiązanie źródłowe z identyfikatorem EIM. Można na przykład utworzyć powiązanie źródłowe dla użytkownika Kerberos, gdyż ta postać tożsamości użytkownika jest używana do uwierzytelniania. Aby zapewnić poprawne działanie operacji wyszukiwania odwzorowania dla identyfikatorów EIM, dla pojedynczego identyfikatora EIM muszą być używane obydwa powiązania, źródłowe i docelowe.

Powiązanie docelowe

Powiązanie docelowe umożliwia zwrócenie tożsamości użytkownika w wyniku wykonania operacji wyszukiwania EIM. Tożsamości użytkowników reprezentujące użytkowników końcowych zwykle wymagają tylko powiązania docelowego.

Jeśli tożsamość użytkownika jest używana do *autoryzacji*, a nie do uwierzytelniania, z identyfikatorem EIM powinna mieć ona powiązanie docelowe. Można na przykład utworzyć powiązanie docelowe dla profilu użytkownika i5/OS, gdyż ta postać tożsamości użytkownika określa, jakie zasoby i uprawnienia ma ten użytkownik w konkretnym systemie iSeries. Aby zapewnić poprawne działanie operacji wyszukiwania odwzorowania dla identyfikatorów EIM, dla pojedynczego identyfikatora EIM muszą być używane obydwa powiązania, źródłowe i docelowe.

Relacja powiązania źródłowego i docelowego

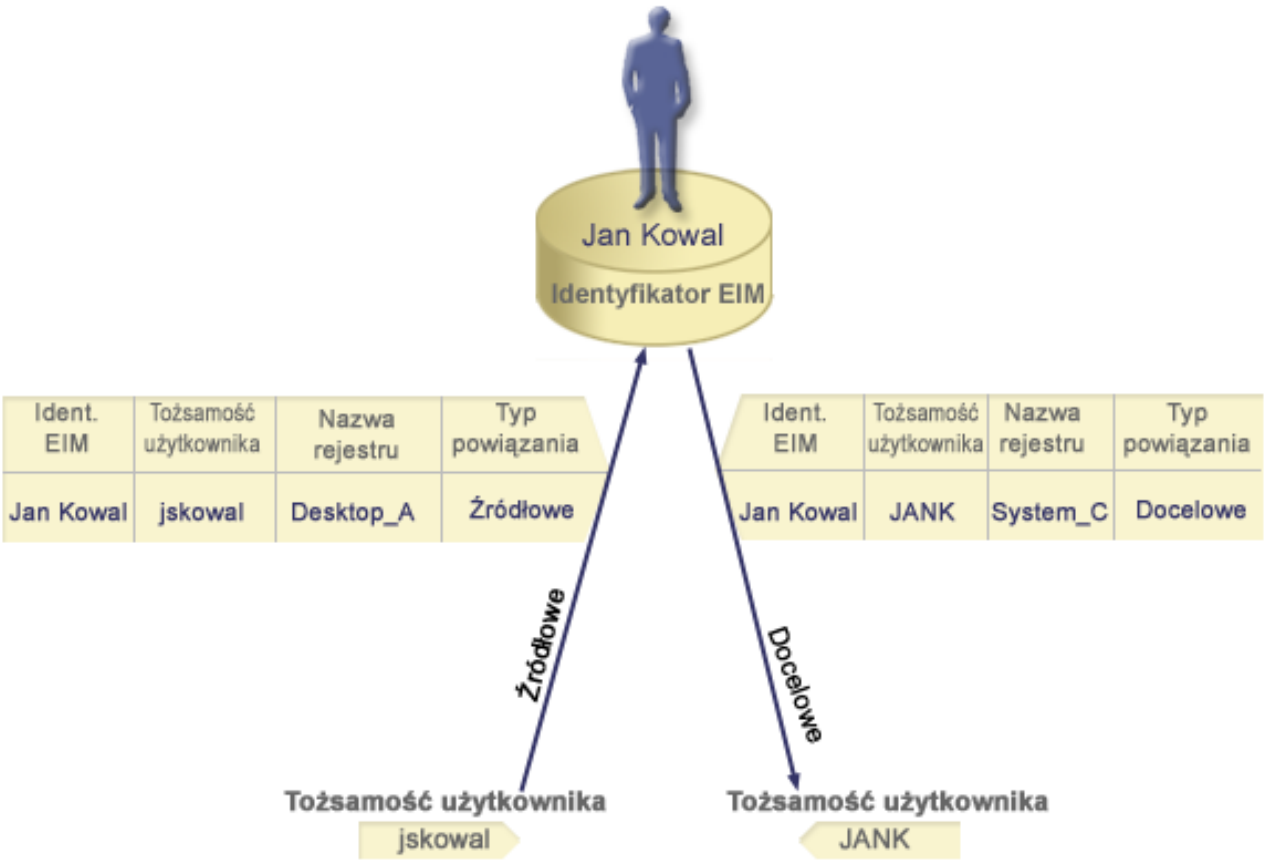
Aby zapewnić poprawne działanie operacji wyszukiwania odwzorowania, należy utworzyć przynajmniej jedno powiązanie źródłowe i jedno lub więcej powiązań docelowych dla pojedynczego identyfikatora EIM. Zazwyczaj tworzone jest powiązanie docelowe dla każdej tożsamości użytkownika w rejestrze użytkowników, którego dana osoba może używać do autoryzacji w systemie lub aplikacji odpowiadającej temu rejestrowi użytkowników.

Na przykład użytkownicy w przedsiębiorstwie zazwyczaj logują się i uwierzytelniają na pulpicie systemu Windows i uzyskują dostęp do serwera iSeries w celu wykonania zadań. Użytkownicy logują się na komputerach korzystając z nazwy użytkownika Kerberos, a na serwerze iSeries używając profilu użytkownika systemu i5/OS. Można utworzyć środowisko pojedynczego logowania, w którym użytkownicy uwierzytelniają się na komputerach używając nazwy użytkownika Kerberos i nie muszą ręcznie uwierzytelniać się na serwerze iSeries.

W tym celu należy utworzyć powiązanie źródłowe dla nazwy użytkownika Kerberos dla każdego użytkownika i jego identyfikatora EIM. Następnie należy utworzyć powiązanie docelowe dla profilu użytkownika i5/OS dla każdego użytkownika i jego identyfikatora EIM. Konfiguracja taka umożliwia systemowi i5/OS wykonywanie operacji wyszukiwania odwzorowań w celu określenia poprawnego profilu użytkownika potrzebnego użytkownikowi do dostępu do serwera iSeries po tym, jak uwierzytelnił się on na swoim komputerze. System i5/OS umożliwia następnie użytkownikowi dostęp do zasobów na serwerze w oparciu o odpowiedni profil użytkownika, nie wymagając od użytkownika ręcznego uwierzytelniania się na serwerze.

Rysunek 6 przedstawia inny przykład, w którym administrator EIM utworzył dwa powiązania, źródłowe i docelowe, dla identyfikatora EIM Jan Kowalski, aby zdefiniować relację między tym identyfikatorem, a dwiema powiązanymi tożsamościami użytkownika. Administrator utworzył powiązanie źródłowe dla nazwy użytkownika Kerberos jskowalski w rejestrze użytkowników Desktopy. Utworzył on także powiązanie docelowe dla profilu użytkownika systemu i5/OS JANK w rejestrze użytkowników System_C. Powiązania te umożliwiają aplikacjom uzyskanie nieznanej tożsamości użytkownika (docelowa: JANK) w oparciu o znaną tożsamość użytkownika (źródłowa: jskowalski) po wykonaniu operacji wyszukiwania EIM.

Rysunek 6: Powiązania docelowe i źródłowe dla identyfikatora EIM Jan Kowalski



Można następnie założyć, że administrator produktu EIM zdaje sobie sprawę, że Jan Kowalski używa profilu systemu i5/OS, jk1, w pięciu różnych systemach. W tej sytuacji administrator musi utworzyć sześć powiązań z identyfikatorem EIM Jan Kowalski, aby zdefiniować zależność między identyfikatorem i powiązaną tożsamością użytkownika w pięciu rejestrach użytkownika: powiązanie źródłowe dla nazwy użytkownika protokołu Kerberos jankowalski, w rejestrze użytkowników Pulpit_A oraz pięć powiązań docelowych dla profilu jsd1 systemui5/OS w pięciu rejestrach użytkowników: System_B, System_C, System_D, System_E i System_F. Aby zmniejszyć ilość pracy, którą musi wykonać w celu skonfigurowania odwzorowania EIM, administrator EIM tworzy definicję rejestru grupowego. Elementami definicji są następujące nazwy definicji rejestrów: System_B, System_C, System_D, System_E i System_F. Grupując elementy, administrator może utworzyć pojedyncze powiązanie. Grupując elementy, administrator może utworzyć pojedyncze powiązanie docelowe z definicją rejestru grupowego zamiast tworzenia wielu powiązań z poszczególnymi definicjami rejestru. Powiązania źródłowe i docelowe umożliwiają aplikacjom pobranie nieznanej tożsamości użytkownika (docelowej jk1) w pięciu rejestrach użytkownika reprezentowanych jako elementy definicji rejestru grupowego na podstawie znanej tożsamości użytkownika (źródłowej jankowalski) przy wykonywaniu operacji wyszukiwania EIM.

Dla niektórych użytkowników konieczne może być utworzenie zarówno powiązania docelowego, jak i źródłowego, dla tej samej tożsamości użytkownika. Wymaga tego sytuacja, gdy jedna osoba używa jednego systemu zarówno jako klienta, jak i serwera lub gdy chodzi o osoby pełniące funkcje administratorów.

Uwaga: Tożsamości użytkowników reprezentujące zwyczajnych użytkowników zwykle wymagają tylko powiązania docelowego.

| Dla niektórych użytkowników konieczne może być utworzenie zarówno powiązania docelowego, jak i źródłowego, dla
| tej samej tożsamości użytkownika. Wymaga tego sytuacja, gdy jedna osoba używa jednego systemu zarówno jako
| klienta, jak i serwera lub gdy chodzi o osoby pełniące funkcje administratorów.

Na przykład administrator korzysta z funkcji Centrum Zarządzania w programie iSeries Navigator do zarządzania systemem centralnym i kilkoma systemami końcowymi. Wykonuje on różne funkcje i mogą one mieć początek w systemie centralnym lub w systemie końcowym. W takim przypadku należy utworzyć zarówno powiązanie źródłowe, jak i docelowe, dla każdej z tożsamości użytkownika administratora w każdym z systemów. Dzięki temu niezależnie od tego, z którego z systemów korzysta administrator do dostępu do innych systemów, jego tożsamość użytkownika użyta do dostępu do jednego systemu może być odwzorowana na odpowiednią tożsamość użytkownika w następnych systemach, do których potrzebuje on dostępu.

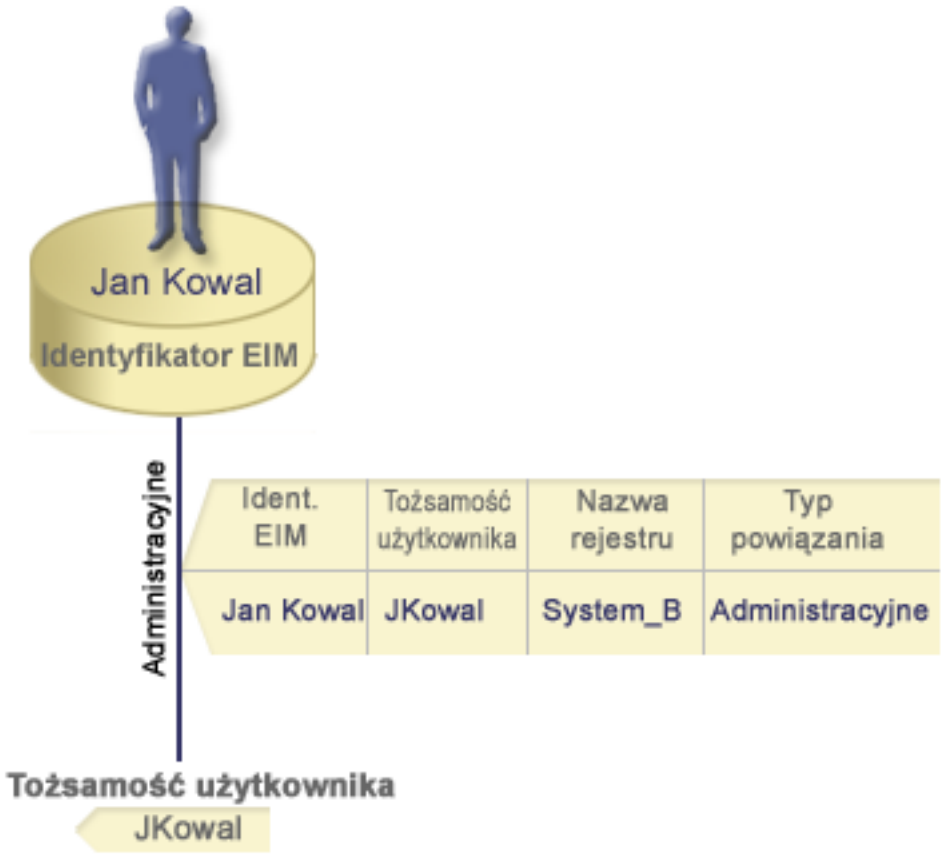
Powiązanie administracyjne

Powiązanie administracyjne z identyfikatorem EIM jest najczęściej stosowane, aby podkreślić, że osoba lub jednostka reprezentowana przez ten identyfikator EIM ma tożsamość użytkownika wymagającą szczególnej uwagi w podanym systemie. Tego typu powiązania można na przykład używać w rejestrach użytkowników objętych szczególną ochroną.

Z uwagi na swój szczególny charakter powiązania administracyjne nie mogą uczestniczyć w operacjach wyszukiwania odwzorowania EIM. Dlatego też operacja wyszukiwania EIM mająca dostarczyć źródłowej tożsamości użytkownika z powiązaniem administracyjnym nie zwraca żadnych rezultatów. Analogicznie tożsamość użytkownika z powiązaniem administracyjnym nigdy nie jest zwracana jako wynik działania operacji wyszukiwania EIM.

Rysunek 7 przedstawia przykład powiązania administracyjnego. W tym przykładzie pracownik Jan Kowalski ma jedną tożsamość użytkownika, Jan_Kowalski, w systemie A i drugą tożsamość, JKowalski, w systemie B, który jest systemem objętym najwyższą ochroną. Administrator systemu chce mieć pewność, że użytkownicy będą uwierzytelniani w systemie B tylko za pomocą lokalnego rejestru użytkowników znajdującego się w tym systemie. Administrator nie chce zezwolić na to, aby aplikacje uwierzytelniały użytkownika Jan Kowalski w systemie za pomocą innego mechanizmu uwierzytelniania. Używając powiązania administracyjnego dla tożsamości użytkownika JKowalski w systemie B, administrator EIM może stwierdzić, że Jan Kowalski ma konto w systemie B, ale EIM nie zwraca informacji na temat tożsamości JKowalski w wyniku wykonania operacji wyszukiwania EIM. Nawet jeśli w tym systemie istnieją aplikacje używające operacji wyszukiwania EIM, nie mogą one znaleźć tożsamości użytkowników, którzy mają powiązania administracyjne.

Rysunek 7: Powiązanie administracyjne EIM z identyfikatorem EIM Jan Kowalski



Powiązania strategii

Informacje o tym, jak używać powiązań strategii do opisania relacji między wieloma tożsamościami użytkownika a pojedynczą tożsamością użytkownika w rejestrze użytkowników.

Strategie odwzorowań EIM umożliwiają administratorowi EIM tworzenie powiązań strategii i zarządzanie nimi w celu definiowania relacji między wieloma tożsamościami użytkowników w jednym lub większej liczbie rejestrów użytkowników, a pojedynczą tożsamością użytkownika w innym rejestrze użytkowników. Powiązania strategii korzystają z obsługi strategii odwzorowania EIM do utworzenia odwzorowań wielu tożsamości użytkownika do jednej bez wymagania identyfikatora EIM. Można ich używać zamiast powiązań identyfikatorów udostępniających odwzorowanie między identyfikatorem EIM a pojedynczą tożsamością użytkownika lub w połączeniu z tymi powiązaniami.

Powiązanie strategii dotyczy tylko tych tożsamości użytkowników, dla których nie istnieje określone pojedyncze powiązanie EIM. Gdy między identyfikatorem EIM a tożsamościami użytkownika istnieje takie powiązanie, wtedy do aplikacji wykonującej operację wyszukiwania zostaje zwrócona tożsamość użytkownika docelowego z powiązania identyfikatora, nawet jeśli powiązanie strategii istnieje i jest włączone.

Można utworzyć trzy różne rodzaje powiązań strategii:

Pojęcia pokrewne

“Operacje wyszukiwania EIM” na stronie 27
Informacje objaśniające proces odwzorowania EIM i wyświetlania przykładów.

Domyślne powiązania strategii domeny:

Poniższe informacje objaśniają, jak ustanawiać relację odwzorowania dla wszystkich identyfikatorów użytkowników w domenie.

Domyślne powiązanie strategii domeny jest jednym z typów powiązań strategii, umożliwiających tworzenie odwzorowań wielu tożsamości użytkowników do jednej. Za pomocą domyślnego powiązania strategii domeny można odwzorować źródłowy zestaw wielu tożsamości użytkowników (w tym przypadku wszystkich użytkowników w domenie) na pojedynczą tożsamość użytkownika docelowego w określonym rejestrze użytkowników docelowych. W domyślnym powiązaniu strategii domeny wszyscy użytkownicy w jednej domenie są źródłem powiązania strategii i są odwzorowani na jeden rejestr docelowy i tożsamość użytkownika docelowego.

Aby użyć domyślnych powiązań strategii domeny, należy włączyć dla domeny wyszukiwanie odwzorowań za pomocą powiązań strategii. Należy również włączyć wyszukiwanie odwzorowań dla rejestru użytkowników docelowych powiązania strategii. Po odpowiednim skonfigurowaniu w operacjach wyszukiwania odwzorowania brane są pod uwagę rejestry użytkowników w powiązaniu strategii.

Domyślne powiązanie strategii domeny jest brane pod uwagę, jeśli operacja wyszukania odwzorowań nie znajdzie powiązań identyfikatorów, powiązań strategii filtrów certyfikatów ani domyślnych powiązań strategii rejestru dla rejestru docelowego. W wyniku tego wszystkie tożsamości użytkowników w domenie są odwzorowywane na pojedynczą tożsamość użytkownika docelowego zgodnie z domyślnym powiązaniem strategii domeny.

Na przykład tworzone jest domyślne powiązanie strategii domeny z tożsamością użytkownika docelowego Jan_Kowalski w rejestrze docelowym Rejestr_xyz i nie zostało utworzone żadne powiązanie identyfikatora ani inne powiązanie strategii do odwzorowania tej tożsamości użytkownika. Dlatego jeśli Rejestr_xyz został podany jako rejestr docelowy w operacjach wyszukiwania, domyślna strategia domeny zapewnia, że tożsamość użytkownika docelowego Jan_Kowalski zostanie zwrócona dla wszystkich tożsamości użytkowników w domenie, które nie mają zdefiniowanych żadnych innych powiązań.

Aby zdefiniować domyślne powiązanie strategii domeny, należy podać następujące dane:

- **Rejestr docelowy**. Podany rejestr docelowy jest to nazwa definicji rejestru EIM zawierająca tożsamości użytkowników, do których będą odwzorowane wszystkie tożsamości użytkowników w domenie.
- **Użytkownik docelowy**. Użytkownik docelowy jest to nazwa tożsamości użytkownika zwracana jako wynik operacji wyszukiwania odwzorowania EIM na podstawie tego powiązania strategii.

Można zdefiniować domyślne powiązanie strategii domeny dla każdego rejestru w domenie. Jeśli dwa lub więcej powiązań strategii domeny odnosi się do tego samego rejestru docelowego, trzeba zdefiniować unikalne dane wyszukiwania dla każdego z tych powiązań strategii, aby zapewnić ich rozróżnianie przez operacje wyszukiwania odwzorowań. W przeciwnym przypadku operacje wyszukiwania odwzorowań mogą zwrócić wiele tożsamości użytkowników docelowych. W wyniku tego aplikacje bazujące na odwzorowaniach EIM mogą nie być w stanie określić, której tożsamości użytkownika docelowego użyć.

Ponieważ powiązań strategii można używać na wiele sposobów, często łącząc je ze sobą, przed ich utworzeniem i korzystaniem z nich należy gruntownie zapoznać się z obsługą strategii odwzorowań EIM i działaniem operacji wyszukiwania.

Uwaga: Istnieje możliwość utworzenia powiązania domyślnej strategii domeny z docelową tożsamością użytkownika, istniejącą w definicji rejestru grupowego. Wszyscy użytkownicy w domenie są źródłem powiązania strategii. Są oni odwzorowywani na docelowe tożsamości użytkowników w docelowej definicji rejestru grupowego. Tożsamości użytkowników zdefiniowane w powiązaniu domyślnej strategii domeny istnieją w obrębie elementów definicji rejestru grupowego.

Na przykład Jan Kowalski używa tego samego profilu użytkownika systemui5/OS, Jan_Kowalski, w pięciu systemach: System B, System C, System D, System E i System F. Aby zmniejszyć ilość pracy, którą musi on wykonać, aby skonfigurować odwzorowanie EIM, administrator produktu EIM tworzy definicję rejestru grupowego o nazwie Grupa_1. Elementami definicji są następujące nazwy definicji rejestrów: System_B, System_C, System_D, System_E i System_F. Grupując elementy, administrator może utworzyć pojedyncze powiązanie docelowe z definicją rejestru grupowego zamiast tworzenia wielu powiązań z poszczególnymi definicjami rejestru.

Administrator produktu EIM tworzy domyślne powiązanie strategii domeny z tożsamością użytkownika docelowego Jan_Kowlaski w rejestrze docelowym Grupa_1. W tym przypadku nie występują żadne powiązania identyfikatora ani inne powiązania strategii. Dlatego jeśli rejestr Grupa_1 został podany jako rejestr docelowy w operacjach wyszukiwania, domyślna strategia domeny zapewnia, że tożsamość użytkownika docelowego Jan_Kowalski zostanie zwrócona dla wszystkich tożsamości użytkowników w domenie, które nie mają zdefiniowanych żadnych innych powiązań.

Domyślne powiązania strategii rejestru:

Poniższe informacje objaśniają, jak ustanawiać relację odwzorowania dla wszystkich identyfikatorów użytkowników w pojedynczym rejestrze.

Domyślne powiązanie strategii rejestru jest jednym z typów powiązań strategii, umożliwiających tworzenie odwzorowań wielu tożsamości użytkowników do jednej. Za pomocą domyślnego powiązania strategii rejestru można odwzorować źródłowy zestaw wielu tożsamości użytkowników (w tym przypadku tych w jednym rejestrze) na pojedynczą tożsamość użytkownika docelowego w określonym rejestrze użytkowników docelowych. W domyślnym powiązaniu strategii rejestru wszyscy użytkownicy w jednym rejestrze są źródłem powiązania strategii i są odwzorowani na jeden rejestr docelowy i użytkownika docelowego.

Aby użyć domyślnych powiązań strategii rejestru należy, włączyć dla domeny wyszukiwanie odwzorowań za pomocą powiązań strategii. Należy również włączyć wyszukiwanie odwzorowań dla rejestru źródłowego oraz wyszukiwanie odwzorowań i korzystanie z powiązań strategii dla rejestru użytkowników docelowych powiązania strategii. Po odpowiednim skonfigurowaniu w operacjach wyszukiwania odwzorowania brane są pod uwagę rejestry użytkowników w powiązaniu strategii.

Domyślne powiązanie strategii rejestru jest brane pod uwagę, jeśli operacja wyszukania odwzorowań nie znajdzie powiązań identyfikatorów, powiązań strategii filtrów certyfikatów ani innych domyślnych powiązań strategii rejestru dla rejestru docelowego. W wyniku tego wszystkie tożsamości użytkowników w rejestrze źródłowym są odwzorowywane na pojedynczą tożsamość użytkownika docelowego zgodnie z powiązaniem strategii rejestru docelowego.

Tworzone jest na przykład domyślne powiązanie strategii rejestru, które ma rejestr źródłowy moja_dziedzina.com, z nazwami użytkowników w określonej dziedzinie Kerberos. Dla tego powiązania strategii określona zostaje również tożsamość użytkownika docelowego użytkownik_ogólny1 w rejestrze docelowym rej_syst_i5/os, która jest określonym profilem użytkownika w rejestrze użytkowników systemu i5/OS. W tym przypadku nie zostały utworzone żadne powiązania identyfikatorów ani powiązania strategii dotyczące jakichkolwiek tożsamości użytkowników w rejestrze źródłowym. Dlatego jeśli w operacjach wyszukiwania jako rejestr docelowy podano rej_syst_i5/os, a jako rejestr źródłowy moja_dziedzina.com, domyślne powiązanie strategii rejestru zapewnia, że dla wszystkich tożsamości użytkowników w rejestrze moja_dziedzina.com, którzy nie mają zdefiniowanych określonych powiązań identyfikatorów lub powiązań strategii filtrów certyfikatów, jest zwracana tożsamość użytkownika docelowego uzytkownik_ogolny1.

Aby zdefiniować domyślne powiązanie strategii rejestru, należy podać następujące trzy elementy:

- **Rejestr źródłowy**. Definicja rejestru, której powiązanie strategii ma używać jako źródła odwzorowania. Wszystkie tożsamości użytkowników w tym źródle będą odwzorowywane na określonego użytkownika docelowego powiązania strategii.
- **Rejestr docelowy**. Podany rejestr docelowy jest to nazwa definicji rejestru EIM. Rejestr docelowy musi zawierać tożsamość użytkownika docelowego, na którą będą odwzorowywane wszystkie tożsamości użytkowników z rejestru źródłowego.
- **Użytkownik docelowy**. Użytkownik docelowy jest to nazwa tożsamości użytkownika zwracana jako wynik operacji wyszukiwania odwzorowania EIM na podstawie tego powiązania strategii.

Można zdefiniować więcej niż jedno domyślne powiązanie strategii rejestru. Jeśli dwa lub więcej powiązań strategii z tym samym rejestrem źródłowym odnosi się do tego samego rejestru docelowego, należy zdefiniować unikalne dane wyszukiwania dla każdego z tych powiązań strategii, aby zapewnić ich rozróżnienie przez operacje wyszukiwania

odwzorowań. W przeciwnym przypadku operacje wyszukiwania odwzorowań mogą zwrócić wiele tożsamości użytkowników docelowych. W wyniku tego aplikacje bazujące na odwzorowaniach EIM mogą nie być w stanie określić, której tożsamości docelowej użyć.

Ponieważ powiązań strategii można używać na wiele sposobów, często łącząc je ze sobą, przed ich utworzeniem i korzystaniem z nich należy gruntownie zapoznać się z obsługą strategii odwzorowań EIM i działaniem operacji wyszukiwania.

Uwaga: Istnieje możliwość utworzenia powiązania domyślnej strategii rejestru z docelową tożsamością użytkownika, istniejącą w definicji rejestru grupowego. Wszyscy użytkownicy w źródłowym rejestrze użytkowników są źródłem powiązania strategii. Są oni odwzorowywani na docelowe tożsamości użytkowników w docelowej definicji rejestru grupowego. Tożsamości użytkowników zdefiniowane w powiązaniu domyślnej strategii rejestru istnieją w obrębie elementów definicji rejestru grupowego.

Na przykład Jan Kowalski używa tego samego profilu użytkownika systemu i5/OS, Jan_Kowalski, w pięciu systemach: System_B, System_C, System_D, System_E i System_F. Aby zmniejszyć ilość pracy, którą musi on wykonać, aby skonfigurować odwzorowanie EIM, administrator produktu EIM tworzy definicję rejestru grupowego Grupa_1. Elementami definicji są następujące nazwy definicji rejestrów: System_B, System_C, System_D, System_E i System_F. Grupując elementy, administrator może utworzyć pojedyncze powiązanie. Grupując elementy, administrator może utworzyć pojedyncze powiązanie docelowe z definicją rejestru grupowego zamiast tworzenia wielu powiązań z poszczególnymi definicjami rejestru.

Administrator EIM tworzy powiązanie strategii domyślnych rejestrów o źródłowym rejestrze moja_dziedzina.com, który występuje w jednostkach konkretnej dziedziny Kerberos. Podaje dla tego powiązania strategii w rejestrze docelowym Grupa_1 wartość Jan_Kowalski jako tożsamość użytkownika docelowego. W tym przypadku nie stosują się żadne inne powiązania identyfikatora lub powiązania strategii. Dlatego też gdy określono Grupa_1 jako rejestr docelowy oraz moja_dziedzina.com jako rejestr źródłowy w operacjach wyszukania, powiązanie strategii domyślnych rejestrów powoduje, że docelowy identyfikator użytkownika Jan_Kowalski jest zwracany dla wszystkich identyfikatorów użytkowników w moja_dziedzina.com nie posiadających zdefiniowanych powiązań identyfikatora.

Powiązania strategii filtrów certyfikatów:

Poniższe informacje ułatwiają utworzenie odwzorowania dla zbioru tożsamości użytkownika (w formie certyfikatów cyfrowych) w pojedynczym rejestrze X.509.

Powiązanie strategii filtrów certyfikatów jest jednym z typów powiązań strategii, umożliwiających tworzenie odwzorowań wielu tożsamości użytkownika do jednej. Za pomocą powiązania strategii filtrów certyfikatów można odwzorować źródłowy zestaw certyfikatów na pojedynczą tożsamość użytkownika docelowego w określonym rejestrze użytkowników docelowych.

W powiązaniu strategii filtrów certyfikatów jako źródło powiązania strategii podawany jest zestaw certyfikatów w pojedynczym rejestrze X.509. Certyfikaty te są odwzorowywane na określony pojedynczy rejestr docelowy i docelowego użytkownika. W przeciwieństwie do domyślnego powiązania strategii rejestru, w którym wszyscy użytkownicy w pojedynczym rejestrze są źródłem powiązania strategii, zasięg powiązania strategii filtrów certyfikatów jest bardziej elastyczny. Jako źródło można podać podzbiór certyfikatów w rejestrze. Podany dla powiązania strategii filtr certyfikatu określa jego zasięg.

Uwaga: Aby odwzorować wszystkie certyfikaty w rejestrze użytkowników X.509 na pojedynczą tożsamość użytkownika docelowego, należy utworzyć domyślne powiązanie strategii rejestru.

Aby użyć powiązania strategii filtrów certyfikatów, należy włączyć dla domeny wyszukiwanie odwzorowań za pomocą powiązań strategii. Należy również włączyć wyszukiwanie odwzorowań dla rejestru źródłowego oraz wyszukiwanie odwzorowań i korzystanie z powiązań strategii dla rejestru użytkowników docelowych powiązania strategii. Po odpowiednim skonfigurowaniu w operacjach wyszukiwania odwzorowania brane są pod uwagę rejestry użytkowników w powiązaniu strategii.

Jeśli w operacji wyszukiwania odwzorowania produktu Enterprise Identity Mapping (EIM) źródłową tożsamością użytkownika jest certyfikat cyfrowy (po utworzeniu nazwy tożsamości użytkownika za pomocą funkcji API EIM eimFormatUserIdentity()), funkcje EIM sprawdzają, czy istnieje powiązanie identyfikatora EIM i podanej tożsamości użytkownika. Jeśli nie istnieje, funkcje EIM porównują informacje nazwy wyróżniającej w certyfikacie z informacjami nazwy wyróżniającej lub części nazwy wyróżniającej podanymi w filtrze dla powiązania strategii. Jeśli informacje nazwy wyróżniającej spełniają kryterium filtru, odwzorowanie EIM zwraca tożsamość użytkownika docelowego określoną przez powiązanie strategii. W wyniku tego certyfikaty w źródłowym rejestrze X.509 spełniające kryterium filtru certyfikatów są odwzorowywane na pojedynczą tożsamość użytkownika docelowego, tak jak zostało to określone przez powiązanie strategii filtrów certyfikatów.

Tworzymy na przykład powiązanie strategii filtrów certyfikatów z rejestrem źródłowym certyfikaty.x509. Rejestr ten zawiera certyfikaty dla wszystkich pracowników w przedsiębiorstwie, włącznie z tymi, których menedżerowie wydziału kadr używają do dostępu do różnych prywatnych, wewnętrznych stron WWW i innych zasobów, do których mają oni dostęp poprzez serwer iSeries. Dla tego powiązania strategii określono również tożsamość użytkownika docelowego menedżerowie_kadr w rejestrze docelowym system_abc, która jest określonym profilem użytkownika w rejestrze użytkowników i5/OS. Aby mieć pewność, że tylko certyfikaty należące do menedżerów kadr spełniają reguły tego powiązania strategii, filtr certyfikatu został określony z nazwą wyróżniającą podmiotu (SDN): ou=mgrkdr,o=firma.com,c=pl.

W tym przypadku nie zostały utworzone żadne powiązania identyfikatorów ani inne powiązania strategii filtrów certyfikatów dotyczące jakichkolwiek tożsamości użytkownika rejestru źródłowego. Dlatego jeśli w operacjach wyszukiwania jako rejestr docelowy podano system_abc, a jako rejestr źródłowy certyfikaty.x509, powiązanie strategii filtrów certyfikatów sprawdza, że tożsamość użytkownika docelowego menedżerowie_kadr jest zwracana dla wszystkich certyfikatów w rejestrze certyfikaty.x509, które są zgodne z określonym filtrem certyfikatu i dla których nie są zdefiniowane żadne konkretne powiązania identyfikatorów.

Aby zdefiniować powiązanie strategii filtrów certyfikatów, podane zostały następujące informacje:

- **Rejestr źródłowy**. Podana definicja rejestru źródłowego musi być rejestrem użytkowników typu X.509. Strategia filtrów certyfikatów tworzy powiązanie między tożsamościami użytkowników w tym rejestrze użytkowników X.509 i pojedynczą, określoną tożsamością użytkownika docelowego. Powiązanie to jest stosowane tylko do tych tożsamości użytkowników w rejestrze, które spełniają kryterium filtru certyfikatów podanego dla tej strategii.
- **Filtr certyfikatu**. Filtr certyfikatu definiuje zestaw podobnych atrybutów certyfikatów użytkowników. Powiązanie strategii filtrów certyfikatów odwzorowuje dowolne certyfikaty ze zdefiniowanymi atrybutami w rejestrze użytkowników X.509 na określoną tożsamość użytkownika docelowego. Filtr jest określany w oparciu o połączenie nazwy wyróżniającej podmiotu (SDN) i nazwy wyróżniającej wystawcy (IDN), która jest zgodna z certyfikatami, które mają być używane jako źródło odwzorowania. Podany dla strategii filtr certyfikatu musi już istnieć w domenie EIM.
- **Rejestr docelowy**. Podana definicja rejestru docelowego to rejestr użytkowników zawierający tożsamość użytkownika, na którą mają być odwzorowane certyfikaty zgodne z filtrem certyfikatu.
- **Użytkownik docelowy**. Użytkownik docelowy jest to nazwa tożsamości użytkownika zwracana w wyniku operacji wyszukiwania odwzorowania EIM na podstawie tego powiązania strategii.

Ponieważ powiązań strategii certyfikatu i innych powiązań można używać na wiele sposobów, często łącząc je ze sobą, przed utworzeniem powiązań strategii certyfikatu i korzystaniem z nich należy gruntownie zapoznać się z obsługą strategii odwzorowania EIM i działaniem operacji wyszukiwania.

Uwaga: Istnieje możliwość utworzenia powiązania strategii filtru certyfikatów z docelową tożsamością użytkownika, istniejącą w definicji rejestru grupowego. Użytkownicy w rejestrze źródłowym spełniający kryteria określone przez filtr certyfikatów są źródłem powiązania strategii. Są oni odwzorowywani na docelowe tożsamości użytkowników w docelowej definicji rejestru grupowego. Tożsamości użytkowników zdefiniowane w powiązaniu strategii filtru certyfikatów istnieją w obrębie elementów definicji rejestru grupowego.

Na przykład Jan Kowalski używa tego samego profilu użytkownika systemui5/OS, Jan_Kowalski, w pięciu systemach: System B, System C, System D, System E i System F. Aby zmniejszyć ilość pracy, którą musi on wykonać, aby skonfigurować odwzorowanie EIM, administrator produktu EIM tworzy definicję rejestru

| grupowego. Elementami definicji są następujące nazwy definicji rejestrów: System_B, System_C, System_D, System_E i System_F. Grupując elementy, administrator może utworzyć pojedyncze powiązanie docelowe z definicją rejestru grupowego zamiast tworzenia wielu powiązań z poszczególnymi definicjami rejestru.

| Administrator produktu EIM tworzy powiązanie strategii filtru certyfikatów, w którym jako źródło powiązania strategii określa zestaw certyfikatów w pojedynczym rejestrze X.509. Podaje w rejestrze docelowym Grupa_1 wartość Jan_Kowalski jako tożsamość użytkownika docelowego. W tym przypadku nie używa się z innych wybranych powiązań identyfikatorów lub powiązań strategii filtru certyfikatów. W rezultacie, jeśli w operacji wyszukiwania dla docelowego rejestru podana zostaje wartość Grupa_1, wszystkie certyfikaty w rejestrze źródłowym X.509 pasujące do kryteriów filtrów certyfikatów zostaną odwzorowane na określony docelowy identyfikator użytkownika.

Filtry certyfikatów:

Poniższy temat opisuje, jak utworzyć powiązanie strategii filtrów certyfikatów, odwzorowujące certyfikaty ze zdefiniowanymi atrybutami w rejestrze użytkowników X.509 na określony docelowy identyfikator użytkownika.

Filtr certyfikatu określa zestaw podobnych atrybutów nazwy wyróżniającej certyfikatu dla grupy certyfikatów użytkowników w źródłowym rejestrze użytkowników X.509. Filtru certyfikatu można użyć jako bazy powiązania strategii filtrów certyfikatów. Filtr certyfikatu w powiązaniu strategii określa, które certyfikaty w określonym rejestrze źródłowym X.509 odwzorować na określonego użytkownika docelowego. Certyfikaty, które mają informacje SDN i IDN spełniające kryterium filtru są odwzorowywane na określonego użytkownika docelowego podczas operacji wyszukiwania odwzorowań produktu EIM.

Tworzymy na przykład filtr certyfikatu z nazwą wyróżniającą podmiotu (SDN): o=ibm,c=pl. Wszystkie certyfikaty z taką nazwą wyróżniającą jako częścią ich informacji SDN spełniają kryterium filtru, na przykład certyfikat z SDN: cn=JanKowalski,ou=WydziałPrawa,o=ibm,c=pl. Jeśli jest więcej niż jeden filtr certyfikatu, którego kryteria spełnia dany certyfikat, pod uwagę brana jest ta wartość filtru certyfikatu, z którą certyfikat jest bardziej zgodny. Istnieje na przykład filtr certyfikatu z nazwą SDN o=ibm,c=pl i inny filtr certyfikatu z nazwą SDN ou=WydziałPrawa,o=ibm,c=pl. Jeśli w rejestrze źródłowym X.509 jest certyfikat z nazwą SDN cn=JanKowalski,ou=WydziałPrawa,o=ibm,c=pl, to używany jest drugi filtr certyfikatu lub inny, jeszcze dokładniej określony. Jeśli w rejestrze źródłowym X.509 jest certyfikat z nazwą SDN cn=MariaKowalczyk,o=ibm,c=pl, to używany jest mniej dokładny filtr certyfikatu, gdyż certyfikat jest z nim bardziej zgodny.

Aby zdefiniować filtr certyfikatu, można podać jeden lub więcej spośród poniższych elementów:

- Nazwa wyróżniająca podmiotu (SDN). Pełna lub częściowa nazwa wyróżniająca, która jest podawana dla filtru, musi odpowiadać części podmiotu nazwy wyróżniającej certyfikatu cyfrowego, która określa właściciela certyfikatu. Można podać pełny łańcuch nazwy wyróżniającej podmiotu albo jedną lub więcej częściowych nazw wyróżniających, które składają się na pełną nazwę SDN.
- Nazwa wyróżniająca wystawcy (IDN). Pełna lub częściowa nazwa wyróżniająca, która jest podawana dla filtru musi odpowiadać części wystawcy nazwy wyróżniającej certyfikatu cyfrowego, która określa ośrodek certyfikacji, który wystawił certyfikat. Można podać pełny łańcuch nazwy wyróżniającej wystawcy albo jedną lub więcej częściowych nazw wyróżniających, które składają się na pełną nazwę IDN.

Istnieje kilka metod, z których można skorzystać, aby utworzyć filtr certyfikatu, na przykład można użyć funkcji API Format EIM Policy Filter (eimFormatPolicyFilter()) do wygenerowania filtrów certyfikatów korzystając z certyfikatu jako wzorca do utworzenia niezbędnych nazw wyróżniających w odpowiednim porządku i formacie dla nazw SDN i IDN.

Operacje wyszukiwania EIM

Informacje objaśniające proces odwzorowania EIM i wyświetlania przykładów.

Aplikacja lub system operacyjny korzysta z funkcji API EIM w celu wykonania *operacji wyszukiwania*, aby odwzorować jedną tożsamość użytkownika w jednym rejestrze na inną tożsamość użytkownika w innym rejestrze.

Operacja wyszukiwania EIM jest procesem, za pomocą którego aplikacja lub system operacyjny poprzez podanie niektórych znanych i zaufanych informacji znajduje nieznaną powiązaną tożsamość użytkownika w konkretnym rejestrze docelowym. Aplikacje używające funkcji API EIM mogą wykonywać operacje wyszukiwania EIM w informacjach tylko wtedy, gdy informacje te są przechowywane w danej domenie EIM. Aplikacja może wykonać jeden z dwóch typów operacji wyszukiwania EIM w oparciu o typ informacji dostarczanych przez aplikacje jako źródło operacji wyszukiwania EIM: tożsamość użytkownika lub identyfikator EIM.

Jeśli aplikacja lub system operacyjny używa funkcji API eimGetTargetFromSource() do uzyskania tożsamości użytkownika docelowego dla danego rejestru docelowego, musi dostarczyć *tożsamość użytkownika jako źródło* operacji wyszukiwania. Aby tożsamość użytkownika mogła być używana jako źródło w operacji wyszukiwania EIM, musi ona mieć zdefiniowane powiązanie źródłowe lub być objęta powiązaniem strategii. Gdy aplikacja lub system operacyjny korzysta z tej funkcji API, musi dostarczyć trzy rodzaje informacji:

- Tożsamość użytkownika jako źródło lub punkt startowy operacji.
- Nazwę definicji rejestru EIM dla tożsamości użytkownika źródłowego.
- Nazwę definicji rejestru EIM, który jest docelowy dla operacji wyszukiwania EIM. Dana definicja rejestru opisuje rejestr użytkowników zawierający poszukiwaną przez aplikację tożsamość użytkownika.

Jeśli aplikacja lub system operacyjny używa funkcji API eimGetTargetFromIdentifier() w celu uzyskania tożsamości użytkownika dla danego rejestru docelowego, musi dostarczyć *identyfikator EIM jako źródło* operacji wyszukiwania EIM. Gdy aplikacja korzysta z tej funkcji API, musi dostarczyć dwa rodzaje informacji:

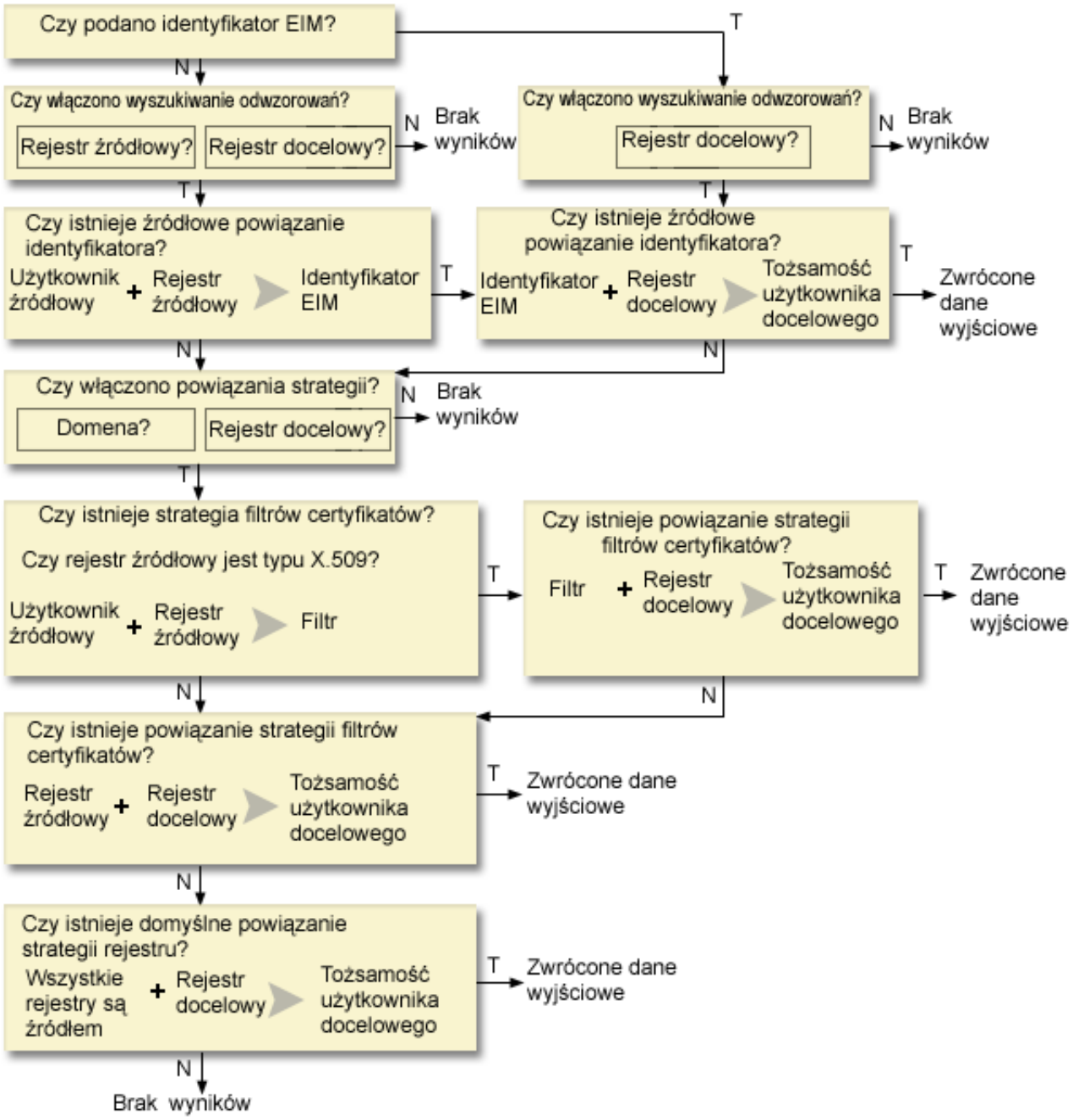
- Identyfikator EIM jako źródło lub punkt startowy operacji.
- Nazwę definicji rejestru EIM, który jest docelowy dla operacji wyszukiwania EIM. Dana definicja rejestru opisuje rejestr użytkowników zawierający poszukiwaną przez aplikację tożsamość użytkownika.

Aby tożsamość użytkownika została zwrócona jako cel dowolnego typu z operacji wyszukiwania EIM, dla tej tożsamości użytkownika musi być zdefiniowane powiązanie docelowe. Powiązanie to może być powiązaniem identyfikatora lub powiązaniem strategii.

Dostarczone informacje są przekazywane do EIM i operacja wyszukiwania EIM wyszukuje i zwraca tożsamości użytkownika docelowego przeszukując dane EIM w następującej kolejności, jak to pokazano na rysunku 10:

1. Powiązanie docelowe identyfikatora dla identyfikatora EIM. Identyfikator EIM jest identyfikowany jedną z dwóch metod: jest otrzymywany przez funkcję API eimGetTargetFromIdentifier(). Może również być określony na podstawie informacji otrzymanych przez funkcję API eimGetTargetFromSource().
2. Powiązanie strategii filtrów certyfikatów.
3. Domyślne powiązanie strategii rejestru.
4. Domyślne powiązanie strategii domeny.

Rysunek 10: Diagram przepływów ogólnego przetwarzania operacji wyszukiwania EIM



Uwaga: W poniższym przepływie operacje wyszukiwania w pierwszej kolejności sprawdzają definicjepojedynczych rejestrów, np. podanego rejestru źródłowego lub docelowego. Jeśli odwzorowanie nie zostanie tam odnalezione, operacja wyszukiwania określa, czy definicja jest elementem definicji rejestru grupowego. Jeśli jest elementem definicji rejestru grupowego, operacja wyszukiwania sprawdza tę definicję.

Operacja wyszukiwania działa w następujący sposób:

1. Najpierw sprawdza, czy wyszukiwanie odwzorowań jest włączone. Operacja wyszukiwania określa, czy wyszukiwanie odwzorowań jest włączone dla określonego rejestru źródłowego, określonego rejestru docelowego lub dla obu tych rejestrów. Jeśli wyszukiwanie odwzorowań nie jest włączone dla jednego lub obu rejestrów, operacja wyszukiwania kończy się nie zwracając tożsamości użytkownika docelowego.

2. Operacja wyszukiwania sprawdza, czy istnieją powiązania identyfikatorów zgodne z kryterium wyszukiwania. Jeśli dostarczony został identyfikator EIM, operacja wyszukiwania użyje tego identyfikatora. W przeciwnym przypadku operacja wyszukiwania sprawdza, czy istnieje określone powiązanie źródłowe identyfikatora zgodne z dostarczoną tożsamością użytkownika źródłowego i rejestrem źródłowym. Jeśli operacja wyszukiwania znajdzie takie powiązanie, użyje go do określenia odpowiedniej nazwy identyfikatora EIM. Następnie użyje tej nazwy do wyszukania powiązania docelowego identyfikatora dla identyfikatora EIM zgodnego z podaną nazwą definicji docelowego rejestru EIM. Jeśli istnieje zgodne powiązanie docelowe identyfikatora, operacja wyszukiwania zwróci tożsamość użytkownika docelowego zdefiniowaną w tym powiązaniu docelowym.
3. Operacja wyszukiwania sprawdza, czy włączone jest korzystanie z powiązań strategii. Operacja wyszukiwania sprawdza, czy w domenie włączone jest wyszukiwanie odwzorowań za pomocą powiązań strategii. Ponadto sprawdza, czy dla rejestru docelowego włączone jest korzystanie z powiązań strategii. Jeśli dla domeny lub rejestru nie są włączone powiązania strategii, operacja wyszukiwania zakończy się nie zwracając tożsamości użytkownika docelowego.
4. Operacja wyszukiwania sprawdza powiązania strategii filtrów certyfikatów. Operacja wyszukiwania sprawdza, czy rejestr źródłowy jest rejestrem typu X.509. Jeśli tak, operacja wyszukiwania sprawdza, czy istnieje powiązanie strategii filtrów certyfikatu zgodne z nazwami definicji rejestrów źródłowego i docelowego. Operacja wyszukiwania sprawdza, czy w źródłowym rejestrze X.509 są certyfikaty spełniające kryterium podane w powiązaniu strategii filtrów certyfikatów. Jeśli operacja wyszukiwania znajdzie zgodne powiązanie strategii i istnieją certyfikaty spełniające kryterium filtru certyfikatów, zwróci odpowiednią tożsamość użytkownika docelowego dla tego powiązania strategii.
5. Operacja wyszukiwania sprawdza domyślne powiązania strategii rejestru. Operacja wyszukiwania sprawdza, czy istnieją domyślne powiązania strategii rejestru zgodne z nazwami definicji rejestrów źródłowego i docelowego. Jeśli znajdzie zgodne powiązania strategii, to zwróci odpowiednią tożsamość użytkownika docelowego dla tego powiązania strategii.
6. Operacja wyszukiwania sprawdza domyślne powiązania strategii domeny.Operacja wyszukiwania sprawdza, czy są zdefiniowane domyślne powiązania strategii domeny dla definicji rejestru docelowego. Jeśli znajdzie zgodne powiązania strategii, to zwróci powiązane tożsamości użytkownika docelowego dla tego powiązania strategii.
7. Operacja wyszukiwania nie może zwrócić wyników.

Więcej informacji dotyczących operacji wyszukiwania odwzorowania EIM można uzyskać, wyświetlając poniższe przykłady:

Pojęcia pokrewne

“Domena EIM” na stronie 7
Informacje objaśniające sposób użycia domeny do składowania wszystkich identyfikatorów.

