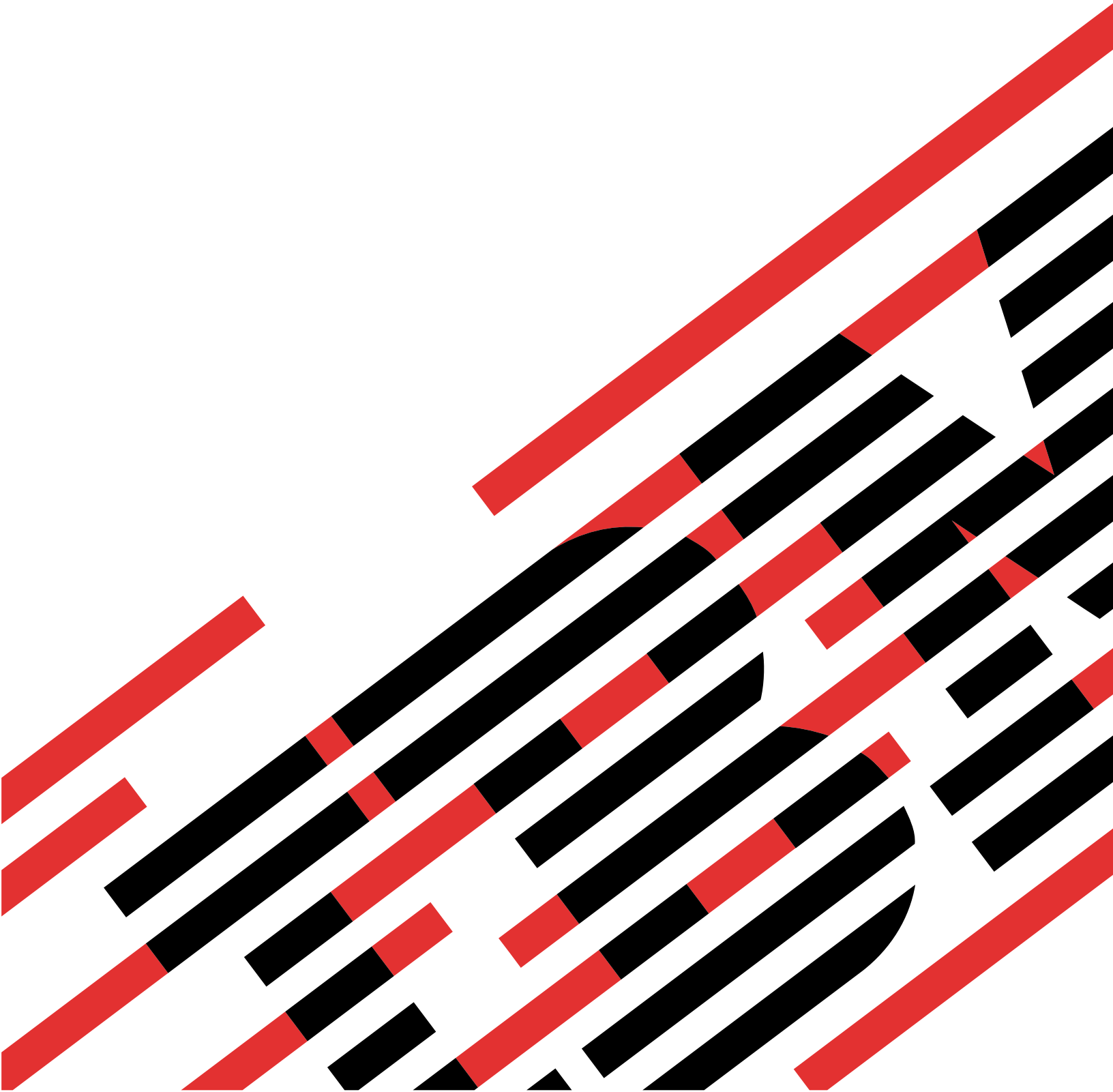
IBM

eserver

iSeries

Enterprise Identity Mapping



IBM

@server

iSeries

Enterprise Identity Mapping

Spis treści

Enterprise Identity Mapping (EIM)

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.