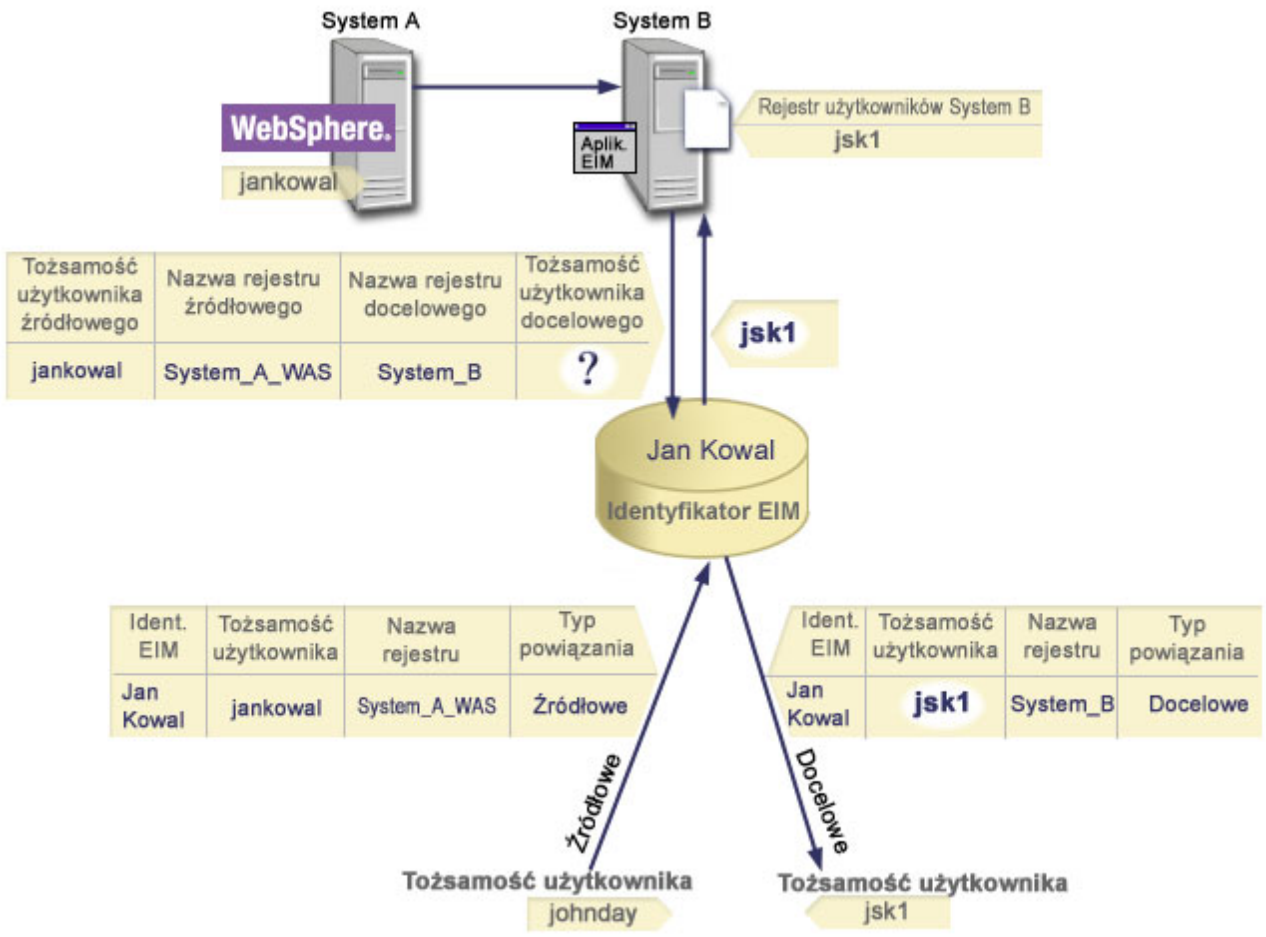
“Powiązania strategii” na stronie 22
Informacje o tym, jak używać powiązań strategii do opisania relacji między wieloma tożsamościami użytkownika a pojedynczą tożsamością użytkownika w rejestrze użytkowników.

Przykłady operacji wyszukiwania: Przykład 1

Przykład objaśniający przepływ dla operacji wyszukiwania, która zwraca tożsamość użytkownika docelowego z określonych powiązań identyfikatora na podstawie znanej tożsamości użytkownika.

Na rysunku 11 użytkownik o tożsamości jankowalski jest uwierzytelniany w WebSphere Application Server za pomocą uwierzytelniania Lightweight Third-Party Authentication (LPTA) w systemie A. WebSphere Application Server w systemie A wywołuje zintegrowany program w systemie B w celu uzyskania dostępu do danych w systemie B. Program ten korzysta z funkcji API EIM do wykonania operacji wyszukiwania EIM na podstawie tożsamości użytkownika w systemie A będącym źródłem operacji. Aplikacja w celu wykonania operacji dostarcza następujące informacje: jankowalski jako źródłowa tożsamość użytkownika, System_A_WAS jako źródłowa nazwa definicji rejestru EIM i System_B jako docelowa nazwa definicji rejestru EIM. Informacje źródłowe są przekazywane do EIM i operacja wyszukiwania EIM znajduje powiązanie źródłowe identyfikatora, które jest zgodne z podanymi informacjami. Za pomocą nazwy identyfikatora EIM, Jan Kowalski, operacja wyszukiwania wyszukuje powiązanie docelowe identyfikatora dla tego identyfikatora, które jest zgodne z nazwą definicji docelowego rejestru EIM dla systemu System_B. Jeśli znalezione zostanie zgodne powiązanie docelowe, operacja wyszukiwania EIM zwróci do aplikacji tożsamość użytkownika jsk1.

Rysunek 11: Operacja wyszukiwania EIM zwraca tożsamość użytkownika docelowego z określonych powiązań identyfikatora na podstawie znanej tożsamości użytkownika jankowalski



Przykłady operacji wyszukiwania: Przykład 2

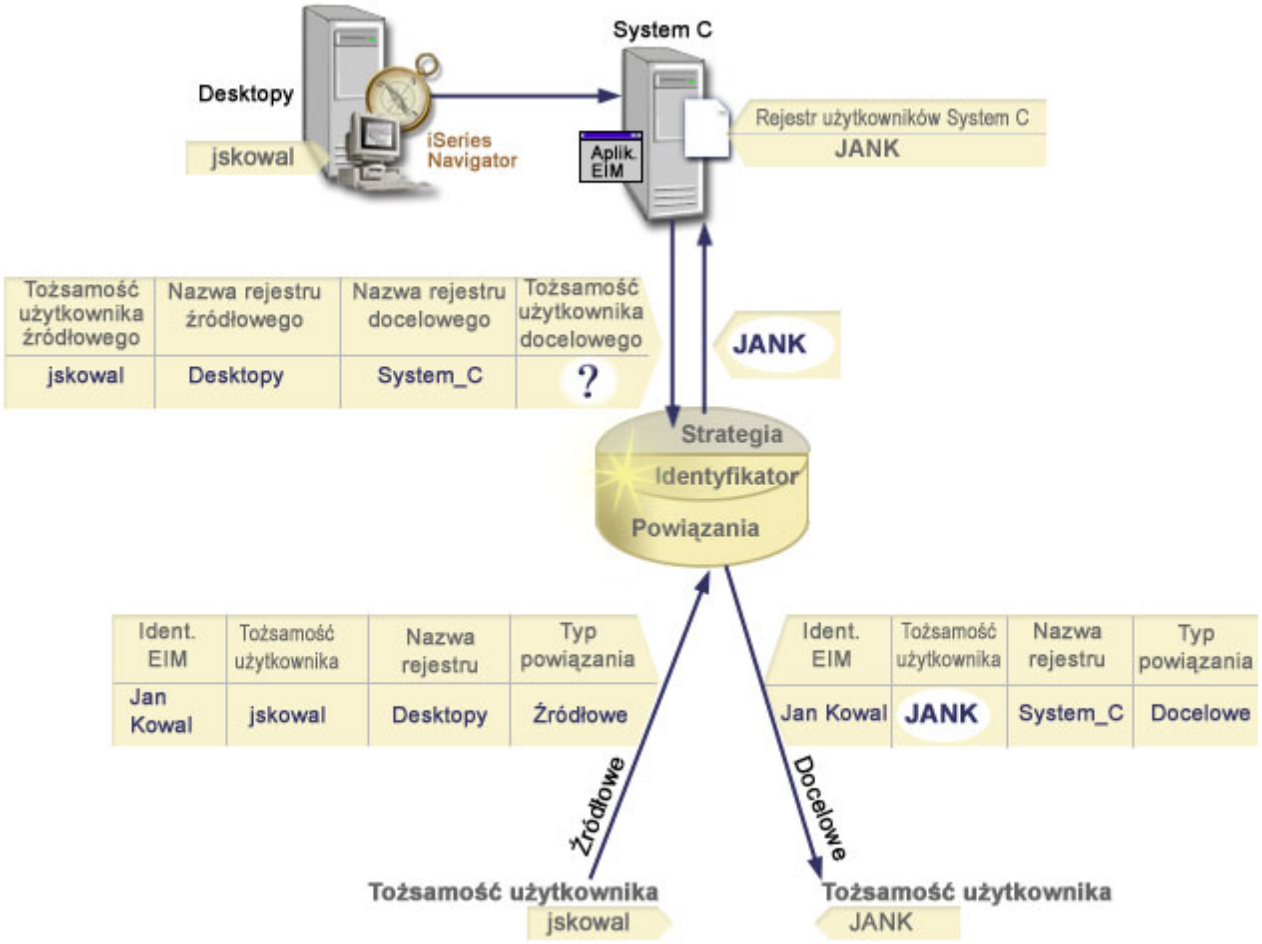
Przykład objaśniający przepływ dla operacji wyszukiwania, która zwraca tożsamość użytkownika docelowego z określonych powiązań identyfikatora na podstawie znanej tożsamości użytkownika protokołu Kerberos.

Rysunek 12 przedstawia sytuację, w której administrator chce odwzorować użytkownika systemu Windows w rejestrze Windows Active Directory na profil użytkownika i5/OS. Używaną przez system Windows metodą uwierzytelniania jest Kerberos, a nazwa rejestru Windows Active Directory zdefiniowaną przez administratora w EIM jest Desktopy. Tożsamość użytkownika, którą administrator chce odwzorować, to nazwa użytkownika Kerberos jskowalski. Nazwa rejestru i5/OS zdefiniowana w EIM to System_C, a tożsamość użytkownika, na którą administrator chce odwzorować, to profil użytkownika o nazwie JANK.

Administrator tworzy identyfikator EIM o nazwie Jan Kowalski. Następnie do tego identyfikatora dodaje dwa powiązania:

- Powiązanie źródłowe dla nazwy użytkownika Kerberos jskowalski w rejestrze Desktopy.
- Powiązanie docelowe dla profilu użytkownika i5/OS o nazwie JANK w rejestrze System_C.

Rysunek 12: Operacja wyszukiwania EIM zwraca tożsamość użytkownika docelowego z określonych powiązań identyfikatora na podstawie znanej nazwy użytkownika Kerberos jskowalski



Konfiguracja taka umożliwia operacji wyszukiwania odwzorowań odwzorowanie z nazwy użytkownika Kerberos na profil użytkownika i5/OS w następujący sposób:

Rejestr i tożsamość użytkownika źródłowego	**--->**	**Identyfikator EIM**	**--->**	**Tożsamość użytkownika docelowego**
jskowalski w rejestrze Desktopy	--->	Jan Kowalski	--->	JANK (w rejestrze System_C)

Operacja wyszukiwania działa w następujący sposób:

1. Użytkownik jskowalski loguje się i uwierzytelnia na platformie Windows za pomocą nazwy użytkownika Kerberos w rejestrze Windows Active Directory Desktopy.
2. Użytkownik otwiera program iSeries Navigator, aby uzyskać dostęp do danych w systemie System_C.
3. System i5/OS używa funkcji API EIM do wykonania operacji wyszukiwania EIM z tożsamością użytkownika źródłowego jskowalski, rejestrem źródłowym Desktopy i rejestrem docelowym System_C.
4. Operacja wyszukiwania EIM sprawdza, czy dla rejestrów źródłowego (Desktopy) i docelowego (System_C) włączono wyszukiwanie odwzorowań. Tak.
5. Operacja wyszukiwania sprawdza, czy istnieje powiązanie źródłowe identyfikatora, zgodne z dostarczoną tożsamością użytkownika źródłowego, jskowalski, w rejestrze źródłowym Desktopy.
6. Operacja wyszukiwania używa zgodnego powiązania źródłowego identyfikatora do określenia odpowiedniej nazwy identyfikatora EIM, którą jest Jan Kowalski.

7. Operacja wyszukiwania używa nazwy identyfikatora EIM do wyszukania powiązania docelowego identyfikatora dla identyfikatora EIM zgodnego z określoną docelową nazwą definicji rejestru EIM, System_C.
8. Odpowiednie powiązanie docelowe identyfikatora istnieje i operacja wyszukiwania zwraca tożsamość użytkownika docelowego, JANK, zgodnie z definicją w powiązaniu docelowym.
9. Operacja wyszukiwania odwzorowania zakończyła się i program iSeries Navigator uruchamia się z profilem użytkownika JANK. Uprawnienia użytkownika do dostępu do zasobów i podejmowania działań w programie iSeries Navigator są określone przez uprawnienia zdefiniowane dla profilu użytkownika JANK, a nie przez uprawnienia zdefiniowane dla tożsamości użytkownika jskowalski.

Przykłady operacji wyszukiwania: Przykład 3

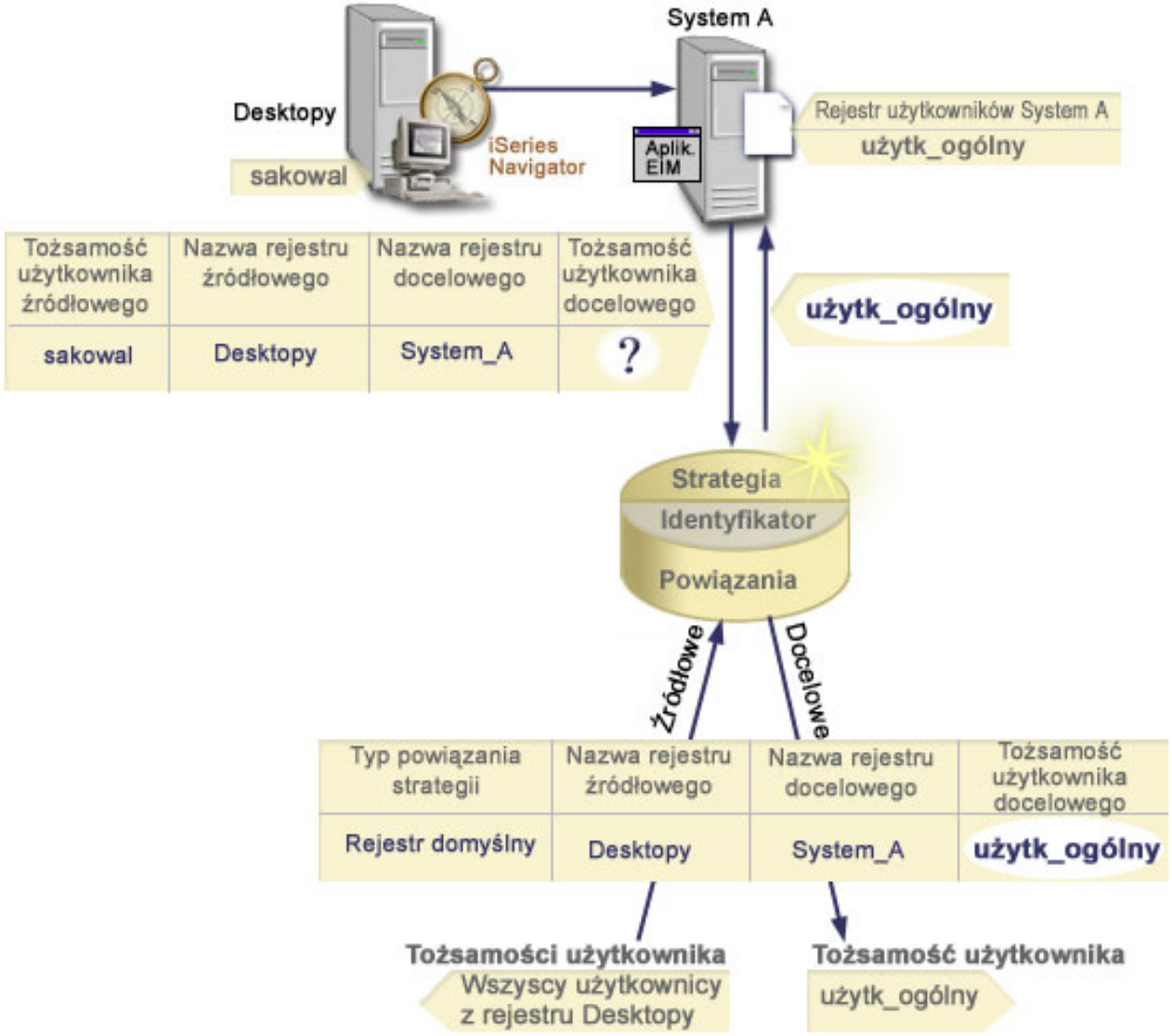
Przykład objaśniający przepływ dla operacji wyszukiwania, która zwraca tożsamość użytkownika docelowego z domyślnego powiązania strategii rejestru.

Rysunek 13 przedstawia sytuację, w której administrator chce odwzorować wszystkich użytkowników stacji roboczych z rejestru Windows Active Directory na pojedynczy profil użytkownika i5/OS o nazwie użytkownik_ogólny w rejestrze i5/OS o nazwie System_A w EIM. Używaną przez system Windows metodą uwierzytelniania jest Kerberos, a nazwa rejestru Windows Active Directory zdefiniowaną przez administratora w EIM jest Desktopy. Jedną z tożsamości użytkowników spośród tych, które administrator chce odwzorować, jest nazwa użytkownika Kerberos sakowalczyk.

Administrator tworzy domyślne powiązanie strategii rejestru z następującymi danymi:

- Rejestr źródłowy Desktopy.
- Rejestr docelowy System_A.
- Tożsamość użytkownika docelowego użytkownik_ogólny.

Rysunek 13: Operacja wyszukiwania zwraca tożsamość użytkownika docelowego z domyślnego powiązania strategii rejestru.



Konfiguracja taka umożliwia operacji wyszukiwania odwzorowań odwzorowanie wszystkich nazw użytkowników Kerberos z rejestru Desktopy, w tym nazwy użytkownika sakowalczyk, na profil użytkownika i5/OS o nazwie użytkownik_ogólny w następujący sposób:

Rejestr i tożsamość użytkownika źródłowego	**--->**	**Domyślne powiązanie strategii rejestru**	**--->**	**Tożsamość użytkownika docelowego**
sakowalczyk w rejestrze Desktopy	--->	Domyślne powiązanie strategii rejestru	--->	użytkownik_ogólny (w rejestrze System_A)

Operacja wyszukiwania działa w następujący sposób:

1. Użytkownik sakowalczyk loguje się i uwierzytelnia na swoim komputerze desktop z systemem Windows za pomocą nazwy użytkownika Kerberos w rejestrze Desktopy.
2. Użytkownik otwiera program iSeries Navigator, aby uzyskać dostęp do danych w systemie System A.
3. System i5/OS używa funkcji API EIM do wykonania operacji wyszukiwania EIM z tożsamością użytkownika źródłowego sakowalczyk, rejestrem źródłowym Desktopy i rejestrem docelowym System_A.

4. Operacja wyszukiwania EIM sprawdza, czy dla rejestrów źródłowego (Desktopy) i docelowego (System_A) włączono wyszukiwanie odwzorowań. Tak.
5. Operacja wyszukiwania sprawdza, czy istnieje powiązanie źródłowe identyfikatora, zgodne z dostarczoną tożsamością użytkownika źródłowego, sakowalczyk, w rejestrze źródłowym Desktopy. Nie znajduje zgodnego powiązania identyfikatora.
6. Operacja wyszukiwania sprawdza, czy dla domeny włączone jest używanie powiązań strategii. Jest włączone.
7. Operacja wyszukiwania sprawdza, czy dla rejestru docelowego (System_A) jest włączone używanie powiązań strategii. Jest włączone.
8. Operacja wyszukiwania sprawdza, czy rejestr źródłowy (Desktopy) jest rejestrem typu X.509. Nie jest.
9. Operacja wyszukiwania sprawdza, czy istnieje domyślne powiązanie strategii rejestru zgodne z nazwą definicji rejestru źródłowego (Desktopy) i nazwą definicji rejestru docelowego (System_A).
10. Operacja wyszukiwania znajduje takie powiązanie i zwraca wartość użytkownik_ogólny jako tożsamość użytkownika docelowego.

Czasem operacja wyszukiwania EIM zwraca niejednoznaczne wyniki. Może się tak zdarzyć na przykład jeśli więcej niż jedna tożsamość użytkownika docelowego jest zgodna z określonymi kryteriami operacji wyszukiwania. Niektóre aplikacje z obsługą EIM, w tym aplikacje i produkty systemu i5/OS, nie potrafią obsłużyć takich wyników i zgłaszają błąd lub działają w sposób nieprzewidziany. W takich przypadkach może zajść potrzeba podjęcia odpowiednich działań. Można na przykład zmienić konfigurację EIM lub zdefiniować dane wyszukiwania dla każdej tożsamości użytkownika docelowego, aby zapobiec wystąpieniu wielu zgodnych tożsamości użytkownika docelowego. Ponadto można sprawdzić odwzorowania, aby określić, czy wprowadzone zmiany dają oczekiwany skutek.

Przykłady operacji wyszukiwania: Przykład 4

Przykład objaśniający przepływ dla operacji wyszukiwania, która zwraca tożsamość użytkownika docelowego w rejestrze użytkowników będącym elementem definicji rejestru grupowego.

Administrator chce odwzorować użytkownika systemu Windows na profil użytkownika i5/OS. Protokół Kerberos jest metodą uwierzytelniania stosowaną przez system Windows, a nazwa rejestru Kerberos zdefiniowana przez administratora w EIM to Pulpit_A. Tożsamość użytkownika, którą administrator chce odwzorować to jednostka Kerberos o nazwie jkowalski. Nazwa definicji rejestru i5/OS zdefiniowana w EIM to Grupa_1, a tożsamość użytkownika, na którą administrator chce odwzorować, to profil użytkownika o nazwie JANK. Istnieje ona w trzech rejestrach: System_B, System_C i System_D. Każdy z nich jest elementem definicji rejestru grupowego Grupa_1.

Administrator tworzy identyfikator EIM o nazwie Jan Kowalski. Następnie do tego identyfikatora dodaje dwa powiązania:

- Źródłowe powiązanie dla jednostki Kerberos o nazwie jkowalski w rejestrzePulpit_A.
- Powiązanie docelowe dla profilu użytkownika systemu i5/OS o nazwie JANK w rejestrze Grupa_1.

Konfiguracja taka umożliwia operacji wyszukiwania odwzorowań odwzorowanie z nazwy użytkownika Kerberos na profil użytkownika i5/OS w następujący sposób:

Rejestr i tożsamość użytkownika źródłowego	**--->**	**Identyfikator EIM**	**--->**	**Tożsamość użytkownika docelowego**
jkowalski w rejestrze Pulpit_A	--->	John Day	--->	JANK (w definicji rejestru grupowego Grupa_1)

Operacja wyszukiwania działa w następujący sposób:

1. Użytkownik (jkowalski) loguje się i jest uwierzytelniany w systemie Windows na komputerze Pulpit_A.
2. Użytkownik otwiera program iSeries Navigator, aby uzyskać dostęp do danych w systemie System_B.
3. System i5/OS używa funkcji API EIM do wykonania operacji wyszukiwania EIM z tożsamością użytkownika źródłowego jkowalski, rejestrem źródłowym Pulpit_A i rejestrem docelowym System_B.

4. Operacja wyszukania produktu EIM sprawdza, czy włączono wyszukania odwzorowania dla rejestru źródłowego (Desktop_A) i rejestru docelowego (System_B).
5. Operacja wyszukania sprawdza, czy istnieje określone indywidualne powiązanie źródłowe pasujące do dostarczonego źródłowego identyfikatora użytkownika jkowalski w rejestrze źródłowym Pulpit_A.
6. Operacja wyszukania używa pasującego powiązania źródłowego do określenia odpowiedniej nazwy identyfikatora EIM, którą jest John Day.
7. Operacja wyszukania używa następnie nazwy identyfikatora EIM do wyszukania indywidualnego powiązania docelowego dla identyfikatora EIM, pasującego do określonej docelowej nazwy definicji rejestrów EIM w systemie System_B. (Brak powiązań).
8. Operacja wyszukiwania sprawdza, czy rejestr źródłowy (Pulpit_A) jest elementem definicji rejestru grupowego. (Nie jest).
9. Operacja wyszukiwania sprawdza, czy rejestr docelowy (Pulpit_B) jest elementem definicji rejestru grupowego. Jest on elementem definicji rejestru grupowego Grupa_1.
10. Operacja wyszukania używa następnie nazwy identyfikatora EIM do wyszukania indywidualnego powiązania docelowego dla identyfikatora EIM, pasującego do określonej docelowej nazwy definicji rejestrów EIM w systemie Grupa_1.
11. Jeśli istnieje odpowiednie indywidualne powiązanie docelowe, operacja wyszukania zwraca docelowy identyfikator użytkownika JANK zdefiniowany w powiązaniu docelowym.

Uwaga: W niektórych przypadkach operacja wyszukania EIM zwraca niejednoznaczne wyniki, gdy więcej niż jeden docelowy identyfikator użytkownika jest zgodny z określonymi kryteriami operacji wyszukiwania. Ponieważ system EIM nie może zwracać pojedynczej tożsamości docelowej użytkownika, aplikacje używające EIM, w tym aplikacje systemu i5/OS i produkty, które nie są przystosowane do obsługi niejednoznacznych wyników i zgłaszają błąd lub działają w sposób nieprzewidziany. W takich przypadkach może zajść potrzeba podjęcia odpowiednich działań. Na przykład można zmienić konfigurację EIM lub zdefiniować dane wyszukiwania dla każdej docelowej tożsamości użytkownika, aby zapobiec powstaniu wielu zgodności docelowych tożsamości użytkownika. Istnieje możliwość testowania odwzorowania w celu określenia, czy wprowadzone zmiany działają zgodnie z oczekiwaniem.

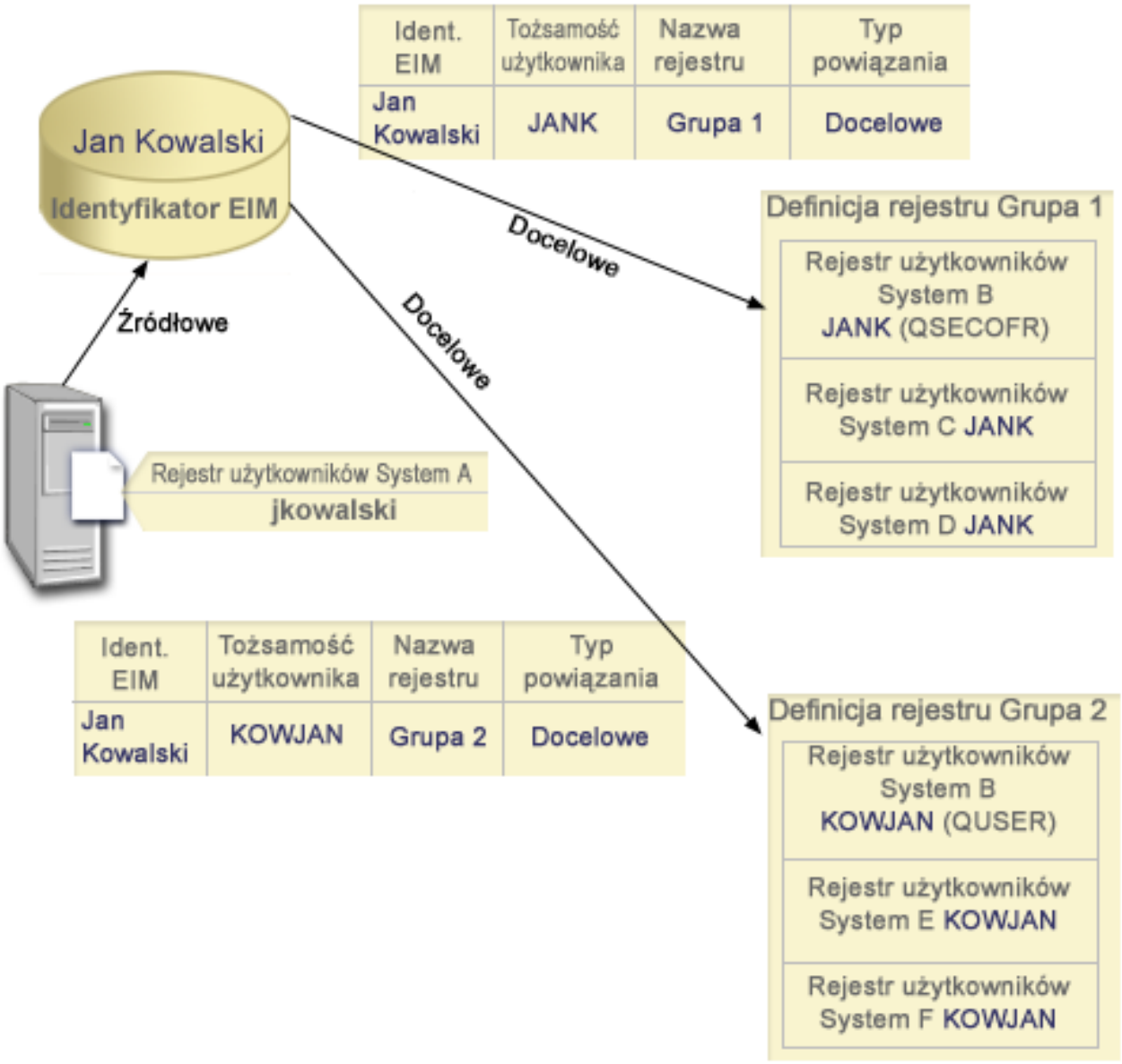
Przykłady operacji wyszukiwania: przykład 5

Poniższy przykład zawiera informacje o operacjach wyszukiwania, które zwracają niejednoznaczne wyniki związane z definicjami rejestrów grupowych.

W niektórych przypadkach operacja wyszukiwania odwzorowania zwraca niejednoznaczne wyniki, kiedy więcej niż jedna docelowa tożsamość użytkownika jest zgodna z określonymi kryteriami wyszukiwania. Ponieważ niejednoznaczne wyniki mogą doprowadzić do błędów lub nieoczekiwanych zachowań aplikacji używających EIM, należy podjąć odpowiednie działania zapobiegawcze lub naprawcze.

W szczególności należy pamiętać, że operacje wyszukiwania mogą zwracać niejednoznaczne wyniki, jeśli w zapytaniu pojedyncza definicja rejestru użytkownika zostanie określona jako element wielu definicji rejestrów grupowych. Jeśli pojedyncza definicja rejestru użytkownika jest elementem wielu definicji rejestrów grupowych i tworzone są pojedyncze powiązania identyfikatora EIM lub strategii, dla których definicje te są rejestrami źródłowymi lub docelowymi, operacje wyszukiwania mogą zwracać wieloznaczne wyniki. Można na przykład użyć dwóch różnych tożsamości użytkownika dla dwóch typów wykonywanych zadań systemowych - zadania wykonywane jako administrator ochrony uruchamiane są z tożsamością użytkownika posiadającego uprawnienie QSECOFR, a typowe zadania użytkownika uruchamiane są z tożsamością użytkownika posiadającego uprawnienie QUSER. Jeśli obie tożsamości użytkownika znajdują się w rejestrze użytkownika, będącym elementem dwóch różnych definicji rejestrów grupowych, i do obu z nich zostaną utworzone powiązania identyfikatora docelowego, wynikiem operacji wyszukiwania będzie odnalezienie obu tożsamości użytkownika docelowego, a zatem będą one zwracały niejednoznaczne wyniki.

Poniższy przykład ilustruje, w jaki sposób ten problem może wystąpić, kiedy pojedynczy profil użytkownika zostanie określony jako element dwóch definicji rejestrów grupowych, z których jedna będzie rejestrem docelowym dwóch powiązań identyfikatorów EIM.



Przykład:

Użytkownik Jan Kowalski ma następujące tożsamości użytkownika w definicji rejestru systemu, nazywanej rejestrem użytkowników System B:

- JANK
- KOWJAN

Rejestr użytkowników System B jest elementem następujących definicji rejestrów grupowych:

- Grupa 1
- Grupa 2

Identyfikator produktu EIM Jan Kowalski posiada dwa powiązania docelowe o następujących właściwościach:

- Powiązanie docelowe: rejestr docelowy Grupa 1, zawierający tożsamość użytkownika JANK w rejestrze użytkowników System B.

| • Powiązanie docelowe: rejestr docelowy Grupa 2, zawierający tożsamość użytkownika KOWJAN w rejestrze
| użytkowników System B.

| W tej sytuacji operacja wyszukiwania odwzorowania zwraca niejednoznaczne wyniki, ponieważ więcej niż jedna
| docelowa tożsamość (JANK and KOWJAN) użytkownika jest zgodna z określonymi kryteriami wyszukiwania.

| Analogicznie, operacje wyszukiwania odwzorowania mogą zwracać niejednoznaczne wyniki, jeśli utworzone zostaną
| dwa powiązania strategii (zamiast powiązań identyfikatora EIM), używające definicji raportów grupowych jako
| rejestrów docelowych.

| Aby zapobiec wykonywaniu operacji wyszukiwania, które zwracają niejednoznaczne wyniki związane z definicjami
| rejestrów grupowych, należy zastosować poniższe wskazówki:
| • Należy określić w zapytaniu pojedynczy rejestr użytkowników jako element tylko jednej definicji rejestrów
| grupowych.
| • Należy zachować ostrożność podczas tworzenia pojedynczych powiązań identyfikatorów EIM używających definicji
| rejestrów grupowych jako rejestrów źródłowych lub docelowych. Należy sprawdzić, czy pojedynczy rejestr
| użytkowników został określony jako element tylko jednej definicji rejestrów grupowych. Jeśli element docelowej
| definicji rejestru grupowego jest jednocześnie elementem innej definicji rejestru grupowego, operacje wyszukiwania
| mogą zwracać niejednoznaczne wyniki.
| • Jeśli niejednoznaczne wyniki zostały zwrócone w wyniku określenia jednej definicji rejestru jako elementu wielu
| definicji rejestrów grupowych i utworzenia pojedynczego powiązania identyfikatora lub powiązania strategii,
| używającego jednej z tych definicji jako rejestru źródłowego lub docelowego, można zdefiniować w każdym
| powiązaniu unikalne informacje wyszukiwania.

| W przykładzie dotyczącym Jana Kowalskiego można zdefiniować następujące informacje wyszukiwania dla każdego z
| docelowych użytkowników:
| • Dla użytkownika JANK: zdefiniuj wartość Administrator jako informację wyszukiwania
| • Dla użytkownika KOWJAN: zdefiniuj wartość Użytkownik jako informację wyszukiwania

| Jednakże podstawowe aplikacje systemu i5/OS, takie jak iSeries Access for Windows, nie używają danych
| wyszukiwania do rozróżnienia między wieloma tożsamościami użytkowników docelowych zwracanych przez operację
| wyszukiwania. Dlatego też należy rozważyć ponowne zdefiniowanie powiązań dla domeny, aby zapewnić, że operacja
| wyszukiwania odwzorowań będzie mogła zwrócić pojedynczą tożsamość użytkownika docelowego i że podstawowe
| aplikacje systemu i5/OS będą mogły pomyślnie wykonywać operacje wyszukiwania i odwzorować tożsamości.

Obsługa i włączanie strategii odwzorowań EIM

Informacje objaśniające sposób włączania i wyłączania powiązań strategii dla domeny.

Obsługa strategii odwzorowań EIM umożliwia użycie powiązań strategii oraz powiązań konkretnego identyfikatora w domenie EIM. Powiązań strategii można używać zamiast powiązań identyfikatorów lub w połączeniu z nimi.

Obsługa strategii odwzorowań EIM daje możliwość włączania i wyłączania powiązań strategii dla całej domeny lub dla każdego wybranego rejestru użytkowników docelowych. EIM umożliwia również określenie, czy wybrany rejestr ma brać udział w ogólnych operacjach wyszukiwania odwzorowań. W wyniku tego można używać obsługi strategii odwzorowań do bardziej precyzyjnego sterowania zwracaniem wyników przez operacje wyszukiwania odwzorowań.

Domyślnym ustawieniem dla domeny EIM jest wyłączenie dla tej domeny wyszukiwania odwzorowań używającego powiązań strategii. Gdy dla domeny wyłączone jest korzystanie z powiązań strategii, wszystkie operacje wyszukiwania odwzorowań dla tej domeny zwracają wyniki używając tylko konkretnych powiązań identyfikatorów między tożsamościami użytkowników a identyfikatorami EIM.

Domyślnym ustawieniem dla każdego pojedynczego rejestru jest włączony udział w wyszukiwaniu odwzorowań i wyłączone korzystanie z powiązań strategii. Włączając korzystanie z powiązań strategii dla pojedynczego rejestru należy się upewnić, że ustawienie to jest włączone również dla domeny.

Są trzy metody skonfigurowania udziału w wyszukiwaniu odwzorowań i korzystania z powiązań strategii dla każdego rejestru:

- Dla danego rejestru nie można wcale używać operacji wyszukiwania odwzorowań. Innymi słowy aplikacja, która wykonuje operację wyszukiwania odwzorowania korzystając z tego rejestru, nie otrzyma żadnych wyników.
- Operacje wyszukiwania odwzorowań mogą używać tylko konkretnych powiązań identyfikatorów między tożsamościami użytkowników a identyfikatorami EIM. Wyszukiwanie odwzorowań jest włączone dla rejestru, ale korzystanie z powiązań strategii jest wyłączone.
- Operacje wyszukiwania odwzorowań mogą używać konkretnych powiązań identyfikatorów jeśli one istnieją, jeśli zaś nie istnieją, mogą używać powiązań strategii (wszystkie ustawienia są włączone).

Zadania pokrewne

"Włączanie powiązań strategii dla domeny" na stronie 86

"Włączanie obsługi wyszukiwania odwzorowań i korzystania z powiązań strategii dla rejestru docelowego" na stronie 93

Kontrola dostępu EIM

Informacje objaśniające, jak zezwolić użytkownikowi na dostęp do grupy użytkowników LDAP w celu sterowania domeną.

Użytkownik produktu EIM to użytkownik posiadający prawa dostępu EIM w oparciu o przynależność do predefiniowanej grupy użytkowników LDAP dla konkretnej domeny. Określając *kontrolę dostępu* EIM dla użytkownika dodajemy tego użytkownika do określonej grupy użytkowników LDAP dla danej domeny. Każda grupa LDAP ma uprawnienia do wykonywania konkretnych zadań administracyjnych EIM w tej domenie. To, które zadania administracyjne i jakiego typu może wykonać użytkownik, włącznie z operacjami wyszukiwania, jest określone przez grupę kontroli dostępu, do której dany użytkownik EIM należy.

Uwaga: Aby skonfigurować odwzorowania EIM, należy udowodnić swoje uprawnienia w kontekście sieci, a nie jednego konkretnego systemu. Autoryzacja do konfigurowania EIM nie jest oparta na uprawnieniach profilu użytkownika systemu i5/OS, ale na uprawnieniach kontroli dostępu EIM. Odwzorowania EIM to zasób sieciowy, a nie zasób dla jednego, określonego systemu; w konsekwencji EIM przy konfiguracji nie uwzględnia uprawnień specjalnych charakterystycznych dla systemu i5/OS, takich jak *ALLOBJ i *SECADM. Gdy odwzorowania EIM są już skonfigurowane, autoryzacja wymagana do wykonania zadań może być oparta na różnych typach użytkowników, w tym na profilach użytkowników i5/OS. Na przykład produkt IBM Directory Server for iSeries (LDAP) uznaje profile użytkowników i5/OS z uprawnieniami specjalnymi *ALLOBJ i *IOSYSCFG za administratorów katalogu.

Tylko użytkownicy z prawem dostępu administratora EIM mogą dodawać innych użytkowników do grupy kontroli dostępu EIM lub zmieniać ich ustawienia kontroli dostępu. Zanim użytkownik stanie się członkiem grupy kontroli dostępu EIM, musi mieć pozycję w serwerze katalogów działającym jako kontroler domeny EIM. Ponadto tylko określone rodzaje użytkowników mogą należeć do grupy kontroli dostępu EIM. Tożsamość użytkownika może mieć postać nazwy użytkownika Kerberos, nazwy wyróżniającej LDAP lub profilu użytkownika i5/OS, dopóki jest ona zdefiniowana w serwerze katalogów.

Uwaga: Aby udostępnić w EIM nazwę użytkownika Kerberos, w systemie musi być skonfigurowana usługa uwierzytelniania sieciowego. Aby udostępnić w EIM profile użytkowników i5/OS, na serwerze katalogów należy skonfigurować przyrostek obiektów systemowych. Umożliwia on serwerowi katalogów odniesienie do obiektów systemowych i5/OS takich jak profile użytkowników i5/OS.

Poniżej przedstawiono krótki opis funkcji, które mogą wykonywać poszczególne grupy uprawnień EIM:

Administrator protokołu LDAP (Lightweight Directory Access Protocol)

Administrator LDAP jest to specjalna nazwa wyróżniająca w katalogu, jest on administratorem dla całego katalogu. W ten sposób administrator LDAP ma dostęp do wszystkich funkcji administracyjnych EIM oraz dostęp do całego katalogu. Użytkownik z tą kontrolą dostępu może wykonywać następujące funkcje:

- Tworzenie domeny.
- Usuwanie domeny.
- Tworzenie i usuwanie identyfikatorów EIM.
- Tworzenie i usuwanie definicji rejestrów EIM.
- Tworzenie i usuwanie powiązań źródłowych, docelowych i administracyjnych.
- Tworzenie i usuwanie powiązań strategii.
- Tworzenie i usuwanie filtrów certyfikatów.
- Włączanie i wyłączanie korzystania z powiązań strategii dla domeny.
- Włączanie i wyłączanie wyszukiwania odwzorowań dla rejestru.
- Włączanie i wyłączanie powiązań strategii dla rejestru.
- Wykonywanie operacji wyszukiwania EIM.
- Pobieranie powiązań identyfikatorów, powiązań strategii, filtrów certyfikatów, identyfikatorów EIM i definicji rejestrów EIM.
- Dodawanie, usuwanie i wyświetlanie informacji o kontroli dostępu EIM.
- Zmiana i usuwanie informacji referencyjnych dla użytkownika rejestru.

Administrator EIM

Użytkownik należący do tej grupy kontroli dostępu może zarządzać wszystkimi danymi EIM w domenie EIM. Użytkownik z tą kontrolą dostępu może wykonywać następujące funkcje:

- Usuwanie domeny.
- Tworzenie i usuwanie identyfikatorów EIM.
- Tworzenie i usuwanie definicji rejestrów EIM.
- Tworzenie i usuwanie powiązań źródłowych, docelowych i administracyjnych.
- Tworzenie i usuwanie powiązań strategii.
- Tworzenie i usuwanie filtrów certyfikatów.
- Włączanie i wyłączanie korzystania z powiązań strategii dla domeny.
- Włączanie i wyłączanie wyszukiwania odwzorowań dla rejestru.
- Włączanie i wyłączanie powiązań strategii dla rejestru.
- Wykonywanie operacji wyszukiwania EIM.
- Pobieranie powiązań identyfikatorów, powiązań strategii, filtrów certyfikatów, identyfikatorów EIM i definicji rejestrów EIM.
- Dodawanie, usuwanie i wyświetlanie informacji o kontroli dostępu EIM.
- Zmiana i usuwanie informacji referencyjnych dla użytkownika rejestru.

Administrator identyfikatorów

Użytkownik należący do tej grupy kontroli dostępu może dodawać i zmieniać identyfikatory EIM i zarządzać powiązaniami źródłowymi i administracyjnymi. Użytkownik z tą kontrolą dostępu może wykonywać następujące funkcje:

- Tworzenie identyfikatorów EIM.
- Dodawanie i usuwanie powiązań źródłowych.
- Dodawanie i usuwanie powiązań administracyjnych.
- Wykonywanie operacji wyszukiwania EIM.
- Pobieranie powiązań identyfikatorów, powiązań strategii, filtrów certyfikatów, identyfikatorów EIM i definicji rejestrów EIM.

Operacje odwzorowania EIM

Użytkownik należący do tej grupy kontroli dostępu może przeprowadzać operacje wyszukiwania odwzorowań EIM. Użytkownik z tą kontrolą dostępu może wykonywać następujące funkcje:

- Wykonywanie operacji wyszukiwania EIM.
- Pobieranie powiązań identyfikatorów, powiązań strategii, filtrów certyfikatów, identyfikatorów EIM i definicji rejestrów EIM.

Administrator rejestru

Użytkownik należący do tej grupy kontroli dostępu może zarządzać wszystkimi definicjami rejestrów EIM. Użytkownik z tą kontrolą dostępu może wykonywać następujące funkcje:

- Dodawanie i usuwanie powiązań docelowych.
- Tworzenie i usuwanie powiązań strategii.
- Tworzenie i usuwanie filtrów certyfikatów.
- Włączanie i wyłączanie wyszukiwania odwzorowań dla rejestru.
- Włączanie i wyłączanie powiązań strategii dla rejestru.
- Wykonywanie operacji wyszukiwania EIM.
- Pobieranie powiązań identyfikatorów, powiązań strategii, filtrów certyfikatów, identyfikatorów EIM i definicji rejestrów EIM.

Administrator dla wybranych rejestrów

Użytkownik należący do tej grupy kontroli dostępu może zarządzać informacjami EIM tylko dla określonej definicji rejestru użytkowników (na przykład Rejestr_X). Użytkownik należący do tej grupy kontroli dostępu może także dodawać i usuwać powiązania docelowe tylko dla określonej definicji rejestru użytkowników. Aby w pełni wykorzystać operacje wyszukiwania odwzorowań i powiązania strategii, użytkownik z tą kontrolą dostępu powinien mieć również kontrolę dostępu **Operacje odwzorowania EIM**. Ta kontrola dostępu umożliwia użytkownikowi wykonanie następujących funkcji dla określonych autoryzowanych definicji rejestrów:

- Tworzenie, usuwanie i wyświetlanie powiązań docelowych tylko dla określonych definicji rejestrów EIM.
- Dodawanie i usuwanie domyślnych powiązań strategii domeny.
- Dodawanie i usuwanie powiązań strategii tylko dla określonych definicji rejestrów.
- Dodawanie filtrów certyfikatów tylko dla określonych definicji rejestrów.
- Włączanie i wyłączanie wyszukiwania odwzorowań tylko dla określonych definicji rejestrów.
- Włączanie i wyłączanie powiązań strategii tylko dla określonych definicji rejestrów.
- Pobieranie identyfikatorów EIM.
- Pobieranie powiązań identyfikatorów i filtrów certyfikatów tylko dla określonych definicji rejestrów.
- Pobieranie informacji definicji rejestru EIM tylko dla określonych definicji rejestrów.

Uwaga: Jeśli podana definicja rejestru jest definicją rejestru grupowego, użytkownik posiadający uprawnienie Administrator do wybranych rejestrów ma dostęp z prawami administratora tylko do grupy, a nie do jej elementów.

Użytkownik z kontrolą dostępu **Administrator wybranych rejestrów** i **Operacje wyszukiwania odwzorowań EIM** może wykonywać następujące funkcje:

- Dodawanie i usuwanie powiązań strategii tylko dla określonych rejestrów.
- Wykonywanie operacji wyszukiwania EIM.
- Pobieranie wszystkich powiązań identyfikatorów, powiązań strategii, filtrów certyfikatów, identyfikatorów EIM i definicji rejestrów EIM.

Wyszukiwanie referencji

Ta grupa kontroli dostępu umożliwia użytkownikowi pobieranie informacji referencyjnych, np. haseł.

Jeśli użytkownik z tej grupy kontroli pragnie wykonać dodatkową operację EIM, musi być członkiem grupy kontroli dostępu dającej uprawnienia wymagane dla żądanej operacji EIM. Na przykład jeśli użytkownik z tej grupy kontroli pragnie pobrać powiązanie docelowe ze źródłowego, musi być członkiem jednej z następujących grup:

- Administrator EIM
- Administrator identyfikatorów
- operacje wyszukiwania odwzorowania EIM,
- Administrator rejestru

Grupa kontroli dostępu EIM: uprawnienie API

W poniższych informacjach znajdują się tabele zawierające posortowane operacje produktu Enterprise Identity Mapping (EIM) wykonywane przez interfejs API.

Na poszczególne tabele składają się funkcje API EIM, różne grupy kontroli dostępu EIM i uprawnienia grupy kontroli dostępu do wykonywania danej funkcji EIM.

Tabela 1. Praca z domenami

Funkcja API EIM	Administrator LDAP	Administrator EIM	Administrator identyfikatorów	Wyszukiwanie odwzorowań EIM	Administrator rejestru	Administrator dla wybranego rejestru
eimChangeDomain	X	X	-	-	-	-
eimCreateDomain	X	-	-	-	-	-
eimDeleteDomain	X	X	-	-	-	-
eimListDomains	X	X	-	-	-	-

Tabela 2. Praca z identyfikatorami

Funkcja API EIM	Administrator LDAP	Administrator EIM	Administrator identyfikatorów EIM	Wyszukiwanie odwzorowań EIM	Administrator rejestrów EIM	Administrator rejestru 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

Tabela 3. Praca z rejestrami

Funkcja API EIM	Administrator LDAP	Administrator EIM	Administrator identyfikatorów EIM	Wyszukiwanie odwzorowań EIM	Administrator rejestrów EIM	Administrator rejestru 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

Tabela 3. Praca z rejestrami (kontynuacja)

Funkcja API EIM	Administrator LDAP	Administrator EIM	Administrator identyfikatorów EIM	Wyszukiwanie odwzorowań EIM	Administrator rejestrów EIM	Administrator rejestru X EIM
eimListRegistry Powiązania	X	X	X	X	X	X
eimListRegistryAliases	X	X	X	X	X	X
eimListRegistry Użytkownicy	X	X	X	X	X	X
eimRemoveRegistry	X	X	-	-	-	-

Tabela 4. Praca z powiązaniami identyfikatorów. Dla funkcji API eimAddAssociation() i eimRemoveAssociation() istnieją cztery parametry określające typ dodawanego lub usuwanego powiązania. Uprawnienie do tych funkcji API zależy od typu powiązania podanego w tych parametrach. W poniższej tabeli dla każdej z tych funkcji API podano typ powiązania.

Funkcja API EIM	Administrator LDAP	Administrator EIM	Administrator identyfikatorów EIM	Wyszukiwanie odwzorowań EIM	Administrator rejestrów EIM	Administrator rejestru X EIM
eimAddAssociation (administracyjne)	X	X	X	-	-	-
eimAddAssociation (źródłowe)	X	X	X	-	-	-
eimAddAssociation (źródłowe i docelowe)	X	X	X	-	X	X
eimAddAssociation (docelowe)	X	X	-	-	X	X
eimListAssociations	X	X	X	X	X	X
eimRemoveAssociation (administracyjne)	X	X	X	-	-	-
eimRemoveAssociation (źródłowe)	X	X	X	-	-	-
eimRemoveAssociation (źródłowe i docelowe)	X	X	X	-	X	X
eimRemoveAssociation (docelowe)	X	X	-	-	X	X

Tabela 5. Praca z powiązaniami strategii

Funkcja API EIM	Administrator LDAP	Administrator EIM	Administrator identyfikatorów EIM	Wyszukiwanie odwzorowań EIM	Administrator rejestrów EIM	Administrator rejestru 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	-	-	-	-	-	

Tabela 6. Praca z odwzorowaniami

Funkcja API EIM	Administrator LDAP	Administrator EIM	Administrator identyfikatorów EIM	Wyszukiwanie odwzorowań EIM	Administrator rejestrów EIM	Administrator rejestru X EIM
eimGetAssociatedIdentifier	X	X	X	X	X	X
eimGetTargetFromIdentifier	X	X	X	X	X	X
eimGetTargetFromSource	X	X	X	X	X	X

Tabela 7. Praca z dostępem

Funkcja API EIM	Administrator LDAP	Administrator EIM	Administrator identyfikatorów EIM	Wyszukiwanie odwzorowań EIM	Administrator rejestrów EIM	Administrator rejestru X EIM
eimAddAccess	X	X	-	-	-	-
eimListAccess	X	X	-	-	-	-
eimListUserAccess	X	X	-	-	-	-
eimQueryAccess	X	X	-	-	-	-
eimRemoveAccess	X	X	-	-	-	-

Grupa kontroli dostępu produktu EIM: uprawnienie zadania EIM

Poniższa tabela przedstawia relacje między różnymi grupami kontroli dostępu EIM a zadaniami EIM, które mogą one wykonać.

W tabeli nie jest wymieniony administrator LDAP, jednak ten poziom kontroli dostępu jest wymagany do utworzenia nowej domeny EIM. Administrator LDAP ma również taką samą kontrolę dostępu jak administrator EIM, ale administrator EIM nie ma nadawanej automatycznie kontroli dostępu administratora LDAP.

Tabela 8. Tabela 1: Grupy kontroli dostępu EIM

Zadanie EIM	Administrator EIM	Administrator identyfikatorów	Operacje wyszukiwania odwzorowania EIM	Administrator rejestru	Administrator dla wybranego rejestru	Wyszukiwanie referencji
Tworzenie domeny	-	-	-	-	-	
Usuwanie domeny	X	-	-	-	-	
Modyfikacja domeny	X	-	-	-	-	
Włączenie/wyłączenie powiązań strategii dla domeny	X	-	-	-	-	
Wyszukiwanie domen	X	-	-	-	-	
Dodanie rejestru systemu	X	-	-	-	-	
Dodanie rejestru aplikacji	X	-	-	-	-	
Usuwanie rejestru	X	-	-	-	-	
Modyfikacja rejestru	X	-	-	X	X	
Włączenie/wyłączenie wyszukiwania odwzorowań dla rejestru	X	-	-	X	X	
Włączenie/wyłączenie powiązań strategii dla rejestru	X	-	-	X	X	

Tabela 8. Tabela 1: Grupy kontroli dostępu EIM (kontynuacja)

Zadanie EIM	Administrator EIM	Administrator identyfikatorów	Operacje wyszukiwania odwzorowania EIM	Administrator rejestru	Administrator dla wybranego rejestru	Wyszukiwanie referencji
Wyszukiwanie rejestrów	X	X	X	X	X	
Dodawanie identyfikatora	X	X	-	-	-	
Usuwanie identyfikatora	X	-	-	-	-	
Modyfikacja identyfikatora	X	X	-	-	-	
Wyszukiwanie identyfikatorów	X	X	X	X	X	
Odtwarzanie powiązanych identyfikatorów	X	X	X	X	X	
Dodawanie/usuwanie powiązania administracyjnego	X	X	-	-	-	
Dodawanie/usuwanie powiązania źródłowego	X	X	-	-	-	
Dodawanie/usuwanie powiązania docelowego	X	-	-	X	X	
Dodawanie/usuwanie powiązania strategii	X	-	-	X	X	
Dodawanie/usuwanie filtrów certyfikatów	X	-	-	X	X	
Wyszukiwanie filtrów certyfikatów	X	X	X	X	X	
Wyszukiwanie powiązań	X	X	X	X	X	
Wyszukiwanie powiązań strategii	X	X	X	X	X	
Odtwarzanie powiązania docelowego z powiązania źródłowego	X	X	X	X	-	
Odtwarzanie powiązania docelowego z identyfikatora	X	X	X	X	X	

Tabela 8. Tabela 1: Grupy kontroli dostępu EIM (kontynuacja)

Zadanie EIM	Administrator EIM	Administrator identyfikatorów	Operacje wyszukiwania odwzorowania EIM	Administrator rejestru	Administrator dla wybranego rejestru	Wyszukiwanie referencji
Modyfikacja użytkowników rejestru	X	-	-	X	X	
Wyszukiwanie użytkowników rejestru	X	X	X	X	X	
Modyfikacja aliasu rejestru	X	-	-	X	X	
Wyszukiwanie aliasów rejestrów	X	X	X	X	X	
Odtworzenie rejestrów z aliasów	X	X	X	X	X	
Dodawanie/usuwanie kontroli dostępu EIM	X	-	-	-	-	
Wyświetlenie członków grupy kontroli dostępu	X	-	-	-	-	
Wyświetlenie kontroli dostępu EIM dla konkretnego użytkownika	X	-	-	-	-	
Tworzenie zapytania dla kontroli dostępu EIM	X	-	-	-	-	
Modyfikacja referencji	X	-	-	-	-	-
Pobranie referencji	X	-	-	-	-	X
1 - jeśli podana definicja rejestru jest definicją rejestru grupowego, użytkownik posiadający uprawnienie Administrator do wybranych rejestrów ma dostęp z prawami administratora tylko do grupy, a nie do jej elementów.						

Koncepcje dotyczące LDAP w kontekście EIM

Informacje objaśniające, jak używać protokołu LDAP z produktem EIM.

Produkt EIM używa serwera LDAP jako kontrolera domeny w celu przechowywania danych EIM. Dlatego należy zrozumieć niektóre pojęcia związane z LDAP, odnoszące się do konfigurowania i używania EIM w przedsiębiorstwie. Na przykład można użyć nazwy wyróżniającej LDAP jako tożsamości użytkownika do skonfigurowania EIM i uwierzytelnienia na kontrolerze domeny EIM.

Aby lepiej zrozumieć konfigurowanie i używanie EIM, należy zrozumieć następujące pojęcia związane z LDAP:

Pojęcia pokrewne

"Pojęcia związane z EIM" na stronie 5
Ważne pojęcia związane z EIM i niezbędne do pomyślnej implementacji.

Nazwa wyróżniająca

Informacje omawiające używanie nazw wyróżniających z protokołem LDAP.

Nazwa wyróżniająca jest pozycją protokołu LDAP jednoznacznie identyfikującą i opisującą pozycje w serwerze katalogów (LDAP). Do skonfigurowania serwera katalogów tak, aby przechowywał informacje domeny EIM, można użyć kreatora konfiguracji EIM. Ponieważ EIM używa serwera katalogów do przechowywania danych EIM, nazwy wyróżniające można wykorzystywać jako sposób uwierzytelniania w kontrolerze domeny EIM.

Nazwy wyróżniające składają się z nazwy pozycji oraz z nazw, zamieszczonych w kolejności od dołu do góry, obiektów znajdujących się nad nią w katalogu LDAP. Przykładem pełnej nazwy wyróżniającej jest cn=Jan Kowalski, o=IBM, c=US. Każda pozycja zawiera co najmniej jeden atrybut, który jest używany do nadania nazwy pozycji. Atrybut nazywający jest określany jako względna nazwa wyróżniająca (RDN) pozycji. Pozycja powyżej danej nazwy RDN to pozycja"Nadrzędna nazwa wyróżniająca". W powyższym przykładzie cn=Tim Jones nazywa pozycję, jest więc nazwą RDN. Określenie o=IBM, c=US jest nadrzędną nazwą wyróżniającą dla cn=Tim Jones.

Ponieważ EIM używa serwera katalogów do przechowywania danych EIM, można użyć nazwy wyróżniającej dla tożsamości użytkownika w celu uwierzytelnienia w kontrolerze domeny. Można również użyć nazwy wyróżniającej dla tożsamości użytkownika, który konfiguruje EIM dla serwera iSeries. Nazw wyróżniających można używać podczas:

- konfigurowania serwera katalogów jako kontrolera domeny EIM, zadanie to wykonuje się, tworząc i używając nazwy wyróżniającej identyfikującej administratora LDAP w serwerze Directory; jeśli serwer Directory nie został wcześniej skonfigurowany, można go skonfigurować podczas używania kreatora konfiguracji EIM do tworzenia i podłączania nowej domeny,
- stosowania kreatora konfiguracji EIM do wybrania typu tożsamości użytkownika, której kreator ma używać do nawiązywania połączenia z kontrolerem domeny EIM; nazwa wyróżniająca to jeden z dopuszczalnych typów użytkownika; nazwa wyróżniająca musi reprezentować użytkownika, który ma uprawnienia do tworzenia obiektów w lokalnej przestrzeni nazw serwera Directory,
- stosowania kreatora konfiguracji EIM do wybrania typu użytkownika w celu wykonania operacji EIM w imieniu funkcji systemu operacyjnego; Do operacji tych należą wyszukiwanie odwzorowań i usuwanie powiązań podczas usuwania lokalnego profilu użytkownika i5/OS. nazwa wyróżniająca to jeden z dopuszczalnych typów użytkownika;
- łączenia się z kontrolerem domeny w celu wykonania zadań administrowania EIM, na przykład zarządzania rejestrami i identyfikatorami oraz wykonania operacji wyszukiwania odwzorowań.
- Tworzenie filtrów certyfikatów do określenia zasięgu powiązania strategii filtrów certyfikatów. Podczas tworzenia filtru certyfikatu należy podać dane nazwy wyróżniającej dla podmiotu lub dostawcy lub certyfikat, w celu określenia kryterium używanego przez filtr do określenia, które certyfikaty są objęte powiązaniem strategii.

Informacje pokrewne

Serwer katalogów - pojęcia

Nadrzędna nazwa wyróżniająca

Informacje omawiające hierarchię nazw wyróżniających.

Nadrzędna nazwa wyróżniająca jest pozycją w przestrzeni nazw serwera katalogów LDAP. Pozycje serwera LDAP tworzą strukturę hierarchiczną, która może odzwierciedlać granice polityczne, geograficzne, organizacyjne lub granice domeny. Nazwę wyróżniającą uważa się za nadrzędną nazwę wyróżniającą, gdy nazwa ta jest pozycją katalogu bezpośrednio nadrzędną nad daną nazwą wyróżniającą.

Przykładem pełnej nazwy wyróżniającej jest cn=Tim Jones, o=IBM, c=US. Każda pozycja zawiera co najmniej jeden atrybut, który jest używany do nadania nazwy pozycji. Atrybut nazywający jest określany jako względna nazwa

wyróżniająca (RDN) pozycji. Pozycja powyżej danej nazwy RDN jest nazywana nadrzędną nazwą wyróżniającą. W powyższym przykładzie cn=Tim Jones nazywa pozycję, jest więc nazwą RDN. Określenie o=IBM, c=US jest nadrzędną nazwą wyróżniającą dla cn=Tim Jones.

Odwzorowania EIM używają serwera katalogów jako kontrolera domeny do przechowywania danych domeny EIM. Nadrzędna nazwa wyróżniająca w połączeniu z nazwą domeny EIM określa położenie danych domeny EIM w przestrzeni nazw serwera katalogów. Podczas używania kreatora konfiguracji EIM do utworzenia i podłączenia nowej domeny można określić nadrzędną nazwę wyróżniającą dla tworzonej domeny. Stosując nadrzędną nazwę wyróżniającą można określić miejsce, w którym mają znajdować się dane EIM w przestrzeni nazw dla tej domeny. Jeśli nadrzędna nazwa wyróżniająca nie zostanie podana, dane EIM znajdują się w przestrzeni nazw w miejscu wskazywanym przez przyrostek a domyślnym położeniem danych domeny EIM jest ibm-eimDomainName=EIM.

Informacje pokrewne

Serwer katalogów - pojęcia

Schemat LDAP i inne uwagi dotyczące produktu EIM

Poniższe informacje opisują komponenty wymagane przez serwer katalogów do obsługi produktu Enterprise Identity Mapping (EIM).

Produkt EIM wymaga, aby kontroler domeny był udostępniany przez serwer katalogów obsługujący protokół LDAP w wersji 3. Ponadto serwer katalogów musi akceptować schemat EIM i rozróżniać następujące atrybuty i klasy obiektów:

- Atrybut ibm-entryUUID.
- Typy ibmattributetypes:
  - acIEntry
  - acIPropagate
  - acISource
  - entryOwner
  - ownerPropagate
  - ownerSource
- Atrybuty EIM, w tym trzy nowe atrybuty do obsługi powiązania strategii:
  - 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
- Klasy obiektów EIM, w tym trzy nowe klasy do obsługi powiązania strategii:
  - ibm-eimApplicationRegistry
  - ibm-eimDomain
  - ibm-eimIdentifier
  - ibm-eimRegistry

– ibm-eimRegistryUser
– ibm-eimSourceRelationship
– ibm-eimSystemRegsitry
– ibm-eimTargetRelationship
– ibm-eimFilterPolicy
– ibm-eimDefaultPolicy
– ibm-eimPolicyListAux

Wersja V5R3 i późniejsze serwera IBM Directory Server for iSeries udostępniają niezbędną obsługę. Więcej informacji o tym, które serwery katalogów IBM udostępniają obsługę wymaganą przez EIM oraz uwagi dotyczące kontrolerów domeny EIM zawiera temat Planowanie kontrolera domeny EIM.

Jeśli serwer katalogów w systemie iSeries w wersji V5R2 jest już używany jako kontroler domeny EIM, należy zaktualizować schemat LDAP i obsługę EIM dla tego serwera katalogów, aby nadal go używać do zarządzania danymi domeny EIM w wersji V5R3 lub późniejszych.

Informacje pokrewne

Serwer iSeries - protokół LDAP

Pojęcia związane z serwerem iSeries i EIM

Poniższe informacje zawierają listę aplikacji produktu Enterprise Identity Mapping (EIM).

Odwzorowania EIM można zaimplementować na dowolnej platformie IBM @server . Jednak podczas implementacji EIM na serwerze iSeries należy zwrócić uwagę na pewne informacje, które są charakterystyczne dla implementacji tego serwera. Poniżej przedstawione zostały informacje o aplikacjach i5/OS z obsługą EIM, uwagi dotyczące profili użytkowników i inne tematy pomocne w efektywnym korzystaniu z EIM w systemie iSeries:

Pojęcia pokrewne

“Pojęcia związane z EIM” na stronie 5
Ważne pojęcia związane z EIM i niezbędne do pomyślnej implementacji.

Uwagi dotyczące profili użytkownika systemu i5/OS dla produktu EIM

Możliwość wykonywania zadań w EIM nie jest oparta na uprawnieniu profilu użytkownika i5/OS, ale na uprawnieniu “Kontrola dostępu EIM” na stronie 39. Istnieją jednak pewne zadania dodatkowe, które należy wykonać, aby skonfigurować system i5/OS do korzystania z odwzorowań EIM. Zadania te wymagają profilu użytkownika systemu i5/OS z odpowiednimi uprawnieniami specjalnymi.

Aby za pomocą programu iSeries Navigator skonfigurować system i5/OS do korzystania z produktu EIM, profil użytkownika musi mieć następujące uprawnienia specjalne:

- Administrator ochrony (*SECADM).
- Wszystkie obiekty (*ALLOBJ).
- Konfiguracja systemu (*IOSYSCFG).

Rozszerzenie komend profilu użytkownika systemu i5/OS dla identyfikatorów EIM

Po skonfigurowaniu w systemie odwzorowań EIM można używać nowego parametru komend Tworzenie profilu użytkownika (Create user profile - CRTUSRPRF) i Zmiana profilu użytkownika (Change user profile - CHGUSRPRF) nazwanego EIMASSOC. Parametr ten służy do definiowania powiązań identyfikatora EIM dla określonego profilu użytkownika dla rejestru lokalnego.

Używając tego parametru, należy podać następujące informacje:

- Nazwa identyfikatora EIM, może to być nazwa nowa lub istniejąca.
- Opcja działania dla powiązania, może to być dodanie (*ADD), zastąpienie (*REPLACE) lub usunięcie (*REMOVE) podanego powiązania.

Uwaga: Aby skonfigurować nowe powiązanie, użyj *ADD. Opcja *REPLACE jest przydatna, jeśli na przykład wcześniej zdefiniowane zostało powiązanie do złego identyfikatora. Opcja ta usuwa istniejące powiązania danego rodzaju dla rejestru lokalnego do dowolnych innych identyfikatorów, a następnie dodaje jedno, podane w parametrze. Opcja *REMOVE usuwa dowolne podane powiązania z podanego identyfikatora.

- Rodzaj powiązania identyfikatora, może to być powiązanie docelowe, źródłowe, docelowe i źródłowe lub administracyjne.
- Czy utworzyć podany identyfikator EIM, jeśli jeszcze nie istnieje.

Zazwyczaj powiązanie docelowe jest tworzone dla profilu systemu i5/OS w środowisku pojedynczego logowania. Po utworzeniu komendą potrzebnego powiązania docelowego dla profilu użytkownika (i, jeśli to potrzebne, identyfikatora EIM) można utworzyć odpowiadające mu powiązanie źródłowe. Do utworzenia powiązania źródłowego dla innej tożsamości użytkownika, na przykład nazwy użytkownika Kerberos, z którą użytkownik wpisuje się do sieci, można użyć programu iSeries Navigator.

Podczas konfigurowania odwzorowań EIM dla systemu podawana jest tożsamość użytkownika i hasło dla systemu używane do wykonywania operacji EIM w systemie operacyjnym. Ta tożsamość użytkownika musi mieć uprawnienie kontroli dostępu EIM umożliwiające tworzenie identyfikatorów i dodawanie powiązań.

Hasła profili użytkowników systemu i5/OS i odwzorowania EIM

Podstawowym celem administratora konfigurującego odwzorowania EIM jako część środowiska pojedynczego logowania jest zmniejszenie nakładów pracy na zarządzanie hasłami użytkowników w przedsiębiorstwie. Używając odwzorowania tożsamości udostępnianego przez EIM wraz z uwierzytelnianiem Kerberos masz pewność, że użytkownicy muszą mniej razy się logować i pamiętać mniej haseł. Korzyścią jest mniej zgłoszeń związanych z problemami z odwzorowanymi tożsamościami użytkowników, takich jak zerowanie haseł zapomnianych przez użytkowników. Jednak nadal działają reguły haseł strategii ochrony i nadal trzeba zarządzać tymi profilami użytkowników dla użytkowników, których hasła straciły ważność.

Aby osiągnąć większe korzyści ze środowiska pojedynczego logowania, można rozważyć zmianę ustawień haseł dla tych profili użytkowników, które są docelowe w odwzorowywaniu tożsamości. Użytkownik będący docelowym w odwzorowywaniu tożsamości nie musi udostępniać hasła profilu użytkownika przy dostępie do systemu iSeries lub zasobów i5/OS z obsługą EIM. Dla typowych użytkowników można zmienić ustawienie hasła na *NONE, aby żadne hasło nie było używane z profilem użytkownika. Właściciel tego profilu użytkownika nie potrzebuje hasła dzięki odwzorowywaniu tożsamości i pojedynczemu logowaniu. Ustawienie hasła na *NONE będzie korzystne, gdyż nie trzeba będzie zarządzać ważnością hasła; ponadto nikt nie użyje tego profilu do bezpośredniego wpisania się do serwera iSeries lub dostępu do zasobów i5/OS z obsługą EIM. Można jednak zostawić wartość hasła dla profili użytkowników administratorów na wypadek, gdyby potrzebowali oni kiedykolwiek wpisać się bezpośrednio do systemu iSeries. Na przykład gdy kontroler domeny EIM jest wyłączony i odwzorowywanie tożsamości nie działa, administrator może potrzebować wpisać się bezpośrednio do systemu iSeries zanim problem z kontrolerem domeny nie zostanie rozwiązany.

Kontrola systemu i5/OS dla produktu EIM

Wykonanie kontroli jest niezwykle istotne dla całego planu ochrony. Podczas konfigurowania i używania EIM można skonfigurować obsługę kontroli dla serwera katalogów zapewniając odpowiedni poziom odpowiedzialności wymagany przez strategię ochrony. Obsługa kontroli może być na przykład pomocna przy określeniu, który z użytkowników odwzorowanych przez powiązanie strategii wykonał działanie w systemie lub zmienił obiekt.

Więcej informacji na temat obsługi kontroli dla IBM Directory Server for iSeries (LDAP) zawiera temat Kontrola w Centrum informacyjnym IBM Directory Server for iSeries (LDAP). Wśród informacji tych znajdują się również odpowiednie odniesienia do ustawień i założeń związanych z kontrolą i5/OS potrzebnych do upewnienia się, że kontrola serwera katalogów została skonfigurowana poprawnie.

Aplikacje z obsługą EIM dla systemu i5/OS

Poniższe aplikacje systemu i5/OS można skonfigurować tak, aby używały odwzorowań EIM:

- Serwery hostów i5/OS (używane obecnie przez programy iSeries Access for Windows i iSeries Navigator)

- Serwer Telnet (używany obecnie przez PC5250 i IBM Websphere Host On-Demand)
- QFileSrv.400 ODBC (umożliwia użycie pojedynczego logowania przez SQL)
- JDBC (umożliwia użycie EIM przez SQL)
- Distributed Relational Database Architecture (DRDA) (umożliwia użycie EIM przez SQL)
- IBM WebSphere Host On-Demand Version 8, (opcja Web Express Logon)
- NetServer
- QFileSvr.400

Scenariusze wykorzystania EIM

Informacje ułatwiające zarządzanie w jednym środowisku wpisania się tożsamościami użytkowników wielu systemów.

Produkt EIM to technologia infrastruktury firmy IBM pozwalająca na śledzenie tożsamości użytkowników w przedsiębiorstwie i zarządzanie nimi. Zazwyczaj odwzorowania EIM używane są z technologią uwierzytelniania, na przykład z usługą uwierzytelniania sieciowego, w celu zaimplementowania środowiska pojedynczego logowania.

Aby zapoznać się z tym szerszym wykorzystaniem EIM, przeczytaj sekcję Scenariusze w temacie dotyczącym pojedynczego logowania w Centrum informacyjnym.

Planowanie EIM

Informacje o tworzeniu planu implementacji produktu EIM potrzebnego do pomyślnego skonfigurowania EIM dla serwera iSeries lub w środowisku z różnymi platformami.

Plan implementacji jest niezbędny do pomyślnego skonfigurowania i korzystania z EIM w przedsiębiorstwie. Aby utworzyć plan, należy zebrać dane o systemach, aplikacjach i użytkownikach, którzy będą korzystali z EIM. Zebrane informacje będą pomocne podczas podejmowania decyzji dotyczącej najlepszego skonfigurowania EIM dla danego przedsiębiorstwa.

Ponieważ EIM jest opracowaną przez firmę IBM @server technologią infrastruktury dostępną dla wszystkich platform IBM, planowanie implementacji zależy od platform w danym przedsiębiorstwie. Pewne zadania planowania są specyficzne dla konkretnej platformy, jednak wiele zadań planowania dotyczy wszystkich platform IBM. Należy zapoznać się z ogólnymi zadaniami planowania i utworzyć ogólny plan implementacji. Więcej informacji na temat planowania implementacji EIM zawierają następujące strony:

Planowanie EIM dla serwera eServer

Plan implementacji jest niezbędny do pomyślnego skonfigurowania i korzystania z EIM w przedsiębiorstwie używającym wielu platform. Aby utworzyć plan implementacji, należy zebrać dane o systemach, aplikacjach i użytkownikach, którzy będą korzystali z EIM. Zebrane informacje zostaną wykorzystane przy podejmowaniu decyzji dotyczącej najlepszego skonfigurowania EIM dla danego środowiska wielu platform.

Poniższa lista przedstawia przewodnik przejścia przez zadania planowania, które należy wykonać, zanim rozpocznie się konfigurowanie i używanie odwzorowań EIM w środowisku wielu platform. Zapoznaj się z informacjami na tych stronach, przedstawiającymi planowanie wymagań konfiguracyjnych EIM, w tym niezbędne umiejętności zespołu implementującego, informacje, które należy zebrać, i decyzje odnośnie konfiguracji, które należy podjąć. Przydatne może być wydrukowanie arkuszy roboczych planowania EIM (numer 8 na poniższej liście), aby można je było wypełniać w miarę realizacji procesu planowania.

Wymagania konfiguracji EIM dla serwera eServer

Aby pomyślnie zaimplementować odwzorowania EIM w przedsiębiorstwie, należy spełnić trzy zestawy wymagań:

1. Wymagania dotyczące przedsiębiorstwa lub sieci.
2. Wymagania dotyczące systemu.
3. Wymagania dotyczące aplikacji.

Wymagania dotyczące przedsiębiorstwa lub sieci.

Konieczne jest takie skonfigurowanie jednego systemu w przedsiębiorstwie lub w sieci, aby pełnił on funkcję kontrolera domeny EIM, czyli specjalnie skonfigurowanego serwera LDAP, który przechowuje i udostępnia dane domeny EIM. Jest wiele czynników, które należy wziąć pod uwagę wybierając, którego serwera katalogów użyć jako kontrolera domeny; należy zauważyć, że nie wszystkie serwery LDAP udostępniają obsługę kontrolera domeny EIM.

Innym czynnikiem jest dostępność narzędzi do administrowania. Inną opcją jest wykonywanie funkcji administracyjnych za pomocą własnych aplikacji używających funkcji API EIM. Jeśli produkt Directory Server for iSeries (LDAP) ma być używany jako kontroler domeny EIM, można do zarządzania EIM użyć programu iSeries Navigator. Jeśli ma być używany produkt IBM Directory, można użyć programu narzędziowego eimadmin, który jest częścią V1R4 LDAP SPE.

Poniżej przedstawione zostały informacje podstawowe o platformach IBM udostępniających serwer katalogów obsługujący odwzorowania EIM. Więcej szczegółowych informacji o wyborze serwera katalogów do udostępniania obsługi kontrolera domeny EIM zawiera temat Planowanie kontrolera domeny EIM.

Wymagania dotyczące systemu i aplikacji

Każdy system, który należy do domeny EIM, musi spełniać następujące wymagania:

- Musi mieć zainstalowane oprogramowanie klienta LDAP.
- Musi mieć implementację funkcji API EIM.

Każda aplikacja, która należy do domeny EIM, powinna korzystać z funkcji API EIM do wyszukiwania odwzorowań i innych operacji.

Uwaga: W przypadku aplikacji rozproszonej może być wymagane korzystanie z funkcji API EIM zarówno po stronie serwera, jak i klienta. Zazwyczaj tylko strona serwera aplikacji potrzebuje korzystać z funkcji API EIM.

Poniższa tabela zawiera informacje o obsłudze EIM udostępnianej przez platformy @server . Informacje są pogrupowane według platform, w kolumnie zaznaczono następujące elementy:

- Klient EIM potrzebny dla platformy do obsługi funkcji API EIM.
- Rodzaj narzędzi do konfigurowania odwzorowań EIM i zarządzania nimi dostępnych dla platformy.
- Serwer katalogów, który można zainstalować dla platformy, aby służył jako kontroler domeny EIM.

Aby platforma mogła być częścią domeny EIM, nie musi spełniać wymagań dotyczących kontrolera domeny EIM.

Tabela 9. Obsługa produktu EIM przez serwer eServer

Platforma	Klient EIM (obsługa API)	Kontroler domeny	Narzędzia do administrowania EIM
System AIX na serwerze pSeries	AIX R5.2	IBM Directory V5.1	Niedostępna
Linux • SLES8 i procesor PPC64 • Red Hat 7.3 i procesor i386 • SLES7 on zSeries	Pobierz jednego z następujących klientów: • Klient IBM Directory V4.1 • Klient IBM Directory V5.1 • Klient Open LDAP v2.0.23	IBM Directory V5.1	Niedostępne
System i5/OS na serwerze iSeries	System OS/400 V5R2 i i5/OS V5R3 lub nowszy	System OS/400 V5R2 i i5/OS V5R3 lub nowsza wersja Directory Server	Serwer iSeries Navigator V5R2 i V5R3 lub nowszy

Tabela 9. Obsługa produktu EIM przez serwer eServer (kontynuacja)

Platforma	Klient EIM (obsługa API)	Kontroler domeny	Narzędzia do administrowania EIM
Windows 2000 on xSeries	Pobierz jednego z następujących klientów: • Klient IBM Directory V4.1 • Klient IBM Directory V5.1	Klient IBM Directory V5.1	Niedostępne
System z/OS na serwerze zSeries	z/OS V1R4 LDAP SPE OW57137	z/OS V1R4 LDAP	V1R4 LDAP SPE OW57137

Uwaga: Więcej informacji o produkcie IBM Directory Server zawiera serwis WWW produktu firmy IBM pod adresem http://www-3.ibm.com/software/network/help-directory/

Jeśli platforma udostępnia obsługę klienta EIM (API), system ten może działać w domenie EIM. Platforma nie musi udostępniać obsługi kontrolera domeny EIM jeśli nie ma być używana jako kontroler domeny EIM, w przedsiębiorstwie.

Po sprawdzeniu spełnienia wszystkich wymagań odwzorowań EIM można rozpocząć określanie niezbędnych umiejętności, ról i uprawnień do konfigurowania EIM.

Określenie potrzebnych ról i umiejętności

Odwzorowania EIM są tak określone, że pojedyncza osoba w niewielkiej organizacji może łatwo odpowiadać zarówno za konfigurowanie, jak i administrowanie. Można również, w większej organizacji, odpowiedzialność tę rozłożyć na więcej osób. To, ile osób będzie potrzebnych w zespole, zależeć będzie od posiadanych przez te osoby niezbędnych umiejętności, rodzaju platform włączonych do implementacji EIM i preferowanego w danej organizacji podziału ról i odpowiedzialności ochrony.

Aby przeprowadzić pomyślną implementację EIM, niezbędne jest skonfigurowanie kilku produktów oprogramowania oraz zapewnienie ich współpracy. Ponieważ każdy z tych produktów wymaga określonych ról i umiejętności, można utworzyć zespół implementujący EIM składający się z osób z kilku różnych działów, szczególnie, jeśli w grę wchodzi duża organizacja.

Poniżej przedstawione zostały informacje opisujące umiejętności i uprawnienia wymagane do pomyślnego zaimplementowania EIM (patrz też “Kontrola dostępu EIM” na stronie 39). Umiejętności te zostały przedstawione jako stanowiska dla ludzi, którzy specjalizują się w tych umiejętnościach. Na przykład zadanie wymagające umiejętności związanych z protokołem LDAP zostało określone jako zadanie dla administratora serwera katalogów.

Członkowie zespołu i ich role

Poniżej opisane zostały odpowiedzialność i wymagane uprawnienia ról potrzebne do zarządzania EIM. Listy tej można użyć do określenia członków zespołu potrzebnych do zainstalowania i skonfigurowania wstępnie wymaganych produktów oraz do skonfigurowania odwzorowań EIM w jednej lub większej liczbie domen EIM.

Jednym z pierwszych zestawów ról, które trzeba zdefiniować, jest liczba i rodzaj administratorów domeny EIM. Każda osoba z obowiązkami i uprawnieniami administratora EIM musi być wpisana podczas procesu planowania EIM jako członek zespołu implementującego EIM.

Uwaga: Administratorzy EIM pełnią ważną funkcję w organizacji i mają taki sam wpływ na system, jak osoba mogąca tworzyć w tym systemie tożsamości użytkowników. Tworząc powiązania EIM dla tożsamości użytkowników, określają oni tym samym, kto ma dostęp do systemów i z jakimi uprawnieniami. Firma IBM zaleca, aby uprawnienie to nadawać tylko osobom mającym najwyższy poziom zaufania w strategii ochrony przedsiębiorstwa.

Poniższa tabela przedstawia możliwe role członków zespołu i zadania oraz umiejętności potrzebne do skonfigurowania odwzorowań EIM i zarządzania nimi. Szczegółowe informacje o zadaniach administracyjnych EIM, które każda z ról może wykonać, zawiera temat “Kontrola dostępu EIM” na stronie 39.

Uwaga: Jeśli w organizacji jedna osoba będzie odpowiedzialna za wszystkie zadania konfiguracyjne i administracyjne EIM, to powinna mieć ona rolę i uprawnienia administratora EIM.

Tabela 10. Role, zadania i umiejętności potrzebne do konfigurowania EIM

Rola	Autoryzowane zadania	Wymagane umiejętności
Administrator EIM	• Koordynacja operacji związanych z domeną • Dodawanie, usuwanie i zmiana definicji rejestrów, identyfikatorów EIM i powiązań dla tożsamości użytkowników • Kontroler uprawnień do danych w domenie EIM	Znajomość narzędzi administrowania EIM
Administrator identyfikatorów EIM	• Tworzenie i zmiana identyfikatorów EIM • Dodawanie i usuwanie powiązań administracyjnych i źródłowych (nie może dodawać ani usuwać powiązań docelowych)	Znajomość narzędzi administrowania EIM
Administrator rejestrów EIM	Zarządzanie wszystkimi definicjami rejestrów EIM: • Dodawanie i usuwanie powiązań docelowych (nie może dodawać ani usuwać powiązań źródłowych ani administracyjnych) • Aktualizowanie definicji rejestrów EIM	Znajomość: • Wszystkich rejestrów użytkowników zdefiniowanych w domenie EIM (na przykład informacji o tożsamościach użytkowników) • Narzędzi do administrowania EIM
Administrator rejestru X EIM	Zarządzanie określoną definicją rejestru EIM: • Dodawanie i usuwanie powiązań docelowych dla określonego rejestru użytkowników (na przykład rejestru X) • Aktualizowanie określonej definicji rejestru EIM	Znajomość: • Konkretnego rejestru użytkowników zdefiniowanego w domenie EIM (na przykład informacji o tożsamościach użytkowników) • Narzędzi do administrowania EIM
Administrator serwera katalogów (LDAP)	• Instalowanie i konfigurowanie serwera katalogów (jeśli jest to potrzebne) • Dostosowanie konfiguracji serwera katalogów dla EIM • Tworzenie domeny EIM (patrz uwaga) • Definiowanie użytkowników autoryzowanych do dostępu do kontrolera domeny EIM • Opcjonalnie: definiowanie pierwszego administratora EIM **Uwaga:** Administrator serwera katalogów może wykonywać dokładnie te same czynności, co administrator EIM.	Znajomość: • Instalowania, konfigurowania i dostosowanie serwera katalogów • Narzędzi do administrowania EIM

Tabela 10. Role, zadania i umiejętności potrzebne do konfigurowania EIM (kontynuacja)

Rola	Autoryzowane zadania	Wymagane umiejętności
Administrator rejestru użytkowników	• Konfigurowanie profili użytkowników lub tożsamości użytkowników dla określonego rejestru użytkowników • Opcjonalnie: pełnienie funkcji administratora rejestru EIM dla określonego rejestru użytkowników	Znajomość: • Narzędzi do administrowania rejestrem użytkowników • Narzędzi do administrowania EIM
Programista lub administrator systemu	Instalowanie potrzebnego oprogramowania (może obejmować instalowanie EIM)	Znajomość: • Umiejętności programowania systemowego i administrowania • Procedury instalacyjne dla platformy
Programista aplikacji	Pisanie aplikacji korzystających z funkcji API EIM	Znajomość: • Platformy • Umiejętność programowania • Kompilowania programów

Po określeniu ról, które będą używane do konfigurowania odwzorowań EIM w przedsiębiorstwie i zarządzania nimi, można przejść do planowania domeny EIM.

Planowanie domeny EIM

Część początkowego procesu planowania implementacji EIM wymaga zdefiniowania domeny EIM. Aby osiągnąć najwięcej korzyści z posiadania scentralizowanego repozytorium informacji odwzorowania, należy zaplanować domenę współużytkowaną przez wiele aplikacji i systemów.

W ramach tematu dotyczącego planowania EIM zbierane są informacje potrzebne do zdefiniowania domeny i do zapisania w arkuszach roboczych planowania. Sekcja przykładowa arkuszy roboczych pomaga w zebraniu i zapisaniu tych informacji na każdym etapie planowania.

W poniższej tabeli wymieniono informacje potrzebne podczas planowania domeny i zasugerowano rolę (lub role) zespołu implementującego EIM, która powinna być odpowiedzialna za każdą potrzebną informację.

Uwaga: Wprawdzie w tabeli wymieniono konkretną rolę sugerując przypisanie do niej odpowiedzialności za zebranie opisanych informacji, jednak role należy przypisać na podstawie strategii ochrony danej organizacji. W mniejszej organizacji można na przykład wyznaczyć jedną osobę jako administratora EIM odpowiedzialnego za wszystkie aspekty planowania, konfigurowania i zarządzania EIM.

Tabela 11. Informacje potrzebne do planowania domeny EIM

Potrzebne informacje	Rola
1. Czy istnieje już domena dopasowana do potrzeb, czy trzeba ją dopiero utworzyć.	Administrator EIM
2. Który serwer katalogów będzie pełnił funkcję kontrolera domeny EIM. (Więcej informacji odnośnie wyboru kontrolera domeny zawiera temat Planowanie kontrolera domeny EIM.)	Administrator serwera katalogów (LDAP) lub EIM
3. Nazwa domeny. (Opcjonalnie można również dodać opis.)	Administrator EIM
4. W którym katalogu będą przechowywane dane domeny EIM. **Uwaga:** W zależności od wybranego systemu do obsługi serwera katalogów i katalogu do przechowywania danych domeny EIM przed utworzeniem domeny może być potrzebne wykonanie pewnych zadań konfiguracyjnych usług katalogowych.	Administrator serwera katalogów (LDAP) i administrator EIM

Tabela 11. Informacje potrzebne do planowania domeny EIM (kontynuacja)

Potrzebne informacje	Rola
5. Aplikacje i systemy operacyjne należące do domeny. Jeśli konfigurowana jest pierwsza domena, to zestaw początkowy może nawet składać się tylko z jednego systemu. (Więcej informacji zawiera temat Tworzenie planu nazewnictwa dla definicji rejestru EIM.)	Zespół EIM
6. Ludzie i jednostki należący do domeny. **Uwaga:** Aby uprościć początkowe testy, można ograniczyć liczbę uczestników do jednego lub dwóch.	Zespół EIM

Jeśli nic z tego, co jest potrzebne do zdefiniowania domeny EIM, nie budzi już wątpliwości, można przejść do sekcji opisującej planowanie kontrolera domeny EIM do przechowywania danych domeny EIM.

Planowanie kontrolera domeny EIM

Po zebraniu informacji do zdefiniowania domeny EIM należy określić, jaki serwer katalogów będzie używany jako kontroler domeny. Odwzorowania EIM wymagają, aby kontroler domeny był udostępniany przez serwer katalogów obsługujący protokół LDAP w wersji 3. Ponadto serwer katalogów musi akceptować schemat LDAP i inne założenia związane z EIM a także rozróżniać różne atrybuty i klasy obiektów.

Jeśli w przedsiębiorstwie jest więcej serwerów katalogów, które mogą udostępniać kontroler domeny EIM, należy rozważyć użycie dodatkowego, replikowanego serwera domeny. Na przykład jeśli ma być przeprowadzanych wiele operacji wyszukiwania odwzorowań EIM, repliki mogą poprawić wydajność tych operacji.

Należy również rozważyć, czy kontroler domeny ma być *lokalny* czy *zdalny* w relacji do systemu, który będzie wykonywał najwięcej operacji wyszukiwania odwzorowań. Jeśli kontroler domeny będzie lokalny systemu o dużym obciążeniu, to można w ten sposób poprawić wydajność operacji wyszukiwania dla systemu lokalnego. Takie decyzje podejmowane w trakcie planowania oraz inne, związane z domeną i innymi informacjami o katalogach, należy zapisać w arkuszach roboczych planowania.

Po określeniu, który serwer katalogów w przedsiębiorstwie będzie służył jako kontroler domeny EIM, należy podjąć kilka decyzji dotyczących dostępu do kontrolera domeny.

Planowanie dostępu do kontrolera domeny

Należy zaplanować dostęp do serwera katalogów udostępniającego kontroler domeny EIM dla aplikacji z obsługą EIM i systemów operacyjnych. Warunki niezbędne do uzyskania dostępu do domeny EIM:

1. Możliwość połączenia z kontrolerem domeny EIM
2. Upewnij się, że łączący się podmiot jest członkiem grupy kontroli dostępu EIM lub administratorem LDAP. Więcej informacji zawiera temat Zarządzanie kontrolą dostępu EIM.

Wybierz typ wiązania EIM

Funkcje API EIM obsługują kilka różnych mechanizmów do nawiązywania połączenia z kontrolerem domeny EIM. Każdy z tych mechanizmów zapewnia inny poziom uwierzytelnienia i szyfrowania połączenia. Można wybrać następujące polecenia:

- **Połączenie proste** Jest to połączenie LDAP, w którym klient LDAP do uwierzytelnienia podaje nazwę wyróżniającą i hasło połączenia dla serwera LDAP. Nazwa wyróżniająca i hasło połączenia są zdefiniowane przez administratora LDAP w katalogu LDAP. Jest to najsłabsza forma uwierzytelnienia i najmniej chroniona, gdyż nazwa wyróżniająca i hasło połączenia są przesyłane w postaci nieszyfrowanej i można je podsłuchać. Użycie protokołu CRAM-MD5 w celu dodania dodatkowego poziomu ochrony dla hasła połączenia. Przy użyciu protokołu CRAM-MD5 klient wysyła do serwera hasło uwierzytelnienia w postaci zakodowanej, a nie jawnym tekstem.
- **Uwierzytelnianie serwera protokołem SSL - uwierzytelnianie po stronie serwera** Serwer LDAP można skonfigurować do połączeń SSL lub TLS. Serwer LDAP korzysta z certyfikatu cyfrowego do uwierzytelnienia się

przed klientem LDAP i nawiązania szyfrowanej sesji komunikacyjnej. Tylko serwer LDAP jest uwierzytelniany przez certyfikat. Użytkownik końcowy jest uwierzytelniany przez nazwę wyróżniającą i hasło połączenia. Poziom złożoności uwierzytelnienia jest taki sam, jak w przypadku prostego połączenia, ale wszystkie dane (włącznie z nazwą wyróżniającą i hasłem połączenia) są szyfrowane w celu zapewnienia prywatności.

- **Uwierzytelnianie klienta protokołem SSL** Serwer LDAP można skonfigurować w taki sposób, aby do nawiązania chronionego połączenia SSL lub TLS wymagał uwierzytelnienia użytkownika za pomocą certyfikatu cyfrowego zamiast nazwy wyróżniającej i hasła połączenia. Uwierzytelnienie obejmuje zarówno klienta, jak i serwer, a sesja jest szyfrowana. Opcja ta zapewnia wyższy poziom uwierzytelnienia użytkownika i chroni prywatność wszystkich przesyłanych danych.
- **Uwierzytelnianie Kerberos** Klient LDAP może być uwierzytelniony przez serwer za pomocą biletu Kerberos, jest to opcjonalne rozwiązanie stosowane zamiast nazwy wyróżniającej i hasła połączenia. Kerberos jest to zaufany system uwierzytelnienia innej firmy i umożliwia użytkownikowi lub usłudze przedstawienie tożsamości wobec innej usługi poprzez niechronioną sieć. Uwierzytelnianie nazw użytkownika Kerberos nadzoruje centralny serwer, nazywany Centrum dystrybucji kluczy (KDC). Centrum KDC uwierzytelnia użytkownika przy użyciu biletu Kerberos. Bilety te potwierdzają tożsamość nazwy użytkownika Kerberos w komunikacji z innymi usługami w sieci. Po uwierzytelnieniu przy użyciu tych biletów użytkownik i usługa mogą wymienić zaszyfrowane dane z usługą docelową. Opcja ta zapewnia wyższy poziom uwierzytelnienia użytkownika i chroni prywatność informacji uwierzytelniających.

Wybór mechanizmu połączenia zależy od poziomu ochrony wymaganego przez aplikację z obsługą EIM i mechanizmów uwierzytelnienia obsługiwanych przez serwer LDAP udostępniający domenę EIM.

Można również wykonać dodatkowe zadania konfiguracyjne dla serwera LDAP włączające wybrany mechanizm uwierzytelnienia. Aby określić te zadania, sprawdź dokumentację danego serwera LDAP.

Przykładowy arkusz roboczy planowania: informacje kontrolera domeny

Po podjęciu decyzji odnośnie kontrolera domeny EIM należy zapisać w arkuszu roboczym planowania informacje dotyczące kontrolera domeny EIM potrzebne dla aplikacji i systemów operacyjnych z obsługą EIM. Informacje zebrane w ramach części tego procesu mogą być wykorzystane przez administratora LDAP do zdefiniowania tożsamości połączenia aplikacji lub systemu operacyjnego z serwerem katalogów LDAP udostępniającym kontroler domeny EIM.

Poniżej znajduje się przykładowy fragment arkusza roboczego planowania pokazujący, jakie informacje należy zebrać. Przedstawione zostały również przykładowe wartości, których można użyć podczas konfigurowania kontrolera domeny EIM.

Tabela 12. Informacje o domenie i kontrolerze domeny w arkuszu roboczym planowania EIM

Informacje potrzebne do skonfigurowania domeny EIM i kontrolera domeny EIM	**Przykładowe odpowiedzi**
Nazwa znacząca dla domeny. Może to być nazwa przedsiębiorstwa, wydziału lub aplikacji używającej domeny.	MojaDomena
Opcjonalnie: jeśli domena EIM jest konfigurowana w istniejącym katalogu LDAP, należy podać nadrzędną nazwę wyróżniającą domeny. Nazwa wyróżniająca reprezentująca pozycję znajdującą się bezpośrednio nad pozycją nazwy domeny w hierarchii drzewa informacji o katalogach, na przykład o=ibm,c=pl.	o=ibm,c=pl

Tabela 12. Informacje o domenie i kontrolerze domeny w arkuszu roboczym planowania EIM (kontynuacja)

Informacje potrzebne do skonfigurowania domeny EIM i kontrolera domeny EIM	**Przykładowe odpowiedzi**
Pełna wynikowa nazwa wyróżniająca domeny EIM. Zdefiniowana pełna nazwa domeny EIM opisująca położenie katalogu dla danych domeny EIM. Pełna nazwa wyróżniająca domeny składa się przynajmniej z nazwy wyróżniającej domeny (ibm-eimDomainName=) i podanej nazwy domeny. Jeśli wybrano podawanie nadrzędnej nazwy wyróżniającej dla domeny, to pełna nazwa wyróżniająca domeny składa się ze względnej nazwy wyróżniającej domeny (ibm-eimDomainName=), nazwy domeny (MojaDomena) i nadrzędnej nazwy wyróżniającej (o=ibm,c=pl). **Uwaga:**	Jedna z poniższych, w zależności od wybranej nadrzędnej nazwy wyróżniającej: • ibm-eimDomainName=MojaDomena • ibm-eimDomainName=MojaDomena,o=ibm,c=pl
Adres połączenia dla kontrolera domeny. Składa się on z typu połączenia (proste połączenie ldap lub chronione, na przykład ldap:// lub ldaps://) oraz z następujących informacji:	ldap://
• Opcjonalnie: nazwa hosta lub adres IP • Opcjonalnie: numer portu	• jakiś.host.ldap • 389
Pełny wynikowy adres połączenia dla kontrolera domeny.	ldap://jakiś.host.ldap:389
Mechanizm połączenia wymagany przez aplikacje lub systemy. Do wyboru jest: • Proste połączenie • Protokół CRAM MD5 • Uwierzytelnianie serwera • Uwierzytelnianie klienta • Kerberos	Kerberos

Jeśli zespoły konfigurujące i administrujące EIM składają się z wielu członków, należy określić tożsamość i mechanizm połączenia, którego ma używać każdy członek zespołu do dostępu do domeny EIM w oparciu o jego rolę. Należy również określić tożsamość i mechanizm połączenia dla użytkowników aplikacji EIM. Przy zbieraniu tych informacji pomocny może być poniższy przykładowy arkusz roboczy.

Tabela 13. Przykładowy arkusz roboczy planowania tożsamości połączeń

Uprawnienie lub rola EIM	**Tożsamość połączenia**	**Mechanizm połączenia**	**Do czego potrzebne**
Administrator EIM	eimadmin@krbrealm1.com	kerberos	konfigurowanie i zarządzanie EIM
Administrator LDAP	cn=administrator	proste połączenie	konfigurowanie kontrolera domeny EIM
Administrator rejestru X EIM	cn=admin2	Protokół CRAM MD5	zarządzanie specyficzną definicją rejestru
Wyszukiwanie odwzorowań EIM	cn=MojaApl,c=PL	proste połączenie	wykonywanie operacji wyszukiwania odwzorowań aplikacji

Po zebraniu informacji potrzebnych do skonfigurowania kontrolera domeny można przystąpić do tworzenia planu odwzorowywania tożsamości.

Tworzenie planu nazewnictwa definicji rejestru EIM

Aby korzystać z odwzorowań EIM do odwzorowania tożsamości użytkownika w jednym rejestrze użytkowników na odpowiadającą jej tożsamość użytkownika w innym rejestrze użytkowników, oba rejestry użytkowników muszą być

zdefiniowane w EIM. Dla każdego rejestru użytkowników aplikacji lub systemu operacyjnego, który będzie należeć do domeny EIM, należy utworzyć definicję rejestru EIM. Rejestry użytkowników mogą reprezentować rejestry systemowe, na przykład Resource Access Control Facility (RACF) lub i5/OS, rejestry rozproszone, na przykład Kerberos lub podzbiór rejestru systemowego używany wyłącznie przez aplikację.

Domena EIM może zawierać definicje rejestrów dla rejestrów użytkowników dowolnej platformy. Na przykład domena zarządzana przez kontroler domeny w systemie i5/OS może zawierać definicje rejestrów dla platform innych niż i5/OS (na przykład rejestru systemu AIX). Dla domeny EIM można zdefiniować dowolny rejestr użytkowników, ale konieczne jest zdefiniowanie rejestrów użytkowników dla tych aplikacji i systemów operacyjnych, które obsługują odwzorowania EIM.

Nazwa definicji rejestru EIM jest dowolna, jednak musi być unikalna w domenie EIM. Można na przykład nazwać definicję rejestru EIM na podstawie nazwy systemu, który udostępnia rejestr użytkowników. Jeśli to nie wystarcza do rozróżnienia definicji rejestru od podobnych definicji, można użyć kropki (.) lub podkreślenia (_), aby dodać rodzaj definiowanego rejestru użytkowników. Niezależnie od wybranego kryterium należy rozważyć utworzenie konwencji nazewnictwa dla definicji rejestrów EIM. W ten sposób zapewniona będzie spójność nazw definicji w domenie oraz to, że będą one odpowiednio opisywać rodzaj i instancję zdefiniowanego rejestru użytkowników, a także jego wykorzystanie. Można na przykład nazywać każdą definicję rejestru za pomocą kombinacji nazwy systemu operacyjnego lub aplikacji korzystającej z rejestru i fizycznego położenia rejestru użytkowników w przedsiębiorstwie.

W aplikacji z obsługą EIM można określić alias rejestru źródłowego, alias rejestru docelowego lub aliasy dla obu rejestrów. Podczas tworzenia definicji rejestrów EIM należy sprawdzić w dokumentacji aplikacji, czy trzeba określić jeden, czy więcej aliasów dla definicji rejestrów. Jeśli aliasy te są przypisane do odpowiednich definicji rejestrów, aplikacja może wykonać wyszukiwanie aliasu w celu znalezienia definicji rejestru lub rejestrów EIM zgodnych z aliasami w aplikacji.

Poniższy przykład arkusza roboczego planowania może być pomocą przy zapisywaniu informacji o rejestrach użytkowników. Bieżącego arkusza roboczego można użyć do podania nazwy definicji rejestru dla każdego rejestru użytkowników, do określenia, czy używa on aliasów oraz do opisania położenia i wykorzystania rejestru użytkowników. Niektóre z informacji potrzebnych w tym arkuszu roboczym zawiera dokumentacja instalowania i konfigurowania aplikacji.

Tabela 14. Przykładowy arkusz roboczy planowania informacji definicji rejestru EIM

Nazwa definicji rejestru	Typ rejestru użytkowników	Alias definicji rejestru	Opis rejestru
System_C	Rejestr użytkowników systemu i5/OS	Patrz dokumentacja aplikacji	Główny rejestr użytkowników systemu i5/OS w systemie C
System_A_WAS	WebSphere LTPA	app_23_alias_source	Rejestr użytkowników WebSphere LTPA w systemie A
System_B	Linux	Patrz dokumentacja aplikacji	Rejestr użytkowników systemu Linux w systemie B
System_A	Rejestr użytkowników systemu i5/OS	app_23_alias_target app_xx_alias_target	Główny rejestr użytkowników systemu i5/OS w systemie A
System_D	Rejestr użytkowników Kerberos	app_xx_alias_source	Dziedzina Kerberos prawo.mojadomena.com
System_4	Rejestr użytkowników systemu Windows 2000	Patrz dokumentacja aplikacji	Rejestr użytkowników aplikacji kadrowej w systemie 4

Uwaga: Rodzaje powiązań dla każdego rejestru zostaną określone w dalszej części procesu planowania.

Po zakończeniu niniejszej sekcji arkusza roboczego planowania należy utworzyć plan odwzorowywania tożsamości, aby określić, czy do tworzenia odwzorowań potrzebnych dla tożsamości użytkowników w każdym ze zdefiniowanych rejestrów użytkowników używać powiązań identyfikatorów, powiązań strategii, czy obu rodzajów powiązań.