EIM jest mechanizmem odwzorowywania (wiązania) osoby lub jednostki z odpowiednimi tożsamościami użytkowników w różnych rejestrach w przedsiębiorstwie. EIM udostępnia funkcje API umożliwiające tworzenie i zarządzanie tymi relacjami odwzorowywania tożsamości, a także funkcje API używane przez aplikacje do odpytywania tych informacji. Ponadto system OS/400(R) używa EIM i funkcji Kerberos do obsługi środowiska pojedynczego wpisywania się.

Program iSeries Navigator, który jest graficznym interfejsem użytkownika serwera iSeries, udostępnia kreatory umożliwiające konfigurowanie i zarządzanie EIM. Ponadto za pomocą tego programu administratorzy mogą zarządzać relacjami EIM profili użytkowników.

Serwer iSeries(TM) używa EIM, aby umożliwić interfejsom OS/400 uwierzytelnianie użytkowników za pomocą usługi uwierzytelniania sieciowego. Aplikacje i system OS/400 mogą akceptować bilety Kerberos i używać EIM do znalezienia profilu użytkownika reprezentującego tę samą osobę, co bilet Kerberos.

Wymienione poniżej tematy zawierają konkretne informacje o EIM.

Drukowanie tego tematu
Drukuje plik PDF zawierający dany temat dotyczący EIM i inne powiązane z nim tematy.

Przegląd EIM
Opisuje, w rozwiązaniu których problemów EIM może pomóc, podaje aktualnie stosowane rozwiązania tych problemów i informuje, dlaczego rozwiązanie z wykorzystaniem EIM jest lepsze.

Koncepcje dotyczące EIM
Koncepcje dotyczące EIM służące do pomyślnej implementacji.

Koncepcje dotyczące LDAP w kontekście EIM
Koncepcje dotyczące protokołu LDAP podane po to, aby móc pomyślnie zaimplementować EIM.

Obsługa pojedynczego wpisywania się
Opisuje korzyści wynikające z zastosowania EIM do wpisywania się użytkowników.

Planowanie EIM
Rozpoczęcie konfigurowania EIM wymaga sprawdzenia, czy skonfigurowane są wszystkie wymagane usługi i aplikacje.

Konfigurowanie EIM
Opisuje wykorzystanie kreatora konfiguracji EIM do rozpoczęcia pracy z EIM.

Zarządzanie EIM
Ułatwia zarządzanie właściwościami EIM, domenami EIM, rejestrami użytkowników, uprawnieniami użytkowników EIM i innymi elementami.

Funkcje API EIM
Informuje o użytkowaniu funkcji API EIM w aplikacjach i sieci.

Rozwiązywanie problemów dotyczących EIM
Opisuje rozwiązania często występujących problemów i błędów, które mogą powstać podczas korzystania z EIM w sieci.

Informacje pokrewne dotyczące EIM
Zapoznaje z informacjami pokrewnymi dotyczącymi EIM.

Drukowanie tego tematu

Aby przejrzeć lub pobrać wersję PDF tej dokumentacji, wybierz Enterprise Identity Mapping

(około 390 kB, 50 stron).

Inne informacje

Możesz przejrzeć lub pobrać następujące tematy pokrewne:

- Usługi uwierzytelniania sieciowego (około 199 kB, 60 stron) zawiera informacje na temat sposobu konfigurowania usług uwierzytelniania sieciowego wraz z EIM w celu utworzenia środowiska pojedynczego wpisywania się.
- Directory Services (LDAP) (około 323 kB, 66 stron) zawiera informacje na temat sposobu konfigurowania serwera LDAP, którego można użyć jako kontrolera domeny EIM, oraz informacje dotyczące zaawansowanego konfigurowania LDAP.