Tworzenie planu odwzorowywania tożsamości

Newralgiczna część początkowego procesu planowania implementacji odwzorowania EIM wymaga określenia sposobu używania odwzorowania tożsamości w przedsiębiorstwie. Są dwie metody odwzorowania tożsamości w EIM:

- **Powiązania identyfikatorów** opisują relacje między identyfikatorem EIM a reprezentującą daną osobę tożsamością użytkownika w rejestrach użytkowników. Powiązanie identyfikatora tworzy bezpośrednie odwzorowanie typu jeden-do-jednego między identyfikatorem EIM a daną tożsamością użytkownika. Powiązań identyfikatorów można użyć również do pośredniego zdefiniowania relacji między tożsamościami użytkowników za pomocą identyfikatora EIM.

  Jeśli strategia ochrony wymaga wysokiego stopnia szczegółowego potwierdzania, można używać powiązań identyfikatorów niemal wyłącznie do implementacji odwzorowywania tożsamości. Ponieważ powiązania identyfikatorów są używane do tworzenia odwzorowań typu jeden-do-jednego tożsamości użytkownika danego użytkownika, zawsze można dokładnie określić, kto wykonał działanie na obiekcie lub w systemie.
- **Powiązania strategii** opisują relację między wieloma tożsamościami użytkownika a pojedynczą tożsamością użytkownika w rejestrze użytkowników. Powiązania strategii korzystają z obsługi strategii odwzorowania EIM do utworzenia odwzorowań wielu tożsamości użytkownika do jednej bez wymagania identyfikatora EIM.

  Powiązania strategii mogą być przydatne, jeśli jest co najmniej jedna duża grupa, która potrzebuje dostępu do systemów lub aplikacji w przedsiębiorstwie, a której członkowie nie mają mieć konkretnych tożsamości użytkowników do uzyskiwania tego dostępu. Na przykład istnieje aplikacja WWW mająca dostęp do określonej wewnętrznej aplikacji. Nie chcesz konfigurować setek lub tysięcy tożsamości użytkowników do uwierzytelniania użytkowników w tej aplikacji. W takiej sytuacji można skonfigurować odwzorowanie tożsamości, na przykład wszyscy użytkownicy tej aplikacji WWW są odwzorowywani na pojedynczą tożsamość użytkownika z minimalnym poziomem autoryzacji wymaganym do uruchomienia aplikacji. Ten typ odwzorowywania tożsamości jest możliwy dzięki użyciu powiązań strategii.

Można użyć powiązań identyfikatorów, aby osiągnąć najlepszą kontrolę tożsamości użytkowników w przedsiębiorstwie przy jednoczesnym sprawnym zarządzaniu hasłami. Można również użyć połączenia powiązań strategii i powiązań identyfikatorów, aby osiągnąć pojedyncze logowanie tam, gdzie jest to potrzebne, i jednocześnie zapewnić administratorom dokładną kontrolę nad tożsamościami użytkowników. Niezależnie od tego, który typ odwzorowywania tożsamości najlepiej spełnia dane wymagania i jest zgodny ze strategią ochrony, należy utworzyć plan odwzorowywania tożsamości, aby zapewnić jego odpowiednie zaimplementowanie.

Aby utworzyć plan odwzorowywania tożsamości, wykonaj następujące czynności:

Pojęcia pokrewne

“Tworzenie powiązań” na stronie 99

Planowanie powiązań EIM: Powiązania to pozycje tworzone w domenie EIM w celu zdefiniowania relacji między tożsamościami użytkowników w różnych rejestrach użytkowników. Można utworzyć jedno z dwóch typów powiązań w EIM: powiązanie identyfikatora, definiujące odwzorowanie typu jeden-do-jednego lub powiązanie strategii, definiujące odwzorowanie typu wiele-do-jednego. Powiązań strategii można używać zamiast powiązań identyfikatorów lub w połączeniu z nimi.

Rodzaje połączeń wybranych do utworzenia zależą od tego, jak użytkownik korzysta z danej tożsamości oraz od całego planu odwzorowań tożsamości.

Można utworzyć dowolne z następujących typów połączeń identyfikatorów:

- **Powiązania docelowe**

  Powiązania tego typu definiowane są dla użytkowników, którzy mają tylko dostęp do danego systemu jako do serwera z innych systemów klienta. Ten typ powiązania jest używany, gdy aplikacja wykonuje operacje wyszukiwania odwzorowań.
- **Powiązania źródłowe**

  Powiązania są definiowane, gdy tożsamość użytkownika jest pierwszą, którą użytkownik udostępnia wpisując się do systemu lub sieci. Ten typ powiązania jest używany, gdy aplikacja wykonuje operacje wyszukiwania odwzorowań.
- **Powiązania administracyjne**

Powiązania używane, jeśli śledzona ma być przynależność tożsamości użytkownika do danego użytkownika, ale tożsamość ta nie powinna być dostępna dla operacji wyszukiwania odwzorowań. Można ich użyć do śledzenia wszystkich tożsamości użytkownika, których dana osoba używa w przedsiębiorstwie.

Powiązanie strategii zawsze definiuje połączenie docelowe.

Pojedyncza definicja rejestru może mieć więcej niż jeden typ powiązania w zależności o tego, jak jest używany rejestr użytkowników, do którego się ona odnosi. Wprawdzie nie istnieje limit ilości lub kombinacji powiązań, które można zdefiniować, jednak aby uprościć administrowanie domeną EIM, wskazane jest ich zminimalizowanie.

Zazwyczaj aplikacja udostępnia wskazówki informujące, które definicje rejestru mają być rejestrami źródłowymi i docelowymi, ale nie typy powiązań. Każdy użytkownik końcowy aplikacji musi być odwzorowany na aplikację przez co najmniej jedno powiązanie. Powiązanie to może być odwzorowaniem typu jeden-do-jednego między unikalnym identyfikatorem EIM użytkownika i jego tożsamością w żądanym rejestrze docelowym lub odwzorowaniem typu wiele-do-jednego między rejestrem źródłowym, którego członkiem jest tożsamość użytkownika, a żądanym rejestrem docelowym. Użycie danego typu powiązania zależy od wymagań dotyczących odwzorowania tożsamości i kryterium udostępnionego przez aplikację.

Wcześniej, w ramach części procesu planowania, wypełnione zostały dwa arkusze robocze planowania dla tożsamości użytkowników w organizacji i zawierają one informacje o potrzebnych identyfikatorach EIM i definicjach rejestrów EIM. W tym momencie należy połączyć te informacje określając typy powiązań, które mają być używane do odwzorowania tożsamości użytkowników w przedsiębiorstwie. Należy określić, czy definiować połączenia strategii dla poszczególnych aplikacji i ich rejestrów użytkowników, albo czy definiować konkretne powiązania identyfikatorów (źródłowe, docelowe lub administracyjne) dla każdej tożsamości użytkownika w systemie lub w rejestrze aplikacji. W tym celu należy zapisać informacje o wymaganych typach powiązań w arkuszach roboczych planowania definicji rejestru i w odpowiednim wierszu każdego arkusza roboczego powiązań.

Aby zakończyć planowanie odwzorowań tożsamości, można użyć następujących przykładowych arkuszy roboczych planowania jako podręcznika pomocnego przy zapisywaniu informacji o powiązaniu, które są potrzebne do opisania pełnego obrazu planu implementacji odwzorowania tożsamości.

Tabela 15. Przykładowy arkusz roboczy planowania informacji definicji rejestru EIM

Nazwa definicji rejestru	Typ rejestru użytkowników	Alias definicji rejestru	Opis rejestru	Typy powiązań
System_C	Rejestr użytkowników systemu i5/OS	Patrz dokumentacja aplikacji	Główny rejestr użytkowników systemu i5/OS w systemie C	Docelowe
System_A_WAS	WebSphere LTPA	app_23_alias_source	Rejestr użytkowników WebSphere LTPA w systemie A	Źródło pierwotne
System_B	Linux	Patrz dokumentacja aplikacji	Rejestr użytkowników systemu Linux w systemie B	Źródłowe i docelowe
System_A	Rejestr użytkowników systemu i5/OS	app_23_alias_target app_xx_alias_target	Główny rejestr użytkowników systemu i5/OS w systemie A	Docelowe
System_D	Rejestr użytkowników Kerberos	app_xx_alias_source	Dziedzina Kerberos prawo.mojadomena.com	Źródłowe
System_4	Rejestr użytkowników systemu Windows 2000	Patrz dokumentacja aplikacji	Rejestr użytkowników aplikacji kadrowej w systemie 4	Administracyjne
zamów.domena.com	Rejestr użytkowników systemu Windows 2000		Główny rejestr logowania dla pracowników wydziału zamówień	Strategia rejestru domyślnego (rejestr źródłowy)

Tabela 15. Przykładowy arkusz roboczy planowania informacji definicji rejestru EIM (kontynuacja)

Nazwa definicji rejestru	Typ rejestru użytkowników	Alias definicji rejestru	Opis rejestru	Typy powiązań
System_A_order_app	Aplikacja wydziału zamówień		Rejestr aplikacji do aktualizacji zamówień	Strategia rejestru domyślnego (rejestr docelowy)
System_C_order_app	Aplikacja wydziału zamówień		Rejestr aplikacji do aktualizacji zamówień	Strategia rejestru domyślnego (rejestr docelowy)

Tabela 16. Przykładowy arkusz roboczy planowania identyfikatorów EIM

Unikalna nazwa identyfikatora	Opis identyfikatora lub tożsamości użytkownika	Alias identyfikatora
Jan S Kowalski	Menedżer kadr	app_23_admin
Jan J Kowalski	Wydział prawniczy	app_xx_admin
Maria A. Kowalczyk	Administrator wydziału zamówień	

Tabela 17. Przykładowy arkusz roboczy planowania powiązania identyfikatora

Nazwa unikalna identyfikatora: _____Jan S Kowalski_____		
Rejestr użytkowników	**Tożsamość użytkownika**	**Typy powiązań**
System A WAS w systemie A	jankowalski	Źródłowe
Rejestr użytkowników systemu Linux w systemie B	jsk1	Źródłowe i docelowe
i5/OS w systemie C	JANK	Docelowe
Registry 4 w Windows 2000 z aplikacją do obsługi kadr	JKOWALSKI	Administracyjne

Tabela 18. Przykładowy arkusz roboczy planowania dla powiązań strategii

Typ powiązania strategii	Rejestr użytkowników źródłowych	Rejestr użytkowników docelowych	Tożsamość użytkownika	Opis
Rejestr domyślny	zamów.domena.com	System_A_order_app	SYSUSERA	Odwzorowuje uwierzytelnionego użytkownika systemu Windows wydziału zamówień na odpowiednią tożsamość użytkownika aplikacji
Rejestr domyślny	zamów.domena.com	System_C_order_app	SYSUSERB	Odwzorowuje uwierzytelnionego użytkownika systemu Windows wydziału zamówień na odpowiednią tożsamość użytkownika aplikacji

Tworzenie planu nazewnictwa identyfikatorów EIM: Podczas planowania wymagań odwzorowania tożsamości produktu EIM można utworzyć unikalne identyfikatory EIM dla użytkowników aplikacji i systemów operacyjnych w przedsiębiorstwie z obsługą odwzorowań EIM jeśli dla użytkowników mają być utworzone odwzorowania typu jeden-do-jednego między ich tożsamościami. Korzystając z powiązań identyfikatorów do utworzenia odwzorowań typu jeden-do-jednego można osiągnąć maksymalne korzyści z zarządzania hasłami udostępnianego przez EIM.

Tworzony plan nazewnictwa zależy od wymagań i preferencji biznesowych; jedynym wymaganiem wobec nazw identyfikatorów EIM jest ich unikalność. Niektóre przedsiębiorstwa wolą używać imienia i nazwiska danej osoby, inne wolą używać innego typu danych, na przykład numeru pracownika. Jeśli nazwy identyfikatorów EIM mają być tworzone na podstawie imienia i nazwiska każdej osoby, możliwe jest zduplikowanie nazw. Sposób obsługi potencjalnych duplikatów zależy od preferencji osobistych. Można obsłużyć każdy przypadek ręcznie dodając do każdej nazwy identyfikatra zapewniający unikalność, wstępnie określony łańcuch znaków; na przykład można dodać numer wydziału danej osoby.

Jako część tworzenia planu nazewnictwa identyfikatorów EIM należy podjąć decyzję w sprawie ogólnego planu odwzorowywania tożsamości. Może to pomóc w decyzji dotyczącej odwzorowywania tożsamości w przedsiębiorstwie za pomocą identyfikatorów i powiązań identyfikatorów lub powiązań strategii. Aby utworzyć plan nazewnictwa identyfikatorów EIM, można skorzystać z poniższego arkusza roboczego pomagającego w zebraniu informacji o tożsamościach użytkowników w organizacji i w zaplanowaniu identyfikatorów EIM dla tych tożsamości. Arkusz roboczy przedstawia, jakie informacje są niezbędne dla administratora EIM podczas tworzenia identyfikatorów EIM lub powiązań strategii dla użytkowników aplikacji.

Tabela 19. Przykładowy arkusz roboczy planowania identyfikatorów EIM

Unikalna nazwa identyfikatora	**Opis identyfikatora lub tożsamości użytkownika**	**Alias identyfikatora**
Jan S Kowalski	Menedżer kadr	app_23_admin
Jan J Kowalski	Wydział prawniczy	app_xx_admin
Maria A. Kowalczyk	Administrator wydziału zamówień	

Aplikacja napisana tak, aby korzystała z odwzorowań EIM, może określić alias używany do wyszukania odpowiedniego identyfikatora EIM dla aplikacji, z którego może ona korzystać do określenia konkretnej tożsamości użytkownika, której ma używać. Należy sprawdzić dokumentację aplikacji, aby określić, czy dla identyfikatora trzeba podać jeden lub więcej aliasów. Pola identyfikatora EIM i tożsamości użytkownika mają dowolny format i można ich użyć do opisania użytkownika.

Nie trzeba jednocześnie utworzyć identyfikatorów EIM dla wszystkich członków przedsiębiorstwa. Po utworzeniu początkowego identyfikatora EIM i użyciu go do testów konfiguracji EIM można utworzyć dodatkowe identyfikatory EIM w zależności od celów, którym w przedsiębiorstwie mają służyć odwzorowania EIM. Można na przykład dodać identyfikatory EIM w ramach wydziałów lub danego obszaru. Można również dodać identyfikatory EIM w ramach wdrażania dodatkowych aplikacji EIM.

Po zebraniu informacji niezbędnych do utworzenia planu nazewnictwa identyfikatorów EIM można zaplanować powiązania dla tożsamości użytkowników.

Arkusze robocze planowania implementacji EIM

Podczas procesu planowania EIM do zbierania danych niezbędnych do skonfigurowania i używania EIM w przedsiębiorstwie pomocne mogą być przedstawione poniżej arkusze robocze. Przykłady wypełnionych sekcji tych arkuszy znajdują się na odpowiednich stronach planowania.

Arkusze te są przykładem arkuszy planowania potrzebnych do utworzenia planu implementacji EIM. Liczba pozycji jest prawdopodobnie mniejsza od potrzebnej do zgromadzenia informacji o odwzorowaniach EIM. Arkusze te można edytować i dostosowywać do własnych potrzeb.

Tabela 20. Arkusz roboczy informacji o domenie i kontrolerze domeny

Informacje potrzebne do skonfigurowania domeny EIM i kontrolera domeny EIM	**Odpowiedzi**
Nazwa znacząca dla domeny. Może to być nazwa przedsiębiorstwa, wydziału lub aplikacji używającej domeny.	

Tabela 20. Arkusz roboczy informacji o domenie i kontrolerze domeny (kontynuacja)

Opcjonalnie: nadrzędna nazwa wyróżniająca dla domeny. Nazwa wyróżniająca reprezentująca pozycję znajdującą się bezpośrednio nad pozycją nazwy domeny w hierarchii drzewa informacji o katalogach, na przykład o=ibm,c=pl.	
Pełna wynikowa nazwa wyróżniająca domeny EIM. Zdefiniowana pełna nazwa domeny EIM opisująca położenie katalogu dla danych domeny EIM. Pełna nazwa wyróżniająca domeny składa się przynajmniej z nazwy wyróżniającej domeny (ibm-eimDomainName=) i podanej nazwy domeny. Jeśli wybrano podawanie nadrzędnej nazwy wyróżniającej dla domeny, to pełna nazwa wyróżniająca domeny składa się ze względnej nazwy wyróżniającej domeny (ibm-eimDomainName=), nazwy domeny (MojaDomena) i nadrzędnej nazwy wyróżniającej (o=ibm,c=pl).	
Adres połączenia dla kontrolera domeny. Składa się on z typu połączenia (proste połączenie ldap lub chronione, na przykład ldap:// lub ldaps://) oraz z następujących informacji:	
• Opcjonalnie: nazwa hosta lub adres IP • Opcjonalnie: numer portu	
Pełny wynikowy adres połączenia dla kontrolera domeny.	
Mechanizm połączenia wymagany przez aplikacje lub systemy. Do wyboru jest: • Proste połączenie • Protokół CRAM MD5 • Uwierzytelnianie serwera • Uwierzytelnianie klienta • Kerberos	

Przykład korzystania z tego arkusza roboczego zawiera temat Planowanie kontrolera domeny EIM.

Tabela 21. Arkusz roboczy planowania tożsamości połączeń

Uprawnienie lub rola EIM	Tożsamość połączenia	Mechanizm połączenia	Do czego potrzebne

Przykład korzystania z tego arkusza roboczego zawiera temat Planowanie kontrolera domeny EIM.

Tabela 22. Arkusz roboczy planowania informacji definicji rejestru EIM

Nazwa definicji rejestru	Typ rejestru użytkowników	Alias definicji rejestru	Opis rejestru	Typy powiązań

Tabela 22. Arkusz roboczy planowania informacji definicji rejestru EIM (kontynuacja)

Przykład korzystania z tego arkusza roboczego zawiera temat Tworzenie planu nazewnictwa dla definicji rejestru EIM.

Tabela 23. Arkusz roboczy planowania identyfikatorów EIM

Unikalna nazwa identyfikatora	**Opis identyfikatora lub tożsamości użytkownika**	**Alias identyfikatora**

Przykład korzystania z tego arkusza roboczego zawiera temat Tworzenie planu nazewnictwa identyfikatorów EIM.

Tabela 24. Arkusz roboczy planowania powiązania identyfikatora

Nazwa unikalna identyfikatora: _____Jan S Kowalski_____		
Rejestr użytkowników	Tożsamość użytkownika	Typy powiązań

Przykład korzystania z tego arkusza roboczego zawiera temat Planowanie powiązań EIM.

Tabela 25. Arkusz roboczy planowania powiązania strategii

Typ powiązania strategii	Rejestr użytkowników źródłowych	Rejestr użytkowników docelowych	Tożsamość użytkownika	Opis

Przykład korzystania z tego arkusza roboczego zawiera temat Planowanie powiązań EIM.

Planowanie projektowania aplikacji EIM

Aby aplikacja mogła używać EIM i być w domenie, musi mieć możliwość korzystania z funkcji API EIM. Przejrzyj dokumentację dotyczącą funkcji API EIM i dokumentację EIM dla danej platformy pod kątem założeń, które należy wziąć pod uwagę pisząc lub adaptując aplikacje, aby korzystały z funkcji API EIM. Na przykład mogą to być założenia związane z aplikacjami w języku C lub C++, które wywołują funkcje API EIM. W zależności od platformy aplikacji mogą do być założenia związane z łączeniem, edycją itp.

Planowanie EIM dla serwera i5/OS

Istnieje wiele technologii i usług towarzyszących EIM na serwerze iSeries. Przed skonfigurowaniem EIM na serwerze należy zdecydować, jakie funkcje mają być zaimplementowane za pomocą EIM i obsługi pojedynczego logowania.

Przed zaimplementowaniem EIM należy określić i zaimplementować podstawowe wymagania dotyczące ochrony sieci. EIM umożliwia administratorom i użytkownikom łatwiejsze zarządzanie tożsamościami w przedsiębiorstwie. EIM używane wraz z usługą uwierzytelniania sieciowego zapewnia w przedsiębiorstwie obsługę pojedynczego logowania.

Jeśli do uwierzytelniania użytkowników, jako części implementacji pojedynczego logowania, ma być używany protokoł Kerberos, należy skonfigurować usługę uwierzytelniania sieciowego. Informacje o planowaniu usług uwierzytelniania sieciowego zawiera temat Planowanie usług uwierzytelniania sieciowego, a informacje o planowaniu środowiska pojedynczego logowania zawiera temat Planowanie pojedynczego logowania.

Więcej informacji na temat planowania konfiguracji EIM na serwerze iSeries zawierają następujące tematy:

Wymagania wstępne instalacji produktu EIM dla serwera iSeries

W poniższym arkuszu roboczym planowania wymienione zostały usługi, które należy zainstalować przed konfigurowaniem EIM.

Tabela 26. Arkusz roboczy planowania instalacji EIM

Arkusz roboczy planowania wymagań wstępnych EIM	**Odpowiedzi**
Czy wersją systemu operacyjnego jets V5R4 (5722-SS1)?	
Czy na serwerze iSeries™ zainstalowano następujące opcje i produkty licencjonowane? • i5/OS Host Servers (5722-SS1 opcja 12) • iSeries Access for Windows® (5722-XE1) • Interpreter Qshell (5722-SS1 opcja 30) Konieczny, jeśli oprócz EIM planujesz konfigurować usługę uwierzytelniania sieciowego.	
Czy na komputerze PC administratora zainstalowano program iSeries Navigator z następującymi komponentami? • Ochrona Konieczna, jeśli oprócz EIM planujesz konfigurować usługę uwierzytelniania sieciowego. • Sieć	

Tabela 26. Arkusz roboczy planowania instalacji EIM (kontynuacja)

Czy zainstalowano najnowszy pakiet serwisowy programu iSeries Access for Windows? Najnowszy pakiet serwisowy można znaleźć na stronie iSeries Access 	
Czy serwer katalogów, na przykład IBM Directory Server for iSeries (LDAP) został już skonfigurowany i czy ma działać jako kontroler domeny EIM, czy znasz nazwę wyróżniającą i hasło administratora LDAP?	
Jeśli serwer katalogów jest już skonfigurowany, czy można do na moment zatrzymać? (Będzie to wymagane w celu zakończenia procesu konfigurowania EIM.)	
Czy masz uprawnienia specjalne *SECADM, *ALLOBJ i *IOSYSCFG?	
Czy zostały zastosowane najnowsze poprawki PTF?	

Instalowanie wymaganych opcji programu iSeries Navigator

Aby aktywować środowisko pojedynczego logowania za pomocą produktu EIM i usługi uwierzytelniania sieciowego, należy zainstalować opcje **Sieć** i **Ochrona** programu iSeries Navigator. EIM znajduje się w opcji **Sieć**, a usługa uwierzytelniania sieciowego znajduje się w opcji **Ochrona**. Jeśli nie planuje się użycia usługi uwierzytelniania sieciowego, nie trzeba instalować opcji **Ochrona** programu iSeries Navigator.

Aby zainstalować opcję Sieć programu iSeries Navigator lub sprawdzić, czy opcja ta jest już zainstalowana, sprawdź, czy oprogramowanie iSeries Access for Windows jest zainstalowane na komputerze PC używanym do administrowania serwerem iSeries.

Aby zainstalować opcję **Sieć**:

1. Kliknij **Start > Programy > IBM iSeries Access for Windows > Instalacja selektywna**.
2. Postępuj zgodnie z instrukcjami wyświetlanymi w oknie dialogowym. W oknie dialogowym **Wybór komponentów** rozwiń pozycję **iSeries Navigator**, a następnie wybierz opcję **Sieć**. Jeśli planujesz używanie usługi uwierzytelniania sieciowego, musisz także wybrać opcję **Ochrona**.
3. Kontynuuj pracę z programem instalacyjnym.

Uwagi dotyczące składowania i odtwarzania EIM

Bardzo ważne jest utworzenie planu tworzenia i odzyskiwania kopii zapasowych danych EIM, aby dane te były chronione i mogły być odtworzone w przypadku wystąpienia problemu z serwerem katalogów obsługującym kontroler domeny EIM. Równie ważne są informacje o konfiguracji EIM, dlatego należy zapoznać się z informacjami dotyczącymi ich odzyskiwania.

Składowanie i odtwarzanie danych domeny produktu EIM:

Sposób składowania danych EIM zależy od podjętej decyzji dotyczącej zarządzania tym aspektem serwera katalogów, który pełni rolę kontrolera domeny dla danych EIM.

Jedną z metod składowania danych, szczególnie dla celów odzyskiwania po awarii, jest składowanie biblioteki bazy danych. Domyślnie jest to QUSRDIRDB. Jeśli włączona jest opcja changelog, należy składować również bibliotekę QUSRDIRCL. Serwer katalogów w systemie, w którym ma być odtworzona biblioteka, musi mieć taki sam schemat LDAP i taką samą konfigurację, jak oryginalny serwer katalogów. Pliki, w których przechowywane są te informacje, znajdują się w katalogu /QIBM/UserData/OS400/DirSrv. Dodatkowe dane konfiguracyjne są przechowywane w QUSRSYS/QGLDCFG (obiekt *USRSPC) i QUSRSYS/QGLDVLDL (obiekt *VLDL). Aby uzyskać pełną kopię zapasową wszystkich danych serwera katalogów, należy składować obie biblioteki, pliki zintegrowanego systemu plików i obiekty QUSRSYS.

Więcej informacji o składowaniu i odtwarzaniu niezbędnych danych serwera katalogów można znaleźć w temacie Składowanie i odtwarzanie informacji serwera katalogów Centrum informacyjnego serwera IBM Directory Server for iSeries (LDAP).

Można na przykład użyć pliku w formacie LDIF do składowania całej zawartości serwera katalogów lub jego części. Aby składować informacje domeny dla kontrolera domeny serwera IBM Directory Server for iSeries, wykonaj następujące czynności:

1. W programie iSeries Navigator rozwiń **Sieć > Serwery > TCP/IP**.
2. Kliknij prawym przyciskiem myszy **IBM Directory Server**, wybierz **Narzędzia**, a następnie **Eksportuj plik**, aby wyświetlić stronę umożliwiającą określenie, które elementy zawartości serwera katalogów wyeksportować do pliku.
3. Prześlij ten plik do serwera iSeries, który ma być używany jako zapasowy serwer katalogów.
4. W programie iSeries Navigator serwera zapasowego rozwiń **Sieć > Serwery > TCP/IP**.
5. Kliknij prawym przyciskiem myszy **IBM Directory Server**, wybierz **Narzędzia**, a następnie **Importuj**, aby załadować przesłany plik do nowego serwera katalogów.

Inną wartą rozważenia metodą składowania danych domeny EIM jest skonfigurowanie i używanie serwera repliki katalogów. Wszystkie zmiany danych domeny EIM są automatycznie przekazywane do serwera repliki katalogów, dzięki czemu jeśli serwer katalogów obsługujący kontroler domeny ulegnie awarii lub utraci dane EIM, można będzie odzyskać dane z serwera repliki.

Konfigurowanie serwera repliki katalogów zależy od wybranego typu modelu replikacji. Więcej informacji na temat replikacji i konfigurowania serwera katalogów dla replikacji zawierają tematy Replikacja i Zarządzanie replikacją w artykule IBM Directory Server for iSeries (LDAP) w Centrum informacyjnym.

Składowanie i odtwarzanie informacji konfiguracyjnych EIM:

Gdy zajdzie konieczność wyłączenia systemu, potrzebne może być odtworzenie informacji konfiguracyjnych EIM dla tego systemu. Informacji tych nie można łatwo składować i odtwarzać w różnych systemach.

Do składowania i odtwarzania konfiguracji EIM dostępne są następujące opcje:

- Aby składować informacje konfiguracyjne EIM i inne ważne informacje konfiguracyjne, użyj w każdym systemie komendy Składowanie danych ochrony (Save Security Data - SAVSECDTA). Następnie w każdym systemie odtwórz profil użytkownika QSYS.

  Uwaga: Użycie komendy SAVSECDTA i odtworzenie profilu użytkownika QSYS jest konieczne w każdym systemie z konfiguracją EIM. Próba odtworzenia obiektu profilu użytkownika QSYS w innym systemie, niż w tym, w którym został utworzony, może spowodować problemy.
- Uruchom ponownie kreatora konfiguracji EIM lub ręcznie zaktualizuj właściwości folderu konfiguracji EIM. Aby ułatwić ten proces, należy zachować arkusze robocze planowania implementacji EIM lub zapisać informacje konfiguracyjne EIM dla każdego systemu.

Dodatkowo należy rozważyć i zaplanować sposób składowania i odtwarzania danych usługi uwierzytelniania sieciowego, jeśli usługa uwierzytelniania sieciowego została skonfigurowana jako część implementacji środowiska pojedynczego logowania.

Konfigurowanie EIM

Informacje o używaniu kreatora konfigurowania EIM do skonfigurowania produktu EIM dla serwerów iSeries.

Kreator konfiguracji EIM umożliwia szybkie i łatwe wykonanie podstawowej konfiguracji produktu EIM dla serwera iSeries. Kreator przeprowadza przez trzy opcje konfiguracji systemu EIM. Sposób użycia kreatora do konfigurowania EIM w danym systemie zależy od ogólnego planu używania EIM w przedsiębiorstwie i od wymagań wobec konfiguracji EIM. Na przykład wielu administratorów korzysta z EIM w połączeniu z usługą uwierzytelniania

sieciowego tworząc środowisko pojedynczego logowania w wielu systemach i na wielu platformach bez zmieniania podstawowych strategii ochrony. Dlatego też kreator konfigurowania EIM umożliwia skonfigurowanie usługi uwierzytelniania sieciowego w ramach części konfigurowania EIM. Skonfigurowanie i używanie usługi uwierzytelniania sieciowego nie stanowi jednak wymagania wstępnego dotyczącego konfigurowania i używania EIM.

Przed rozpoczęciem procesu konfigurowania EIM dla jednego lub większej liczby systemów, należy zaplanować implementację EIM, aby zebrać potrzebne dane. Trzeba na przykład podjąć decyzje dotyczące następujących spraw:

- Który serwer iSeries ma być skonfigurowany jako kontroler domeny EIM? Najpierw należy użyć kreatora konfigurowania EIM do utworzenia nowej domeny na tym systemie, a następnie za pomocą kreatora należy skonfigurować wszystkie pozostałe serwery iSeries i dołączyć je do domeny.
- Czy usługa uwierzytelniania sieciowego ma być konfigurowana na każdym systemie konfigurowanym dla EIM? Jeśli tak, można użyć kreatora konfigurowania EIM do utworzenia prostej konfiguracji usługi uwierzytelniania sieciowego na każdym serwerze iSeries. Jednakże konieczne jest wykonanie innych zadań niezbędnych do zakończenia konfigurowania usługi uwierzytelniania sieciowego.

Po utworzeniu kreatorem konfigurowania EIM podstawowej konfiguracji dla każdego serwera iSeries, a przed zakończeniem konfigurowania EIM, nadal niezbędne jest wykonanie pewnych zadań konfiguracji EIM. Przykład ilustrujący konfigurowanie środowiska pojedynczego logowania za pomocą usługi uwierzytelniania sieciowego i EIM w fikcyjnym przedsiębiorstwie zawiera temat Scenariusz: aktywowanie pojedynczego logowania.

Aby skonfigurować odwzorowania EIM, należy mieć wszystkie poniżej wymienione uprawnienia specjalne:

- Administrator ochrony (*SECADM).
- Wszystkie obiekty (*ALLOBJ).
- Konfiguracja systemu (*IOSYSCFG).

Przed użyciem kreatora konfigurowania EIM należy zakończyć wszystkie czynności opisane w sekcji “Planowanie EIM” na stronie 51, aby dokładnie określić sposób wykorzystania EIM. Jeśli konfigurujesz EIM jako część tworzenia środowiska pojedynczego logowania, wykonaj również wszystkie czynności planowania pojedynczego logowania.

Aby uzyskać dostęp do kreatora konfigurowania EIM:

1. Uruchom program iSeries Navigator.
2. Wpisz się do serwera iSeries, dla którego chcesz skonfigurować EIM. Jeśli konfigurujesz EIM dla więcej niż jednego serwera iSeries, rozpocznij konfigurowanie od serwera, który chcesz skonfigurować jako kontroler domeny dla EIM.
3. Rozwiń gałąź **Sieć → Odwzorowanie EIM**.
4. Kliknij prawym przyciskiem myszy **Konfiguracja** i wybierz **Konfiguruj...**, aby uruchomić kreatora konfigurowania EIM.
5. Wybierz opcję konfigurowania EIM, i wykonaj po kolei instrukcje kreatora.
6. Kliknij **Pomoc**, jeśli chcesz przeczytać, jakie dane podać w danym momencie.

Po zakończeniu planowania można za pomocą kreatora konfigurowania EIM utworzyć jedną z trzech podstawowych konfiguracji EIM. Kreatora można użyć do połączenia z istniejącą domeną, albo do utworzenia nowej domeny i połączenia się z nią. Jeśli używasz kreatora konfigurowania EIM do utworzenia nowej domeny i połączenia się z nią, możesz wybrać, czy kontroler domeny EIM skonfigurować na systemie lokalnym, czy zdalnym. Poniżej przedstawione zostały instrukcje konfigurowania EIM w zależności od wybranego rodzaju konfiguracji EIM:

Tworzenie nowej domeny lokalnej i jej przyłączanie

Informacje objaśniające, jak utworzyć nową domenę EIM dla przedsiębiorstwa i skonfigurować lokalny serwer katalogów jako kontroler domeny EIM dla tej domeny.

Jeśli używasz kreatora konfigurowania EIM do utworzenia nowej domeny i połączenia się z nią, możesz w ramach części konfiguracji EIM skonfigurować kontroler domeny EIM na systemie lokalnym. Jeśli to konieczne, kreator

konfiguracji EIM sprawdza, czy podano podstawowe informacje konfiguracyjne dla serwera katalogów. Ponadto, jeśli na serwerze iSeries nie skonfigurowano protokołu Kerberos, kreator wyświetla zachętę do uruchomienia kreatora konfigurowania usługi uwierzytelniania sieciowego.

Po zakończeniu działania kreatora konfigurowania EIM można wykonać następujące zadania:

- Tworzenie nowej domeny EIM.
- Konfigurowanie lokalnego serwera katalogów jako kontrolera domeny EIM.
- Konfigurowanie usługi uwierzytelniania sieciowego dla systemu.
- Tworzenie definicji rejestrów EIM dla rejestru lokalnego i5/OS i rejestru Kerberos.
- Konfigurowanie systemu do udziału w nowej domenie EIM.

Aby skonfigurować system do utworzenia nowej domeny EIM i połączenia się z nią, niezbędne są następujące uprawnienia specjalne:

- Administrator ochrony (*SECADM).
- Wszystkie obiekty (*ALLOBJ).
- Konfiguracja systemu (*IOSYSCFG).

Aby za pomocą kreatora konfigurowania EIM utworzyć nową domenę lokalną i ją przyłączyć, wykonaj następujące czynności:

1. W programie iSeries Navigator wybierz system, dla którego chcesz skonfigurować EIM, i rozwiń gałąź **Sieć > Odwzorowanie EIM**.
2. Kliknij prawym przyciskiem myszy **Konfiguracja** i wybierz **Konfiguruj...**, aby uruchomić kreatora konfigurowania EIM.

   Uwaga: Jeśli w systemie zostały już skonfigurowane odwzorowania EIM, opcja nosi nazwę **Rekonfiguruj...**.
3. Na stronie **Witamy** wybierz opcję **Utwórz i przyłącz nową domenę** i kliknij przycisk **Dalej**.
4. Na stronie **Określanie położenia domeny EIM** wybierz opcję **Na lokalnym serwerze katalogów** i kliknij **Dalej**.

   Uwaga: Opcja ta konfiguruje lokalny serwer katalogów jako kontroler domeny EIM. Ponieważ serwer katalogów przechowuje wszystkie dane EIM dla domeny, musi on być cały czas aktywny, aby obsługiwać operacje wyszukiwania odwzorowań i inne.

   Jeśli na serwerze iSeries nie jest skonfigurowana usługa uwierzytelniania sieciowego lub potrzebne są dodatkowe informacje konfiguracyjne uwierzytelniania sieciowego aby skonfigurować środowisko pojedynczego logowania, wyświetlona zostanie strona **Konfigurowanie usługi uwierzytelniania sieciowego**. Strona ta umożliwia uruchomienie kreatora i skonfigurowanie usługi uwierzytelniania sieciowego. Można również skonfigurować usługę uwierzytelniania sieciowego później, używając kreatora konfigurowania dla tej usługi z programu iSeries Navigator. Po zakończeniu konfigurowania usługi uwierzytelniania sieciowego można kontynuować pracę w kreatorze konfiguracji EIM.
5. Aby skonfigurować usługę uwierzytelniania sieciowego, wykonaj następujące czynności:
   a. Na stronie **Konfigurowanie usługi uwierzytelniania sieciowego** wybierz **Tak**, aby uruchomić kreatora konfigurowania usługi uwierzytelniania sieciowego. Korzystając z tego kreatora można skonfigurować kilka interfejsów i usług systemu i5/OS, w tym dziedzinę Kerberos, lub skonfigurować środowisko pojedynczego logowania używające jednocześnie EIM i usługi uwierzytelniania sieciowego.
   b. Na stronie **Podaj dane dziedziny** podaj nazwę domyślnej dziedziny w polu **Dziedzina domyślna**. Jeśli używasz uwierzytelniania Microsoft Active Directory for Kerberos, wybierz **Do uwierzytelniania Kerberos używana jest funkcja Microsoft Active Directory** i kliknij **Dalej**.
   c. Na stronie **Podaj dane KDC** w polu **KDC** podaj pełną nazwę serwera Kerberos dla tej dziedziny, w polu **Port** wpisz 88 i kliknij **Dalej**.
   d. Na stronie **Podaj dane serwera haseł** wybierz **Tak** lub **Nie** decydując, czy skonfigurować serwer haseł. Serwer haseł umożliwia użytkownikom zmianę haseł na serwerze Kerberos. Jeśli wybierzesz **Tak**, w polu **Serwer haseł** wprowadź nazwę serwera haseł. W polu **Port** akceptuj domyślną wartość 464 i kliknij Dalej.

e. Na stronie **Wybór pozycji tabeli kluczy** wybierz **Uwierzytelnianie Kerberos i5/OS** i kliknij **Dalej**.

Uwaga: Można ponadto utworzyć również pozycje tabeli kluczy dla serwera IBM Directory Server for iSeries (LDAP), iSeries NetServer i serwera iSeries HTTP, jeśli te usługi mają korzystać z uwierzytelniania Kerberos. W tym celu może być potrzebna dodatkowa konfiguracja dla tych usług.

f. Na stronie **Tworzenie pozycji tabeli kluczy i5/OS** wpisz hasło i potwierdź je, a następnie kliknij **Dalej**. Jest to to samo hasło, którego będziesz używać przy dodawaniu nazw użytkowników i5/OS do serwera Kerberos.

g. Opcjonalne: Na stronie **Tworzenie pliku wsadowego** wybierz **Tak**, podaj poniższe dane i kliknij **Dalej**:

- W polu **Plik wsadowy** aktualizuj ścieżkę katalogu. Kliknij **Przeglądaj**, aby znaleźć odpowiednią ścieżkę katalogu lub edytować ścieżkę w polu **Plik wsadowy**.
- W polu **Włączyć hasło** wybierz **Tak**. Zapewni to, że wszystkie hasła powiązane z użytkownikiem usługi i5/OS będą zawarte w pliku wsadowym. Należy zauważyć, że hasła są wyświetlone w jawnym tekście i mogą być czytane przez każdą osobę mającą prawo odczytu do pliku wsadowego. Dlatego też bardzo istotne jest usunięcie pliku wsadowego z serwera Kerberos i komputera PC natychmiast po jego użyciu. Jeśli hasło nie będzie włączone, po uruchomieniu pliku wsadowego zostanie wyświetlona prośba o jego wprowadzenie.

  Uwaga: Użytkowników usługi wygenerowanych przez kreatora można również dodać ręcznie do Microsoft Active Directory. Aby dowiedzieć się, jak to zrobić, zapoznaj się z tematem Dodawanie użytkowników i5/OS do serwera Kerberos.
- Na stronie **Podsumowanie** przejrzyj szczegóły dotyczące konfiguracji usługi uwierzytelniania sieciowego i kliknij **Zakończ**, aby wrócić do kreatora konfigurowania EIM.

6. Jeśli lokalny serwer katalogów nie jest skonfigurowany, po powrocie do kreatora konfigurowania EIM zostanie wyświetlona strona **Konfiguruj serwer katalogów**. Aby skonfigurować lokalny serwer katalogów, podaj następujące dane:

   Uwaga: Jeśli konfigurujesz lokalny serwer katalogów przed użyciem kreatora konfigurowania EIM, zostanie wyświetlona strona **Podaj użytkownika połączenia**. Na tej stronie podaj nazwę wyróżniającą i hasło administratora LDAP, aby kreator miał wystarczające uprawnienia do administrowania domeną EIM i obiektami w tej domenie, a następnie przejdź do następnej czynności niniejszej procedury. Kliknij **Pomoc**, aby dowiedzieć się, jakie dane wpisać na tej stronie.

   a. W polu **Port** akceptuj domyślny numer portu 389, lub podaj inny numer portu, aby z serwerem katalogów używać niechronionej komunikacji EIM.

   b. W polu **Nazwa wyróżniająca** podaj nazwę wyróżniającą LDAP identyfikującą administratora LDAP dla serwera katalogów. Kreator konfigurowania EIM tworzy nazwę wyróżniającą administratora LDAP i używa jej do skonfigurowania kontrolera domeny dla nowo tworzonej domeny.

   c. W polu **Hasło** wpisz hasło administratora LDAP.

   d. W polu **Potwierdź hasło** wpisz ponownie hasło w celu weryfikacji.

   e. Kliknij przycisk **Dalej**.

7. Na stronie **Określ domenę** wpisz następujące dane:

   a. W polu **Domena** wpisz nazwę tworzonej domeny EIM. Zaakceptuj domyślną nazwę EIM lub użyj dowolnego łańcucha znaków. Nie możesz jednak używać znaków specjalnych, takich jak **= + < > , # ;** \ i *****.

   b. W polu **Opis** wpisz opis domeny.

   c. Kliknij przycisk **Dalej**.

8. Na stronie **Podaj nadrzędną nazwę wyróżniającą dla domeny**, wybierz **Tak**, aby podać nadrzędną nazwę wyróżniającą dla tworzonej domeny, lub **Nie**, aby przechowywać dane EIM w położeniu katalogu z przyrostkiem wskazującym nazwę domeny EIM.

   Uwaga: Jeśli tworzysz domenę na lokalnym serwerze katalogów, nadrzędna nazwa wyróżniająca jest opcjonalna. Używając nadrzędnej nazwy wyróżniającej można określić miejsce, w którym mają znajdować się dane EIM w lokalnej przestrzeni nazw dla tej domeny. Jeśli nadrzędna nazwa wyróżniająca nie zostanie podana, dane EIM znajdują się w przestrzeni nazw w miejscu wskazywanym przez przyrostek. Jeśli

wybierzesz **Tak**, użyj okna listy, aby wybrać przyrostek lokalnego serwera LDAP, który ma być używany jako nadrzędna nazwa wyróżniająca lub wpisz własny tekst, aby utworzyć nazwę nowej nadrzędnej nazwy wyróżniającej. Określenie nadrzędnej nazwy wyróżniającej dla nowej domeny nie jest konieczne. Kliknij **Pomoc**, aby uzyskać więcej informacji o używaniu nadrzędnej nazwy wyróżniającej.

9. Na stronie **Informacje o rejestrach** określ, czy dodawać lokalne rejestry użytkowników do domeny EIM jako definicje rejestrów. Wybierz jeden lub oba poniższe typy rejestrów użytkowników:

   Uwaga: W tym momencie nie jest konieczne tworzenie definicji rejestrów. Jeśli chcesz utworzyć je później, musisz dodać definicje rejestrów systemu i aktualizować właściwości konfiguracji EIM.

   a. Wybierz **Lokalny i5/OS**, aby dodać definicję rejestru dla rejestru lokalnego. W polu akceptuj domyślne wartości lub wpisz własne dla nazwy definicji rejestru. Nazwa rejestru EIM jest arbitralnym łańcuchem reprezentującym typ rejestru i konkretną instancję tego rejestru.
   b. Wybierz **Kerberos**, aby dodać definicję rejestru do rejestru Kerberos. W polu akceptuj wartości domyślne lub wpisz własne dla nazwy definicji rejestru. Domyślna nazwa definicji rejestru jest taka sama, jak nazwa dziedziny. Używając identycznych nazw rejestru Kerberos i dziedziny, możesz zwiększyć wydajność pobierania informacji z rejestru. Jeśli to konieczne, wybierz **W tożsamościach użytkowników Kerberos rozróżniane są wielkości liter**.
   c. Kliknij przycisk **Dalej**.

10. Na stronie **Podaj użytkownika systemu EIM** wybierz **Typ użytkownika**, który ma być używany przez system podczas wykonywania operacji EIM w imieniu funkcji systemu operacyjnego. Do operacji tych należą wyszukiwanie odwzorowań i usuwanie powiązań podczas usuwania lokalnego profilu użytkownika i5/OS. Dostępne są następujące typy użytkowników: **Nazwa wyróżniająca i hasło**, **Plik kluczy Kerberos i nazwa użytkownika** oraz **Nazwa użytkownika Kerberos i hasło**. Wybór typu użytkownika zależy od bieżącej konfiguracji systemu. Jeśli na przykład w systemie nie skonfigurowano usługi uwierzytelniania sieciowego, wybór typów użytkowników protokołu Kerberos nie będzie dostępny. Od wybranego typu użytkownika zależą inne informacje, które należy podać na tej stronie:

    Uwaga: Należy podać użytkownika, który już jest zdefiniowany w serwerze katalogów udostępniającym kontroler domeny EIM. Podany użytkownik musi mieć uprawnienia do wyszukiwania odwzorowania i administrowania rejestrem co najmniej dla lokalnego rejestru użytkowników. Jeśli podany użytkownik nie ma takich uprawnień, niektóre funkcje systemu operacyjnego związane z pojedynczym logowaniem i usuwaniem profili użytkowników mogą się nie powieść.

    Jeśli przed uruchomieniem kreatora nie został skonfigurowany serwer katalogów, jedynym dostępnym typem użytkownika jest **Nazwa wyróżniająca i hasło**, a jedyną nazwą wyróżniającą, którą można podać, jest nazwa wyróżniająca administratora LDAP.

    - Wybierając opcję **Nazwa wyróżniająca i hasło**, musisz podać następujące informacje:
      - W polu **Nazwa wyróżniająca** podaj nazwę wyróżniającą LDAP identyfikującą użytkownika w systemie, nazwa ta będzie używana podczas wykonywania operacji EIM.
      - W polu **Hasło** podaj hasło dla nazwy wyróżniającej.
      - W polu **Potwierdź hasło** wpisz ponownie hasło w celu weryfikacji.
    - Wybierając opcję **Nazwa użytkownika Kerberos i hasło**, musisz podać następujące informacje:
      - W polu **Nazwa użytkownika** podaj nazwę użytkownika Kerberos dla systemu, nazwa ta będzie używana podczas wykonywania operacji EIM.
      - W polu **Dziedzina** podaj pełną nazwę dziedziny Kerberos, której członkiem jest dana nazwa użytkownika. Nazwy użytkownika i dziedziny jednoznacznie identyfikują użytkowników Kerberos w pliku kluczy. Na przykład nazwa użytkownika jkowalski w dziedzinie zamowienia.mojafirma.com jest reprezentowana w pliku kluczy jako jkowalski@zamowienia.mojafirma.com.
      - W polu **Hasło** wpisz hasło użytkownika.
      - W polu **Potwierdź hasło** wpisz ponownie hasło w celu weryfikacji.
    - Wybierając opcję **Plik kluczy Kerberos i nazwa użytkownika**, musisz podać następujące informacje:

- W polu **Plik kluczy** podaj pełną ścieżkę i nazwę pliku kluczy zawierającego nazwę użytkownika Kerberos używaną przez system podczas wykonywania operacji EIM. Możesz również kliknąć **Przeglądaj...**, aby przeszukać katalogi zintegrowanego systemu plików serwera iSeries i wybrać plik kluczy.
- W polu **Nazwa użytkownika** podaj nazwę użytkownika Kerberos dla systemu, nazwa ta będzie używana podczas wykonywania operacji EIM.
- W polu **Dziedzina** podaj pełną nazwę dziedziny Kerberos, której członkiem jest dana nazwa użytkownika. Nazwy użytkownika i dziedziny jednoznacznie identyfikują użytkowników Kerberos w pliku kluczy. Na przykład nazwa użytkownika jkowalski w dziedzinie zamowienia.mojafirma.com jest reprezentowana w pliku kluczy jako jkowalski@zamowienia.mojafirma.com.

- Kliknij **Weryfikacja połączenia**, aby upewnić się, że kreator może użyć podanych informacji o użytkowniku do pomyślnego nawiązania połączenia z kontrolerem domeny EIM.
- Kliknij przycisk **Dalej**.

11. Przejrzyj podane informacje konfiguracyjne na panelu **Podsumowanie**. Jeśli wszystkie podane informacje są poprawne, kliknij przycisk **Zakończ**.

Finalizowanie konfigurowania produktu EIM dla domeny

Kończąc działanie kreator dodaje nową domenę do folderu **Zarządzanie domenami** i można utworzyć prostą konfigurację EIM dla tego serwera. Jednak aby sfinalizować konfigurację EIM dla tej domeny, należy wykonać następujące zadania:

1. Użyj kreatora konfigurowania EIM na każdym dodatkowym serwerze, który ma być podłączony do domeny.
2. Jeśli to konieczne, dodaj definicje rejestrów EIM do domeny EIM dla innych serwerów niż serwery iSeries i aplikacji, które mają należeć do danej domeny EIM. Definicje rejestrów odnoszą się do bieżących rejestrów użytkowników, które muszą należeć do domeny. Możesz dodać definicje rejestrów systemu lub dodać definicje rejestrów aplikacji, w zależności od wymagań implementacji EIM.
3. W zależności od wymagań implementacji EIM określ, czy potrzebne jest:
   - Tworzenie identyfikatorów EIM dla każdego użytkownika lub jednostki w domenie oraz tworzenie dla nich powiązań identyfikatorów.
   - Tworzenie powiązań strategii, aby odwzorować grupę użytkowników na pojedynczą tożsamość użytkownika docelowego.
   - Tworzenie kombinacji powyższych elementów.
4. Użyj funkcji EIM testowanie odwzorowania, aby sprawdzić odwzorowania tożsamości dla konfiguracji EIM.
5. Jeśli jedynym zdefiniowanym użytkownikiem EIM jest nazwa wyróżniająca administratora LDAP, to użytkownik EIM ma najwyższy poziom uprawnień do wszystkich danych na serwerze katalogów. Dlatego należy rozważyć utworzenie co najmniej jednego dodatkowego użytkownika, o bardziej odpowiednich i ograniczonych prawach dostępu do danych EIM. Więcej informacji na temat tworzenia nazw wyróżniających dla serwera katalogów zawiera temat Nazwy wyróżniające w temacie IBM Directory Server for iSeries (LDAP). Liczba zdefiniowanych dodatkowych użytkowników EIM zależy od nacisku strategii ochrony na rozdzielenie poszczególnych obowiązków i odpowiedzialności związanych z ochroną. Zazwyczaj można utworzyć przynajmniej dwa następujące typy nazwy wyróżniającej:
   - **Użytkownika z prawami dostępu administratora EIM**

     Nazwa wyróżniająca administratora EIM ma wystarczający poziom uprawnień dla administratora odpowiedzialnego za zarządzanie domeną EIM. Może ona być używana do połączenia się z kontrolerem domeny do zarządzania wszystkimi aspektami domeny EIM przy użyciu programu iSeries Navigator.
   - **Przynajmniej jeden użytkownik o następujących prawach dostępu**:
     - Administrator identyfikatorów
     - Administrator rejestru
     - Operacje odwzorowania EIM

     Użytkownik ten ma odpowiedni poziom dostępu dla użytkownika systemu, który wykonuje operacje EIM w systemie operacyjnym.

Uwaga: Aby użyć nowej nazwy wyróżniającej dla użytkownika systemu zamiast nazwy wyróżniającej administratora LDAP, trzeba zmienić właściwości konfiguracji EIM dla serwera iSeries. Więcej informacji na ten temat zawiera temat Zarządzanie właściwościami konfiguracji EIM.

Ponadto można użyć Secure Sockets Layer (SSL) lub Transport Layer Security (TLS) do skonfigurowania chronionego połączenia z kontrolerem domeny EIM i zabezpieczenia transmisji danych EIM. Jeśli włączysz SSL dla serwera katalogów, musisz aktualizować właściwości konfiguracji EIM i podać, że serwer iSeries używa chronionego połączenia SSL. Należy również aktualizować właściwości dla domeny i podać, że EIM używa chronionych połączeń SSL do zarządzania domeną za pomocą programu iSeries Navigator.

Uwaga: Jeśli tworzysz prostą konfigurację usługi uwierzytelniania sieciowego, a szczególnie, jeśli implementujesz środowisko pojedynczego logowania, możesz potrzebować wykonać dodatkowe zadania. Informacje na temat tych dodatkowych zadań można znaleźć przeglądając czynności konfigurowania przedstawione w scenariuszu Włączanie pojedynczego logowania dla i5/OS.

Tworzenie nowej domeny zdalnej i jej przyłączanie

Informacje objaśniające, jak utworzyć nową domenę EIM dla przedsiębiorstwa i skonfigurować zdalny serwer katalogów jako kontroler domeny EIM dla tej domeny.

Jeśli używasz kreatora konfigurowania EIM do utworzenia nowej domeny i połączenia się do niej, możesz, w ramach części konfiguracji EIM, skonfigurować serwer katalogów na systemie zdalnym jako kontroler domeny EIM. Aby połączyć się ze zdalnym serwerem katalogów i skonfigurować EIM, konieczne jest wprowadzenie odpowiednich danych. Jeśli na serwerze iSeries nie skonfigurowano protokołu Kerberos, kreator wyświetla zachętę do uruchomienia kreatora konfigurowania usługi uwierzytelniania sieciowego.

Uwaga: Serwer katalogów na systemie zdalnym musi udostępniać obsługę EIM. Odwzorowania EIM wymagają, aby kontroler domeny był udostępniany przez serwer katalogów z obsługą LDAP w wersji 3. Ponadto serwer katalogów musi mieć skonfigurowany schemat EIM. Obsługę tę udostępnia na przykład produkt IBM Directory Server V5.1. Więcej szczegółowych informacji o wymaganiach kontrolera domeny EIM zawiera temat Planowanie kontrolera domeny EIM.

Po zakończeniu działania kreatora konfigurowania EIM można wykonać następujące zadania:

- Tworzenie nowej domeny EIM.
- Konfigurowanie zdalnego serwera katalogów jako kontrolera domeny EIM.
- Konfigurowanie usługi uwierzytelniania sieciowego dla systemu.
- Tworzenie definicji rejestrów EIM dla rejestru lokalnego i5/OS i rejestru Kerberos.
- Konfigurowanie systemu do udziału w nowej domenie EIM.

Aby skonfigurować system do utworzenia nowej domeny EIM i połączenia się z nią, niezbędne są następujące uprawnienia specjalne:

- Administrator ochrony (*SECADM).
- Wszystkie obiekty (*ALLOBJ).
- Konfiguracja systemu (*IOSYSCFG).

Aby za pomocą kreatora konfigurowania EIM utworzyć domenę w systemie zdalnym i ją przyłączyć, wykonaj następujące czynności:

1. Sprawdź, czy serwer katalogów w systemie zdalnym jest aktywny.
2. W programie iSeries Navigator wybierz system, dla którego chcesz skonfigurować EIM, i rozwiń gałąź **Sieć > Odwzorowanie EIM**.
3. Kliknij prawym przyciskiem myszy **Konfiguracja** i wybierz **Konfiguruj...**, aby uruchomić kreatora konfigurowania EIM.

   Uwaga: Jeśli w systemie zostały już skonfigurowane odwzorowania EIM, opcja nosi nazwę **Rekonfiguruj...**.

4. Na stronie **Witamy** wybierz opcję **Utwórz i przyłącz nową domenę** i kliknij przycisk **Dalej**.
5. Na stronie **Określanie położenia domeny EIM** wybierz opcję **Na lokalnym serwerze katalogów** i kliknij **Dalej**.

   Uwaga: Opcja ta konfiguruje lokalny serwer katalogów jako kontroler domeny EIM. Ponieważ serwer katalogów przechowuje wszystkie dane EIM dla domeny, musi on być cały czas aktywny, aby obsługiwać operacje wyszukiwania odwzorowań i inne.

   Jeśli na serwerze iSeries nie jest skonfigurowana usługa uwierzytelniania sieciowego lub potrzebne są dodatkowe informacje konfiguracyjne uwierzytelniania sieciowego aby skonfigurować środowisko pojedynczego logowania, wyświetlona zostanie strona **Konfigurowanie usługi uwierzytelniania sieciowego**. Strona ta umożliwia uruchomienie kreatora i skonfigurowanie usługi uwierzytelniania sieciowego. Można również skonfigurować usługę uwierzytelniania sieciowego później, używając kreatora konfigurowania dla tej usługi z programu iSeries Navigator. Po zakończeniu konfigurowania usługi uwierzytelniania sieciowego można kontynuować pracę w kreatorze konfiguracji EIM.
6. Aby skonfigurować usługę uwierzytelniania sieciowego, wykonaj następujące czynności:
   a. Na stronie **Konfigurowanie usługi uwierzytelniania sieciowego** wybierz **Tak**, aby uruchomić kreatora konfigurowania usługi uwierzytelniania sieciowego. Korzystając z tego kreatora można skonfigurować kilka interfejsów i usług systemu i5/OS, w tym dziedzinę Kerberos, lub skonfigurować środowisko pojedynczego logowania używające jednocześnie EIM i usługi uwierzytelniania sieciowego.
   b. Na stronie **Podaj dane dziedziny** podaj nazwę domyślnej dziedziny w polu **Dziedzina domyślna**. Jeśli używasz uwierzytelniania Microsoft Active Directory for Kerberos, wybierz **Do uwierzytelniania Kerberos używana jest funkcja Microsoft Active Directory** i kliknij **Dalej**.
   c. Na stronie **Podaj dane KDC** w polu **KDC** podaj pełną nazwę serwera Kerberos dla tej dziedziny, w polu **Port** wpisz 88 i kliknij **Dalej**.
   d. Na stronie **Podaj dane serwera haseł** wybierz **Tak** lub **Nie** decydując, czy skonfigurować serwer haseł. Serwer haseł umożliwia użytkownikom zmianę haseł na serwerze Kerberos. Jeśli wybierzesz **Tak**, w polu **Serwer haseł** wprowadź nazwę serwera haseł. W polu **Port** akceptuj domyślną wartość 464 i kliknij Dalej.
   e. Na stronie **Wybór pozycji tabeli kluczy** wybierz **Uwierzytelnianie Kerberos i5/OS** i kliknij **Dalej**.

      Uwaga: Można ponadto utworzyć również pozycje tabeli kluczy dla serwera IBM Directory Server for iSeries (LDAP), iSeries NetServer i serwera iSeries HTTP, jeśli te usługi mają korzystać z uwierzytelniania Kerberos. W tym celu może być potrzebna dodatkowa konfiguracja dla tych usług.
   f. Na stronie **Tworzenie pozycji tabeli kluczy i5/OS** wpisz hasło i potwierdź je, a następnie kliknij **Dalej**. Jest to to samo hasło, którego będziesz używać przy dodawaniu nazw użytkowników i5/OS do serwera Kerberos.
   g. Opcjonalne: Na stronie **Tworzenie pliku wsadowego** wybierz **Tak**, podaj poniższe dane i kliknij **Dalej**:
      - W polu **Plik wsadowy** aktualizuj ścieżkę katalogu. Kliknij **Przeglądaj**, aby znaleźć odpowiednią ścieżkę katalogu lub edytować ścieżkę w polu **Plik wsadowy**.
      - W polu **Włączyć hasło** wybierz **Tak**. Zapewni to, że wszystkie hasła powiązane z użytkownikiem usługi i5/OS będą zawarte w pliku wsadowym. Należy zauważyć, że hasła są wyświetlone w jawnym tekście i mogą być czytane przez każdą osobę mającą prawo odczytu do pliku wsadowego. Dlatego też bardzo istotne jest usunięcie pliku wsadowego z serwera Kerberos i komputera PC natychmiast po jego użyciu. Jeśli hasło nie będzie włączone, po uruchomieniu pliku wsadowego zostanie wyświetlona prośba o jego wprowadzenie.

        Uwaga: Użytkowników usługi wygenerowanych przez kreatora można również dodać ręcznie do Microsoft Active Directory. Aby dowiedzieć się, jak to zrobić, zapoznaj się z tematem Dodawanie użytkowników i5/OS do serwera Kerberos.
      - Na stronie **Podsumowanie** przejrzyj szczegóły dotyczące konfiguracji usługi uwierzytelniania sieciowego i kliknij **Zakończ**, aby wrócić do kreatora konfigurowania EIM.
7. Użyj strony **Podaj kontroler domeny EIM**, aby podać następujące informacje o połączeniu dla zdalnego kontrolera domeny EIM, który chcesz skonfigurować:

a. W polu **Nazwa kontrolera domeny** podaj nazwę zdalnego serwera katalogów, który chcesz skonfigurować jako kontroler domeny EIM dla tworzonej domeny. Nazwa kontrolera domeny EIM może być nazwą TCP/IP hosta i domeny serwera katalogów lub adresem serwera katalogów.

b. Podaj następujące informacje dla połączenia do kontrolera domeny:

   - Wybierz **Użyj połączenia chronionego (SSL lub TLS)**, aby użyć chronionego połączenia do kontrolera domeny EIM. Wybranie tej opcji powoduje, że połączenie korzysta z SSL lub TLS i jest chronione, a transmisja danych EIM przez niechronioną sieć, na przykład Internet, jest zabezpieczona.

     Uwaga: Należy sprawdzić, czy kontroler domeny EIM jest skonfigurowany do korzystania z połączenia chronionego. W przeciwnym przypadku, połączenie z kontrolerem domeny może nie zostać nawiązane.

   - W polu **Port** podaj port TCP/IP, na którym nasłuchuje serwer katalogów. Jeśli wybrana została opcja **Użyj połączenia chronionego**, domyślnym portem jest 636; w przeciwnym przypadku domyślnym portem jest 389.

c. Kliknij **Weryfikacja połączenia**, aby upewnić się, że kreator może użyć podanych informacji do pomyślnego nawiązania połączenia ze zdalnym kontrolerem domeny EIM.

d. Kliknij przycisk **Dalej**.

8. Na stronie **Podaj użytkownika połączenia** wybierz **Typ użytkownika** dla połączenia. Dostępne są następujące typy użytkowników: **Nazwa wyróżniająca i hasło**, **Plik kluczy Kerberos i nazwa użytkownika**, **Nazwa użytkownika Kerberos i hasło** oraz **Profil użytkownika i hasło**. Typy użytkowników protokołu Kerberos są dostępne, jeśli w lokalnym systemie iSeries skonfigurowano usługę uwierzytelniania sieciowego. Od wybranego typu użytkownika zależą inne informacje, które należy podać w oknie:

   Uwaga: Aby mieć pewność, że kreator ma wystarczające uprawnienia do utworzenia niezbędnych obiektów EIM w katalogu, wybierz jako typ użytkownika **Nazwa wyróżniająca i hasło** i podaj nazwę wyróżniającą i hasło administratora LDAP.

   Dla połączenia można podać innego użytkownika, jednakże podany użytkownik musi mieć uprawnienia do zdalnego serwera katalogów równe uprawnieniom administratora LDAP.

a. Wybierając opcję **Nazwa wyróżniająca i hasło**, musisz podać następujące informacje:

   - W polu **Nazwa wyróżniająca** podaj nazwę wyróżniającą administratora LDAP i hasło, aby mieć pewność, że kreator będzie mieć wystarczające uprawnienia do administrowania domeną EIM i obiektami w niej.
   - W polu **Hasło** podaj hasło dla nazwy wyróżniającej.
   - W polu **Potwierdź hasło** wpisz ponownie hasło w celu weryfikacji.

b. Wybierając opcję **Plik kluczy Kerberos i nazwa użytkownika**, musisz podać następujące informacje:

   - W polu **Plik kluczy** podaj pełną ścieżkę i nazwę pliku kluczy zawierającą nazwę użytkownika Kerberos używaną przez kreatora podczas łączenia z domeną EIM. Możesz również kliknąć **Przeglądaj...**, aby przeszukać katalogi zintegrowanego systemu plików serwera iSeries i wybrać plik kluczy.
   - W polu **Nazwa użytkownika** podaj nazwę użytkownika Kerberos, która ma być używana do zidentyfikowania użytkownika.
   - W polu **Dziedzina** podaj pełną nazwę dziedziny Kerberos, której członkiem jest dana nazwa użytkownika. Nazwy użytkownika i dziedziny jednoznacznie identyfikują użytkowników Kerberos w pliku kluczy. Na przykład nazwa użytkownika jkowalski w dziedzinie zamowienia.mojafirma.com jest reprezentowana w pliku kluczy jako jkowalski@zamowienia.mojafirma.com.

c. Wybierając opcję **Nazwa użytkownika Kerberos i hasło**, musisz podać następujące informacje:

   - W polu **Nazwa użytkownika** podaj nazwę użytkownika Kerberos używaną przez kreatora do łączenia się do domeny EIM.
   - W polu **Dziedzina** podaj pełną nazwę dziedziny Kerberos, której członkiem jest dana nazwa użytkownika. Nazwy użytkownika i dziedziny jednoznacznie identyfikują użytkowników Kerberos w pliku kluczy. Na przykład nazwa użytkownika jkowalski w dziedzinie zamowienia.mojafirma.com jest reprezentowana w pliku kluczy jako jkowalski@zamowienia.mojafirma.com.

- W polu **Hasło** wpisz hasło nazwy użytkownika Kerberos.
- W polu **Potwierdź hasło** wpisz ponownie hasło w celu weryfikacji.

d. Jeśli wybierzesz opcję **Profil użytkownika i hasło**, musisz podać następujące informacje:
   - W polu **Profil użytkownika** podaj nazwę profilu użytkownika używaną przez kreatora do łączenia się z domeną EIM.
   - W polu **Hasło** podaj hasło dla profilu użytkownika.
   - W polu **Potwierdź hasło** wpisz ponownie hasło w celu weryfikacji.

e. Kliknij **Weryfikacja połączenia**, aby sprawdzić, czy kreator może użyć podanych informacji o użytkowniku do pomyślnego nawiązania połączenia z kontrolerem domeny EIM.

f. Kliknij przycisk **Dalej**.

9. Na stronie **Określ domenę** wpisz następujące dane:
   a. W polu **Domena** wpisz nazwę tworzonej domeny EIM. Zaakceptuj domyślną nazwę EIM lub użyj dowolnego łańcucha znaków. Nie możesz jednak używać znaków specjalnych, takich jak **= + < > , # ;** \ i *.
   b. W polu **Opis** wpisz opis domeny.
   c. Kliknij przycisk **Dalej**.
10. W oknie dialogowym **Podaj nadrzędną nazwę wyróżniającą dla domeny** wybierz **Tak**, aby podać nadrzędną nazwę wyróżniającą, której kreator powinien używać dla położenia tworzonej domeny EIM. Nazwa wyróżniająca reprezentuje pozycję znajdującą się bezpośrednio nad pozycją nazwy domeny w hierarchii drzewa informacji katalogu. Możesz również wybrać **Nie**, aby dane EIM były przechowywane w położeniu katalogu z przyrostkiem wskazującym nazwę domeny EIM.

    Uwaga: Jeśli używasz kreatora do skonfigurowania domeny na zdalnym kontrolerze domeny, podaj odpowiednią nadrzędną nazwę wyróżniającą dla domeny. Ponieważ wszystkie niezbędne obiekty konfiguracyjne dla nadrzędnej nazwy wyróżniającej muszą już istnieć, albo konfigurowanie EIM nie powiedzie się, należy raczej użyć przycisku Przeglądaj i znaleźć odpowiednią nadrzędną nazwę wyróżniającą, zamiast ręcznie wpisywać te informacje. Kliknij **Pomoc**, aby uzyskać więcej informacji o używaniu nadrzędnej nazwy wyróżniającej.
11. Na stronie **Informacje o rejestrach** określ, czy dodawać lokalne rejestry użytkowników do domeny EIM jako definicje rejestrów. Wybierz jeden lub oba poniższe typy rejestrów użytkowników:

    Uwaga: W tym momencie nie jest konieczne tworzenie definicji rejestrów. Jeśli chcesz utworzyć je później, musisz dodać definicje rejestrów systemu i aktualizować właściwości konfiguracji EIM.
    a. Wybierz **Lokalny i5/OS**, aby dodać definicję rejestru dla rejestru lokalnego. W polu akceptuj domyślne wartości lub wpisz własne dla nazwy definicji rejestru. Nazwa rejestru EIM jest arbitralnym łańcuchem reprezentującym typ rejestru i konkretną instancję tego rejestru.
    b. Wybierz **Kerberos**, aby dodać definicję rejestru do rejestru Kerberos. W polu akceptuj wartości domyślne lub wpisz własne dla nazwy definicji rejestru. Domyślna nazwa definicji rejestru jest taka sama, jak nazwa dziedziny. Używając identycznych nazw rejestru Kerberos i dziedziny, możesz zwiększyć wydajność pobierania informacji z rejestru. Jeśli to konieczne, wybierz **W tożsamościach użytkowników Kerberos rozróżniane są wielkości liter**.
    c. Kliknij przycisk **Dalej**.
12. Na stronie **Podaj użytkownika systemu EIM** wybierz **Typ użytkownika**, który ma być używany przez system podczas wykonywania operacji EIM w imieniu funkcji systemu operacyjnego. Do operacji tych należą wyszukiwanie odwzorowań i usuwanie powiązań podczas usuwania lokalnego profilu użytkownika i5/OS. Dostępne są następujące typy użytkowników: **Nazwa wyróżniająca i hasło**, **Plik kluczy Kerberos i nazwa użytkownika** oraz **Nazwa użytkownika Kerberos i hasło**. Wybór typu użytkownika zależy od bieżącej konfiguracji systemu. Jeśli na przykład w systemie nie skonfigurowano usługi uwierzytelniania sieciowego, wybór typów użytkowników protokołu Kerberos nie będzie dostępny. Od wybranego typu użytkownika zależą inne informacje, które należy podać na tej stronie:

    Uwaga: Należy podać użytkownika, który już jest zdefiniowany w serwerze katalogów udostępniającym kontroler domeny EIM. Podany użytkownik musi mieć uprawnienia do wyszukiwania odwzorowania i

administrowania rejestrem co najmniej dla lokalnego rejestru użytkowników. Jeśli podany użytkownik nie ma takich uprawnień, niektóre funkcje systemu operacyjnego związane z pojedynczym logowaniem i usuwaniem profili użytkowników mogą się nie powieść.

Jeśli przed uruchomieniem kreatora nie został skonfigurowany serwer katalogów, jedynym dostępnym typem użytkownika jest **Nazwa wyróżniająca i hasło**, a jedyną nazwą wyróżniającą, którą można podać, jest nazwa wyróżniająca administratora LDAP.

a. Wybierając opcję **Nazwa wyróżniająca i hasło**, musisz podać następujące informacje:
   - W polu **Nazwa wyróżniająca** podaj nazwę wyróżniającą LDAP identyfikującą użytkownika w systemie, nazwa ta będzie używana podczas wykonywania operacji EIM.
   - W polu **Hasło** podaj hasło dla nazwy wyróżniającej.
   - W polu **Potwierdź hasło** wpisz ponownie hasło w celu weryfikacji.

b. Wybierając opcję **Nazwa użytkownika Kerberos i hasło**, musisz podać następujące informacje:
   - W polu **Nazwa użytkownika** podaj nazwę użytkownika Kerberos dla systemu, nazwa ta będzie używana podczas wykonywania operacji EIM.
   - W polu **Dziedzina** podaj pełną nazwę dziedziny Kerberos, której członkiem jest dana nazwa użytkownika. Nazwy użytkownika i dziedziny jednoznacznie identyfikują użytkowników Kerberos w pliku kluczy. Na przykład nazwa użytkownika jkowalski w dziedzinie zamowienia.mojafirma.com jest reprezentowana w pliku kluczy jako jkowalski@zamowienia.mojafirma.com.
   - W polu **Hasło** wpisz hasło użytkownika.
   - W polu **Potwierdź hasło** wpisz ponownie hasło w celu weryfikacji.

c. Wybierając opcję **Plik kluczy Kerberos i nazwa użytkownika**, musisz podać następujące informacje:
   - W polu **Plik kluczy** podaj pełną ścieżkę i nazwę pliku kluczy zawierającego nazwę użytkownika Kerberos używaną przez system podczas wykonywania operacji EIM. Możesz również kliknąć **Przeglądaj...**, aby przeszukać katalogi zintegrowanego systemu plików serwera iSeries i wybrać plik kluczy.
   - W polu **Nazwa użytkownika** podaj nazwę użytkownika Kerberos dla systemu, nazwa ta będzie używana podczas wykonywania operacji EIM.
   - W polu **Dziedzina** podaj pełną nazwę dziedziny Kerberos, której członkiem jest dana nazwa użytkownika. Nazwy użytkownika i dziedziny jednoznacznie identyfikują użytkowników Kerberos w pliku kluczy. Na przykład nazwa użytkownika jkowalski w dziedzinie zamowienia.mojafirma.com jest reprezentowana w pliku kluczy jako jkowalski@zamowienia.mojafirma.com.

d. Kliknij **Weryfikacja połączenia**, aby upewnić się, że kreator może użyć podanych informacji o użytkowniku do pomyślnego nawiązania połączenia z kontrolerem domeny EIM.

e. Kliknij przycisk **Dalej**.

13. Przejrzyj podane informacje konfiguracyjne na panelu **Podsumowanie**. Jeśli wszystkie podane informacje są poprawne, kliknij przycisk **Zakończ**.

Finalizowanie konfigurowania produktu EIM dla domeny

Kończąc działanie kreator dodaje nową domenę do folderu **Zarządzanie domenami** i można utworzyć prostą konfigurację EIM dla tego serwera. Jednak aby sfinalizować konfigurację EIM dla tej domeny, należy wykonać następujące zadania:

1. Użyj kreatora konfigurowania EIM na każdym dodatkowym serwerze, który ma być podłączony do nowej domeny.
2. Jeśli to konieczne, dodaj definicje rejestrów EIM do domeny EIM dla innych serwerów niż serwery iSeries i aplikacji, które mają należeć do danej domeny EIM. Definicje rejestrów odnoszą się do bieżących rejestrów użytkowników, które muszą należeć do domeny. Możesz dodać definicje rejestrów systemu lub dodać definicje rejestrów aplikacji, w zależności od wymagań implementacji EIM.
3. W zależności od wymagań implementacji EIM określ, czy potrzebne jest:
   a. Tworzenie identyfikatorów EIM dla każdego użytkownika lub jednostki w domenie oraz tworzenie dla nich powiązań identyfikatorów.

b. Tworzenie powiązań strategii, aby odwzorować grupę użytkowników na pojedynczą tożsamość użytkownika docelowego.
c. Utworzenie kombinacji powyższych elementów.

4. Użyj funkcji EIM testowanie odwzorowania, aby sprawdzić odwzorowania tożsamości dla konfiguracji EIM.
5. Jeśli jedynym zdefiniowanym użytkownikiem EIM jest nazwa wyróżniająca administratora LDAP, to użytkownik EIM ma najwyższy poziom uprawnień do wszystkich danych na serwerze katalogów. Dlatego należy rozważyć utworzenie co najmniej jednego dodatkowego użytkownika, o bardziej odpowiednich i ograniczonych prawach dostępu do danych EIM. Więcej informacji na temat tworzenia nazw wyróżniających dla serwera katalogów zawiera temat Nazwy wyróżniające w temacie IBM Directory Server for iSeries (LDAP). Liczba zdefiniowanych dodatkowych użytkowników EIM zależy od nacisku strategii ochrony na rozdzielenie poszczególnych obowiązków i odpowiedzialności związanych z ochroną. Zazwyczaj można utworzyć przynajmniej dwa następujące typy nazwy wyróżniającej:
   - **Użytkownika z prawami dostępu administratora EIM**

     Nazwa wyróżniająca administratora EIM ma wystarczający poziom uprawnień dla administratora odpowiedzialnego za zarządzanie domeną EIM. Może ona być używana do połączenia się z kontrolerem domeny do zarządzania wszystkimi aspektami domeny EIM przy użyciu programu iSeries Navigator.
   - **Przynajmniej jeden użytkownik o następujących prawach dostępu**:
     - Administrator identyfikatorów
     - Administrator rejestru
     - Operacje odwzorowania EIM

     Użytkownik ten ma odpowiedni poziom dostępu dla użytkownika systemu, który wykonuje operacje EIM w systemie operacyjnym.

   Uwaga: Aby użyć nowej nazwy wyróżniającej dla użytkownika systemu zamiast nazwy wyróżniającej administratora LDAP, trzeba zmienić właściwości konfiguracji EIM dla serwera iSeries. Więcej informacji na ten temat zawiera temat Zarządzanie właściwościami konfiguracji EIM.

Jeśli tworzysz prostą konfigurację usługi uwierzytelniania sieciowego, a szczególnie, jeśli implementujesz środowisko pojedynczego logowania, możesz potrzebować wykonać dodatkowe zadania. Informacje na temat tych dodatkowych zadań można znaleźć przeglądając czynności konfigurowania przedstawione w scenariuszu Włączanie pojedynczego logowania dla i5/OS.

Przyłączenie istniejącej domeny

Informacje dotyczące użycia kreatora konfigurowania EIM na jednym systemie iSeries do skonfigurowania kontrolera domeny i utworzenia domeny EIM, a następnie do skonfigurowania innych serwerów iSeries w taki sposób, aby należały do danej domeny.

Po utworzeniu domeny EIM i skonfigurowaniu serwera katalogów jako kontrolera domeny na jednym systemie, można skonfigurować wszystkie dodatkowe serwery iSeries (V5R2 lub nowsze), aby przyłączyć istniejącą domenę EIM. Podczas pracy w kreatorze należy podać informacje na temat domeny, w tym informacje o połączeniu z kontrolerem domeny EIM. Nawet jeśli używasz kreatora konfigurowania EIM, aby przyłączyć istniejącą domenę, nadal będzie on udostępniał opcję wywołania kreatora konfigurowania usługi uwierzytelniania sieciowego, jeśli w ramach części konfigurowania EIM w systemie wybierzesz konfigurowanie Kerberos.

Po zakończeniu działania kreatora konfigurowania EIM, aby przyłączyć istniejącą domenę, można wykonać następujące zadania:

- Konfigurowanie usługi uwierzytelniania sieciowego dla systemu.
- Tworzenie definicji rejestrów EIM dla rejestru lokalnego i5/OS i rejestru Kerberos.
- Konfigurowanie systemu do udziału w istniejącej domenie EIM.

Aby skonfigurować system do podłączenia do istniejącej domeny EIM, niezbędne są wszystkie poniżej wymienione uprawnienia specjalne:

- Administrator ochrony (*SECADM).
- Wszystkie obiekty (*ALLOBJ).

Aby uruchomić i używać kreatora konfiguracji EIM w celu przyłączenia istniejącej domeny EIM, wykonaj następujące czynności:

1. Sprawdź, czy serwer katalogów w systemie zdalnym jest aktywny.
2. W programie iSeries Navigator wybierz system, dla którego chcesz skonfigurować EIM, i rozwiń gałąź **Sieć > Odwzorowanie EIM**.
3. Kliknij prawym przyciskiem myszy **Konfiguracja** i wybierz **Konfiguruj...**, aby uruchomić kreatora konfigurowania EIM.

   Uwaga: Jeśli w systemie zostały już skonfigurowane odwzorowania EIM, opcja nosi nazwę **Rekonfiguruj...**.
4. Na stronie **Witamy** wybierz **Przyłącz istniejącą domenę** i kliknij przycisk **Dalej**.

   Uwaga: Jeśli na serwerze iSeries nie jest skonfigurowana usługa uwierzytelniania sieciowego lub potrzebne są dodatkowe informacje konfiguracyjne uwierzytelniania sieciowego aby skonfigurować środowisko pojedynczego logowania, wyświetlona zostanie strona **Konfigurowanie usługi uwierzytelniania sieciowego**. Strona ta umożliwia uruchomienie kreatora i skonfigurowanie usługi uwierzytelniania sieciowego. Można również skonfigurować usługę uwierzytelniania sieciowego później, używając kreatora konfigurowania dla tej usługi z programu iSeries Navigator. Po zakończeniu konfigurowania usługi uwierzytelniania sieciowego można kontynuować pracę w kreatorze konfiguracji EIM.
5. Aby skonfigurować usługę uwierzytelniania sieciowego, wykonaj następujące czynności:
   a. Na stronie **Konfigurowanie usługi uwierzytelniania sieciowego** wybierz **Tak**, aby uruchomić kreatora konfigurowania usługi uwierzytelniania sieciowego. Korzystając z tego kreatora można skonfigurować kilka interfejsów i usług systemu i5/OS, w tym dziedzinę Kerberos, lub skonfigurować środowisko pojedynczego logowania używające jednocześnie EIM i usługi uwierzytelniania sieciowego.
   b. Na stronie **Podaj dane dziedziny** podaj nazwę domyślnej dziedziny w polu **Dziedzina domyślna**. Jeśli używasz uwierzytelniania Microsoft Active Directory for Kerberos, wybierz **Do uwierzytelniania Kerberos używana jest funkcja Microsoft Active Directory** i kliknij **Dalej**.
   c. Na stronie **Podaj dane KDC** w polu **KDC** podaj pełną nazwę serwera Kerberos dla tej dziedziny, w polu **Port** wpisz 88 i kliknij **Dalej**.
   d. Na stronie **Podaj dane serwera haseł** wybierz **Tak** lub **Nie** decydując, czy skonfigurować serwer haseł. Serwer haseł umożliwia użytkownikom zmianę haseł na serwerze Kerberos. Jeśli wybierzesz **Tak**, w polu **Serwer haseł** wprowadź nazwę serwera haseł. W polu **Port** akceptuj domyślną wartość 464 i kliknij Dalej.
   e. Na stronie **Wybór pozycji tabeli kluczy** wybierz **Uwierzytelnianie Kerberos i5/OS** i kliknij **Dalej**.

      Uwaga: Można ponadto utworzyć również pozycje tabeli kluczy dla serwera IBM Directory Server for iSeries (LDAP), iSeries NetServer i serwera iSeries HTTP, jeśli te usługi mają korzystać z uwierzytelniania Kerberos. W tym celu może być potrzebna dodatkowa konfiguracja dla tych usług.
   f. Na stronie **Tworzenie pozycji tabeli kluczy i5/OS** wpisz hasło i potwierdź je, a następnie kliknij **Dalej**. Jest to to samo hasło, którego będziesz używać przy dodawaniu nazw użytkowników i5/OS do serwera Kerberos.
   g. Opcjonalne: Na stronie **Tworzenie pliku wsadowego** wybierz **Tak**, podaj poniższe dane i kliknij **Dalej**:
      - W polu **Plik wsadowy** aktualizuj ścieżkę katalogu. Kliknij **Przeglądaj**, aby znaleźć odpowiednią ścieżkę katalogu lub edytować ścieżkę w polu **Plik wsadowy**.
      - W polu **Włączyć hasło** wybierz **Tak**. Zapewni to, że wszystkie hasła powiązane z użytkownikiem usługi i5/OS będą zawarte w pliku wsadowym. Należy zauważyć, że hasła są wyświetlone w jawnym tekście i mogą być czytane przez każdą osobę mającą prawo odczytu do pliku wsadowego. Dlatego też bardzo istotne jest usunięcie pliku wsadowego z serwera Kerberos i komputera PC natychmiast po jego użyciu. Jeśli hasło nie będzie włączone, po uruchomieniu pliku wsadowego zostanie wyświetlona prośba o jego wprowadzenie.

Uwaga: Użytkowników usługi wygenerowanych przez kreatora można również dodać ręcznie do Microsoft Active Directory. Aby dowiedzieć się, jak to zrobić, zapoznaj się z tematem Dodawanie użytkowników i5/OS do serwera Kerberos.

- Na stronie **Podsumowanie** przejrzyj szczegóły dotyczące konfiguracji usługi uwierzytelniania sieciowego i kliknij **Zakończ**, aby wrócić do kreatora konfigurowania EIM.

6. Na stronie **Określ kontroler domeny** wpisz następujące dane:

   Uwaga: Serwer katalogów działający jako kontroler domeny musi być aktywny, aby można było pomyślnie zakończyć konfigurowanie EIM.

   a. W polu **Nazwa kontrolera domeny** wpisz nazwę systemu będącego kontrolerem domeny EIM, która ma być przyłączona do serwera iSeries.

   b. Kliknij **Użyj połączenia chronionego (SSL lub TLS)**, jeśli chcesz użyć chronionego połączenia do kontrolera domeny EIM. Wybranie tej opcji powoduje, że połączenie korzysta z SSL lub TLS i jest chronione, a transmisja danych EIM przez niechronioną sieć, na przykład Internet, jest zabezpieczona.

      Uwaga: Należy sprawdzić, czy kontroler domeny EIM jest skonfigurowany do korzystania z połączenia chronionego. W przeciwnym przypadku, połączenie z kontrolerem domeny może nie zostać nawiązane.

   c. W polu **Port** podaj port TCP/IP, na którym nasłuchuje serwer katalogów. Jeśli wybrana została opcja **Użyj połączenia chronionego**, domyślnym portem jest 636; w przeciwnym przypadku domyślnym portem jest 389.

   d. Kliknij **Weryfikacja połączenia**, aby upewnić się, że kreator może użyć podanych informacji do pomyślnego nawiązania połączenia z kontrolerem domeny EIM.

   e. Kliknij przycisk **Dalej**.

7. Na stronie **Podaj użytkownika połączenia** wybierz **Typ użytkownika** dla połączenia. Można wybrać jeden z następujących typów użytkownika: **Nazwa wyróżniająca i hasło**, **Plik kluczy Kerberos i nazwa użytkownika**, **Nazwa użytkownika Kerberos i hasło** oraz **Profil użytkownika i hasło**. Typy użytkowników Kerberos są dostępne, jeśli w lokalnym systemie iSeries skonfigurowano usługę uwierzytelniania sieciowego. Od wybranego typu użytkownika zależą inne informacje, które należy podać w tym oknie:

   Uwaga: Aby mieć pewność, że kreator ma wystarczające uprawnienia do utworzenia niezbędnych obiektów EIM w katalogu, wybierz jako typ użytkownika **Nazwa wyróżniająca i hasło** i podaj nazwę wyróżniającą i hasło administratora LDAP.

   Dla połączenia można podać innego użytkownika, jednakże podany użytkownik musi mieć uprawnienia do zdalnego serwera katalogów równe uprawnieniom administratora LDAP.

   - Wybierając opcję **Nazwa wyróżniająca i hasło**, musisz podać następujące informacje:
     - W polu **Nazwa wyróżniająca** podaj nazwę wyróżniającą LDAP identyfikującą użytkownika, który ma uprawnienia do tworzenia obiektów w lokalnej przestrzeni nazw serwera LDAP. Jeśli we wcześniejszej czynności użyto kreatora do skonfigurowania serwera LDAP, musisz wprowadzić nazwę wyróżniającą administratora LDAP utworzonej w tej czynności.
     - W polu **Hasło** podaj hasło dla nazwy wyróżniającej.
     - W polu **Potwierdź hasło** wpisz ponownie hasło w celu weryfikacji.
   - Wybierając opcję **Plik kluczy Kerberos i nazwa użytkownika**, musisz podać następujące informacje:
     - W polu **Plik kluczy** podaj pełną ścieżkę i nazwę pliku kluczy zawierającą nazwę użytkownika Kerberos używaną przez kreatora podczas łączenia z domeną EIM. Możesz również kliknąć **Przeglądaj...**, aby przeszukać katalogi zintegrowanego systemu plików serwera iSeries i wybrać plik kluczy.
     - W polu **Nazwa użytkownika** podaj nazwę użytkownika Kerberos, która ma być używana do zidentyfikowania użytkownika.
     - W polu **Dziedzina** podaj pełną nazwę dziedziny Kerberos, której członkiem jest dana nazwa użytkownika. Nazwy użytkownika i dziedziny jednoznacznie identyfikują użytkowników Kerberos w pliku kluczy. Na

przykład nazwa użytkownika jkowalski w dziedzinie zamowienia.mojafirma.com jest reprezentowana w pliku kluczy jako jkowalski@zamowienia.mojafirma.com.

- Wybierając opcję **Nazwa użytkownika Kerberos i hasło**, musisz podać następujące informacje:
  - W polu **Nazwa użytkownika** podaj nazwę użytkownika Kerberos używaną przez kreatora do łączenia się do domeny EIM.
  - W polu **Dziedzina** podaj pełną nazwę dziedziny Kerberos, której członkiem jest dana nazwa użytkownika. Nazwy użytkownika i dziedziny jednoznacznie identyfikują użytkowników Kerberos w pliku kluczy. Na przykład nazwa użytkownika jkowalski w dziedzinie zamowienia.mojafirma.com jest reprezentowana w pliku kluczy jako jkowalski@zamowienia.mojafirma.com.
  - W polu **Hasło** wpisz hasło nazwy użytkownika Kerberos.
  - W polu **Potwierdź hasło** wpisz ponownie hasło w celu weryfikacji.
- Jeśli wybierzesz opcję **Profil użytkownika i hasło**, musisz podać następujące informacje:
  - W polu **Profil użytkownika** podaj nazwę profilu użytkownika używaną przez kreatora do łączenia się z domeną EIM.
  - W polu **Hasło** podaj hasło dla profilu użytkownika.
  - W polu **Potwierdź hasło** wpisz ponownie hasło w celu weryfikacji.
- Kliknij **Weryfikacja połączenia**, aby sprawdzić, czy kreator może użyć podanych informacji o użytkowniku do pomyślnego nawiązania połączenia z kontrolerem domeny EIM.
- Kliknij przycisk **Dalej**.

8. Na stronie **Podaj domenę** wybierz nazwę domeny, którą chcesz przyłączyć, i kliknij przycisk **Dalej**.
9. Na stronie **Informacje o rejestrach** określ, czy dodawać lokalne rejestry użytkowników do domeny EIM jako definicje rejestrów. Wybierz jeden lub oba poniższe typy rejestrów użytkowników:
   - Wybierz **Lokalny i5/OS**, aby dodać definicję rejestru dla rejestru lokalnego. W polu akceptuj domyślne wartości lub wpisz własne dla nazwy definicji rejestru. Nazwa rejestru EIM jest arbitralnym łańcuchem reprezentującym typ rejestru i konkretną instancję tego rejestru.

     Uwaga: W tym momencie nie jest konieczne tworzenie definicji rejestru lokalnego i5/OS. Jeśli chcesz utworzyć definicję rejestru i5/OS później, możesz dodać definicję rejestru systemu i aktualizować właściwości konfiguracji EIM.
   - Wybierz **Kerberos**, aby dodać definicję rejestru do rejestru Kerberos. W polu akceptuj wartości domyślne lub wpisz własne dla nazwy definicji rejestru. Domyślna nazwa definicji rejestru jest taka sama, jak nazwa dziedziny. Używając identycznych nazw rejestru Kerberos i dziedziny, możesz zwiększyć wydajność pobierania informacji z rejestru. Jeśli to konieczne, wybierz **W tożsamościach użytkowników Kerberos rozróżniane są wielkości liter**.

     Uwaga: Jeśli użyto kreatora konfigurowania EIM na innym systemie do dodania definicji rejestru dla rejestru Kerberos, dla którego ten system iSeries jest jednostką główną usługi, należy dodać definicję rejestru Kerberos w ramach części tej konfiguracji. Jednakże po zakończeniu działania kreatora należy podać nazwę rejestru Kerberos we właściwościach konfiguracji dla tego systemu.
   - Kliknij przycisk **Dalej**.
10. Na stronie **Podaj użytkownika systemu EIM** wybierz **Typ użytkownika**, który ma być używany przez system podczas wykonywania operacji EIM w imieniu funkcji systemu operacyjnego. Do operacji tych należą wyszukiwanie odwzorowań i usuwanie powiązań podczas usuwania lokalnego profilu użytkownika i5/OS. Dostępne są następujące typy użytkowników: **Nazwa wyróżniająca i hasło**, **Plik kluczy Kerberos i nazwa użytkownika** oraz **Nazwa użytkownika Kerberos i hasło**. Wybór typu użytkownika zależy od bieżącej konfiguracji systemu. Jeśli na przykład w systemie nie skonfigurowano usługi uwierzytelniania sieciowego, wybór typów użytkowników protokołu Kerberos nie będzie dostępny. Od wybranego typu użytkownika zależą inne informacje, które należy podać na tej stronie:

    Uwaga: Należy podać użytkownika, który już jest zdefiniowany w serwerze katalogów udostępniającym kontroler domeny EIM. Podany użytkownik musi mieć uprawnienia do wyszukiwania odwzorowania i administrowania rejestrem co najmniej dla lokalnego rejestru użytkowników. Jeśli podany użytkownik

nie ma takich uprawnień, niektóre funkcje systemu operacyjnego związane z pojedynczym logowaniem i usuwaniem profili użytkowników mogą się nie powieść.

- Wybierając opcję **Nazwa wyróżniająca i hasło**, musisz podać następujące informacje:
  - W polu **Nazwa wyróżniająca** podaj nazwę wyróżniającą LDAP identyfikującą użytkownika w systemie, nazwa ta będzie używana podczas wykonywania operacji EIM.
  - W polu **Hasło** podaj hasło dla nazwy wyróżniającej.
  - W polu **Potwierdź hasło** wpisz ponownie hasło w celu weryfikacji.
- Wybierając opcję **Nazwa użytkownika Kerberos i hasło**, musisz podać następujące informacje:
  - W polu **Nazwa użytkownika** podaj nazwę użytkownika Kerberos dla systemu, nazwa ta będzie używana podczas wykonywania operacji EIM.
  - W polu **Dziedzina** podaj pełną nazwę dziedziny Kerberos, której członkiem jest dana nazwa użytkownika. Nazwy użytkownika i dziedziny jednoznacznie identyfikują użytkowników Kerberos w pliku kluczy. Na przykład nazwa użytkownika jkowalski w dziedzinie zamowienia.mojafirma.com jest reprezentowana w pliku kluczy jako jkowalski@zamowienia.mojafirma.com.
  - W polu **Hasło** wpisz hasło użytkownika.
  - W polu **Potwierdź hasło** wpisz ponownie hasło w celu weryfikacji.
- Wybierając opcję **Plik kluczy Kerberos i nazwa użytkownika**, musisz podać następujące informacje:
  - W polu **Plik kluczy** podaj pełną ścieżkę i nazwę pliku kluczy zawierającego nazwę użytkownika Kerberos używaną przez system podczas wykonywania operacji EIM. Możesz również kliknąć **Przeglądaj...**, aby przeszukać katalogi zintegrowanego systemu plików serwera iSeries i wybrać plik kluczy.
  - W polu **Nazwa użytkownika** podaj nazwę użytkownika Kerberos dla systemu, nazwa ta będzie używana podczas wykonywania operacji EIM.
  - W polu **Dziedzina** podaj pełną nazwę dziedziny Kerberos, której członkiem jest dana nazwa użytkownika. Nazwy użytkownika i dziedziny jednoznacznie identyfikują użytkowników Kerberos w pliku kluczy. Na przykład nazwa użytkownika jkowalski w dziedzinie zamowienia.mojafirma.com jest reprezentowana w pliku kluczy jako jkowalski@zamowienia.mojafirma.com.
- Kliknij **Weryfikacja połączenia**, aby upewnić się, że kreator może użyć podanych informacji o użytkowniku do pomyślnego nawiązania połączenia z kontrolerem domeny EIM.
- Kliknij przycisk **Dalej**.

11. Przejrzyj podane informacje konfiguracyjne na stronie **Podsumowanie**. Jeśli wszystkie podane informacje są poprawne, kliknij przycisk **Zakończ**.

Finalizowanie konfigurowania produktu EIM dla domeny

Kończąc działanie kreator dodaje domenę do folderu **Zarządzanie domenami** i można utworzyć prostą konfigurację EIM dla tego serwera. Jednak aby sfinalizować konfigurację EIM dla tej domeny, należy wykonać następujące zadania:

1. Jeśli to konieczne, dodaj definicje rejestrów EIM do domeny EIM dla innych serwerów niż serwery iSeries i aplikacji, które mają należeć do danej domeny EIM. Definicje rejestrów odnoszą się do bieżących rejestrów użytkowników, które muszą należeć do domeny. Możesz dodać definicje rejestrów systemu lub dodać definicje rejestrów aplikacji, w zależności od wymagań implementacji EIM.
2. W zależności od wymagań implementacji EIM określ, czy potrzebne jest:
   - Tworzenie identyfikatorów EIM dla każdego użytkownika lub jednostki w domenie oraz tworzenie dla nich powiązań identyfikatorów.
   - Tworzenie powiązań strategii, aby odwzorować grupę użytkowników na pojedynczą tożsamość użytkownika docelowego.
   - Tworzenie kombinacji powyższych elementów.
3. Użyj funkcji EIM testowanie odwzorowania, aby sprawdzić odwzorowania tożsamości dla konfiguracji EIM.
4. Jeśli jedynym zdefiniowanym użytkownikiem EIM jest nazwa wyróżniająca administratora LDAP, to użytkownik EIM ma najwyższy poziom uprawnień do wszystkich danych na serwerze katalogów. Dlatego należy rozważyć utworzenie co najmniej jednego dodatkowego użytkownika, o bardziej odpowiednich i ograniczonych prawach

dostępu do danych EIM. Więcej informacji na temat tworzenia nazw wyróżniających dla serwera katalogów zawiera temat Nazwy wyróżniające w temacie IBM Directory Server for iSeries (LDAP). Liczba zdefiniowanych dodatkowych użytkowników EIM zależy od nacisku strategii ochrony na rozdzielenie poszczególnych obowiązków i odpowiedzialności związanych z ochroną. Zazwyczaj można utworzyć przynajmniej dwa następujące typy nazwy wyróżniającej:

- **Użytkownika z prawami dostępu administratora EIM**

  Nazwa wyróżniająca administratora EIM ma wystarczający poziom uprawnień dla administratora odpowiedzialnego za zarządzanie domeną EIM. Może ona być używana do połączenia się z kontrolerem domeny do zarządzania wszystkimi aspektami domeny EIM przy użyciu programu iSeries Navigator.
- **Przynajmniej jeden użytkownik o następujących prawach dostępu**:
  - Administrator identyfikatorów
  - Administrator rejestru
  - Operacje odwzorowania EIM

  Użytkownik ten ma odpowiedni poziom dostępu dla użytkownika systemu, który wykonuje operacje EIM w systemie operacyjnym.

Uwaga: Aby użyć nowej nazwy wyróżniającej dla użytkownika systemu zamiast nazwy wyróżniającej administratora LDAP, trzeba zmienić właściwości konfiguracji EIM dla serwera iSeries. Więcej informacji na ten temat zawiera temat Zarządzanie właściwościami konfiguracji EIM.

Jeśli tworzysz prostą konfigurację usługi uwierzytelniania sieciowego, a szczególnie, jeśli implementujesz środowisko pojedynczego logowania, możesz potrzebować wykonać dodatkowe zadania. Informacje na temat tych dodatkowych zadań można znaleźć przeglądając czynności konfigurowania przedstawione w scenariuszu Włączanie pojedynczego logowania dla i5/OS.

Konfigurowanie chronionego połączenia z kontrolerem domeny EIM

Informacje objaśniające, jak skonfigurować chronione połączenie z kontrolerem domeny za pomocą protokołu SSL lub TLS.

Aby zabezpieczyć transmisję danych EIM, można użyć protokołów SSL lub TLS do nawiązania chronionego połączenia z kontrolerem domeny EIM.

Aby skonfigurować SSL lub TLS dla EIM:

1. Jeśli to konieczne, użyj programu Menedżer certyfikatów cyfrowych (DCM), aby utworzyć certyfikat wymagany przez serwer katalogów do wykorzystania SSL.
2. Włączanie SSL dla lokalnego serwera katalogów udostępniającego kontroler domeny EIM.
3. Zaktualizuj właściwości konfiguracji EIM, określając, że serwer iSeries używa chronionego połączenia SSL. Aby zaktualizować właściwości konfiguracji EIM, wykonaj następujące czynności:
   a. W programie iSeries Navigator wybierz system, na którym skonfigurowano EIM, i rozwiń gałąź **Sieć → Enterprise Identity Mapping**.
   b. Kliknij prawym przyciskiem myszy **Konfiguracja** i wybierz opcję **Właściwości**.
   c. Na stronie **Domena** wybierz **Użyj chronionego połączenia (SSL lub TLS)**, podaj chroniony port, na którym serwer katalogów nasłuchuje lub akceptuj domyślną wartość 636 w polu **Port**, a następnie kliknij **OK**.
4. Zaktualizuj właściwości domeny EIM dla każdej domeny EIM, podając, że EIM używa połączenia SSL podczas zarządzania domeną za pomocą programu iSeries Navigator. Aby zaktualizować właściwości domeny EIM, wykonaj następujące czynności:
   a. W programie iSeries Navigator wybierz system, na którym skonfigurowano EIM i rozwiń gałąź **Sieć → Enterprise Identity Mapping → Zarządzanie domenami**.
   b. Wybierz domenę EIM, w której chcesz pracować.
      - Jeśli domena EIM, z którą chcesz pracować, nie została wyświetlona w folderze **Zarządzanie domenami**, patrz temat Dodawanie domeny EIM do zarządzania domenami.

- Jeśli w tej chwili nie masz połączenia z domeną EIM, w której chcesz pracować, patrz temat Łączenie się z kontrolerem domeny EIM.

c. Kliknij prawym przyciskiem myszy przyłączoną domenę EIM i wybierz **Właściwości**.

d. Na stronie **Domena** wybierz **Użyj chronionego połączenia (SSL lub TLS)**, podaj chroniony port, na którym serwer katalogów nasłuchuje lub akceptuj domyślną wartość 636 w polu **Port**, a następnie kliknij **OK**.

Zarządzanie EIM

Informacje o zarządzaniu domeną EIM i danymi domeny, w tym o zarządzaniu domenami EIM, identyfikatorami, powiązaniami, definicjami rejestrów, kontrolą dostępu EIM itp.

Po skonfigurowaniu EIM na serwerze iSeries trzeba od czasu do czasu wykonać zadania administracyjne związane z zarządzaniem domeną EIM i danymi dla domeny. Więcej informacji na temat zarządzania EIM w przedsiębiorstwie zawierają następujące strony.

Zarządzanie domenami EIM

Informacje objaśniające zasady zarządzania domenami EIM i ich właściwościami.

Program iSeries Navigator umożliwia zarządzanie wszystkimi domenami EIM. Aby można było zarządzać daną domeną EIM, musi ona znajdować się na liście domen lub być dodana do listy domen w folderze **Zarządzanie domenami** dostępnym w folderze **Sieć** w programie iSeries Navigator. Jeśli do utworzenia domeny i jej konfigurowania jest używany kreator konfiguracji EIM, to domena jest dodawana do folderu **Zarządzanie domenami** automatycznie, dzięki temu można zarządzać i domeną i informacjami w tej domenie.

Do zarządzania domeną EIM istniejącą w dowolnym miejscu tej samej sieci można użyć dowolnego połączenia iSeries, nawet jeśli używany serwer iSeries nie znajduje się w tej domenie.

Dla domeny można wykonywać następujące zadania zarządzania:

Dodanie domeny EIM do folderu Zarządzanie domenami

Aby wykonać to zadanie, konieczne są uprawnienia specjalne *SECADM, ponadto domena, która ma być dodana, musi istnieć przed jej dodaniem do folderu **Zarządzanie domenami**.

Aby dodać istniejącą domenę EIM do folderu **Zarządzanie domenami**, wykonaj następujące czynności:

1. Rozwiń gałąź **Sieć > Odwzorowanie EIM**.
2. Kliknij prawym przyciskiem myszy **Zarządzanie domenami** i wybierz **Dodaj domenę...**
3. W oknie dialogowym **Dodanie domeny** podaj informacje o domenie i połączeniu. Możesz również kliknąć **Przeglądaj...**, aby wyświetlić listę domen, którymi zarządza dany kontroler domeny.