Zapisywanie plików w formacie PDF

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

1. Otwórz dany plik w formacie PDF w przeglądarce (kliknij jeden z dostępnych powyżej odsyłaczy).
2. W menu przeglądarki kliknij **Plik**.
3. Kliknij **Zapisz jako...**
4. Przejdź do katalogu, w którym chcesz zapisać dany plik.
5. Kliknij **Zapisz**.

Pobieranie programu Adobe Acrobat Reader

Jeśli potrzebujesz programu Adobe Acrobat Reader umożliwiającego przejrzenie lub wydrukowanie tych plików PDF, możesz pobrać jego kopię z serwisu WWW firmy Adobe (www.adobe.com/prodindex/acrobat/readstep.html)

.

Przegląd EIM

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. Enterprise Identity Mapping (EIM) jest opracowaną przez firmę IBM

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

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 wpisywania się. 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

Zaletą produktu EIM jest nowatorskie a jednocześnie niedrogie rozwiązanie umożliwiające łatwe zarządzanie w przedsiębiorstwie wieloma rejestrami i tożsamościami użytkowników. 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.

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. Na przykład administrator może odwzorować tożsamość w systemie SAP (a jeszcze lepiej: system SAP może sam wykonać odwzorowanie) w celu uzyskania dostępu do zasobów SAP.

Aby używać odwzorowywania tożsamości, administratorzy muszą:

1. Utworzyć identyfikatory EIM reprezentujące ludzi lub jednostki w przedsiębiorstwie.
2. Utworzyć definicje rejestrów EIM opisujące istniejące w przedsiębiorstwie rejestry użytkowników.
3. Zdefiniować relacje między tożsamościami użytkowników w tych rejestrach a utworzonymi identyfikatorami EIM.

W istniejących rejestrach użytkowników nie są wymagane żadne zmiany w kodzie. Administrator nie musi tworzyć odwzorowań dla wszystkich tożsamości w rejestrze użytkowników. EIM dopuszcza odwzorowania jeden-do-wielu (w jednym rejestrze użytkowników dopuszczalne jest istnienie pojedynczego użytkownika z więcej niż jedną tożsamością). EIM dopuszcza także odwzorowania wiele-do-jednego (wielu użytkowników współużytkuje tę samą tożsamość użytkownika w jednym rejestrze użytkowników; istnieje taka możliwość, ale się jej nie poleca). W EIM administrator może reprezentować dowolny rejestr użytkowników dowolnego typu.

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. Administratorzy zarządzają tymi danymi 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.

Koncepcje dotyczące EIM

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 działają jako klienci EIM i zawierają aplikacje obsługujące EIM, które za pomocą operacji wyszukiwania EIM żądają danych EIM