   Uwaga: Kliknięcie opcji **Przeglądaj...** powoduje wyświetlenie okna dialogowego **Połącz z kontrolerem domeny EIM**. Aby wyświetlić listę domen, należy połączyć się z kontrolerem domeny z prawami dostępu administratora LDAP lub administratora EIM. Zawartość listy domen zależy od tego, jakie masz prawa dostępu EIM. Jeśli masz prawa dostępu administratora LDAP, możesz przeglądać listę wszystkich domen, którymi zarządza dany kontroler domeny. W przeciwnym przypadku na liście będą wyświetlone tylko te domeny, do których masz prawa dostępu administratora EIM.
4. Kliknij **Pomoc**, jeśli chcesz przeczytać, jakie dane wpisać w każdym polu.
5. Kliknij przycisk **OK**, aby dodać domenę.

Połączenie się z domeną EIM.

Przed rozpoczęciem pracy z domeną EIM należy połączyć się z kontrolerem domeny EIM dla tej domeny. Z daną domeną EIM można połączyć się nawet wtedy, gdy używany serwer iSeries nie jest skonfigurowany w tej domenie.

Aby połączyć się z kontrolerem domeny EIM użytkownik, który się łączy, musi być członkiem grupy "Kontrola dostępu EIM" na stronie 39. Członkostwo grupy kontroli dostępu EIM określa, jakie zadania można wykonywać w domenie i jakie dane EIM przeglądać lub zmieniać.

Aby połączyć się z domeną EIM:

1. Rozwiń gałąź **Sieć > Odwzorowanie EIM > Zarządzanie domenami**.
2. Kliknij prawym przyciskiem myszy domenę, z którą chcesz się połączyć.

   Uwaga: Jeśli domena, z którą chcesz pracować, nie jest wymieniona w folderze **Zarządzanie domenami**, patrz "Dodanie domeny EIM do folderu Zarządzanie domenami" na stronie 85.
3. Kliknij prawym przyciskiem myszy domenę EIM, z którą chcesz się połączyć, i wybierz **Połącz...**
4. W oknie dialogowym **Połącz z kontrolerem domeny EIM** określ **Typ użytkownika**, podaj wymagane informacje identyfikacyjne dla użytkownika i wybierz opcję hasła dla połączenia z kontrolerem domeny.
5. Kliknij **Pomoc**, jeśli chcesz przeczytać, jakie dane podać w każdym polu okna dialogowego.
6. Kliknij **OK**, aby połączyć się z kontrolerem domeny.

Włączanie powiązań strategii dla domeny

Powiązanie strategii umożliwia tworzenie odwzorowania typu wiele-do-jednego w przypadkach, gdy powiązania między tożsamościami użytkownika i identyfikatorem EIM nie istnieją. Za pomocą powiązania strategii można odwzorować źródłowy zestaw wielu tożsamości użytkownika na pojedynczą tożsamość użytkownika docelowego w określonym rejestrze użytkowników docelowych. Jednak przed użyciem powiązań strategii należy wpierw upewnić się, że w domenie włączone zostało używanie powiązań strategii dla operacji wyszukiwania odwzorowań.

Aby włączyć używanie powiązań strategii dla domeny przez obsługę strategii odwzorowań, musisz połączyć się z domeną EIM, w której chcesz pracować, i mieć prawa dostępu administratora EIM.

Aby włączyć używanie powiązań strategii dla domeny przez obsługę wyszukiwania odwzorowań, wykonaj następujące czynności:

1. Rozwiń gałąź **Sieć > Odwzorowanie EIM > Zarządzanie domenami**.
2. Prawym przyciskiem myszy kliknij domenę EIM, w której zamierzasz pracować i wybierz opcję **Strategia odwzorowania...**.
   - Jeśli domena EIM, z którą chcesz pracować, nie jest wymieniona w folderze **Zarządzanie domenami**, patrz "Dodanie domeny EIM do folderu Zarządzanie domenami" na stronie 85.
   - Jeśli w tej chwili nie masz połączenia z domeną EIM, w której chcesz pracować, patrz temat Łączenie się z kontrolerem domeny EIM. (Opcja **Strategia odwzorowań...** jest niedostępna, jeśli nie ma połączenia z domeną.)
3. Na stronie **Ogólne** wybierz opcję **Włącz wyszukiwanie odwzorowania przy użyciu powiązań strategii dla domeny**.
4. Kliknij przycisk **OK**.

Uwaga: Musisz włączyć wyszukiwanie odwzorowań i korzystanie z powiązań strategii dla każdej definicji rejestru docelowego, dla której zdefiniowane są powiązania strategii. Jeśli dla definicji rejestru docelowego nie będzie włączone wyszukiwanie odwzorowań, rejestr ten nie będzie brany pod uwagę przez operacje wyszukiwania odwzorowań EIM. Jeśli nie zostanie określone, że rejestr docelowy może używać powiązań strategii, to wszystkie zdefiniowane powiązania strategii dla tego rejestru będą ignorowane przez operacje wyszukiwania odwzorowania EIM.

Pojęcia pokrewne

"Obsługa i włączanie strategii odwzorowań EIM" na stronie 38
Informacje objaśniające sposób włączania i wyłączania powiązań strategii dla domeny.

Testowanie odwzorowań EIM

Obsługa testowania odwzorowania umożliwia wykonywanie operacji wyszukiwania odwzorowania EIM względem konfiguracji EIM. Testowanie umożliwia sprawdzenie, czy dana tożsamość użytkownika źródłowego jest odwzorowana poprawnie na odpowiednią tożsamość użytkownika docelowego. Testowanie takie gwarantuje, że operacje wyszukiwania odwzorowań EIM mogą zwrócić poprawną tożsamość użytkownika docelowego na podstawie podanych danych.

Aby za pomocą funkcji testowania odwzorowania sprawdzić konfigurację EIM, musisz połączyć się z domeną EIM, w której chcesz pracować, i mieć kontrolę dostępu EIM na jednym z poniższych poziomów:

- Administrator EIM
- Administrator identyfikatorów
- Administrator rejestru
- Operacje wyszukiwania odwzorowania EIM

Aby za pomocą obsługi testowania odwzorowań sprawdzić konfigurację EIM, wykonaj następujące czynności:

1. Rozwiń gałąź **Sieć > Odwzorowanie EIM > Zarządzanie domenami**.
2. Wybierz domenę EIM, w której chcesz pracować.
   - Jeśli domena EIM, z którą chcesz pracować, nie została wyświetlona w folderze **Zarządzanie domenami**, patrz temat Dodawanie domeny EIM do zarządzania domenami.
   - Jeśli w tej chwili nie masz połączenia z domeną EIM, w której chcesz pracować, patrz temat Łączenie się z kontrolerem domeny EIM.
3. Kliknij prawym przyciskiem myszy przyłączoną domenę EIM i wybierz **Testowanie odwzorowania...**
4. W oknie dialogowym **Testowanie odwzorowania** podaj następujące dane:
   a. W polu **Rejestr źródłowy** podaj nazwę definicji rejestru odnoszącą się do rejestru użytkowników, który ma być użyty jako źródło do testowania operacji wyszukiwania odwzorowania.
   b. W polu **Użytkownik źródłowy** podaj nazwę tożsamości użytkownika, która ma być użyta jako źródło do testowania operacji wyszukiwania odwzorowania.
   c. W polu **Rejestr docelowy** podaj nazwę definicji rejestru, odnoszącą się do rejestru użytkowników, który ma być użyty jako cel do testowania operacji wyszukiwania odwzorowania.
   d. Opcjonalne: w polu **Informacje wyszukiwania** podaj informacje wyszukiwania zdefiniowane dla użytkownika docelowego.
5. Kliknij **Pomoc**, jeśli chcesz przeczytać, jakie dane należy wpisać w każdym polu okna dialogowego.
6. Kliknij **Test** i sprawdź wyniki operacji wyszukiwania odwzorowania, gdy zostaną one wyświetlone.

   Uwaga: Jeśli operacja wyszukiwania odwzorowań zwraca niejednoznaczne wyniki, wyświetlane jest okno dialogowe Testowanie odwzorowania, zawierające komunikat o błędzie i listę użytkowników docelowych odnalezionych przez operację wyszukiwania.
   a. Aby usunąć problem z niejednoznacznymi wynikami, wybierz użytkownika i kliknij opcję **Szczegóły**.
   b. Wyświetlane jest ono dialogowe Testowanie odwzorowania - szczegóły, zawierające informacje o wynikach operacji wyszukiwania odwzorowania dla podanego użytkownika docelowego. Aby wyświetlić bardziej szczegółowe informacje dotyczące wyników operacji wyszukiwania, kliknij przycisk Pomoc.
   c. Kliknij przycisk **Zamknij**, aby zamknąć okno dialogowe **Testowanie odwzorowania - wyniki**.
7. Możesz kontynuować testowanie konfiguracji lub kliknąć **Zamknij**, aby zakończyć.

Praca z wynikami testu i rozwiązywanie problemów:

Po uruchomieniu testu zwracana jest tożsamość użytkownika docelowego, jeśli proces testujący znajdzie powiązanie między tożsamością użytkownika źródłowego a rejestrem użytkowników docelowych podanymi przez administratora.

Test wskazuje również znaleziony typ powiązania między dwiema tożsamościami użytkownika. Jeśli proces testujący nie znajdzie powiązania na podstawie dostarczonych informacji, zwróci jako tożsamość użytkownika docelowego wartość none.

Funkcja testująca, tak jak każda operacja wyszukiwania odwzorowania EIM, wyszukuje i zwraca pierwszą odpowiednią tożsamość użytkownika docelowego przeszukując kolejno:

1. Dane powiązanie identyfikatora
2. Powiązanie strategii filtrów certyfikatów
3. Domyślne powiązanie strategii rejestru
4. Domyślne powiązanie strategii domeny

W niektórych przypadkach testowanie nie zwróci żadnej tożsamości użytkownika, chociaż dla domeny skonfigurowano powiązania. Sprawdź, czy do testu zostały podane poprawne informacje. Jeśli tak i test nie zwraca wyników, to problem może być spowodowany jedną z następujących przyczyn:

- Na poziomie domeny nie jest włączona obsługa powiązań strategii. Możliwe, że trzeba włączyć powiązania strategii dla domeny.
- Na poziomie danego rejestru nie jest włączona obsługa powiązań strategii. Możliwe, że trzeba włączyć obsługę wyszukiwania odwzorowań i korzystanie z powiązań strategii dla rejestru docelowego.
- Powiązanie źródłowe lub docelowe dla identyfikatora EIM jest skonfigurowane niepoprawnie. Na przykład nie ma powiązania źródłowego dla nazwy użytkownika Kerberos (lub użytkownika Windows) lub jest ono niepoprawne. Możliwe również, że powiązanie docelowe określa niepoprawną tożsamość użytkownika. Wyświetl wszystkie powiązania identyfikatorów dla identyfikatora EIM, aby sprawdzić powiązania określonego identyfikatora.
- Powiązanie strategii jest skonfigurowane niepoprawnie. Wyświetl wszystkie powiązania strategii dla domeny, aby sprawdzić dane źródłowe i docelowe dla wszystkich powiązań strategii zdefiniowanych w domenie.
- Definicja rejestru i tożsamości użytkowników nie są zgodne w związku z rozróżnianiem wielkości znaków. Można usunąć i ponownie utworzyć rejestr lub usunąć i ponownie utworzyć powiązanie stosując poprawną wielkość znaków.

W innych przypadkach wyniki testu mogą być niejednoznaczne. Wówczas zostanie wyświetlony odpowiedni komunikat o błędzie. Test zwraca niejednoznaczne wyniki, jeśli określone kryterium testu spełnia więcej niż jedna tożsamość użytkownika docelowego. Operacja wyszukiwania odwzorowania może zwrócić wiele tożsamości użytkowników docelowych, jeśli wystąpi któraś z poniżej wymienionych sytuacji:

- Identyfikator EIM ma wiele pojedynczych powiązań docelowych do tego samego rejestru docelowego.
- Więcej niż jeden identyfikator EIM ma pewną tożsamość użytkownika podaną w powiązaniu źródłowym i każdy z tych identyfikatorów EIM ma powiązanie docelowe do tego samego rejestru docelowego, jednak tożsamości użytkowników podane dla każdego powiązania docelowego mogą być różne.
- Więcej niż jedno powiązanie strategii domeny domyślnej określa dany rejestr docelowy.
- Więcej niż jedno powiązanie strategii rejestru domyślnego określa dany rejestr źródłowy i rejestr docelowy.
- Więcej niż jedno powiązanie strategii filtrów certyfikatów określa dany rejestr źródłowy X.509, filtr certyfikatu i rejestr docelowy.

Sytuacja taka może stanowić problem dla aplikacji z obsługą EIM, w tym aplikacji i produktów systemu i5/OS. Dlatego należy określić przyczynę powstawania takich wyników i działania, które należy podjąć, aby rozwiązać ten problem. W zależności od przyczyny, można wykonać którąś z poniższych czynności:

- Test zwraca wiele niechcianych tożsamości docelowych. Oznacza to, że konfiguracja powiązania dla domeny jest niepoprawna z jednego z następujących powodów:
  - Powiązanie źródłowe lub docelowe dla identyfikatora EIM jest skonfigurowane niepoprawnie. Na przykład nie ma powiązania źródłowego dla nazwy użytkownika Kerberos (lub użytkownika Windows) lub jest ono niepoprawne. Możliwe również, że powiązanie docelowe określa niepoprawną tożsamość użytkownika. Wyświetl wszystkie powiązania identyfikatorów dla identyfikatora EIM, aby sprawdzić powiązania określonego identyfikatora.

– Powiązanie strategii jest skonfigurowane niepoprawnie. Wyświetl wszystkie powiązania strategii dla domeny, aby sprawdzić dane źródłowe i docelowe dla wszystkich powiązań strategii zdefiniowanych w domenie.

- Test zwraca wiele tożsamości użytkowników docelowych i wyniki te są zgodne z konfiguracją powiązań, dlatego należy określić dane wyszukiwania dla każdej tożsamości użytkownika docelowego. Należy zdefiniować unikalne dane wyszukiwania dla wszystkich tożsamości użytkowników docelowych, które mają to samo źródło (identyfikator EIM w przypadku powiązań identyfikatorów lub rejestr użytkowników źródłowych w przypadku powiązań strategii). Zdefiniowanie danych wyszukiwania dla każdej tożsamości użytkownika docelowego gwarantuje, że operacja wyszukiwania zwróci jedną tożsamość użytkownika docelowego, zamiast wszystkich możliwych tożsamości użytkowników docelowych. Przeczytaj sekcję Dodanie danych wyszukiwania do tożsamości użytkownika docelowego. Należy określić dane wyszukiwania dla operacji wyszukiwania odwzorowania.

  Uwaga: Rozwiązanie to jest skuteczne tylko wtedy, gdy aplikacja ma włączone korzystanie z danych wyszukiwania. Jednakże podstawowe aplikacje systemu i5/OS, takie jak iSeries Access for Windows, nie używają danych wyszukiwania do rozróżnienia między wieloma tożsamościami użytkowników docelowych zwracanych przez operację wyszukiwania. Dlatego też należy rozważyć ponowne zdefiniowanie powiązań dla domeny, aby zapewnić, że operacja wyszukiwania odwzorowań będzie mogła zwrócić pojedynczą tożsamość użytkownika docelowego i że podstawowe aplikacje systemu i5/OS będą mogły pomyślnie wykonywać operacje wyszukiwania i odwzorować tożsamości.

Informacje dodatkowe na temat potencjalnych problemów z odwzorowaniem i ich rozwiązań, poza opisanymi tutaj, zawiera temat “Rozwiązywanie problemów z odwzorowaniem EIM” na stronie 118.

Usuwanie domeny EIM z folderu Zarządzanie domenami

Domenę EIM, która nie chcesz już zarządzać, możesz usunąć z folderu **Zarządzanie domenami**. Jednakże usunięcie domeny z folderu **Zarządzanie domenami nie** jest równoznaczne z usunięciem domeny i nie usuwa danych domeny z kontrolera domeny. Jeśli chcesz usunąć domenę wraz z jej wszystkimi danymi, przeczytaj sekcję na temat usuwania domeny.

Aby usunąć domenę, nie są potrzebne żadne “Kontrola dostępu EIM” na stronie 39.

Aby usunąć domenę, zarządzanie którą ma zostać zakończone, z folderu **Zarządzanie domenami**, wykonaj następujące czynności:

1. Rozwiń gałąź **Sieć > Odwzorowanie EIM**.
2. Kliknij prawym przyciskiem myszy **Zarządzanie domenami** i wybierz **Usuń domenę...**
3. Wybierz domenę EIM, którą chcesz usunąć z folderu **Zarządzanie domenami**.
4. Kliknij przycisk **OK**, aby usunąć domenę.

Usuwanie domeny EIM i wszystkich obiektów konfiguracyjnych

Przed usunięciem domeny EIM konieczne jest usunięcie wszystkich definicji rejestrów i identyfikatorów EIM w domenie. Jeśli nie chcesz usuwać domeny z wszystkimi jej danymi, ale nie chcesz już zarządzać tą domeną, możesz usunąć domenę z folderu Zarządzanie domenami.

Aby usunąć domenę EIM, konieczne są “Kontrola dostępu EIM” na stronie 39 na jednym z następujących poziomów:

- Administrator LDAP.
- Administrator EIM.

1. Rozwiń gałąź **Sieć > Odwzorowanie EIM > Zarządzanie domenami**.
2. Jeśli to potrzebne, usuń wszystkie definicje rejestrów z domeny EIM.
3. Jeśli to potrzebne, usuń wszystkie identyfikatory EIM z domeny EIM.
4. Kliknij prawym przyciskiem myszy domenę, którą chcesz usunąć, i wybierz **Usuń...**
5. W oknie dialogowym **Potwierdzenie usunięcia** kliknij **Tak**.

Uwaga: Wyświetlane jest okno dialogowe Usuwanie w trakcie, informujące o statusie procesu usuwania domeny.

Zarządzanie definicjami rejestrów EIM

Informacje dotyczące tworzenia definicji rejestrów EIM i zarządzania nimi dla tych rejestrów użytkowników w przedsiębiorstwie, które są uwzględniane w odwzorowaniach EIM.

Aby rejestry użytkowników i identyfikatory użytkowników, które one zawierają mogły uczestniczyć w EIM, należy dla nich utworzyć definicje rejestrów. Zarządzając tymi definicjami rejestrów EIM można następnie zarządzać udziałem rejestrów użytkowników i ich tożsamości użytkowników w EIM.

Dla definicji rejestrów można wykonywać następujące zadania zarządzania:

Pojęcia pokrewne

"Tworzenie powiązania strategii" na stronie 101

Zadania pokrewne

"Usuwanie powiązania strategii" na stronie 113

Dodanie definicji rejestru systemu

Aby utworzyć definicję rejestru systemu, należy połączyć się z domeną EIM, w której odbywać się będzie praca, i mieć prawa dostępu administratora EIM.

Aby dodać definicję rejestru systemu do domeny EIM, wykonaj następujące czynności.

1. Rozwiń gałąź **Sieć > Odwzorowanie EIM > Zarządzanie domenami**.
2. Wybierz domenę EIM, w której chcesz pracować.
   - Jeśli domena EIM, z którą chcesz pracować, nie jest wymieniona w folderze Zarządzanie domenami, patrz "Dodanie domeny EIM do folderu Zarządzanie domenami" na stronie 85.
   - Jeśli w tej chwili nie masz połączenia z domeną EIM, w której chcesz pracować, patrz "Połączenie się z domeną EIM." na stronie 85.
3. Rozwiń domenę EIM, z którą masz połączenie.
4. Kliknij prawym przyciskiem myszy **Rejestry użytkowników**, wybierz opcję **Dodaj rejestr**, a następnie **System...**.
5. W oknie dialogowym **Dodanie rejestru systemu** wpisz następujące dane definicji rejestru systemu:
   a. Nazwę definicji rejestru systemu.
   b. Typ definicji rejestru.
   c. Opis definicji rejestru systemu.
   d. (Opcjonalnie.) Adres URL rejestru użytkowników.
   e. Jeśli to niezbędne, jeden lub więcej aliasów dla definicji rejestru systemu.
6. Kliknij **Pomoc**, jeśli chcesz przeczytać, jakie dane podać w każdym polu.
7. Kliknij **OK**, aby zapisać podane informacje i dodać definicję rejestru do domeny EIM.

Dodanie definicji rejestru aplikacji

Aby utworzyć definicję rejestru aplikacji, należy połączyć się z domeną EIM, w której odbywać się będzie praca, i mieć prawa dostępu administratora EIM.

Aby dodać definicję rejestru aplikacji do domeny EIM, wykonaj następujące czynności:

1. Rozwiń gałąź **Sieć > Odwzorowanie EIM > Zarządzanie domenami**.
2. Wybierz domenę EIM, w której chcesz pracować.
   - Jeśli domena EIM, z którą chcesz pracować, nie jest wymieniona w folderze Zarządzanie domenami, patrz "Dodanie domeny EIM do folderu Zarządzanie domenami" na stronie 85.

- Jeśli w tej chwili nie masz połączenia z domeną EIM, w której chcesz pracować, patrz “Połączenie się z domeną EIM.” na stronie 85.

3. Rozwiń domenę EIM, z którą masz połączenie.
4. Kliknij prawym przyciskiem myszy **Rejestry użytkowników**, wybierz opcję **Dodaj rejestr**, a następnie **Aplikacja...**.
5. W oknie dialogowym **Dodanie rejestru aplikacji** wpisz następujące dane definicji rejestru aplikacji:
   a. Nazwę definicji rejestru aplikacji.
   b. Nazwę definicji rejestru systemu, którego podzbiorem jest definiowany rejestr użytkowników aplikacji. Podana definicja rejestru systemu musi istnieć w EIM, w przeciwnym przypadku tworzenie definicji rejestru aplikacji nie powiedzie się.
   c. Typ definicji rejestru.
   d. Opis definicji rejestru aplikacji.
   e. Jeśli to niezbędne, jeden lub więcej aliasów dla definicji rejestru aplikacji.
6. Kliknij **Pomoc**, jeśli chcesz przeczytać, jakie dane podać w każdym polu.
7. Kliknij **OK**, aby zapisać podane informacje i dodać definicję rejestru do domeny EIM.

Dodanie definicji rejestru grupowego

Aby utworzyć definicję rejestru grupowego, konieczne jest połączenie użytkownika z domeną EIM, w której zamierza on pracować oraz posiadanie przez niego kontroli dostępu na poziomie administratora EIM.

Aby dodać definicję rejestru grupowego do domeny EIM, należy wykonać poniższe czynności:

1. Rozwiń gałąź **Sieć → Odwzorowanie EIM → Zarządzanie domenami**.
2. Wybierz domenę EIM, w której chcesz pracować.
   a. Jeśli przyszła robocza domena EIM nie jest wymieniona pod hasłem Zarządzanie domenami, patrz temat Dodawanie domeny EIM do Zarządzania domenami.
   b. Jeśli komputer w tej chwili nie jest połączony z domeną EIM, w której będzie pracować, patrz temat Łączenie się z kontrolerem domeny EIM.
3. Rozwiń domenę EIM, z którą masz połączenie.
4. Kliknij prawym przyciskiem myszy **Rejestry użytkowników**, wybierz opcję **Dodaj rejestr**, a następnie **Grupa....**.
5. W oknie dialogowym Dodanie rejestru grupowego podaj informacje dotyczące definicji rejestrów aplikacji:
   a. Nazwę definicji rejestru grupowego.
   b. Jeśli dla wszystkich elementów definicji rejestru grupowego rozróżniana jest wielkość liter, wybierz opcję **Rozróżnianie wielkości liter w elementach definicji rejestru grupowego**.
   c. Opis definicji rejestru grupowego.
   d. Jeśli to niezbędne, jeden lub więcej aliasów dla definicji rejestru grupowego.
6. Kliknij **Pomoc**, jeśli chcesz przeczytać, jakie dane podać w każdym polu.
7. 7. Kliknij przycisk **OK**, aby zapisać informacje i dodać definicję rejestrów do domeny EIM.

Dodanie aliasu do definicji rejestru

Użytkownik lub programista aplikacji może potrzebować określić dodatkowe informacje wyróżniające dla definicji rejestru. Można to zrealizować tworząc alias dla definicji rejestru. Alias ten może być następnie używany przez użytkowników do lepszego rozróżniania rejestrów użytkowników.

Obsługa aliasów umożliwia programistom pisanie aplikacji nawet wtedy, gdy nie znają arbitralnej nazwy definicji rejestru EIM wybranej przez administratora wdrażającego aplikację. Alias używany przez aplikację może być udostępniony administratorowi EIM w dokumentacji aplikacji. Za pomocą tych informacji administrator EIM może przypisać dany alias definicji rejestru EIM reprezentujący rzeczywisty rejestr użytkowników, który został wybrany przez administratora do użycia przez aplikację.

Aby dodać alias do definicji rejestru, musisz połączyć się z domeną EIM, w której chcesz pracować, i mieć uprawnienia (patrz “Kontrola dostępu EIM” na stronie 39) na jednym z poniższych poziomów:

- Administrator rejestru.
- Administrator dla wybranych rejestrów (dla modyfikowanego rejestru).
- Administrator EIM.

Aby dodać alias do definicji rejestru EIM, wykonaj następujące czynności:

1. Rozwiń gałąź **Sieć > Odwzorowanie EIM > Zarządzanie domenami**.
2. Wybierz domenę EIM, w której chcesz pracować.
   - Jeśli domena EIM, z którą chcesz pracować, nie jest wymieniona w folderze Zarządzanie domenami, patrz “Dodanie domeny EIM do folderu Zarządzanie domenami” na stronie 85.
   - Jeśli w tej chwili nie masz połączenia z domeną EIM, w której chcesz pracować, patrz “Połączenie się z domeną EIM.” na stronie 85.
3. Rozwiń domenę EIM, z którą masz połączenie.
4. Kliknij **Rejestry użytkowników**, aby wyświetlić listę definicji rejestrów w domenie.

   Uwaga: W przypadku administratora wybranych rejestrów lista zawiera tylko rejestry, do których bezpośrednio określono uprawnienia.
5. Kliknij prawym przyciskiem myszy definicję rejestru, do którego chcesz dodać alias, i wybierz **Właściwości...**.
6. Wybierz stronę **Aliasy** i podaj nazwę i typ aliasu, który chcesz dodać.

   Uwaga: Możesz podać typ aliasu, którego nie ma na liście typów.
7. Kliknij **Pomoc**, jeśli chcesz przeczytać, jakie dane wpisać w każdym polu.
8. Kliknij przycisk **Dodaj**.
9. Kliknij **OK**, aby zachować zmiany w definicji rejestru.

Definiowanie prywatnego typu rejestru użytkowników w EIM

Podczas tworzenia definicji rejestru EIM można podać jeden z listy wstępnie zdefiniowanych typów rejestrów użytkowników jako przedstawiciela bieżącego rejestru użytkowników istniejących w systemie w przedsiębiorstwie. Wprawdzie udostępnione są predefiniowane typy definicji rejestrów dla większości rejestrów użytkowników systemu operacyjnego, jednak może zaistnieć potrzeba utworzenia definicji rejestru, dla którego EIM nie zawiera takiego typu definicji. W takim przypadku są dwie możliwości. Można użyć istniejącej definicji rejestru, która jest zgodna z charakterystyką danego rejestru użytkowników lub zdefiniować prywatny typ rejestru użytkowników.

Aby zdefiniować typ rejestru użytkowników, który nie jest domyślnie rozpoznawany przez EIM, należy użyć identyfikatora obiektu, aby określić typ tego rejestru w postaci **IdentyfikatorObiektu-normalizacja**, gdzie **IdentyfikatorObiektu** oznacza identyfikator obiektu w postaci dziesiętnej z kropkami, taki jak 1.2.3.4.5.6.7, a **normalizacja** jest wartością **caseExact** lub **caseIgnore**. Na przykład identyfikatorem obiektu (OID) w systemie iSeries jest 1.3.18.0.2.33.2-caseIgnore.

Aby utworzyć unikalne identyfikatory obiektów, należy je uzyskać od uznanego ośrodka rejestracji takich identyfikatorów. Posługiwanie się unikalnymi identyfikatorami obiektów chroni przed potencjalnymi konfliktami, które mogłyby powstać między identyfikatorami utworzonymi przez inne organizacje lub aplikacje.

Istnieją dwa sposoby uzyskania identyfikatorów obiektów:

- **Zarejestrowanie obiektów w ośrodku**. Ta metoda jest przydatna szczególnie wtedy, gdy do reprezentowania informacji potrzebujemy niewielkiej ilości stałych identyfikatorów obiektów. Identyfikatory te mogłyby na przykład reprezentować strategie certyfikatów przeznaczone dla użytkowników w przedsiębiorstwie.
- **Uzyskanie przypisania łukowego od ośrodka i przypisanie własnych identyfikatorów obiektów stosownie do potrzeb**. Metoda, w której stosowane jest przypisanie zakresu identyfikatorów obiektów w postaci dziesiętnej z kropkami, jest przydatna, jeśli potrzebujemy wielu identyfikatorów obiektów lub jeśli przypisania tych identyfikatorów podlegają zmianom. Przypisanie łukowe składa się z początkowych numerów w postaci dziesiętnej

z kropkami, na których należy oprzeć **IdentyfikatorObiektu**. Na przykład przypisanie łukowe może mieć postać 1.2.3.4.5.. Następnie można utworzyć identyfikatory obiektów, dodając pozycje do tego przypisania. Identyfikatory te mogą mieć na przykład postać 1.2.3.4.5.x.x.x).

Więcej informacji na temat rejestrowania identyfikatorów obiektów w ośrodkach można znaleźć w następujących zasobach w sieci Internet:

- American National Standards Institute (ANSI) jest ośrodkiem rejestrowania w Stanach Zjednoczonych umożliwiającym rejestrowanie nazw organizacji z użyciem globalnego procesu rejestrowania ustanowionego przez organizacje International Standards Organization (ISO) i International Telecommunication Union (ITU). Arkusz informacyjny w formacie Microsoft Word na temat zastosowania Registered Application Provider Identifier (RID) jest dostępny w serwisie WWW ANSI Public Document Library http://public.ansi.org/ansionline/Documents/ . Aby go odnaleźć, należy wybrać opcje **Other Services > Registration Programs**. Łukowy identyfikator obiektów ANSI dla organizacji to 2.16.840.1. Przypisania łukowe w instytucie ANSI są odpłatne. Uzyskanie przypisanego łuku identyfikatorów obiektów od instytucji ANSI trwa około dwa tygodnie. ANSI przypisuje numer (NOWYNUMER), aby utworzyć nowy łuk identyfikatorów obiektów, na przykład: 2.16.840.1.NOWYNUMER.
- W większości krajów lub rejonów rejestr identyfikatorów obiektów jest obsługiwany przez narodowe stowarzyszenia zajmujące się standardami. W przypadku łuku w ANSI są to zwykle łuki przypisane pod identyfikatorem obiektów 2.16. Znalezienie ośrodka zajmującego się identyfikatorami obiektów w danym kraju lub rejonie może wymagać pewnego nakładu pracy. Adresy członków narodowych organizacji ISO są dostępne na stronie WWW: http://www.iso.ch/addresse/membodies.html .Podano tam adres pocztowy lub adres poczty elektronicznej. Często zamieszcza się tam także adres serwisu WWW.
- Ośrodek Internet Assigned Numbers Authority (IANA) przypisuje prywatne numery przedsiębiorstw, które są identyfikatorami obiektów, w łuku 1.3.6.1.4.1. Ośrodek IANA przypisał łuki ponad 7500 przedsiębiorstwom. Wniosek można złożyć na stronie http://www.iana.org/cgi-bin/enterprise.pl . Przypisanie numeru w ośrodku IANA zwykle trwa tydzień. Uzyskanie identyfikatora obiektów w ośrodku IANA jest bezpłatne. Ośrodek IANA przypisuje numer (NOWYNUMER), tworząc nowy łuk identyfikatorów obiektów 1.3.6.1.4.1.NOWYNUMER.
- Rząd Federalny Stanów Zjednoczonych obsługuje rejestr CSOR (Computer Security Objects Registry). CSOR jest ośrodkiem nadawania nazw dla łuku 2.16.840.1.101.3 i obecnie rejestruje obiekty dla etykiet ochrony, algorytmów szyfrowania i strategii certyfikatów. Identyfikatory obiektów strategii certyfikatów są zdefiniowane w łuku 2.16.840.1.101.3.2.1. Ośrodek CSOR udostępnia identyfikatory obiektów strategii agencjom rządowym Stanów Zjednoczonych. Więcej informacji na temat ośrodka CSOR można znaleźć w serwisie http://csrc.nist.gov/csor/ .

  Informacje pokrewne

  http://csrc.nist.gov/csor/pkireg.htm

Włączanie obsługi wyszukiwania odwzorowań i korzystania z powiązań strategii dla rejestru docelowego

Obsługa strategii odwzorowań produktu EIM umożliwia korzystanie z powiązań strategii jako środka służącego do utworzenia odwzorowań typu wiele-do-jednego w sytuacjach, w których nie istnieją powiązania między tożsamościami użytkownika a identyfikatorem EIM. Za pomocą powiązania strategii można odwzorować źródłowy zestaw wielu tożsamości użytkownika na pojedynczą tożsamość użytkownika docelowego w określonym rejestrze użytkowników docelowych.

Jednak przed użyciem powiązań strategii należy upewnić się, że w domenie włączone zostało wyszukiwanie odwzorowań za pomocą powiązań strategii. Należy również włączyć jedno lub dwa ustawienia dla każdego rejestru:

- **Włącz wyszukiwania odwzorowań dla rejestru** Opcję tę należy wybrać, aby zapewnić, że rejestr będzie brany pod uwagę w operacjach wyszukiwania odwzorowań EIM, niezależnie od tego, czy zdefiniowano dla niego jakieś powiązania strategii.
- **Użyj powiązań strategii** Opcję tę należy wybrać, aby rejestr mógł być rejestrem docelowym powiązania strategii i aby zapewnić, że będzie brany pod uwagę w operacjach wyszukiwania odwzorowań EIM.

Jeśli dla rejestru nie będzie włączone wyszukiwanie odwzorowań, nie będzie on w ogóle brany pod uwagę w operacjach wyszukiwania odwzorowań EIM. Jeśli nie zostanie określone, ze rejestr używa powiązań strategii, wtedy operacje wyszukiwania odwzorowań EIM będą ignorować wszystkie powiązania strategii dla rejestru, gdy jest on rejestrem docelowym operacji.

Aby włączyć używanie powiązań strategii przez wyszukiwanie odwzorowań dla rejestru docelowego, musisz połączyć się z domeną EIM, w której chcesz pracować, i mieć “Kontrola dostępu EIM” na stronie 39 na jednym z poniższych poziomów:

- Administrator EIM
- Administrator rejestru
- Administrator dla wybranych rejestrów (dla rejestru, który chcesz włączyć)

Aby włączyć ogólną obsługę wyszukiwania odwzorowań i umożliwić używanie powiązań strategii w określonych przypadkach dla rejestru docelowego, wykonaj następujące czynności:

1. Rozwiń gałąź **Sieć > Odwzorowanie EIM > Zarządzanie domenami**.
2. Wybierz domenę EIM, w której chcesz pracować.
   - Jeśli domena EIM, z którą chcesz pracować, nie jest wymieniona w folderze **Zarządzanie domenami**, patrz “Dodanie domeny EIM do folderu Zarządzanie domenami” na stronie 85.
   - Jeśli w tej chwili nie masz połączenia z domeną EIM, w której chcesz pracować, patrz temat Łączenie się z kontrolerem domeny EIM.
3. Wybierz opcję **Rejestry użytkowników**, aby wyświetlić definicje rejestrów dla domeny.

   Uwaga: W przypadku administratora wybranych rejestrów lista zawiera tylko rejestry, do których bezpośrednio określono uprawnienia.
4. Kliknij prawym przyciskiem myszy definicję rejestru, dla której chcesz włączyć obsługę strategii odwzorowań dla powiązań strategii i wybierz opcję **Strategia odwzorowań...**
5. Na stronie **Ogólne** wybierz opcję **Włącz wyszukiwanie odwzorowań dla rejestru**. Wybranie tej opcji powoduje, że rejestr jest brany pod uwagę w operacjach wyszukiwania odwzorowań EIM. Jeśli opcja ta nie będzie wybrana, operacja wyszukiwania nie będzie mogła zwrócić danych dla rejestru, niezależnie od tego, czy rejestr jest rejestrem źródłowym czy docelowym w operacji wyszukiwania.
6. Wybierz opcję **Użyj powiązań strategii**. Wybranie tej opcji powoduje, że operacje wyszukiwania mogą użyć powiązań strategii jako podstawy do zwrócenia danych, jeśli rejestr jest rejestrem docelowym operacji wyszukiwania.
7. Kliknij przycisk **OK**, aby zachować zmiany.

Uwaga: Zanim jakikolwiek rejestr będzie mógł użyć powiązań strategii, należy upewnić się, że włączono powiązania strategii dla domeny.

Pojęcia pokrewne

“Obsługa i włączanie strategii odwzorowań EIM” na stronie 38
Informacje objaśniające sposób włączania i wyłączania powiązań strategii dla domeny.

Usuwanie definicji rejestru

Usuwanie definicji rejestrów z domeny EIM nie wpływa na rejestr użytkowników, którego dotyczy definicja rejestrów, ale rejestr ten nie może dłużej uczestniczyć w domenie EIM. Jednakże przy usuwaniu definicji rejestru należy rozważyć następujące sprawy:

- Podczas usuwania definicji rejestru tracone są wszystkie powiązania dla tego rejestru użytkowników. Jeśli rejestr zostanie ponownie utworzony w domenie, konieczne będzie ponowne utworzenie potrzebnych powiązań.
- Podczas usuwania definicji rejestru X.509 tracone są wszystkie filtry certyfikatów zdefiniowane dla tego rejestru. Jeśli rejestr X.509 zostanie ponownie utworzony w domenie, konieczne będzie ponowne utworzenie potrzebnych filtrów certyfikatów.

- Nie można usunąć definicji rejestru systemu, jeśli są jakieś definicje rejestrów aplikacji, dla których podano ten rejestr jako rejestr nadrzędny.

Aby usunąć definicję rejestru, musisz połączyć się z domeną EIM, w której chcesz pracować, i mieć prawa dostępu administratora EIM.

Aby usunąć definicję rejestru EIM, wykonaj następujące czynności:

1. Rozwiń gałąź **Sieć > Odwzorowanie EIM > Zarządzanie domenami**.
2. Wybierz domenę EIM, w której chcesz pracować.
   - Jeśli domena EIM, z którą chcesz pracować, nie jest wymieniona w folderze **Zarządzanie domenami**, patrz "Dodanie domeny EIM do folderu Zarządzanie domenami" na stronie 85.
   - Jeśli w tej chwili nie masz połączenia z domeną EIM, w której chcesz pracować, patrz temat Łączenie się z kontrolerem domeny EIM.
3. Rozwiń domenę EIM, z którą masz połączenie.
4. Kliknij **Rejestry użytkowników**, aby wyświetlić listę definicji rejestrów dla domeny.

   Uwaga: W przypadku administratora wybranych rejestrów lista zawiera tylko rejestry, do których bezpośrednio określono uprawnienia.
5. Kliknij prawym przyciskiem myszy rejestr użytkowników, który chcesz usunąć, i kliknij **Usuń...**.
6. W oknie dialogowym **Potwierdzenie** kliknij przycisk **Tak**, aby usunąć definicję rejestru.

Usuwanie aliasu z definicji rejestru

Aby usunąć alias z definicji rejestru EIM, należy połączyć się z domeną EIM, w odbywać się będzie praca, i mieć uprawnienie (patrz "Kontrola dostępu EIM" na stronie 39) na jednym z poniższych poziomów:

- Administrator rejestru.
- Administrator dla wybranych rejestrów (dla definicji rejestru, z którą chcesz pracować).
- Administrator EIM.

1. Rozwiń gałąź **Sieć > Odwzorowanie EIM > Zarządzanie domenami**.
2. Wybierz domenę EIM, w której chcesz pracować.
   - Jeśli domena EIM, z którą chcesz pracować, nie jest wymieniona w folderze **Zarządzanie domenami**, patrz "Dodanie domeny EIM do folderu Zarządzanie domenami" na stronie 85.
   - Jeśli w tej chwili nie masz połączenia z domeną EIM, w której chcesz pracować, patrz temat Łączenie się z kontrolerem domeny EIM.
3. Rozwiń domenę EIM, z którą masz połączenie.
4. Kliknij **Rejestry użytkowników**, aby wyświetlić listę definicji rejestrów dla domeny.

   Uwaga: W przypadku administratora wybranych rejestrów lista zawiera tylko rejestry, do których bezpośrednio określono uprawnienia.
5. Kliknij prawym przyciskiem myszy definicję rejestru i wybierz **Właściwości...**.
6. Wybierz stronę **Alias**.
7. Wybierz alias, który chcesz usunąć, i kliknij **Usuń**.
8. Kliknij przycisk **OK**, aby zapisać zmiany.

Dodanie elementu do definicji rejestru grupowego

Aby dodać element do definicji rejestrów, konieczne jest połączenie użytkownika z domeną EIM, w której zamierza on pracować oraz posiadanie przez niego kontroli dostępu EIM na jednym z poniższych poziomów:

- Administrator EIM.
- Administrator rejestru

- Administrator wybranych rejestrów (dla definicji rejestru grupowego, do którego dodawany jest element oraz do tego elementu).

Aby dodać element do definicji rejestru grupowego, należy wykonać poniższe czynności:

1. Rozwiń gałąź **Sieć → Odwzorowanie EIM → Zarządzanie domenami**.
2. Wybierz domenę EIM, w której chcesz pracować.
   a. Jeśli przyszła robocza domena EIM nie jest wymieniona pod hasłem Zarządzanie domenami, patrz temat Dodawanie domeny EIM do Zarządzania domenami.
   b. Jeśli komputer w tej chwili nie jest połączony z domeną EIM, w której będzie pracować, patrz temat Łączenie się z kontrolerem domeny EIM.
3. Rozwiń domenę EIM, z którą masz połączenie.
4. 4. Kliknij opcję **Rejestry użytkowników**, aby wyświetlić listę definicji rejestrów w domenie.
5. 5. Prawym klawiszem myszy kliknij definicję rejestru grupowego, do której chcesz dodać użytkownika i wybierz opcję **Właściwości...**.
6. 6. Wybierz stronę **Elementy** i kliknij polecenie **Dodaj**.
7. 7. Wybierz w oknie dialogowym **Dodaj element rejestru grupowego EIM** jeden lub wiele definicji rejestrów i kliknij przycisk OK. **OK**. Zawartość listy zmienia się w zależności od posiadanych praw dostępu EIM; jest ona ograniczona do definicji rejestrów o tym samym statusie rozpoznawania wielkości znaków, co pozostałe elementy grupy.
8. 8. Kliknij przycisk **OK**, aby wyjść.

Zarządzanie identyfikatorami EIM

Informacje ułatwiające tworzenie i zarządzanie identyfikatorami produktu Enterprise Identity Mapping (EIM) dla domeny.

Utworzenie identyfikatorów EIM reprezentujących użytkowników w sieci i zarządzanie tymi identyfikatorami może być pomocne w wyśledzeniu, kto jest właścicielem danej tożsamości użytkownika. Użytkownicy w przedsiębiorstwie prawie zawsze zmieniają się. Jedni przychodzą, drudzy odchodzą, a jeszcze inni są przenoszeni między działami. Zmiany te stanowią ciągły problem administracyjny związany ze śledzeniem tożsamości i haseł użytkowników w systemach i aplikacjach w sieci. Ponadto zarządzanie hasłami w przedsiębiorstwie zabiera bardzo dużo czasu. Dzięki utworzeniu identyfikatorów EIM i powiązaniu ich z tożsamościami danego użytkownika można prześledzić, kto jest właścicielem danej tożsamości użytkownika. Upraszcza to znacznie zarządzanie hasłami.

Zaimplementowanie środowiska pojedynczego logowania ułatwia również proces zarządzania tożsamościami użytkowników samym użytkownikom, szczególnie jeśli przenoszą się oni do innego wydziału lub oddziału w przedsiębiorstwie. Dzięki obsłudze pojedynczego logowania użytkownicy ci nie muszą pamiętać nowych nazw i haseł w nowych systemach.

Uwaga: Sposób utworzenia identyfikatorów EIM i ich używania zależy od potrzeb danej organizacji. Więcej informacji zawiera temat “Tworzenie planu nazewnictwa identyfikatorów EIM” na stronie 62.

Można zarządzać identyfikatorami EIM dla dowolnej domeny EIM dostępnej w folderze **Zarządzanie domenami**. Do zarządzania identyfikatorami EIM w domenie EIM służą następujące zadania:

Tworzenie identyfikatora EIM

Aby utworzyć identyfikator EIM, musisz połączyć się z domeną EIM, w której chcesz pracować, i mieć uprawnienie (patrz “Kontrola dostępu EIM” na stronie 39) na jednym z poniższych poziomów:

- Administrator identyfikatora.
- Administrator EIM.

Aby utworzyć identyfikator EIM dla wybranej osoby lub jednostki w przedsiębiorstwie, wykonaj następujące czynności:

1. Rozwiń gałąź **Sieć > Odwzorowanie EIM > Zarządzanie domenami**.
2. Wybierz domenę EIM, w której chcesz pracować.
   - Jeśli domena EIM, z którą chcesz pracować, nie jest wymieniona w folderze **Zarządzanie domenami**, patrz “Dodanie domeny EIM do folderu Zarządzanie domenami” na stronie 85.
   - Jeśli w tej chwili nie masz połączenia z domeną EIM, w której chcesz pracować, patrz temat Łączenie się z kontrolerem domeny EIM.
3. Rozwiń domenę EIM, z którą masz połączenie.
4. Kliknij prawym przyciskiem myszy **Identyfikatory** i wybierz **Nowy identyfikator...**
5. W oknie dialogowym **Nowy identyfikator EIM** podaj następujące dane identyfikatora EIM:
   a. Nazwa identyfikatora.
   b. Czy system ma wygenerować unikalną nazwę, jeśli to niezbędne.
   c. Opis identyfikatora.
   d. Jeśli to niezbędne, jeden lub więcej aliasów dla identyfikatora.
6. Kliknij **Pomoc**, jeśli chcesz przeczytać, jakie dane wpisać w każdym polu.
7. Po wprowadzeniu wymaganych danych kliknij **OK**, aby utworzyć identyfikator EIM.

Uwaga: Jeśli utworzono dużo identyfikatorów EIM, rozwinięcie folderu **Identyfikatory** i wyświetlenie listy identyfikatorów może trwać dość długo. Aby poprawić wydajność w takim przypadku, można użyć metody opisanej w sekcji “Dostosowanie widoku identyfikatorów EIM” na stronie 99.

Dodawanie aliasu do identyfikatora EIM

Aby udostępnić dodatkowe informacje wyróżniające, można utworzyć alias wskazujący na “Identyfikator EIM” na stronie 9. Aliasy mogą być pomocne w znalezieniu konkretnego identyfikatora EIM podczas wykonywania operacji wyszukiwania EIM. Mogą one być na przykład pomocne w sytuacji, gdy czyjaś nazwa formalna jest inna niż nazwa, pod jaką dana osoba jest znana.

Nazwy identyfikatorów EIM muszą być unikalne w domenie EIM. Stosowanie aliasów bywa pomocne w sytuacji, gdy używanie unikalnych nazw identyfikatorów może być utrudnione. Na przykład różne osoby w przedsiębiorstwie mogą współużytkować tę samą nazwę, co może być mylące, jeśli jako identyfikatorów EIM używa się nazw własnych. Na przykład, jeśli istnieje dwóch użytkowników o nazwisku Jan P. Kowalski, dla jednego z nich można utworzyć alias Jan Paweł Kowalski, a dla drugiego Jan Piotr Kowalski, co ułatwi odróżnienie tożsamości tych osób. Dodatkowe aliasy mogą zawierać numery pracowników przypisane poszczególnym użytkownikom, numer wydziału, stanowisko lub inny wyróżniający atrybut.

Aby dodać alias do identyfikatora EIM, musisz połączyć się z domeną EIM, w której chcesz pracować, i mieć uprawnienie (patrz “Kontrola dostępu EIM” na stronie 39) na jednym z poniższych poziomów:

- Administrator EIM.
- Administrator identyfikatora.

Aby do identyfikatora EIM dodać alias:

1. Rozwiń gałąź **Sieć > Odwzorowanie EIM > Zarządzanie domenami**.
2. Wybierz domenę EIM, w której chcesz pracować.
   - Jeśli domena EIM, z którą chcesz pracować, nie jest wymieniona w folderze **Zarządzanie domenami**, patrz “Dodanie domeny EIM do folderu Zarządzanie domenami” na stronie 85.
   - Jeśli w tej chwili nie masz połączenia z domeną EIM, w której chcesz pracować, patrz temat Łączenie się z kontrolerem domeny EIM.
3. Rozwiń domenę EIM, z którą masz połączenie.
4. Kliknij opcję **Identyfikatory**, aby w prawym panelu wyświetlić listę identyfikatorów EIM dostępnych w domenie.

Uwaga: Czasem rozwinięcie folderu **Identyfikatory** może trwać dość długo. Aby poprawić wydajność przy dużej liczbie identyfikatorów EIM w domenie, można użyć metody opisanej w sekcji “Dostosowanie widoku identyfikatorów EIM” na stronie 99.

5. Kliknij prawym przyciskiem myszy identyfikator EIM, dla którego chcesz dodać alias, i wybierz opcję **Właściwości**.
6. W polu **Alias** podaj nazwę aliasu, który chcesz dodać do identyfikatora EIM, i kliknij **Dodaj**.
7. Kliknij **OK**, aby zachować zmiany w identyfikatorze EIM.

Usuwanie aliasu z identyfikatora EIM

Aby usunąć alias z identyfikatora EIM, musisz połączyć się z domeną EIM, w której chcesz pracować, i mieć uprawnienie (patrz “Kontrola dostępu EIM” na stronie 39) na jednym z poniższych poziomów:

- Administrator identyfikatorów
- Administrator EIM

Aby usunąć alias z identyfikatora EIM, wykonaj następujące czynności:

1. Rozwiń gałąź **Sieć > Odwzorowanie EIM > Zarządzanie domenami**.
2. Wybierz domenę EIM, w której chcesz pracować.
   - Jeśli domena EIM, z którą chcesz pracować, nie jest wymieniona w folderze **Zarządzanie domenami**, patrz “Dodanie domeny EIM do folderu Zarządzanie domenami” na stronie 85.
   - Jeśli w tej chwili nie masz połączenia z domeną EIM, w której chcesz pracować, patrz temat Łączenie się z kontrolerem domeny EIM.
3. Rozwiń domenę EIM, z którą masz połączenie.
4. Kliknij opcję **Identyfikatory**, aby w prawym panelu wyświetlić listę identyfikatorów EIM dostępnych w domenie.

   Uwaga: Czasem rozwinięcie folderu **Identyfikatory** może trwać dość długo. Aby poprawić wydajność przy dużej liczbie identyfikatorów EIM w domenie, można użyć metody opisanej w sekcji “Dostosowanie widoku identyfikatorów EIM” na stronie 99.
5. Kliknij prawym przyciskiem myszy identyfikator EIM, dla którego chcesz dodać alias, i wybierz opcję **Właściwości**.
6. Wybierz alias, który chcesz usunąć, i kliknij **Usuń**.
7. Kliknij przycisk **OK**, aby zachować zmiany.

Usuwanie identyfikatora EIM

Aby usunąć identyfikator EIM, musisz połączyć się z domeną EIM, w której chcesz pracować, i mieć prawa dostępu administratora EIM.

Aby usunąć identyfikator EIM, wykonaj następujące czynności:

1. Rozwiń gałąź **Sieć > Odwzorowanie EIM > Zarządzanie domenami**.
2. Wybierz domenę EIM, w której chcesz pracować.
   - Jeśli domena EIM, z którą chcesz pracować, nie jest wymieniona w folderze **Zarządzanie domenami**, patrz “Dodanie domeny EIM do folderu Zarządzanie domenami” na stronie 85.
   - Jeśli w tej chwili nie masz połączenia z domeną EIM, w której chcesz pracować, patrz temat Łączenie się z kontrolerem domeny EIM.
3. Rozwiń domenę EIM, z którą masz połączenie.
4. Kliknij **Identyfikatory**.

   Uwaga: Czasem rozwinięcie folderu **Identyfikatory** może trwać dość długo. Aby poprawić wydajność przy dużej liczbie identyfikatorów EIM w domenie, można użyć metody opisanej w sekcji “Dostosowanie widoku identyfikatorów EIM” na stronie 99.

5. Wybierz identyfikator EIM, który chcesz usunąć. Aby usunąć wiele identyfikatorów, podczas ich wybierania trzymaj naciśnięty klawisz **Ctrl**.
6. Kliknij prawym przyciskiem myszy wybrane identyfikatory EIM i wybierz **Usuń**.
7. W oknie dialogowym **Potwierdzenie usunięcia** kliknij **Tak**, aby usunąć wybrane identyfikatory EIM.

Dostosowanie widoku identyfikatorów EIM

Czasem rozwinięcie folderu **Identyfikatory** może trwać dość długo. Aby poprawić wydajność przy dużej liczbie identyfikatorów EIM w domenie, można dostosować widok dla folderu **Identyfikatory**.

Aby dostosować widok folderu **Identyfikatory**, wykonaj następujące czynności:

1. Rozwiń gałąź **Sieć —> Odwzorowanie EIM —> Zarządzanie domenami**.
2. Wybierz domenę EIM, w której chcesz pracować.
   - Jeśli domena EIM, z którą chcesz pracować, nie jest wymieniona w folderze **Zarządzanie domenami**, patrz "Dodanie domeny EIM do folderu Zarządzanie domenami" na stronie 85.
   - Jeśli w tej chwili nie masz połączenia z domeną EIM, w której chcesz pracować, patrz temat Łączenie się z kontrolerem domeny EIM.
3. Kliknij prawym przyciskiem myszy folder **Identyfikatory**, a następnie wybierz opcję **Dostosuj ten widok**.
4. Określ kryterium, według którego chcesz wyświetlać identyfikatory EIM w domenie. Aby ograniczyć liczbę wyświetlanych identyfikatorów EIM, podaj znaki, które mają być używane do stortowania identyfikatorów. W nazwie identyfikatora można podać jeden lub więcej znaków zastępczych (*). Jako kryterium sortowania w polu **Identyfikatory** można na przykład wprowadzić *KOWAL*. W wyniku tego zostaną zwrócone wszystkie identyfikatory EIM, w których częścią nazwy identyfikatora EIM lub aliasu dla identyfikatora EIM jest łańcuch znaków KOWAL.
5. Kliknij przycisk **OK**, aby zachować zmiany.

Zarządzanie powiązaniami

Poniższe informacje opisują typy komponentów, którymi można zarządzać za pomocą produktu Enterprise Identity Mapping (EIM).

EIM umożliwia tworzenie dwóch rodzajów powiązań i zarządzanie nimi, definiują one bezpośrednie lub pośrednie relacje między tożsamościami użytkowników: powiązania identyfikatorów i powiązania strategii. EIM pozwala na tworzenie powiązań identyfikatorów między identyfikatorami EIM i ich tożsamościami użytkowników oraz na zarządzanie nimi, co umożliwia definiowanie pośrednich, ale określonych, pojedynczych relacji między tożsamościami użytkowników. Ponadto EIM umożliwia tworzenie powiązań strategii do opisania relacji między wieloma tożsamościami użytkownika w jednym lub większej liczbie rejestrów a pojedynczą tożsamością użytkownika docelowego w innym rejestrze. Powiązania strategii korzystają z obsługi strategii odwzorowania EIM do utworzenia odwzorowań wielu tożsamości użytkownika do jednej bez wymagania identyfikatora EIM. Ponieważ oba rodzaje powiązań definiują relacje między tożsamościami użytkowników w przedsiębiorstwie, zarządzanie powiązaniami jest ważnym elementem zarządzania EIM.

Obsługa powiązań w domenie umożliwia uproszczenie zadań administracyjnych wymaganych do śledzenia, którzy użytkownicy mają konta w różnych systemach w danej sieci. Implementując chronioną sieć z pojedynczym logowaniem należy regularnie aktualizować powiązania identyfikatorów i strategii.

Dla powiązań można wykonywać następujące zadania zarządzania:

Tworzenie powiązań

Powiązania można utworzyć na jeden z dwóch sposobów:

- Można utworzyć powiązanie identyfikatora, aby pośrednio zdefiniować relację między dwiema tożsamościami użytkownika używanymi przez jedną osobę. Powiązanie identyfikatora opisuje relację między identyfikatorem EIM

a tożsamością użytkownika w rejestrze użytkowników. Dzięki powiązaniom identyfikatorów można utworzyć odwzorowania typu jeden-do-jednego między identyfikatorem EIM i każdą z tożsamości użytkownika reprezentowanego przez ten identyfikator.

- Można utworzyć powiązanie strategii bezpośrednio definiując relację między wieloma tożsamościami użytkownika w jednym lub większej liczbie rejestrów a pojedynczą tożsamością użytkownika docelowego w innym rejestrze. Powiązania strategii korzystają z obsługi strategii odwzorowania EIM do utworzenia odwzorowań wielu tożsamości użytkownika do jednej bez wymagania identyfikatora EIM. Powiązania strategii umożliwiają szybkie tworzenie wielu odwzorowań między pokrewnymi tożsamościami użytkownika w różnych rejestrach użytkowników.

Wybór konkretnego powiązania lub połączenia obu metod zależy od danych wymagań implementacji EIM.

Pojęcia pokrewne

"Tworzenie planu odwzorowywania tożsamości" na stronie 60

Tworzenie powiązania identyfikatora:

Powiązanie identyfikatora definiuje relację między identyfikatorem produktu EIM a tożsamością użytkownika w przedsiębiorstwie dla osoby lub jednostki, do której odnosi się identyfikator EIM. Można utworzyć trzy rodzaje powiązań identyfikatora: docelowe, źródłowe i administracyjne. Aby zapobiegać potencjalnym problemom z powiązaniami i ich odwzorowaniem tożsamości, należy utworzyć ogólny plan odwzorowywania tożsamości dla przedsiębiorstwa przed rozpoczęciem definiowania powiązań.

Aby utworzyć powiązanie identyfikatora, musisz połączyć się z domeną EIM, w której chcesz pracować, i mieć uprawnienie (patrz "Kontrola dostępu EIM" na stronie 39) wymagane przez rodzaj powiązania, które chcesz utworzyć.

Aby utworzyć powiązanie źródłowe lub administracyjne, musisz mieć prawa dostępu EIM na jednym z następujących poziomów:

- Administrator identyfikatora.
- Administrator EIM.

Aby utworzyć powiązanie docelowe, musisz mieć prawa dostępu EIM na jednym z następujących poziomów:

- Administrator rejestru.
- Administrator dla wybranych rejestrów (dla definicji rejestru odnoszącej się do rejestru użytkowników, który zawiera tożsamość użytkownika docelowego).
- Administrator EIM.

Aby utworzyć powiązanie identyfikatora, wykonaj następujące czynności:

1. Rozwiń gałąź **Sieć > Odwzorowanie EIM > Zarządzanie domenami**.
2. Wybierz domenę EIM, w której chcesz pracować.
   - Jeśli domena EIM, z którą chcesz pracować, nie jest wymieniona w folderze **Zarządzanie domenami**, patrz "Dodanie domeny EIM do folderu Zarządzanie domenami" na stronie 85.
   - Jeśli w tej chwili nie masz połączenia z domeną EIM, w której chcesz pracować, patrz temat Łączenie się z kontrolerem domeny EIM.
3. Rozwiń domenę EIM, z którą masz połączenie.
4. Kliknij **Identyfikatory**, aby wyświetlić listę identyfikatorów EIM dla domeny.

   Uwaga: Czasem rozwinięcie folderu **Identyfikatory** może trwać dość długo. Aby poprawić wydajność przy dużej liczbie identyfikatorów EIM w domenie, można użyć metody opisanej w sekcji "Dostosowanie widoku identyfikatorów EIM" na stronie 99.
5. Kliknij prawym przyciskiem myszy identyfikator EIM, dla którego chcesz utworzyć powiązanie, i wybierz opcję **Właściwości...**.
6. Wybierz stronę **Powiązania** i kliknij **Dodaj...**.
7. W oknie dialogowym **Dodanie powiązania** wpisz następujące dane definiujące powiązanie:

- Nazwa rejestru zawierającego tożsamość użytkownika, który ma być powiązany z identyfikatorem EIM. Podaj dokładną nazwę istniejącej definicji rejestru lub przeglądaj, aby jakąś wybrać.
- Nazwa tożsamości użytkownika, którą chcesz powiązać z identyfikatorem EIM.
- Rodzaj powiązania. Możesz utworzyć jeden z trzech różnych typów powiązań:
  - Administracyjne
  - Źródłowe
  - Docelowe

8. Kliknij **Pomoc**, jeśli chcesz przeczytać, jakie dane wpisać w każdym polu.
9. Opcjonalne. Dla powiązania docelowego kliknij **Zaawansowane...**, aby wyświetlić okno dialogowe **Dodaj powiązanie - Zaawansowane**. Podaj dane wyszukiwania dla tożsamości użytkownika docelowego i kliknij **OK**, aby wrócić do okna dialogowego **Dodanie powiązania**.
10. Po wprowadzeniu wymaganych danych kliknij **OK**, aby utworzyć powiązanie.

Tworzenie powiązania strategii: Powiązanie strategii umożliwia zdefiniowanie relacji między wieloma tożsamościami użytkownika w jednym lub większej liczbie rejestrów a pojedynczą tożsamością użytkownika docelowego w innym rejestrze. Powiązania strategii korzystają z obsługi strategii odwzorowania EIM do utworzenia odwzorowań wielu tożsamości użytkownika do jednej bez wymagania identyfikatora EIM. Ponieważ powiązań strategii można używać na wiele sposobów, często łącząc je ze sobą, przed ich utworzeniem i korzystaniem z nich należy gruntownie zapoznać się z obsługą strategii odwzorowań. Ponadto, aby zapobiegać potencjalnym problemom z powiązaniami i ich odwzorowaniem tożsamości, należy utworzyć ogólny plan odwzorowywania tożsamości dla przedsiębiorstwa przed rozpoczęciem definiowania powiązań.

Wybór konkretnego powiązania lub połączenia obu metod zależy od danych wymagań implementacji EIM.

Sposób tworzenia powiązania strategii zależy od rodzaju powiązania. Więcej informacji na temat tworzenia powiązania strategii zawierają sekcje:

Pojęcia pokrewne

“Zarządzanie definicjami rejestrów EIM” na stronie 90
Informacje dotyczące tworzenia definicji rejestrów EIM i zarządzania nimi dla tych rejestrów użytkowników w przedsiębiorstwie, które są uwzględniane w odwzorowaniach EIM.

Tworzenie domyślnego powiązania strategii domeny:

Aby utworzyć domyślne powiązanie strategii domeny, musisz połączyć się z domeną EIM, w której chcesz pracować, i mieć uprawnienie (patrz “Kontrola dostępu EIM” na stronie 39) na jednym z poniższych poziomów:

- Administrator EIM
- Administrator rejestru

Uwaga: Powiązanie strategii opisuje relację między wieloma tożsamościami użytkownika a pojedynczą tożsamością użytkownika w rejestrze użytkowników docelowych. Powiązania strategii można użyć do opisania relacji między źródłowym zestawem wielu tożsamości użytkownika a pojedynczą tożsamością użytkownika docelowego w określonym rejestrze użytkowników docelowych. Powiązania strategii korzystają z obsługi strategii odwzorowania EIM do utworzenia odwzorowań wielu tożsamości użytkownika do jednej bez wymagania identyfikatora EIM.

Ponieważ powiązań strategii można używać na wiele sposobów, często łącząc je ze sobą, przed ich utworzeniem i korzystaniem z nich należy gruntownie zapoznać się z obsługą strategii odwzorowań. Ponadto, aby zapobiegać potencjalnym problemom z powiązaniami i ich odwzorowaniem tożsamości, należy utworzyć ogólny plan odwzorowywania tożsamości dla przedsiębiorstwa przed rozpoczęciem definiowania powiązań.

W domyślnym powiązaniu strategii domeny wszyscy użytkownicy w jednej domenie są źródłem powiązania strategii i są odwzorowani na jeden rejestr docelowy i użytkownika docelowego. Można zdefiniować domyślne powiązanie strategii domeny dla każdego rejestru w domenie. Jeśli dwa lub więcej powiązań strategii domeny odnosi się do tego

samego rejestru docelowego, można zdefiniować unikalne dane wyszukiwania dla każdego z tych powiązań strategii, aby zapewnić ich rozróżnianie przez operacje wyszukiwania odwzorowań. W przeciwnym przypadku operacje wyszukiwania odwzorowań mogą zwrócić wiele tożsamości użytkowników docelowych. W wyniku tego aplikacje bazujące na odwzorowaniach EIM mogą nie być w stanie określić, której tożsamości docelowej użyć.

Aby utworzyć domyślne powiązanie strategii domeny, wykonaj następujące czynności:

1. Rozwiń gałąź **Sieć > Odwzorowanie EIM > Zarządzanie domenami**.
2. Kliknij prawym przyciskiem myszy domenę EIM, w której chcesz pracować, i wybierz **Strategia odwzorowania...**
   - Jeśli domena EIM, z którą chcesz pracować, nie jest wymieniona w folderze **Zarządzanie domenami**, patrz “Dodanie domeny EIM do folderu Zarządzanie domenami” na stronie 85.
   - Jeśli w tej chwili nie masz połączenia z domeną EIM, w której chcesz pracować, patrz temat Łączenie się z kontrolerem domeny EIM.
3. Na stronie Ogólne wybierz opcję **Włącz wyszukiwanie odwzorowania przy użyciu powiązań strategii dla domeny**.
4. Wybierz stronę **Domena** i kliknij **Dodaj...**.
5. W oknie dialogowym **Dodanie domyślnego powiązania strategii domeny** podaj następujące wymagane dane:
   - Nazwa definicji rejestru, **Rejestr docelowy** dla powiązania strategii.
   - Nazwa tożsamości użytkownika, **Użytkownik docelowy** dla powiązania strategii.
6. Kliknij **Pomoc**, jeśli chcesz poznać bardziej szczegółowe informacje o tym, jak wypełnić to i następne okna dialogowe.
7. Opcjonalne. Kliknij **Zaawansowane...**, aby wyświetlić okno dialogowe **Dodaj powiązanie - Zaawansowane**. Podaj **Dane wyszukiwania** dla powiązania strategii i kliknij **OK**, aby wrócić do okna dialogowego **Dodaj domyślne powiązanie strategii domeny**.

   Uwaga: Jeśli dwa lub więcej domyślnych powiązań strategii domeny odnosi się do tego samego rejestru docelowego, należy zdefiniować unikalne dane wyszukiwania dla każdej tożsamości użytkownika docelowego w tych powiązaniach strategii. Definiując dane wyszukiwania dla każdej tożsamości użytkownika docelowego w takiej sytuacji zapewnia się, że operacje wyszukiwania odwzorowań będą mogły rozróżnić te tożsamości. W przeciwnym przypadku operacje wyszukiwania odwzorowań mogą zwrócić wiele tożsamości użytkowników docelowych. W wyniku tego aplikacje bazujące na odwzorowaniach EIM mogą nie być w stanie określić, której tożsamości docelowej użyć.
8. Kliknij **OK**, aby utworzyć nowe powiązanie strategii i wrócić do strony **Domena**. Nowe powiązanie strategii zostanie wyświetlone w tabeli **Domyślne powiązania strategii**.
9. Sprawdź, czy nowe powiązanie strategii jest włączone dla rejestru docelowego.
10. Kliknij **OK**, aby zachować zmiany i wyjść z okna dialogowego **Strategia odwzorowań**.

Uwaga: Sprawdź, czy obsługa strategii odwzorowań i użycie powiązań strategii dla rejestru użytkowników docelowych zostały poprawnie włączone. Jeśli nie, powiązanie strategii może nie działać.

Tworzenie domyślnego powiązania strategii rejestru:

Aby utworzyć domyślne powiązanie strategii rejestru, musisz połączyć się z domeną EIM, w której chcesz pracować, i mieć uprawnienie (patrz “Kontrola dostępu EIM” na stronie 39) na jednym z poniższych poziomów:

- Administrator EIM
- Administrator rejestru

Uwaga: Powiązanie strategii opisuje relację między wieloma tożsamościami użytkownika a pojedynczą tożsamością użytkownika w rejestrze użytkowników docelowych. Powiązania strategii można użyć do opisania relacji między źródłowym zestawem wielu tożsamości użytkownika a pojedynczą tożsamością użytkownika

docelowego w określonym rejestrze użytkowników docelowych. Powiązania strategii korzystają z obsługi strategii odwzorowania EIM do utworzenia odwzorowań wielu tożsamości użytkownika do jednej bez wymagania identyfikatora EIM.

Ponieważ powiązań strategii można używać na wiele sposobów, często łącząc je ze sobą, przed ich utworzeniem i korzystaniem z nich należy gruntownie zapoznać się z obsługą strategii odwzorowań. Ponadto, aby zapobiegać potencjalnym problemom z powiązaniami i ich odwzorowaniem tożsamości, należy utworzyć ogólny plan odwzorowywania tożsamości dla przedsiębiorstwa przed rozpoczęciem definiowania powiązań.

W domyślnym powiązaniu strategii rejestru wszyscy użytkownicy w jednym rejestrze są źródłem powiązania strategii i są odwzorowani na jeden rejestr docelowy i użytkownika docelowego. Jeśli dla rejestru docelowego włączone jest domyślne powiązanie strategii rejestru, powiązanie strategii gwarantuje, że wszystkie źródłowe tożsamości użytkowników będą mogły być odwzorowane na pojedynczy określony rejestr docelowy i użytkownika docelowego.

Aby utworzyć domyślne powiązanie strategii rejestru, wykonaj następujące czynności:

1. Rozwiń gałąź **Sieć > Odwzorowanie EIM > Zarządzanie domenami**.
2. Wybierz domenę EIM, w której chcesz pracować.
   - Jeśli domena EIM, z którą chcesz pracować, nie jest wymieniona w folderze **Zarządzanie domenami**, patrz “Dodanie domeny EIM do folderu Zarządzanie domenami” na stronie 85.
   - Jeśli w tej chwili nie masz połączenia z domeną EIM, w której chcesz pracować, patrz temat Łączenie się z kontrolerem domeny EIM.
3. Na stronie Ogólne wybierz opcję **Włącz wyszukiwanie odwzorowania przy użyciu powiązań strategii dla domeny**.
4. Na stronie Ogólne wybierz opcję **Włącz wyszukiwanie odwzorowania przy użyciu powiązań strategii dla domeny**.
5. W oknie dialogowym **Dodanie domyślnego powiązania strategii rejestru** podaj następujące wymagane dane:
   - Nazwa definicji rejestru, **Rejestr źródłowy** dla powiązania strategii.
   - Nazwa definicji rejestru, **Rejestr docelowy** dla powiązania strategii.
   - Nazwa tożsamości użytkownika, **Użytkownik docelowy** dla powiązania strategii.
6. Kliknij **Pomoc**, jeśli chcesz poznać bardziej szczegółowe informacje o tym, jak wypełnić to i następne okna dialogowe.
7. Opcjonalne. Kliknij **Zaawansowane...**, aby wyświetlić okno dialogowe **Dodaj powiązanie - Zaawansowane**. Podaj **dane wyszukiwania** dla powiązania strategii i kliknij **OK**, aby wrócić do okna dialogowego **Dodaj domyślne powiązanie strategii rejestru**. Jeśli dwa lub więcej powiązań strategii z tym samym rejestrem źródłowym odnosi się do tego samego rejestru docelowego, należy zdefiniować unikalne dane wyszukiwania dla każdej tożsamości użytkownika docelowego w tych powiązaniach strategii. Definiując dane wyszukiwania dla każdej tożsamości użytkownika docelowego w takiej sytuacji zapewnia się, że operacje wyszukiwania odwzorowań będą mogły rozróżnić te tożsamości. W przeciwnym przypadku operacje wyszukiwania odwzorowań mogą zwrócić wiele tożsamości użytkowników docelowych. W wyniku tego aplikacje bazujące na odwzorowaniach EIM mogą nie być w stanie określić, której tożsamości docelowej użyć.
8. Kliknij **OK**, aby utworzyć nowe powiązanie strategii i wrócić do strony **Rejestr**. Nowe domyślne powiązanie strategii rejestru zostanie wyświetlone na liście **Domyślne powiązania strategii**.
9. Sprawdź, czy nowe powiązanie strategii jest włączone dla rejestru docelowego.
10. Kliknij **OK**, aby zachować zmiany i wyjść z okna dialogowego **Strategia odwzorowań**.

Uwaga: Sprawdź, czy obsługa strategii odwzorowań i użycie powiązań strategii dla rejestru użytkowników docelowych zostały poprawnie włączone. Jeśli nie, powiązanie strategii może nie działać.

Tworzenie powiązania strategii filtrów certyfikatów:

Aby utworzyć powiązanie strategii filtrów certyfikatów, musisz połączyć się z domeną EIM, w której chcesz pracować, i mieć uprawnienie (patrz “Kontrola dostępu EIM” na stronie 39) na jednym z poniższych poziomów:

- Administrator EIM
- Administrator rejestru

Uwaga: Powiązanie strategii opisuje relację między źródłowym zestawem wielu tożsamości użytkownika i pojedynczą tożsamością użytkownika docelowego w określonym rejestrze użytkowników docelowych. Powiązania strategii korzystają z obsługi strategii odwzorowania EIM do utworzenia odwzorowań wielu tożsamości użytkownika do jednej bez wymagania identyfikatora EIM.

Ponieważ powiązań strategii można używać na wiele sposobów, często łącząc je ze sobą, przed ich utworzeniem i korzystaniem z nich należy gruntownie zapoznać się z obsługą strategii odwzorowań. Ponadto, aby zapobiegać potencjalnym problemom z powiązaniami i ich odwzorowaniem tożsamości, należy utworzyć ogólny plan odwzorowywania tożsamości dla przedsiębiorstwa przed rozpoczęciem definiowania powiązań.

W powiązaniu strategii filtrów certyfikatów jako źródło powiązania strategii podawany jest zestaw certyfikatów w pojedynczym rejestrze X.509. Certyfikaty te są odwzorowywane na określony pojedynczy rejestr docelowy i docelowego użytkownika. W przeciwieństwie do domyślnego powiązania strategii rejestru, w którym wszyscy użytkownicy w pojedynczym rejestrze są źródłem powiązania strategii, zasięg powiązania strategii filtrów certyfikatów jest bardziej elastyczny. Jako źródło można podać podzbiór certyfikatów w rejestrze. Podany dla powiązania strategii filtr certyfikatu określa jego zasięg.

Uwaga: Domyślne powiązanie strategii rejestru należy utworzyć i użyć go do odwzorowania wszystkich certyfikatów w rejestrze użytkowników X.509 na pojedynczą tożsamość użytkownika docelowego.

Filtr certyfikatu steruje odwzorowaniem przez powiązanie strategii filtrów certyfikatów jednego źródłowego zestawu tożsamości użytkownika, w danym przypadku certyfikatów cyfrowych, na określoną tożsamość użytkownika docelowego. Dlatego zanim będzie można utworzyć powiązanie strategii filtrów certyfikatów, musi istnieć filtr certyfikatu, który będzie w tym celu użyty.

Przed utworzeniem powiązania strategii filtrów certyfikatów trzeba wpierw utworzyć filtry certyfikatów, które będą użyte jako podstawa powiązania strategii.

Aby utworzyć powiązanie strategii filtrów certyfikatów, wykonaj następujące czynności:

1. Rozwiń gałąź **Sieć > Odwzorowanie EIM > Zarządzanie domenami**.
2. Kliknij prawym przyciskiem myszy domenę EIM, w której chcesz pracować, i wybierz **Strategia odwzorowania...**
   - Jeśli domena EIM, z którą chcesz pracować, nie jest wymieniona w folderze **Zarządzanie domenami**, patrz “Dodanie domeny EIM do folderu Zarządzanie domenami” na stronie 85.
   - Jeśli w tej chwili nie masz połączenia z domeną EIM, w której chcesz pracować, patrz temat Łączenie się z kontrolerem domeny EIM.
3. Na stronie Ogólne wybierz opcję **Włącz wyszukiwanie odwzorowania przy użyciu powiązań strategii dla domeny**.
4. Wybierz stronę **Filtr certyfikatu** i kliknij **Dodaj...**, aby wyświetlone zostało okno dialogowe **Dodanie powiązania strategii filtrów certyfikatów**.
5. Kliknij **Pomoc**, jeśli chcesz poznać bardziej szczegółowe informacje o tym, jak wypełnić to i następne okna dialogowe.
6. Aby zdefiniować powiązanie strategii, podaj następujące wymagane dane:
   a. Wpisz nazwę definicji rejestru dla rejestru użytkowników X.509, który będzie używany jako **Rejestr źródłowy X.509** dla powiązania strategii. Można także nacisnąć przycisk **Przeglądaj...**, aby wybrać jedną definicję z listy definicji rejestru dla domeny.
   b. Kliknij **Wybierz**, aby wyświetlone zostało okno dialogowe **Wybór filtru certyfikatu**, a następnie wybierz istniejący filtr certyfikatu, który będzie użyty jako podstawa dla nowego powiązania strategii filtrów certyfikatów.

Uwaga: **Koniecznie** trzeba użyć istniejącego filtru certyfikatu. Jeśli na liście nie ma filtru certyfikatu, którego chcesz użyć, kliknij **Dodaj...**, aby utworzyć nowy filtr certyfikatu.

c. Podaj nazwę definicji rejestru jako **Rejestr docelowy** lub kliknij **Przeglądaj...**, aby wybrać rejestr z listy istniejących definicji rejestrów dla domeny.

d. Podaj nazwę użytkownika jako **Użytkownik docelowy**, do której będą odwzorowane wszystkie certyfikaty z rejestru **Rejestr źródłowy X.509** zgodne z filtrem certyfikatów. Możesz również kliknąć **Przeglądaj...**, aby wybrać jednego z listy użytkowników znanych w domenie.

e. Opcjonalne. Kliknij **Zaawansowane...**, aby wyświetlić okno dialogowe **Dodaj powiązanie - Zaawansowane**. Podaj **Dane wyszukiwania** dla tożsamości użytkownika docelowego i kliknij **OK**, aby wrócić do okna dialogowego **Dodanie powiązania strategii filtrów certyfikatów**.

Uwaga: Jeśli dwa lub więcej powiązań strategii z takim samym rejestrem źródłowym X.509 i kryterium filtru certyfikatów odnosi się do tego samego rejestru docelowego, konieczne jest zdefiniowanie unikalnych danych wyszukiwania dla tożsamości użytkowników docelowych w każdym z tych powiązań strategii. Definiując dane wyszukiwania dla każdej tożsamości użytkownika docelowego w takiej sytuacji zapewnia się, że operacje wyszukiwania odwzorowań będą mogły rozróżnić te tożsamości. W przeciwnym przypadku operacje wyszukiwania odwzorowań mogą zwrócić wiele tożsamości użytkowników docelowych. W wyniku tego aplikacje bazujące na odwzorowaniach EIM mogą nie być w stanie określić, której tożsamości docelowej użyć.

7. Kliknij **OK**, aby utworzyć nowe powiązanie strategii filtrów certyfikatów i wrócić do strony **Filtr certyfikatu**. Nowe powiązanie strategii zostanie wyświetlone na liście.
8. Sprawdź, czy nowe powiązanie strategii jest włączone dla rejestru docelowego.
9. Kliknij **OK**, aby zachować zmiany i wyjść z okna dialogowego **Strategia odwzorowań**.

Uwaga: Sprawdź, czy obsługa strategii odwzorowań i użycie powiązań strategii dla rejestru użytkowników docelowych zostały poprawnie włączone. Jeśli nie, powiązanie strategii może nie działać.

Tworzenie filtru certyfikatu:

Filtr certyfikatu określa zestaw podobnych atrybutów nazwy wyróżniającej certyfikatu dla grupy certyfikatów użytkowników w źródłowym rejestrze użytkowników X.509. Filtru certyfikatów można użyć jako bazy powiązania strategii filtrów certyfikatów. Filtr certyfikatu w powiązaniu strategii określa, które certyfikaty w określonym rejestrze źródłowym X.509 odwzorować na określonego użytkownika docelowego. Certyfikaty, które mają informacje SDN i IDN spełniające kryterium filtru są odwzorowywane na określonego użytkownika docelowego podczas operacji wyszukiwania odwzorowań produktu EIM.

Aby utworzyć filtr certyfikatu, musisz połączyć się z domeną EIM, w której chcesz pracować, i mieć uprawanienie (patrz “Kontrola dostępu EIM” na stronie 39) na jednym z poniższych poziomów:

- Administrator EIM
- Administrator rejestru
- Administrator dla wybranych rejestrów (dla definicji rejestru odnoszącej się do rejestru użytkowników X.509, dla którego chcesz utworzyć filtr certyfikatu)

Filtr certyfikatu jest tworzony na podstawie określonych informacji nazwy wyróżniającej certyfikatu cyfrowego. Określone informacje nazwy wyróżniającej to może być na przykład nazwa wyróżniająca podmiotu, wskazująca właściciela certyfikatu, lub nazwa wyróżniająca wystawcy, wskazująca wystawcę certyfikatu. Dla filtru certyfikatu można podać informacje dotyczące pełnej lub częściowej nazwy wyróżniającej.

Jeśli dodajesz filtr certyfikatów do powiązania strategii filtrów certyfikatów, to określa on, które certyfikaty w rejestrze X.509 są odwzorowane na tożsamość użytkownika docelowego określoną przez powiązanie strategii. Jeśli w operacji wyszukiwania odwzorowania EIM źródłową tożsamością użytkownika jest certyfikat cyfrowy (po utworzeniu nazwy tożsamości użytkownika funkcją API EIM eimFormatUserIdentity()) i istnieje powiązanie strategii filtrów certyfikatów, odwzorowania EIM porównują informacje nazwy wyróżniającej w certyfikacie z informacjami pełnej lub

częściowej nazwy wyróżniającej podanymi w filtrze. Jeśli informacje nazwy wyróżniającej w certyfikacie spełniają kryterium filtru, odwzorowanie EIM zwróci tożsamość użytkownika docelowego określoną przez powiązanie strategii filtrów certyfikatów.

Podczas tworzenia filtru certyfikatu są trzy metody podania wymaganej nazwy wyróżniającej:

- Można wprowadzić pełną lub częściową nazwę wyróżniającą określonego certyfikatu jako **Nazwa wyróżniająca podmiotu**, **Nazwa wyróżniająca wystawcy** lub w obu miejscach.
- Informacje z danego certyfikatu można skopiować do schowka i użyć do generowania listy kandydatów filtrów certyfikatów na podstawie informacji nazwy wyróżniającej w certyfikacie. Można następnie wybrać, którą nazwę wyróżniającą użyć dla filtru certyfikatów.

  Uwaga: Jeśli chcesz wygenerować wymagane informacje nazwy wyróżniającej, aby utworzyć filtr certyfikatów, musisz skopiować informacje certyfikatu do schowka przed wykonaniem tego zadania. Ponadto certyfikat musi być w formacie zakodowanym base64. Więcej szczegółowych informacji dotyczących metod uzyskiwania certyfikatów we właściwym formacie zawiera temat Filtr certyfikatu.
- Można wygenerować listę kandydatów filtrów certyfikatów na podstawie informacji nazwy wyróżniającej z certyfikatu cyfrowego, dla którego istnieje powiązanie źródłowe z identyfikatorem EIM. Można następnie wybrać, którą nazwę wyróżniającą użyć dla filtru certyfikatów.

Aby utworzyć filtr certyfikatów, który będzie używany jako podstawa dla powiązania strategii filtrów certyfikatów, wykonaj następujące czynności:

1. Rozwiń gałąź **Sieć > Odwzorowanie EIM > Zarządzanie domenami**.
2. Kliknij prawym przyciskiem myszy domenę EIM, w której chcesz pracować, i wybierz **Strategia odwzorowania...**
   - Jeśli domena EIM, z którą chcesz pracować, nie jest wymieniona w folderze **Zarządzanie domenami**, patrz “Dodanie domeny EIM do folderu Zarządzanie domenami” na stronie 85.
   - Jeśli w tej chwili nie masz połączenia z domeną EIM, w której chcesz pracować, patrz temat Łączenie się z kontrolerem domeny EIM.
3. Wybierz stronę **Filtr certyfikatu** i kliknij **Filtry certyfikatów...**, aby wyświetlone zostało okno dialogowe **Filtry certyfikatów**.

   Uwaga: Jeśli klikniesz **Filtry certyfikatów...** bez wybrania powiązania strategii, to zostanie wyświetlone okno dialogowe **Przeglądaj rejestry EIM**. W oknie tym można wybrać rejestr X.509 z listy definicji rejestrów X.509 w domenie, dla której chcesz przeglądać filtry certyfikatów. Zawartość listy zależy od posiadanego rodzaju kontroli dostępu EIM.
4. Kliknij **Dodaj...**, aby wyświetlone zostało okno dialogowe **Dodanie filtru certyfikatu**.
5. W oknie dialogowym **Dodanie filtru certyfikatu** należy wybrać, czy dodać pojedynczy filtr certyfikatu czy wygenerować filtr certyfikatu na podstawie określonego certyfikatu cyfrowego. Kliknij **Pomoc**, jeśli chcesz poznać bardziej szczegółowe informacje o tym, jak wypełnić to i następne okna dialogowe.
   a. Jeśli wybierzesz **Dodanie pojedynczego filtru certyfikatu**, możesz podać informacje pełnej lub częściowej **nazwy wyróżniającej podmiotu**, informacje pełnej lub częściowej **nazwy wyróżniającej wystawcy** lub obie te informacje. Kliknij **OK**, aby utworzyć filtr certyfikatu i wrócić do okna dialogowego **Filtry certyfikatów**. Filtr zostanie wyświetlony na liście.
   b. Jeśli wybierzesz **Generowanie filtru certyfikatu z certyfikatu cyfrowego**, kliknij **OK**, aby wyświetlić okno dialogowe **Generowanie filtrów certyfikatów**.
      1) Wklej w polu **Informacje certyfikatu** zakodowaną w base64 wersję informacji certyfikatu skopiowaną wcześniej do schowka.
      2) Kliknij **OK**, aby wygenerować potencjalne filtry certyfikatów na podstawie **nazwy wyróżniającej podmiotu** i **nazwy wyróżniającej wystawcy** certyfikatu.
      3) W oknie dialogowym **Przeglądanie filtrów certyfikatów** co najmniej jeden z filtrów certyfikatów. Kliknij **OK**, aby wrócić do okna dialogowego **Wybór filtrów certyfikatów**, w którym wyświetlone są wybrane filtry certyfikatów.

c. Po wybraniu opcji **Generuj filtr certyfikatów z powiązania źródłowego dla użytkownika X.509** naciśnij przycisk **OK** w celu wyświetlenia okna dialogowego **Generuj filtry certyfikatów**. W oknie tym wyświetlona jest lista tożsamości użytkowników X.509 mających powiązanie źródłowe z identyfikatorem EIM w domenie.
   1) Wybierz tożsamość użytkownika X.509, którego certyfikatu cyfrowego chcesz użyć do wygenerowania jednego lub więcej kandydatów filtrów certyfikatów, i kliknij **OK**.
   2) Kliknij **OK**, aby wygenerować potencjalne filtry certyfikatów na podstawie **nazwy wyróżniającej podmiotu** i **nazwy wyróżniającej wystawcy** certyfikatu.
   3) W oknie dialogowym **Przeglądanie filtrów certyfikatów** wybierz jeden lub więcej potencjalnych filtrów certyfikatów. Kliknij **OK**, aby wrócić do okna dialogowego **Wybór filtrów certyfikatów**, w którym wyświetlone są wybrane filtry certyfikatów.

Nowego filtru certyfikatu można użyć jako bazy do utworzenia powiązania strategii filtrów certyfikatów.

Dodanie danych wyszukiwania do tożsamości użytkownika docelowego

Dane wyszukiwania to opcjonalne, unikalne dane identyfikujące dla tożsamości użytkownika docelowego zdefiniowane w powiązaniu. Powiązanie to może być powiązaniem docelowym identyfikatora lub powiązaniem strategii. Dane wyszukiwania są potrzebne tylko jeśli operacja wyszukiwania odwzorowania może zwrócić więcej niż jedną tożsamość użytkownika docelowego. Sytuacja taka może stanowić problem dla aplikacji z obsługą EIM, w tym aplikacji i produktów systemu i5/OS, które nie potrafią obsłużyć takich wyników.

Gdy jest to konieczne, można dodać unikalne dane wyszukiwania dla każdej tożsamości użytkownika docelowego udostępniając bardziej szczegółowe informacje identyfikujące lepiej opisujące każdą tożsamość użytkownika docelowego. Jeśli dla tożsamości użytkownika docelowego zostaną zdefiniowane dane wyszukiwania, należy je udostępnić operacji wyszukiwania odwzorowania, aby mogła ona zwrócić unikalną tożsamość użytkownika docelowego. W przeciwnym przypadku aplikacje polegające na odwzorowaniu EIM nie będą mogły określić, której dokładnie tożsamości docelowej mają użyć.

Uwaga: Jeśli operacje wyszukiwania EIM mają zwracać tylko jedną tożsamość użytkownika docelowego, należy poprawić konfigurację powiązań EIM, zamiast stosować dane wyszukiwania do rozwiązania tego problemu. Więcej szczegółowych informacji zawiera temat “Rozwiązywanie problemów z odwzorowaniem EIM” na stronie 118.

Sposób dodawania danych wyszukiwania do zdefiniowania tożsamości użytkownika docelowego zależy od tego, czy tożsamość użytkownika docelowego jest zdefiniowana w powiązaniu docelowym, czy w powiązaniu identyfikatora. Niezależnie od użytej metody, podane dane są związane z tożsamością użytkownika docelowego, nie z powiązaniem identyfikatora lub strategii, w którym znaleziona została dana tożsamość użytkownika.

Dodanie danych wyszukiwania do tożsamości użytkownika docelowego w powiązaniu identyfikatora:

Aby dodać dane wyszukiwania do tożsamości użytkownika docelowego w powiązaniu identyfikatora, należy połączyć się z wymaganą domeną EIM i mieć upraawnienie (patrz “Kontrola dostępu EIM” na stronie 39) na jednym z poniższych poziomów:

- Administrator rejestru.
- Administrator dla wybranych rejestrów (dla definicji rejestru odnoszącej się do rejestru użytkowników, który zawiera tożsamość użytkownika docelowego).
- Administrator EIM.

Aby dodać dane wyszukiwania do tożsamości użytkownika docelowego w powiązaniu identyfikatora, wykonaj następujące czynności:

1. Rozwiń gałąź **Sieć > Odwzorowanie EIM > Zarządzanie domenami**.
2. Wybierz domenę EIM, w której chcesz pracować.
   - Jeśli domena EIM, z którą chcesz pracować, nie jest wymieniona w folderze **Zarządzanie domenami**, patrz “Dodanie domeny EIM do folderu Zarządzanie domenami” na stronie 85.

- Jeśli w tej chwili nie masz połączenia z domeną EIM, w której chcesz pracować, patrz temat Łączenie się z kontrolerem domeny EIM.

3. Rozwiń domenę EIM, z którą masz połączenie.
4. Kliknij **Identyfikatory**, aby wyświetlić listę identyfikatorów EIM dla domeny.

   Uwaga: Czasem rozwinięcie folderu **Identyfikatory** może trwać dość długo. Aby poprawić wydajność przy dużej liczbie identyfikatorów EIM w domenie, można dostosować widok folderu **Identyfikatory**, ograniczając kryterium wyszukiwania dla wyświetlania identyfikatorów. Kliknij prawym przyciskiem myszy **Identyfikatory**, wybierz **Dostosuj ten widok... > Włącz** i podaj kryterium wyświetlania dla generowania listy identyfikatorów EIM, które mają być przedstawione w widoku.
5. Kliknij prawym przyciskiem myszy identyfikator EIM i wybierz **Właściwości...**.
6. Wybierz stronę **Powiązania**, wybierz powiązanie docelowe, do którego chcesz dodać dane wyszukiwania, i kliknij **Szczegóły...**. Kliknij **Pomoc**, jeśli chcesz przeczytać, jakie dane wpisać w każdym polu.
7. W oknie dialogowym **Powiązanie - Szczegóły** podaj **Dane wyszukiwania**, których chcesz używać do identyfikowania tożsamości użytkownika docelowego w tym powiązaniu i kliknij **Dodaj**.
8. Powtarzaj tę czynność dla wszystkich danych wyszukiwania, które chcesz dodać do powiązania.
9. Kliknij **OK**, aby zachować zmiany i wrócić do okna dialogowego **Powiązanie - Szczegóły**.
10. Kliknij **OK**, aby wyjść.

Dodanie danych wyszukiwania do tożsamości użytkownika docelowego w powiązaniu strategii:

Aby dodać dane wyszukiwania do tożsamości użytkownika docelowego w powiązaniu strategii, musisz połączyć się z domeną EIM, z którą chcesz pracować, i mieć uprawnienie (patrz “Kontrola dostępu EIM” na stronie 39) na jednym z poniższych poziomów:

- Administrator rejestru.
- Administrator dla wybranych rejestrów (dla definicji rejestru odnoszącej się do rejestru użytkowników, który zawiera tożsamość użytkownika docelowego - ID).
- Administrator EIM.

Aby dodać dane wyszukiwania do tożsamości użytkownika docelowego w powiązaniu strategii, wykonaj następujące czynności:

1. Rozwiń gałąź **Sieć > Odwzorowanie EIM > Zarządzanie domenami**.
2. Wybierz domenę EIM, w której chcesz pracować.
   - Jeśli domena EIM, z którą chcesz pracować, nie jest wymieniona w folderze **Zarządzanie domenami**, patrz “Dodanie domeny EIM do folderu Zarządzanie domenami” na stronie 85.
   - Jeśli w tej chwili nie masz połączenia z domeną EIM, w której chcesz pracować, patrz temat Łączenie się z kontrolerem domeny EIM.
3. W oknie dialogowym **Strategia odwzorowania** obejrzyj powiązania strategii dla domeny.
4. Wyszukaj i wybierz powiązanie strategii dla rejestru docelowego zawierającego tożsamość użytkownika docelowego, dla którego chcesz dodać dane wyszukiwania.
5. Kliknij **Szczegóły...**, aby wyświetlić odpowiednie okno dialogowe **Powiązanie strategii - Szczegóły** dla wybranego rodzaju powiązania strategii. Kliknij **Pomoc**, jeśli chcesz przeczytać, jakie dane wpisać w każdym polu.
6. Określ opcję **Informacje wyszukania**, której chcesz użyć do dokładniejszej identyfikacji docelowego identyfikatora użytkownika w tym powiązaniu i kliknij opcję **Dodaj**. Powtarzaj tę czynność dla wszystkich danych wyszukiwania, które chcesz dodać do powiązania.
7. Kliknij **OK**, aby zachować zmiany i wrócić do początkowego okna dialogowego **Powiązanie strategii - Szczegóły**.
8. Kliknij **OK**, aby wyjść.

Usuwanie danych wyszukiwania z tożsamości użytkownika docelowego

Dane wyszukiwania to opcjonalne, unikalne dane identyfikujące dla tożsamości użytkownika docelowego zdefiniowane w powiązaniu. Powiązanie to może być powiązaniem docelowym identyfikatora lub powiązaniem strategii. Dane wyszukiwania są potrzebne tylko jeśli operacja wyszukiwania odwzorowania może zwrócić więcej niż jedną tożsamość użytkownika docelowego. Sytuacja taka może stanowić problem dla aplikacji z obsługą EIM, w tym aplikacji i produktów systemu i5/OS, które nie potrafią obsłużyć takich wyników.

Dane te muszą być udostępnione operacji wyszukiwania odwzorowań, aby zapewnić, że zwróci ona tylko jedną unikalną tożsamość użytkownika docelowego. Jednak jeśli uprzednio zdefiniowane dane wyszukiwania nie są już potrzebne, można je usunąć, aby nie były podawane dla operacji wyszukiwania.

Sposób usuwania danych wyszukiwania z tożsamości użytkownika docelowego zależy od tego, czy tożsamość użytkownika docelowego jest zdefiniowana w powiązaniu docelowym, czy w powiązaniu identyfikatora. Dane wyszukiwania są związane z tożsamością użytkownika docelowego, nie z powiązaniami identyfikatorów lub strategii, w których znajduje się ta tożsamość użytkownika. Dlatego usunięcie ostatniego powiązania identyfikatora lub strategii, definiującego tożsamość użytkownika docelowego, powoduje usunięcie z domeny EIM zarówno tożsamości użytkownika, jak i danych wyszukiwania.

Usunięcie danych wyszukiwania z tożsamości użytkownika docelowego w powiązaniu identyfikatora:

Aby usunąć dane wyszukiwania z tożsamości użytkownika docelowego w powiązaniu identyfikatora, musisz połączyć się z domeną EIM z którą chcesz pracować, i mieć uprawnienie (patrz “Kontrola dostępu EIM” na stronie 39) na jednym z poniższych poziomów:

- Administrator rejestru.
- Administrator dla wybranych rejestrów (dla definicji rejestru odnoszącej się do rejestru użytkowników, który zawiera tożsamość użytkownika docelowego).
- Administrator EIM.

Aby usunąć dane wyszukiwania z tożsamości użytkownika docelowego w powiązaniu identyfikatora, wykonaj następujące czynności:

1. Rozwiń gałąź **Sieć > Odwzorowanie EIM > Zarządzanie domenami**.
2. Wybierz domenę EIM, w której chcesz pracować.
   - Jeśli domena EIM, z którą chcesz pracować, nie jest wymieniona w folderze **Zarządzanie domenami**, patrz “Dodanie domeny EIM do folderu Zarządzanie domenami” na stronie 85.
   - Jeśli w tej chwili nie masz połączenia z domeną EIM, w której chcesz pracować, patrz temat Łączenie się z kontrolerem domeny EIM.
3. Rozwiń domenę EIM, z którą masz połączenie.
4. Kliknij **Identyfikatory**, aby wyświetlić listę identyfikatorów EIM dla domeny.

   Uwaga: Czasem rozwinięcie folderu **Identyfikatory** może trwać dość długo. Aby poprawić wydajność przy dużej liczbie identyfikatorów EIM w domenie, można dostosować widok folderu **Identyfikatory**, ograniczając kryterium wyszukiwania dla wyświetlania identyfikatorów. Kliknij prawym przyciskiem myszy **Identyfikatory**, wybierz **Dostosuj ten widok... > Włącz** i podaj kryterium wyświetlania dla generowania listy identyfikatorów EIM, które mają być przedstawione w widoku.
5. Kliknij prawym przyciskiem myszy identyfikator EIM i wybierz **Właściwości...**.
6. Wybierz stronę **Powiązania**, wybierz powiązanie docelowe, z którego chcesz usunąć dane wyszukiwania, i kliknij **Szczegóły...**.
7. W oknie dialogowym **Powiązanie - Szczegóły** wybierz dane wyszukiwania, które chcesz usunąć z tożsamości użytkownika docelowego, i kliknij **Usuń**.

   Uwaga: Po kliknięciu **Usuń** nie będzie wyświetlona żadna prośba o potwierdzenie.
8. Kliknij **OK**, aby zachować zmiany i wrócić do okna dialogowego **Powiązanie - Szczegóły**.

9. Kliknij **OK**, aby wyjść.

Usuwanie danych wyszukiwania z tożsamości użytkownika docelowego w powiązaniu strategii:

Aby usunąć dane wyszukiwania z tożsamości użytkownika docelowego w powiązaniu strategii, musisz połączyć się z domeną EIM z którą chcesz pracować, i mieć uprawnienie (patrz “Kontrola dostępu EIM” na stronie 39) na jednym z poniższych poziomów:

- Administrator rejestru.
- Administrator dla wybranych rejestrów (dla definicji rejestru odnoszącej się do rejestru użytkowników, który zawiera tożsamość użytkownika docelowego - ID).
- Administrator EIM.

Aby usunąć dane wyszukiwania z tożsamości użytkownika docelowego w powiązaniu strategii, wykonaj następujące czynności:

1. Rozwiń gałąź **Sieć > Odwzorowanie EIM > Zarządzanie domenami**.
2. Wybierz domenę EIM, w której chcesz pracować.
   - Jeśli domena EIM, z którą chcesz pracować, nie jest wymieniona w folderze **Zarządzanie domenami**, patrz “Dodanie domeny EIM do folderu Zarządzanie domenami” na stronie 85.
   - Jeśli w tej chwili nie masz połączenia z domeną EIM, w której chcesz pracować, patrz temat Łączenie się z kontrolerem domeny EIM.
3. W oknie dialogowym **Strategia odwzorowania** obejrzyj powiązania strategii dla domeny.
4. Wyszukaj i wybierz powiązanie strategii dla rejestru docelowego, który zawiera tożsamość użytkownika docelowego, dla którego chcesz usunąć dane wyszukiwania.
5. Kliknij **Szczegóły...**, aby wyświetlić odpowiednie okno dialogowe **Powiązanie strategii - Szczegóły** dla wybranego rodzaju powiązania strategii.
6. Wybierz dane wyszukiwania, które chcesz usunąć z tożsamości użytkownika docelowego, i kliknij **Usuń**.

   Uwaga: Po kliknięciu **Usuń** nie będzie wyświetlona żadna prośba o potwierdzenie.
7. Kliknij **OK**, aby zachować zmiany i wrócić do początkowego okna dialogowego **Powiązanie strategii - Szczegóły**.
8. Kliknij **OK**, aby wyjść.

Wyświetlenie wszystkich powiązań identyfikatora dla identyfikatora EIM

Aby wyświetlić wszystkie powiązania dla identyfikatora EIM, musisz połączyć się z domeną EIM, w której chcesz pracować, i mieć uprawnienie “Kontrola dostępu EIM” na stronie 39 na wymaganym poziomie, aby wykonać to zadanie. Można przeglądać wszystkie powiązania z dowolnym poziomem kontroli dostępu oprócz Administrator dla wybranych rejestrów. Ten poziom kontroli dostępu umożliwia przeglądanie tylko powiązań do rejestrów, dla których masz jawne uprawnienia, chyba że masz również prawa dostępu do operacji wyszukiwania odwzorowań EIM.

Aby wyświetlić wszystkie powiązania między identyfikatorem EIM a tożsamościami użytkownika, dla których zdefiniowano powiązania, dla identyfikatora EIM, wykonaj następujące czynności:

Aby wyświetlić powiązania dla identyfikatora, wykonaj następujące czynności:

.

1. Rozwiń gałąź **Sieć > Odwzorowanie EIM > Zarządzanie domenami**.
2. Wybierz domenę EIM, w której chcesz pracować.
   - Jeśli domena EIM, z którą chcesz pracować, nie jest wymieniona w folderze **Zarządzanie domenami**, patrz “Dodanie domeny EIM do folderu Zarządzanie domenami” na stronie 85.
   - Jeśli w tej chwili nie masz połączenia z domeną EIM, w której chcesz pracować, patrz temat Łączenie się z kontrolerem domeny EIM.
3. Rozwiń domenę EIM, z którą masz połączenie.

4. Kliknij **Identyfikatory**, aby wyświetlić listę identyfikatorów EIM dla domeny.

   Uwaga: Czasem rozwinięcie folderu **Identyfikatory** może trwać dość długo. Aby poprawić wydajność przy dużej liczbie identyfikatorów EIM w domenie, można dostosować widok folderu **Identyfikatory**, ograniczając kryterium wyszukiwania dla wyświetlania identyfikatorów. Kliknij prawym przyciskiem myszy **Identyfikatory**, wybierz **Dostosuj ten widok... > Włącz** i podaj kryterium wyświetlania dla generowania listy identyfikatorów EIM, które mają być przedstawione w widoku.
5. Wybierz identyfikator EIM, prawym przyciskiem myszy kliknij identyfikator EIM i wybierz opcję **Właściwości**.
6. Wybierz stronę **Powiązania**, aby wyświetlić listę powiązanych tożsamości użytkownika dla wybranego identyfikatora EIM.
7. Kliknij przycisk **OK**, aby zakończyć.
8.

Wyświetlenie wszystkich powiązań strategii dla domeny

Aby wyświetlić wszystkie powiązania strategii zdefiniowane dla domeny, musisz połączyć się z domeną EIM, w której chcesz pracować i mieć uprawnienia (patrz “Kontrola dostępu EIM” na stronie 39) na wymaganym poziomie, aby wykonać to zadanie. Można przeglądać wszystkie powiązania strategii z dowolnym poziomem kontroli dostępu oprócz Administrator dla wybranych rejestrów. Ten poziom kontroli dostępu umożliwia przeglądanie tylko powiązań do rejestrów, dla których masz jawne uprawnienia. Dlatego też z tymi prawami dostępu nie możesz przeglądać żadnych domyślnych powiązań strategii domeny, chyba że masz również prawa dostępu do operacji wyszukiwania odwzorowań EIM.