6

. Kontroler domeny

1

przechowuje informacje na temat domeny EIM

2

zawierające identyfikator EIM

3

, powiązania

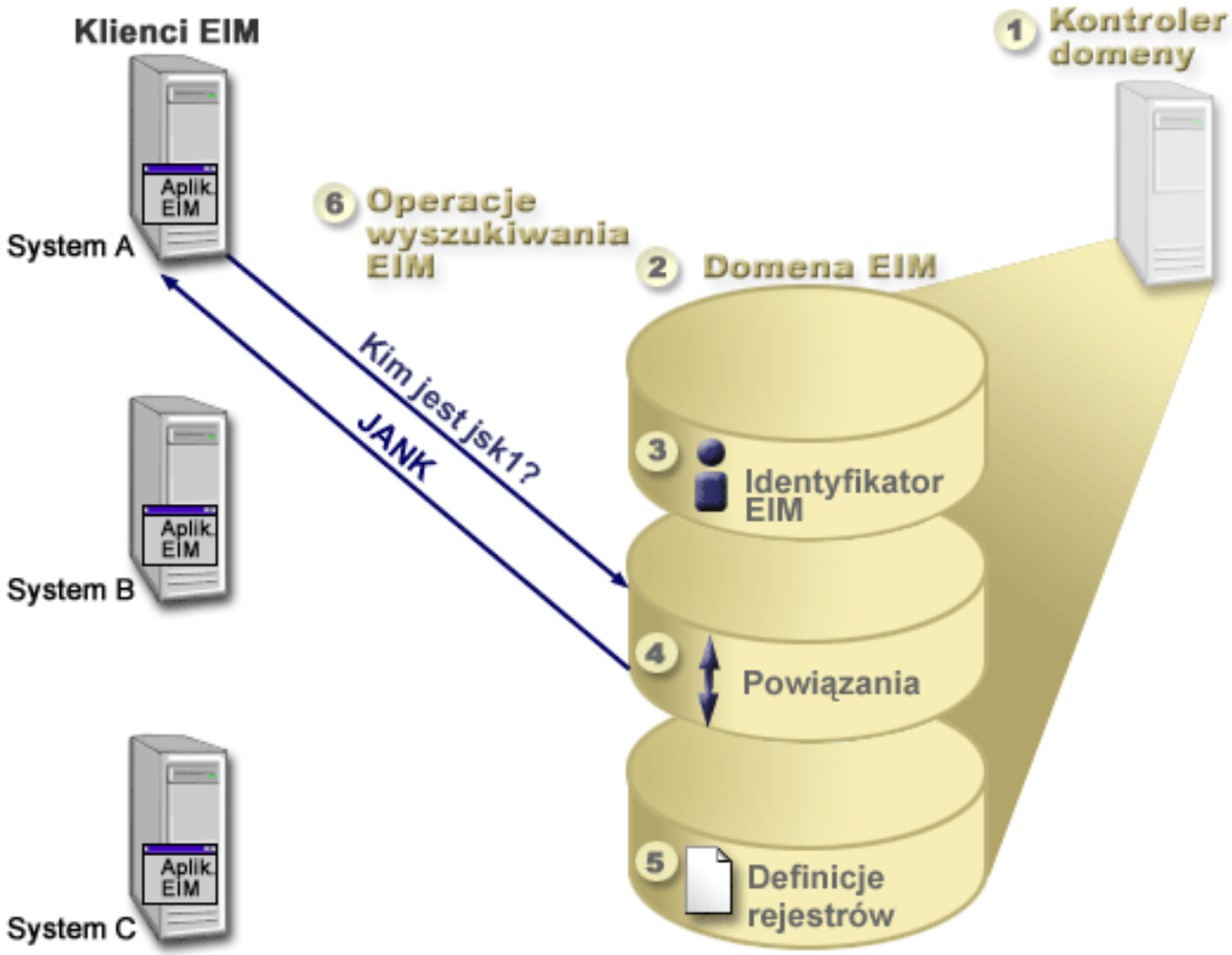
4

między tymi identyfikatorami EIM a tożsamościami użytkowników i definicje rejestrów EIM

5

.

Rysunek 1: Przykład implementacji EIM



Więcej informacji na temat koncepcji dotyczących EIM można uzyskać wybierając poniższe odsyłacze:

- Kontroler domeny EIM
- Domena EIM
- Identyfikator EIM
- Definicje rejestrów EIM
- Powiązania EIM
- Operacja wyszukiwania EIM
- Uprawnienia EIM

Kontroler 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. W przedsiębiorstwie musi istnieć co najmniej jeden kontroler domeny EIM.

Obecnie można skonfigurować niektóre platformy IBM

tak, aby działały jako kontrolery domen 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 operacji wyszukiwania EIM.

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.