Aby wyświetlić wszystkie powiązania strategii dla domeny, wykonaj następujące czynności:

1. Rozwiń gałąź **Sieć > Odwzorowanie EIM > Zarządzanie domenami**.
2. Kliknij prawym przyciskiem myszy domenę EIM, w której chcesz pracować, i wybierz **Strategia odwzorowania...**
   - Jeśli domena EIM, z którą chcesz pracować, nie jest wymieniona w folderze **Zarządzanie domenami**, patrz “Dodanie domeny EIM do folderu Zarządzanie domenami” na stronie 85.
   - Jeśli w tej chwili nie masz połączenia z domeną EIM, w której chcesz pracować, patrz temat Łączenie się z kontrolerem domeny EIM.
3. Wybierz stronę, aby wyświetlić powiązania strategii zdefiniowane dla domeny:
   a. Wybierz stronę **Domena**, aby przeglądać domyślne powiązania strategii domeny zdefiniowane dla domeny i informacje o tym, czy powiązanie strategii jest włączone na poziomie rejestru.
   b. Wybierz stronę **Rejestr**, aby przeglądać domyślne powiązania strategii rejestru zdefiniowane dla domeny. Możesz przeglądać również, których rejestrów źródłowych i docelowych dotyczą powiązania strategii.
   c. Wybierz stronę **Filtr certyfikatu**, aby przeglądać powiązania strategii filtrów certyfikatów zdefiniowane i włączone na poziomie rejestru.
4. Kliknij **OK**, aby zakończyć.

Wyświetlenie wszystkich powiązań strategii dla definicji rejestru

Aby wyświetlić wszystkie powiązania strategii zdefiniowane dla określonego rejestru, musisz połączyć się z domeną EIM, w której chcesz pracować i mieć uprawnienia (patrz “Kontrola dostępu EIM” na stronie 39) na wymaganym poziomie, aby wykonać to zadanie. Można przeglądać wszystkie powiązania strategii z dowolnym poziomem kontroli dostępu oprócz Administrator dla wybranych rejestrów. Ten poziom kontroli dostępu umożliwia przeglądanie tylko powiązań do rejestrów, dla których masz jawne uprawnienia. Dlatego też z tymi prawami dostępu nie możesz przeglądać żadnych domyślnych powiązań strategii domeny, chyba że masz również prawa dostępu do operacji wyszukiwania odwzorowań EIM.

Aby wyświetlić wszystkie powiązania strategii dla definicji rejestru, wykonaj następujące czynności:

1. Rozwiń gałąź **Sieć > Odwzorowanie EIM > Zarządzanie domenami**.
2. Wybierz domenę EIM, w której chcesz pracować.

- Jeśli domena EIM, z którą chcesz pracować, nie jest wymieniona w folderze **Zarządzanie domenami**, patrz “Dodanie domeny EIM do folderu Zarządzanie domenami” na stronie 85.
- Jeśli w tej chwili nie masz połączenia z domeną EIM, w której chcesz pracować, patrz temat Łączenie się z kontrolerem domeny EIM.

3. Prawym przyciskiem myszy kliknij definicję rejestru, z którą chcesz pracować i wybierz opcję **Strategia odwzorowania...**.
4. Wybierz stronę, aby wyświetlić powiązania strategii zdefiniowane dla określonej definicji rejestru:
   - Wybierz stronę **Domena**, aby przeglądać domyślne powiązania strategii domeny zdefiniowane dla rejestru.
   - Wybierz stronę **Rejestr**, aby przeglądać domyślne powiązania strategii rejestru zdefiniowane i włączone dla rejestru.
   - Wybierz stronę **Filtr certyfikatu**, aby przeglądać powiązania strategii filtrów certyfikatów zdefiniowane i włączone dla rejestru.
5. Kliknij **OK**, aby zakończyć.

Usuwanie powiązania identyfikatora

Aby usunąć powiązanie identyfikatora, musisz połączyć się z domeną EIM, w której chcesz pracować, i mieć uprawnienie (patrz “Kontrola dostępu EIM” na stronie 39) wymagane przez typ powiązania, który chcesz usunąć.

Aby usunąć powiązanie źródłowe lub administracyjne, musisz mieć prawa dostępu EIM na jednym z następujących poziomów:

- Administrator identyfikatora.
- Administrator EIM.

Aby usunąć powiązanie docelowe, musisz mieć prawa dostępu EIM na jednym z następujących poziomów:

- Administrator rejestru.
- Administrator dla wybranych rejestrów (dla definicji rejestru odnoszącej się do rejestru użytkowników, który zawiera tożsamość użytkownika docelowego).
- Administrator EIM.

Aby usunąć powiązanie identyfikatora, wykonaj następujące czynności:

1. Rozwiń gałąź **Sieć > Odwzorowanie EIM > Zarządzanie domenami**.
2. Wybierz domenę EIM, w której chcesz pracować.
   - Jeśli domena EIM, z którą chcesz pracować, nie jest wymieniona w folderze **Zarządzanie domenami**, patrz “Dodanie domeny EIM do folderu Zarządzanie domenami” na stronie 85.
   - Jeśli w tej chwili nie masz połączenia z domeną EIM, w której chcesz pracować, patrz temat Łączenie się z kontrolerem domeny EIM.
3. Rozwiń domenę EIM, z którą masz połączenie.
4. Kliknij **Identyfikatory**, aby wyświetlić listę identyfikatorów EIM dla domeny.

   Uwaga: Czasem rozwinięcie folderu **Identyfikatory** może trwać dość długo. Aby poprawić wydajność przy dużej liczbie identyfikatorów EIM w domenie, można dostosować widok folderu **Identyfikatory**, ograniczając kryterium wyszukiwania dla wyświetlania identyfikatorów. Kliknij prawym przyciskiem myszy **Identyfikatory**, wybierz **Dostosuj ten widok... > Włącz** i podaj kryterium wyświetlania dla generowania listy identyfikatorów EIM, które mają być przedstawione w widoku.
5. Wybierz identyfikator EIM, prawym przyciskiem myszy kliknij identyfikator EIM i wybierz opcję **Właściwości**.
6. Wybierz stronę **Powiązania**, aby wyświetlić listę powiązanych tożsamości użytkownika dla wybranego identyfikatora EIM.
7. Wybierz powiązanie, które chcesz usunąć i kliknij **Usuń**.

   Uwaga: Po kliknięciu **Usuń** nie będzie wyświetlona żadna prośba o potwierdzenie.

8. Kliknij przycisk **OK**, aby zachować zmiany.

Uwaga: Po usunięciu powiązania docelowego, operacje wyszukiwania odwzorowań w rejestrze docelowym używające usuniętego powiązania mogą nie powieść się, jeśli dla danego rejestru docelowego nie istnieją inne powiązania (na przykład powiązania strategii lub powiązania identyfikatorów).

Jedyną metodą zdefiniowania tożsamości użytkownika w EIM jest podanie jej w ramach części tworzenia powiązania identyfikatora lub powiązania strategii. W wyniku tego usunięcie ostatniego powiązania docelowego dla tożsamości użytkownika (przez usunięcie pojedynczego powiązania docelowego lub powiązania strategii) powoduje, że tożsamość użytkownika nie jest już zdefiniowana w EIM. W wyniku tego nazwa tożsamości użytkownika i wszystkie dane wyszukiwania z nią związane zostają utracone.

Usuwanie powiązania strategii

Aby usunąć powiązanie strategii, musisz połączyć się z domeną EIM, w której chcesz pracować, i mieć uprawnienie (patrz “Kontrola dostępu EIM” na stronie 39) na jednym z poniższych poziomów:

- Administrator rejestru.
- Administrator EIM.

Aby usunąć powiązanie strategii, wykonaj następujące czynności:

1. Rozwiń gałąź **Sieć > Odwzorowanie EIM > Zarządzanie domenami**.
2. Wybierz domenę EIM, w której chcesz pracować.
   - Jeśli domena EIM, z którą chcesz pracować, nie jest wymieniona w folderze **Zarządzanie domenami**, patrz “Dodanie domeny EIM do folderu Zarządzanie domenami” na stronie 85.
   - Jeśli w tej chwili nie masz połączenia z domeną EIM, w której chcesz pracować, patrz temat Łączenie się z kontrolerem domeny EIM.
3. Wybierz stronę odpowiednią dla rodzaju powiązania strategii, które chcesz usunąć.
4. Na stronie tej wybierz odpowiednie powiązanie strategii i kliknij **Usuń**.

   Uwaga: Po kliknięciu **Usuń** nie będzie wyświetlona żadna prośba o potwierdzenie.
5. Kliknij **OK**, aby zamknąć okno dialogowe **Strategia odwzorowania** i zachować zmiany.

Uwaga: Po usunięciu docelowego powiązania strategii, operacje wyszukiwania odwzorowań w rejestrze docelowym używające usuniętego powiązania strategii mogą nie powieść się, jeśli dla danego rejestru docelowego nie istnieją inne powiązania (na przykład powiązania strategii lub powiązania identyfikatorów).

Jedyną metodą zdefiniowania tożsamości użytkownika w EIM jest podanie jej w ramach części tworzenia powiązania identyfikatora lub powiązania strategii. W wyniku tego usunięcie ostatniego powiązania docelowego dla tożsamości użytkownika (przez usunięcie pojedynczego powiązania docelowego lub powiązania strategii) powoduje, że tożsamość użytkownika nie jest już zdefiniowana w EIM. W wyniku tego nazwa tożsamości użytkownika i wszystkie dane wyszukiwania z nią związane zostają utracone.

Pojęcia pokrewne

“Zarządzanie definicjami rejestrów EIM” na stronie 90
Informacje dotyczące tworzenia definicji rejestrów EIM i zarządzania nimi dla tych rejestrów użytkowników w przedsiębiorstwie, które są uwzględniane w odwzorowaniach EIM.

Zarządzanie kontrolą dostępu użytkownika EIM

Informacje ułatwiające zarządzanie dostępem dla użytkowników korzystających z protokołu LDAP.

Użytkownik produktu EIM to użytkownik, który ma ustalaną kontrolę dostępu (patrz “Kontrola dostępu EIM” na stronie 39) w oparciu o przynależność do predefiniowanych grup użytkowników LDAP. Określenie kontroli dostępu EIM dla użytkownika powoduje dodanie tego użytkownika do określonej grupy użytkowników LDAP. Każda grupa LDAP ma uprawnienia do wykonywania różnych zadań administracyjnych EIM w domenie. To, które zadania

administracyjne i jakiego typu może wykonać użytkownik, włącznie z operacjami wyszukiwania, jest określone przez grupę kontroli dostępu, do której dany użytkownik EIM należy.

Tylko użytkownicy z prawem dostępu administratora LDAP lub EIM mogą dodawać innych użytkowników do grupy kontroli dostępu EIM lub zmieniać ustawienia kontroli dostępu dla innych użytkowników. Zanim użytkownik stanie się członkiem grupy kontroli dostępu EIM, musi mieć pozycję w serwerze katalogów działającym jako kontroler domeny EIM. Oprócz tego do grupy kontroli dostępu EIM można dopisać tylko pewne typy użytkowników: nazwy użytkowników Kerberos, nazwy wyróżniające i profile użytkowników i5/OS.

Uwaga: Aby udostępnić w EIM nazwy użytkowników Kerberos, w systemie należy skonfigurować usługę uwierzytelniania sieciowego. Aby udostępnić w EIM profile użytkowników i5/OS, na serwerze katalogów należy skonfigurować przyrostek obiektów systemowych. Umożliwia on serwerowi katalogów odniesienie do obiektów systemowych i5/OS takich jak profile użytkowników i5/OS.

Aby zarządzać kontrolą dostępu dla istniejącego użytkownika serwera katalogów lub dodać istniejącego użytkownika do grupy kontroli dostępu EIM, wykonaj następujące czynności:

1. Rozwiń gałąź **Sieć > Odwzorowanie EIM > Zarządzanie domenami**.
2. Wybierz domenę EIM, w której chcesz pracować.
   - Jeśli domena EIM, z którą chcesz pracować, nie jest wymieniona w folderze **Zarządzanie domenami**, patrz “Dodanie domeny EIM do folderu Zarządzanie domenami” na stronie 85.
   - Jeśli w tej chwili nie masz połączenia z domeną EIM, w której chcesz pracować, patrz temat Łączenie się z kontrolerem domeny EIM.
3. Kliknij prawym przyciskiem myszy domenę EIM, z którą się łączysz, i wybierz **Kontrola dostępu...**
4. W oknie dialogowym **Edytuj kontrolę dostępu EIM** wybierz opcję **Typ użytkownika**, aby wyświetlić wymagane pola zawierające informacje identyfikujące użytkownika.
5. Wprowadź wymagane dane o użytkowniku identyfikujące użytkownika, dla którego chcesz zarządzać kontrolą dostępu, EIM i kliknij **OK**, aby wyświetlić panel **Edytuj kontrolę dostępu EIM**. Kliknij **Pomoc**, jeśli chcesz przeczytać, jakie dane wpisać w każdym polu.
6. Wybierz dla użytkownika jedną lub więcej grup **Kontroli dostępu** i kliknij **OK**, aby dodać użytkownika do wybranych grup. Kliknij **Pomoc**, aby uzyskać bardziej szczegółowe informacje o uprawnieniach każdej z grup i zapoznać się z wymaganiami specjalnymi.
7. Po wprowadzeniu wymaganych danych kliknij **OK**, aby zachować zmiany.

Zarządzanie właściwościami konfiguracji EIM

Informacje ułatwiające konfigurowanie właściwości produktu Enterprise Identity Mapping (EIM), takich jak domeny, tożsamości użytkowników i definicje rejestrów.

Na serwerze można zarządzać kilkoma różnymi właściwościami konfiguracji EIM. Zazwyczaj nie jest to czynność wymagana zbyt często. Jednak zdarzają się sytuacje, w których wymagane jest zmienienie właściwości konfiguracji. Jeśli na przykład system jest wyłączany i trzeba ponownie utworzyć właściwości konfiguracji EIM, można ponownie uruchomić kreatora konfigurowania EIM, albo zmienić te właściwości w sposób opisany poniżej. Jeśli podczas działania kreatora konfigurowania EIM nie zostały utworzone definicje rejestrów dla rejestrów lokalnych, metodą opisaną tutaj można również aktualizować dane o definicjach rejestrów.

Właściwości, które można zmodyfikować są następujące:

- Domena EIM, do której należy serwer.
- Informacje o połączeniu dla kontrolera domeny EIM.
- Tożsamość użytkownika używana przez system do wykonywania operacji EIM w imieniu funkcji systemu operacyjnego.
- Nazwy definicji rejestrów odnoszące się do rzeczywistych rejestrów użytkowników, których system może używać podczas wykonywania operacji EIM w imieniu funkcji systemu operacyjnego. Nazwy definicji rejestrów odnoszą się do lokalnych rejestrów użytkowników, które można utworzyć podczas działania kreatora konfigurowania EIM.

Uwaga: Jeśli podczas działania kreatora konfigurowania EIM nie zostaną utworzone nazwy definicji lokalnych rejestrów gdyż rejestry zostały już zdefiniowane lub mają być zdefiniowane później, należy zaktualizować właściwości konfiguracji systemu o te definicje rejestrów w sposób opisany poniżej. System potrzebuje danych o definicjach rejestrów do wykonywania operacji EIM w imieniu funkcji systemu operacyjnego.

Aby zmienić właściwości konfiguracji EIM, wymagane są następujące uprawnienia specjalne:

- Administrator ochrony (*SECADM).
- Wszystkie obiekty (*ALLOBJ).

Aby zmienić właściwości konfiguracji EIM dla serwera iSeries, wykonaj następujące czynności:

1. Rozwiń gałąź **Sieć > Odwzorowanie EIM**.
2. Kliknij prawym przyciskiem myszy **Konfiguracja** i wybierz opcję **Właściwości**.
3. Wprowadź zmiany do danych konfiguracji EIM.
4. Kliknij **Pomoc**, aby dowiedzieć się, jakie informacje podać w każdym polu w oknie dialogowym.
5. Kliknij **Weryfikacja konfiguracji**, aby upewnić się, że wszystkie podane dane umożliwiają systemowi pomyślne nawiązanie połączenia z kontrolerem domeny EIM.
6. Kliknij przycisk **OK**, aby zachować zmiany.

Uwaga: Jeśli tworzenie domeny i połączenie z nią nie zostało zrealizowane za pomocą kreatora konfigurowania EIM, nie należy próbować tworzyć konfiguracji EIM przez ręczne wprowadzanie właściwości konfiguracji. Użycie kreatora konfigurowania EIM do utworzenia prostej konfiguracji EIM może zapobiegać potencjalnym problemom z konfiguracją, gdyż kreator wykonuje więcej czynności oprócz konfigurowania tych właściwości.

Rozwiązywanie problemów z EIM

Informacje o najczęściej występujących problemach i błędach, z którymi można się spotkać przy konfigurowaniu i używaniu EIM oraz możliwie rozwiązania.

W EIM zawarto wiele technologii, aplikacji i funkcji. W wyniku tego problemy mogą być związane z wieloma różnymi elementami. Poniższe informacje opisują najczęściej spotykane problemy i błędy związane z korzystaniem EIM i kilka sugestii dotyczących ich usuwania.

Informacje pokrewne

Rozwiązywanie problemów dotyczących konfiguracji pojedynczego wpisywania się (SSO)

Rozwiązywanie problemów z połączeniem kontrolera domeny

Problemy z nawiązaniem połączenia z kontrolerem domeny mogą być spowodowane wieloma czynnikami. Poniższa tabela pomaga określić sposób rozwiązania możliwych problemów z połączeniem z kontrolerem domeny.

Tabela 27. Najczęstsze problemy z połączeniem z kontrolerem domeny EIM i ich rozwiązania

Możliwy problem	Możliwe rozwiązania
Nie można połączyć się z kontrolerem domeny, jeśli do zarządzania EIM używany jest program iSeries Navigator.	Informacje o połączeniu kontrolera domeny mogą być niepoprawne dla domeny, którą chcesz zarządzać. Wykonaj poniższe czynności, aby sprawdzić dane o połączeniu domeny: • Rozwiń gałąź **Sieć-->Odwzorowanie EIM-->Zarządzanie domenami**. Kliknij prawym przyciskiem myszy domenę, którą chcesz zarządzać, i wybierz **Właściwości**. • Sprawdź, czy poprawna jest nazwa w polu **Kontroler domeny** i **Nadrzędna nazwa wyróżniająca**. • Sprawdź, czy poprawne są dane dla kontrolera domeny w polu **Połączenie**. Upewnij się, że numer wpisany w polu **Port** jest prawidłowy. Jeśli wybrana jest opcja **Użyj połączenia chronionego (SSL lub TLS)**, serwer katalogów musi być skonfigurowany do korzystania z SSL. Kliknij **Weryfikacja połączenia**, aby sprawdzić, czy można użyć podanych informacji do pomyślnego nawiązania połączenia z kontrolerem domeny. • Sprawdź poprawność informacji o użytkowniku wpisanych w panelu **Połączenie z kontrolerem domeny**.
System operacyjny lub aplikacje nie mogą połączyć się z kontrolerem domeny w celu uzyskania dostępu do danych EIM. Na przykład operacje wyszukiwania odwzorowania EIM wykonywane dla systemu nie działają. Może to być spowodowane niepoprawną konfiguracją EIM w systemie lub w systemach.	Sprawdź konfigurację EIM. W systemie, z którym próbujesz się uwierzytelnić, rozwiń **Sieć-->Odwzorowanie EIM-->Konfiguracja**. Kliknij prawym przyciskiem myszy folder **Konfiguracja**, wybierz **Właściwości** i sprawdź następujące elementy: • Na stronie **Domena**: – Sprawdź poprawność numerów portów i nazwy kontrolera domeny. – Kliknij **Sprawdzenie konfiguracji**, aby sprawdzić, czy kontroler domeny jest aktywny. – Sprawdź, czy nazwa lokalnego rejestru jest poprawna. – Sprawdź, czy nazwa rejestru Kerberos jest poprawna. – Sprawdź, czy wybrana jest opcja **Włącz operacje EIM na tym systemie**. • Na stronie **Użytkownik systemu**: – Wybrany użytkownik ma odpowiednią kontrolę dostępu EIM niezbędną do wykonania wyszukania odwzorowania, a hasło użytkownika jest poprawne. Więcej informacji na temat rodzajów uwierzytelnienia użytkownika zawiera pomoc elektroniczna. **Uwaga:** Jeśli hasło dla danego użytkownika systemu w serwerze katalogów zostało zmienione, to hasło należy zmienić również w tym miejscu. Jeśli hasła te nie będą zgodne, użytkownik systemu nie będzie mógł wykonywać funkcji EIM dla systemu operacyjnego i operacja wyszukania odwzorowania nie powiedzie się. – Kliknij **Sprawdź połączenie**, aby potwierdzić poprawność podanych informacji o użytkowniku.

Tabela 27. Najczęstsze problemy z połączeniem z kontrolerem domeny EIM i ich rozwiązania (kontynuacja)

Możliwy problem	Możliwe rozwiązania
Informacje konfiguracyjne są poprawne, ale nie można połączyć się z kontrolerem domeny.	• Upewnij się, że serwer katalogów działający jako kontroler domeny EIM jest aktywny. Jeśli kontroler domeny jest serwerem iSeries, możesz użyć programu iSeries Navigator i wykonać następujące czynności: 1. Rozwiń gałąź **Sieć > Serwery > TCP/IP**. 2. Sprawdź, czy Directory Server ma status **Uruchomiony**. Jeśli serwer jest zatrzymany, prawym przyciskiem myszy kliknij **Directory Server** i wybierz **Uruchom...**

Po sprawdzeniu danych połączenia i aktywności serwera spróbuj połączyć się z kontrolerem domeny wykonując następujące czynności:

1. Rozwiń gałąź **Sieć > Odwzorowanie EIM > Zarządzanie domenami**.
2. Prawym przyciskiem myszy kliknij domenę EIM, z którą chcesz się połączyć, i wybierz **Połącz...**
3. Podaj typ użytkownika i wymagane informacje o użytkowniku, które mają być używane do połączenia się z kontrolerem domeny EIM.
4. Kliknij przycisk **OK**.

Rozwiązywanie ogólnych problemów z konfiguracją i domeną EIM

Niektóre problemy mogą wystąpić zarówno przy konfigurowaniu EIM dla danego systemu, jak i przy dostępie do domeny EIM. Poniższa tabela zawiera informacje o niektórych, najczęściej spotykanych problemach i potencjalne rozwiązania, które można zastosować, aby rozwiązać te problemy.

Tabela 28. Najczęstsze problemy związane z konfigurowaniem EIM i domeną oraz ich rozwiązania

Możliwy problem	Możliwe rozwiązania
Kreator konfigurowania EIM wygląda jakby się zawiesił podczas przetwarzania opcji **Zakończ**.	Kreator może oczekiwać na uruchomienie kontrolera domeny. Sprawdź, czy podczas uruchamiania serwera katalogów pojawiły się jakieś problemy. W przypadku serwerów iSeries sprawdź protokół zadania QDIRSRV w podsystemie QSYSWRK. Aby sprawdzić protokół zadania: 1. W programie iSeries Navigator, rozwiń **Zarządzanie pracą > Podsystemy > Qsyswrk**. 2. Prawym przyciskiem myszy kliknij **Qdirsrv** i wybierz **Protokół zadania**.
Podczas korzystania z kreatora konfigurowania EIM do utworzenia domeny w systemie zdalnym, użytkownik otrzymuje następujący komunikat o błędzie: ″Wprowadzona nadrzędna nazwa wyróżniająca jest niepoprawna. Nazwa wyróżniająca musi znajdować się na zdalnym serwerze katalogów. Podaj nową lub wybierz istniejącą nadrzędną nazwę wyróżniającą.″	Nadrzędna nazwa wyróżniająca podana dla domeny zdalnej nie istnieje. Więcej informacji o korzystaniu z kreatora konfigurowania EIM zawiera temat “Tworzenie nowej domeny zdalnej i jej przyłączanie” na stronie 74. Ponadto pomoc elektroniczna zawiera szczegółowe informacje na temat określania nadrzędnej nazwy wyróżniającej podczas tworzenia domeny.
Wyświetlony został komunikat, że domena EIM nie istnieje.	Jeśli domena EIM nie została utworzona, użyj kreatora konfigurowania EIM. Kreator utworzy nową domenę EIM lub umożliwi skonfigurowanie istniejącej. Jeśli domena EIM została utworzona, upewnij się, że dany użytkownik należy do grupy kontroli dostępu EIM (co zostało opisane w sekcji “Kontrola dostępu EIM” na stronie 39) i ma odpowiednie uprawnienia do dostępu do niej.

Tabela 28. Najczęstsze problemy związane z konfigurowaniem EIM i domeną oraz ich rozwiązania (kontynuacja)

Możliwy problem	Możliwe rozwiązania
Został wyświetlony komunikat informujący, że obiekt EIM (identyfikator, rejestr, powiązanie, powiązanie strategii lub filtr certyfikatu) nie został znaleziony lub nie masz uprawnień do danych EIM.	Sprawdź, czy obiekt EIM istnieje i czy podany użytkownik należy do grupy kontroli dostępu EIM (co zostało opisane w sekcji "Kontrola dostępu EIM" na stronie 39) i ma odpowiednie uprawnienia do tego obiektu.
Rozwinięcie folderu **Identyfikatory** zajmuje dużo czasu zanim wyświetlona zostanie lista identyfikatorów.	Może tak się zdarzyć, jeśli w domenie jest dużo identyfikatorów EIM. Aby rozwiązać ten problem, można dostosować widok folderu **Identyfikatory** ograniczając kryteria wyszukiwania używane w celu wyświetlenia identyfikatorów. Aby dostosować widok identyfikatorów EIM, wykonaj następujące czynności: 1. W programie iSeries Navigator, rozwiń **Sieć > Odwzorowanie EIM > Zarządzanie domenami**. 2. Rozwiń domenę, dla której chcesz wyświetlić identyfikatory EIM. 3. Kliknij prawym przyciskiem myszy **Identyfikatory** i wybierz opcję **Dostosuj ten widok > Pokaż...**. 4. Podaj kryterium wyświetlania dla generowania listy identyfikatorów EIM, które mają być przedstawione w widoku. **Uwaga:** Jako znaku zastępczego można użyć gwiazdki (*****). 5. Kliknij przycisk **OK**. Kolejne kliknięcie pozycji **Identyfikatory** spowoduje wyświetlenie tylko tych identyfikatorów EIM, które spełniają podane kryteria.
Podczas zarządzania EIM programem iSeries Navigator użytkownik otrzymuje błąd wskazujący, że uchwyt EIM nie jest poprawny.	Połączenie z kontrolerem domeny zostało utracone. Aby ponownie nawiązać połączenie z kontrolerem domeny: 1. W programie iSeries Navigator, rozwiń **Sieć > Odwzorowanie EIM > Zarządzanie domenami**. 2. Prawym przyciskiem myszy kliknij domenę, z którą chcesz pracować, i kliknij przycisk **Połącz ponownie...** 3. Podaj informacje o połączeniu. 4. Kliknij przycisk **OK**.
Podczas używania protokołu Kerberos do uwierzytelniania w EIM do protokołu zadania jest zapisywany komunikat diagnostyczny CPD3E3F.	Komunikat ten jest generowany za każdym razem, gdy nie powiedzie się operacja uwierzytelniania lub odwzorowania tożsamości. Komunikat diagnostyczny zawiera zarówno główne, jak i poboczne kody statusów, które wskazują miejsce wystąpienia problemu. Najczęściej występujące błędy wraz z działaniami naprawczymi są opisane w komunikacie. Aby rozwiązać problem, należy skorzystać z pomocy powiązanej z danym komunikatem diagnostycznym. Przydatne mogą również być informacje w sekcji Rozwiązywanie problemów z konfiguracją pojedynczego logowania.

Rozwiązywanie problemów z odwzorowaniem EIM

Jest wiele powszechnych problemów, które mogą spowodować, że odwzorowania EIM nie działają wcale, lub nie działają zgodnie z oczekiwaniami. Za pomocą poniższej tabeli można znaleźć informacje o tym, jaki problem może być przyczyną awarii odwzorowań EIM, oraz możliwe rozwiązania tego problemu. Jeśli odwzorowania EIM nie działają, należy zapoznać się z każdym rozwiązaniem przedstawionym w tabeli, aby znaleźć i rozwiązać problem lub problemy, które to powodują.

Tabela 29. Najczęstsze problemy z odwzorowaniem EIM i ich rozwiązania

Możliwy problem	Możliwe rozwiązania
Informacje połączenia dla kontrolera domeny są nieprawidłowe lub kontroler domeny może być nieaktywny.	Zapoznaj się z tematem Problemy z połączeniem kontrolera domeny, aby się dowiedzieć, jak sprawdzić informacje połączenia dla kontrolera domeny i jak sprawdzić, czy kontroler domeny jest aktywny.
Operacje wyszukiwania odwzorowania EIM wykonywane dla systemu nie działają. Może to być spowodowane niepoprawną konfiguracją EIM w systemie lub w systemach.	Sprawdź konfigurację EIM. W systemie, z którym próbujesz się uwierzytelnić, rozwiń **Sieć-->Odwzorowanie EIM-->Konfiguracja**. Kliknij prawym przyciskiem myszy folder **Konfiguracja**, wybierz **Właściwości** i sprawdź następujące elementy: • Na stronie **Domena**: – Sprawdź poprawność numerów portów i nazwy kontrolera domeny. – Kliknij **Sprawdzenie konfiguracji**, aby sprawdzić, czy kontroler domeny jest aktywny. – Sprawdź, czy nazwa lokalnego rejestru jest poprawna. – Sprawdź, czy nazwa rejestru Kerberos jest poprawna. – Sprawdź, czy wybrana jest opcja **Włącz operacje EIM na tym systemie**. • Na stronie **Użytkownik systemu**: – Wybrany użytkownik ma odpowiednią kontrolę dostępu EIM niezbędną do wykonania wyszukania odwzorowania, a hasło użytkownika jest poprawne. Więcej informacji na temat rodzajów uwierzytelnienia użytkownika zawiera pomoc elektroniczna. **Uwaga:** Jeśli hasło dla danego użytkownika systemu w serwerze katalogów zostało zmienione, to hasło należy zmienić również w tym miejscu. Jeśli hasła te nie będą zgodne, użytkownik systemu nie będzie mógł wykonywać funkcji EIM dla systemu operacyjnego i operacja wyszukania odwzorowania nie powiedzie się. – Kliknij **Sprawdź połączenie**, aby potwierdzić poprawność podanych informacji o użytkowniku.

Tabela 29. Najczęstsze problemy z odwzorowaniem EIM i ich rozwiązania (kontynuacja)

Możliwy problem	Możliwe rozwiązania
Operacja wyszukiwania odwzorowania może zwracać wiele tożsamości użytkownika docelowego. Zdarza się tak, gdy wystąpi któraś z poniżej wymienionych sytuacji: • Identyfikator EIM ma wiele pojedynczych powiązań docelowych do tego samego rejestru docelowego. • Więcej niż jeden identyfikator EIM ma pewną tożsamość użytkownika podaną w powiązaniu źródłowym i każdy z tych identyfikatorów EIM ma powiązanie docelowe do tego samego rejestru docelowego, jednak tożsamości użytkowników podane dla każdego powiązania docelowego mogą być różne. • Więcej niż jedno powiązanie strategii domeny domyślnej określa dany rejestr docelowy. • Więcej niż jedno powiązanie strategii rejestru domyślnego określa dany rejestr źródłowy i rejestr docelowy. • Więcej niż jedno powiązanie strategii filtrów certyfikatów określa dany rejestr źródłowy X.509, filtr certyfikatu i rejestr docelowy.	Funkcja Testowanie odwzorowania EIM umożliwia sprawdzenie, że określona źródłowa tożsamość użytkownika jest poprawnie odwzorowana na docelową tożsamość użytkownika. Sposób rozwiązania problemu zależy od wyników uzyskanych przy testowaniu: • Test zwraca wiele niechcianych tożsamości docelowych z jednego z poniższych powodów: – Może to oznaczać, że konfiguracja powiązania dla domeny jest niepoprawna z jednego z następujących powodów: - Powiązanie źródłowe lub docelowe dla identyfikatora EIM jest skonfigurowane niepoprawnie. Na przykład nie ma powiązania źródłowego dla nazwy użytkownika Kerberos (lub użytkownika Windows) lub jest ono niepoprawne. Możliwe również, że powiązanie docelowe określa niepoprawną tożsamość użytkownika. Wyświetl wszystkie powiązania identyfikatorów dla identyfikatora EIM, aby sprawdzić powiązania określonego identyfikatora. - Powiązanie strategii jest skonfigurowane niepoprawnie. Wyświetl wszystkie powiązania strategii dla domeny, aby sprawdzić dane źródłowe i docelowe dla wszystkich powiązań strategii zdefiniowanych w domenie. – Może to oznaczać, że definicje rejestru grupowego zawierające wspólne elementy są rejestrami źródłowymi lub docelowymi powiązań identyfikatora EIM lub powiązań strategii. Szczegółowe informacje zwracane przez operację testowania odwzorowania umożliwiają określenie, czy definicje źródłowe lub docelowe są definicjami rejestrów grupowych. Jeśli tak, należy sprawdzić właściwości definicji, aby określić, czy zawierają wspólne elementy. – Test zwraca wiele tożsamości docelowych i wyniki te są zgodne z konfiguracją powiązań. W takim przypadku dla każdej tożsamości użytkownika docelowego należy określić dane wyszukiwania, aby zapewnić, że operacja wyszukiwania zwróci pojedynczą tożsamość użytkownika docelowego, a nie wszystkie pasujące tożsamości użytkowników docelowych. Przeczytaj sekcję Dodanie danych wyszukiwania do tożsamości użytkownika docelowego. **Uwaga:** Rozwiązanie to jest skuteczne tylko wtedy, gdy aplikacja ma włączone korzystanie z danych wyszukiwania. Jednakże podstawowe aplikacje systemu i5/OS, takie jak iSeries Access for Windows, nie używają danych wyszukiwania do rozróżnienia między wieloma tożsamościami użytkowników docelowych zwracanych przez operację wyszukiwania. Dlatego też należy rozważyć ponowne zdefiniowanie powiązań dla domeny, aby zapewnić, że operacja wyszukiwania odwzorowań będzie mogła zwrócić pojedynczą tożsamość użytkownika docelowego i że podstawowe aplikacje systemu i5/OS będą mogły pomyślnie wykonywać operacje wyszukiwania i odwzorować tożsamości.

Tabela 29. Najczęstsze problemy z odwzorowaniem EIM i ich rozwiązania (kontynuacja)

Możliwy problem	Możliwe rozwiązania
Operacje wyszukiwania EIM nie zwracają wyników chociaż dla domeny są skonfigurowane powiązania.	Funkcja Testowanie odwzorowania EIM umożliwia sprawdzenie, że określona źródłowa tożsamość użytkownika jest poprawnie odwzorowana na docelową tożsamość użytkownika. Sprawdź, czy do testu zostały podane poprawne informacje. Jeśli tak i test nie zwraca wyników, to problem może być spowodowany jedną z następujących przyczyn: • Niepoprawna konfiguracja powiązania. Sprawdź konfigurację powiązania za pomocą wcześniej opisanych metod rozwiązywania problemu. • Na poziomie domeny nie jest włączona obsługa powiązań strategii. Możliwe, że trzeba włączyć powiązania strategii dla domeny. • Na poziomie danego rejestru nie jest włączona obsługa powiązań strategii. Możliwe, że trzeba włączyć obsługę wyszukiwania odwzorowań i korzystanie z powiązań strategii dla rejestru docelowego. • Definicja rejestru i tożsamości użytkowników nie są zgodne w związku z rozróżnianiem wielkości znaków. Można usunąć i ponownie utworzyć rejestr lub usunąć i ponownie utworzyć powiązanie stosując poprawną wielkość znaków.

Funkcje API EIM

Informacje o funkcjach API EIM i sposobie ich używania w aplikacjach i sieci.

Odwzorowania EIM zapewniają mechanizmy do zarządzania tożsamościami użytkowników na wielu platformach. W EIM dostępnych jest wiele funkcji API, które można wykorzystać w aplikacjach do wykonania operacji EIM w imieniu aplikacji lub użytkownika aplikacji. Funkcji tych można użyć do wykonania operacji wyszukiwania odwzorowania, realizacji różnych funkcji konfiguracji i zarządzania EIM oraz do wprowadzania zmian w informacjach i do odpytywania. Każda z tych funkcji jest obsługiwana na platformach firmy IBM.

Funkcje API dla EIM można podzielić na następujące kategorie:

- obsługa EIM i operacje połączeń,
- administrowanie domeną EIM,
- operacje na rejestrze,
- operacje na identyfikatorach EIM,
- zarządzanie powiązaniami EIM,
- operacje wyszukiwania odwzorowania EIM,
- zarządzanie autoryzacją EIM.

W aplikacjach używających tych funkcji API do zarządzania lub korzystania z informacji EIM w domenie EIM zwykle stosuje się następujący model programowania:

1. Uzyskanie uchwytu EIM.
2. Połączenie się z domeną EIM.
3. Zwykłe przetwarzanie aplikacji.
4. Użycie funkcji API administrowania EIM lub wyszukiwania odwzorowania tożsamości EIM.
5. Zwykłe przetwarzanie aplikacji.
6. Zniszczenie uchwytu EIM przed zakończeniem pracy.

Informacje pokrewne

Interfejsy API produktu Enterprise Identity Mapping (EIM)

Informacje pokrewne dotyczące EIM

Inne zasoby i informacje związane z używaniem produktu EIM.

Z odwzorowaniami EIM związane są również inne technologie. W ich poznaniu pomocne są następujące tematy zamieszczone w Centrum informacyjnym:

- **Pojedyncze logowanie** Informacje dotyczące konfigurowania środowiska pojedynczego logowania i zarządzania tym środowiskiem w przedsiębiorstwie, przedstawione zostały tam również scenariusze pokazujące korzyści dla przedsiębiorstwa wynikające z pojedynczego logowania.
- **Usługa uwierzytelniania sieciowego** Informacje związane z konfigurowaniem i dotyczące używania usługi uwierzytelniania sieciowego, implementacji protokołu Kerberos serwera iSeries. Konfigurując usługę uwierzytelniania sieciowego wraz z EIM można utworzyć w przedsiębiorstwie środowisko pojedynczego logowania.
- **Serwer IBM Directory Server for iSeries (LDAP)** Informacje o konfiguracji i pojęciach związanych z produktem IBM Directory Server for iSeries (LDAP). Odwzorowania EIM umożliwiają wykorzystanie serwera katalogów jako kontrolera domeny EIM do przechowywania danych domeny EIM.

Warunki

Zezwolenie na korzystanie z tych publikacji jest przyznawane na poniższych warunkach.

Użytek osobisty: Użytkownik ma prawo kopiować te publikacje do własnego, niekomercyjnego użytku pod warunkiem zachowania wszelkich uwag dotyczących praw własności. Użytkownik nie ma prawa dystrybuować ani wyświetlać tych publikacji czy ich części, ani też wykonywać na ich podstawie prac pochodnych bez wyraźnej zgody IBM.

Użytek służbowy: Użytkownik ma prawo kopiować te publikacje, dystrybuować je i wyświetlać wyłącznie w ramach przedsiębiorstwa Użytkownika pod warunkiem zachowania wszelkich uwag dotyczących praw własności. Użytkownik nie ma prawa wykonywać na podstawie tych publikacji ani ich fragmentów prac pochodnych, kopiować ich, dystrybuować ani wyświetlać poza przedsiębiorstwem Użytkownika bez wyraźnej zgody IBM.

Z wyjątkiem zezwoleń wyraźnie udzielonych w niniejszym dokumencie, nie udziela się jakichkolwiek innych zezwoleń, licencji ani praw, wyraźnych czy domniemanych, odnoszących się do tych publikacji czy jakichkolwiek informacji, danych, oprogramowania lub innej własności intelektualnej, o których mowa w niniejszym dokumencie.

IBM zastrzega sobie prawo do anulowania zezwolenia przyznanego w niniejszym dokumencie w każdej sytuacji, gdy, według uznania IBM, korzystanie z tych publikacji jest szkodliwe dla IBM lub jeśli IBM uzna, że warunki niniejszego dokumentu nie są przestrzegane.

Użytkownik ma prawo pobierać, eksportować lub reeksportować niniejsze informacje pod warunkiem zachowania bezwzględnej i pełnej zgodności z obowiązującym prawem i przepisami, w tym ze wszelkimi prawami i przepisami eksportowymi Stanów Zjednoczonych.

IBM NIE UDZIELA JAKICHKOLWIEK GWARANCJI, W TYM TAKŻE RĘKOJMI, DOTYCZĄCYCH TREŚCI TYCH PUBLIKACJI. PUBLIKACJE TE SĄ DOSTARCZANE W STANIE, W JAKIM SIĘ ZNAJDUJĄ (″AS IS″) BEZ UDZIELANIA JAKICHKOLWIEK GWARANCJI, W TYM TAKŻE RĘKOJMI, WYRAŹNYCH CZY DOMNIEMANYCH, A W SZCZEGÓLNOŚCI DOMNIEMANYCH GWARANCJI PRZYDATNOŚCI HANDLOWEJ, PRZYDATNOŚCI DO OKREŚLONEGO CELU ORAZ NIENARUSZANIA PRAW STRON TRZECICH.

Dodatek. Uwagi

Niniejsza publikacja została przygotowana z myślą o produktach i usługach oferowanych w Stanach Zjednoczonych.

IBM może nie oferować w innych krajach produktów, usług lub opcji, omawianych w tej publikacji. Informacje o produktach i usługach dostępnych w danym kraju można uzyskać od lokalnego przedstawiciela IBM. Odwołanie do produktu, programu lub usługi IBM nie oznacza, że można użyć wyłącznie tego produktu, programu lub usługi. Zamiast nich można zastosować ich odpowiednik funkcjonalny pod warunkiem, że nie narusza to praw własności intelektualnej IBM. Jednakże cała odpowiedzialność za ocenę przydatności i sprawdzenie działania produktu, programu lub usługi pochodzących od producenta innego niż IBM spoczywa na użytkowniku.

IBM może posiadać patenty lub złożone wnioski patentowe na towary i usługi, o których mowa w niniejszej publikacji. Przedstawienie niniejszej publikacji nie daje żadnych uprawnień licencyjnych do tychże patentów. Pisemne zapytania w sprawie licencji można przesyłać na adres:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Zapytania w sprawie licencji na informacje dotyczące zestawów znaków dwubajtowych (DBCS) należy kierować do lokalnych działów własności intelektualnej IBM (IBM Intellectual Property Department) lub zgłaszać na piśmie pod adresem:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokio 106-0032, Japonia

Poniższy akapit nie obowiązuje w Wielkiej Brytanii, a także w innych krajach, w których jego treść pozostaje w sprzeczności z przepisami prawa miejscowego: INTERNATIONAL BUSINESS MACHINES CORPORATION DOSTARCZA TĘ PUBLIKACJĘ W STANIE, W JAKIM SIĘ ZNAJDUJE (“AS IS”), BEZ UDZIELANIA JAKICHKOLWIEK GWARANCJI (W TYM TAKŻE RĘKOJMI), WYRAŹNYCH LUB DOMNIEMANYCH, A W SZCZEGÓLNOŚCI DOMNIEMANYCH GWARANCJI PRZYDATNOŚCI HANDLOWEJ ORAZ PRZYDATNOŚCI DO OKREŚLONEGO CELU LUB GWARANCJI, ŻE PUBLIKACJA TA NIE NARUSZA PRAW STRON TRZECICH. Ustawodawstwa niektórych krajów nie dopuszczają zastrzeżeń dotyczących gwarancji wyraźnych lub domniemanych w odniesieniu do pewnych transakcji; w takiej sytuacji powyższe zdanie nie ma zastosowania.

Informacje zawarte w niniejszej publikacji mogą zawierać nieścisłości techniczne lub błędy typograficzne. Informacje te są okresowo aktualizowane, a zmiany te zostaną uwzględnione w kolejnych wydaniach tej publikacji. IBM zastrzega sobie prawo do wprowadzania ulepszeń i/lub zmian w produktach i/lub programach opisanych w tej publikacji w dowolnym czasie, bez wcześniejszego powiadomienia.

Wszelkie wzmianki w tej publikacji na temat stron internetowych innych firm zostały wprowadzone wyłącznie dla wygody użytkowników i w żadnym wypadku nie stanowią zachęty do ich odwiedzania. Materiały dostępne na tych stronach nie są częścią materiałów opracowanych do tego produktu IBM, a użytkownik korzysta z nich na własną odpowiedzialność.

IBM ma prawo do używania i rozpowszechniania informacji przysłanych przez użytkownika w dowolny sposób, jaki uzna za właściwy, bez żadnych zobowiązań wobec ich autora.

Licencjobiorcy tego programu, którzy chcieliby uzyskać informacje na temat programu w celu: (i) wdrożenia wymiany informacji między niezależnie utworzonymi programami i innymi programami (łącznie z tym opisywanym) oraz (ii) wspólnego wykorzystywania wymienianych informacji, powinni skontaktować się z:

IBM Corporation
Software Interoperability Coordinator, Department 49XA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Informacje takie mogą być udostępnione, o ile spełnione zostaną odpowiednie warunki, w tym, w niektórych przypadkach, uiszczenie odpowiedniej opłaty.

Licencjonowany program opisany w niniejszej publikacji oraz wszystkie inne licencjonowane materiały dostępne dla tego programu są dostarczane przez IBM na warunkach określonych w Umowie IBM z Klientem, Międzynarodowej Umowie Licencyjnej IBM na Program, Licencyjnej Umowie IBM dla Kodu Maszynowego lub w innych podobnych umowach zawartych między IBM i użytkownikami.

Wszelkie dane dotyczące wydajności zostały zebrane w kontrolowanym środowisku. W związku z tym rezultaty uzyskane w innych środowiskach operacyjnych mogą się znacząco różnić. Niektóre pomiary mogły być dokonywane na systemach będących w fazie rozwoju i nie ma gwarancji, że pomiary te wykonane na ogólnie dostępnych systemach dadzą takie same wyniki. Niektóre z pomiarów mogły być estymowane przez ekstrapolację. Rzeczywiste wyniki mogą być inne. Użytkownicy powinni we własnym zakresie sprawdzić odpowiednie dane dla ich środowiska.

Informacje dotyczące produktów firm innych niż IBM pochodzą od dostawców tych produktów, z opublikowanych przez nich zapowiedzi lub innych powszechnie dostępnych źródeł. Firma IBM nie testowała tych produktów i nie może potwierdzić dokładności pomiarów wydajności, kompatybilności ani żadnych innych danych związanych z tymi produktami. Pytania dotyczące produktów firm innych niż IBM należy kierować do dostawców tych produktów.

Wszelkie stwierdzenia dotyczące przyszłych kierunków rozwoju i zamierzeń IBM mogą zostać zmienione lub wycofane bez powiadomienia.

Wszystkie przedstawione ceny IBM są aktualnymi sugerowanymi cenami detalicznymi IBM i podlegają zmianie bez powiadomienia. Ceny dealerów mogą się od nich różnić.

Niniejsze informacje podawane są jedynie do celów związanych z planowaniem. Informacje zawarte w niniejszym dokumencie podlegają zmianie przed udostępnieniem opisanych produktów.

Publikacja ta zawiera przykładowe dane i raporty używane w codziennych operacjach działalności gospodarczej. W celu kompleksowego ich zilustrowania, podane przykłady zawierają nazwiska osób prywatnych, nazwy przedsiębiorstw oraz nazwy produktów. Wszystkie te nazwy/nazwiska są fikcyjne i jakiekolwiek podobieństwo do istniejących nazw/nazwisk i adresów jest całkowicie przypadkowe.

LICENCJA W ZAKRESIE PRAW AUTORSKICH:

Niniejsza publikacja zawiera przykładowe aplikacje w kodzie źródłowym, ilustrujące techniki programowania w różnych systemach operacyjnych. Użytkownik może kopiować, modyfikować i dystrybuować te programy przykładowe w dowolnej formie bez uiszczania opłat na rzecz IBM, w celu projektowania, używania, sprzedaży lub dystrybucji aplikacji zgodnych z aplikacyjnym interfejsem programowym dla tego systemu operacyjnego, dla którego napisane zostały programy przykładowe. Programy przykładowe nie zostały gruntownie przetestowane. IBM nie może zatem gwarantować ani sugerować niezawodności, użyteczności i funkcjonalności tych programów.

Każda kopia programu przykładowego lub jakikolwiek jego fragment, jak też jakiekolwiek prace pochodne muszą zawierać następujące uwagi dotyczące praw autorskich:

© (nazwa przedsiębiorstwa użytkownika) (rok). Fragmenty tego kodu pochodzą z programów przykładowych IBM Corp. © Copyright IBM Corp. (wpisać rok lub lata). Wszelkie prawa zastrzeżone.

W przypadku przeglądania niniejszych informacji w formie elektronicznej, zdjęcia i kolorowe ilustracje mogą nie być wyświetlane.

Znaki towarowe

Następujące nazwy są znakami towarowymi International Business Machines Corporation w Stanach Zjednoczonych i/lub w innych krajach:

AIX
Distributed Relational Database Architecture
Domino
DRDA
eServer
i5/OS
IBM
iSeries
Lotus Notes
NetServer
OS/400
pSeries
RACF
RDN
Tivoli
WebSphere
xSeries
z/OS
zSeries

Lotus, Lotus Notes, Freelance i WordPro są znakami towarowymi International Business Machines Corporation oraz Lotus Development Corporation w Stanach Zjednoczonych i/lub w innych krajach.

Microsoft, Windows, Windows NT i logo Windows są znakami towarowymi Microsoft Corporation w Stanach Zjednoczonych i/lub w innych krajach.

Linux jest znakiem towarowym Linusa Torvaldsa w Stanach Zjednoczonych i/lub w innych krajach.

UNIX jest zastrzeżonym znakiem towarowym The Open Group w Stanach Zjednoczonych i w innych krajach.

Nazwy innych przedsiębiorstw, produktów i usług mogą być znakami towarowymi lub znakami usług innych podmiotów.

Warunki

Zezwolenie na korzystanie z tych publikacji jest przyznawane na poniższych warunkach.

Użytek osobisty: Użytkownik ma prawo kopiować te publikacje do własnego, niekomercyjnego użytku pod warunkiem zachowania wszelkich uwag dotyczących praw własności. Użytkownik nie ma prawa dystrybuować ani wyświetlać tych publikacji czy ich części, ani też wykonywać na ich podstawie prac pochodnych bez wyraźnej zgody IBM.

Użytek służbowy: Użytkownik ma prawo kopiować te publikacje, dystrybuować je i wyświetlać wyłącznie w ramach przedsiębiorstwa Użytkownika pod warunkiem zachowania wszelkich uwag dotyczących praw własności. Użytkownik nie ma prawa wykonywać na podstawie tych publikacji ani ich fragmentów prac pochodnych, kopiować ich, dystrybuować ani wyświetlać poza przedsiębiorstwem Użytkownika bez wyraźnej zgody IBM.

Z wyjątkiem zezwoleń wyraźnie udzielonych w niniejszym dokumencie, nie udziela się jakichkolwiek innych zezwoleń, licencji ani praw, wyraźnych czy domniemanych, odnoszących się do tych publikacji czy jakichkolwiek informacji, danych, oprogramowania lub innej własności intelektualnej, o których mowa w niniejszym dokumencie.

IBM zastrzega sobie prawo do anulowania zezwolenia przyznanego w niniejszym dokumencie w każdej sytuacji, gdy, według uznania IBM, korzystanie z tych publikacji jest szkodliwe dla IBM lub jeśli IBM uzna, że warunki niniejszego dokumentu nie są przestrzegane.

Użytkownik ma prawo pobierać, eksportować lub reeksportować niniejsze informacje pod warunkiem zachowania bezwzględnej i pełnej zgodności z obowiązującym prawem i przepisami, w tym ze wszelkimi prawami i przepisami eksportowymi Stanów Zjednoczonych.

IBM NIE UDZIELA JAKICHKOLWIEK GWARANCJI, W TYM TAKŻE RĘKOJMI, DOTYCZĄCYCH TREŚCI TYCH PUBLIKACJI. PUBLIKACJE TE SĄ DOSTARCZANE W STANIE, W JAKIM SIĘ ZNAJDUJĄ (″AS IS″) BEZ UDZIELANIA JAKICHKOLWIEK GWARANCJI, W TYM TAKŻE RĘKOJMI, WYRAŹNYCH CZY DOMNIEMANYCH, A W SZCZEGÓLNOŚCI DOMNIEMANYCH GWARANCJI PRZYDATNOŚCI HANDLOWEJ, PRZYDATNOŚCI DO OKREŚLONEGO CELU ORAZ NIENARUSZANIA PRAW STRON TRZECICH.