Domena EIM

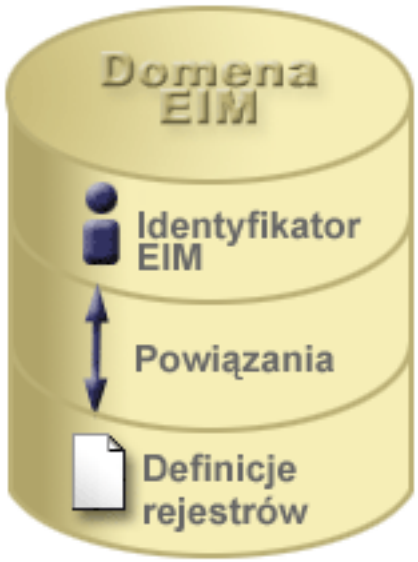
Domena EIM jest katalogiem na serwerze LDAP, który zawiera dane EIM dla przedsiębiorstwa. Domena EIM jest kolekcją wszystkich identyfikatorów EIM, powiązań EIM i rejestrów użytkowników, które zostały zdefiniowane w tej domenie. Systemy (klienci EIM) należące do domeny używają danych domeny do operacji 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. Ponieważ EIM śledzi tylko informacje o relacjach, nie ma czego synchronizować między rejestrami użytkowników a EIM.

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 ludźmi lub jednostkami reprezentowanymi w przedsiębiorstwie przez te tożsamości.

Rysunek 2: Domena EIM i dane w niej przechowywane



Do danych EIM należą:

- **Identyfikatory EIM.** Każdy tworzony identyfikator EIM reprezentuje w przedsiębiorstwie osobę lub jednostkę (taką jak serwer wydruków lub serwer plików). Więcej potrzebnych informacji zawiera temat Identyfikator EIM.
- **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. Więcej potrzebnych informacji zawiera temat Definicje rejestrów EIM.
- **Powiązania EIM.** Każde tworzone powiązanie EIM reprezentuje relację między identyfikatorem EIM a powiązaną tożsamością w przedsiębiorstwie. Powiązania tożsamości tworzy się w rejestrach użytkowników należących do domeny EIM. Powiązania zawierają informacje wiążące identyfikator EIM z konkretną tożsamością użytkownika w konkretnym rejestrze użytkowników. Dlatego powiązania muszą być zdefiniowane, tak aby klienci EIM mogli używać funkcji API EIM do pomyślnego wykonania operacji wyszukiwania EIM. Operacje te wyszukują w domenie EIM zdefiniowane powiązania między identyfikatorami EIM a tożsamościami użytkowników w rozpoznanych rejestrach użytkowników. Więcej potrzebnych informacji zawiera temat Operacje wyszukiwania EIM.

Po utworzeniu identyfikatorów EIM, definicji rejestrów i powiązań można rozpocząć używanie EIM, dzięki czemu praca z tożsamościami w przedsiębiorstwie stanie się łatwiejsza.

Identyfikator EIM

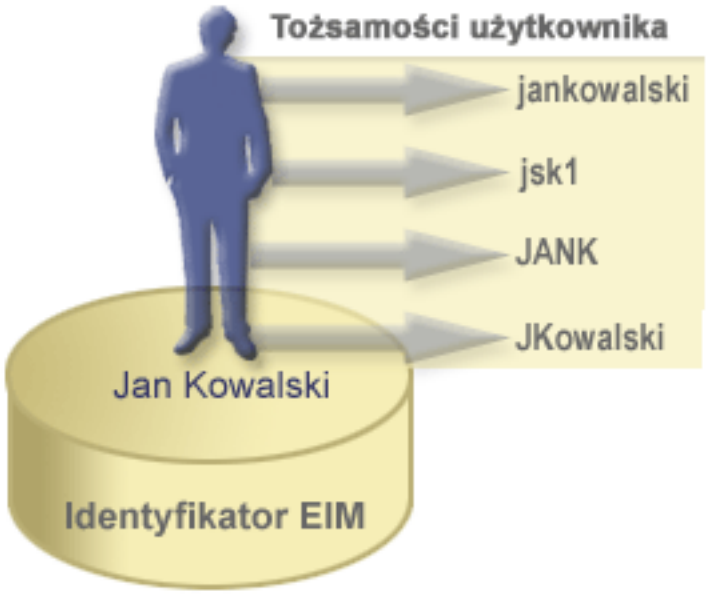
Identyfikator EIM reprezentuje osobę lub jednostkę w przedsiębiorstwie. Typowa sieć składa się z różnych platform sprzętowych oraz aplikacji i powiązanych z nimi rejestrów użytkowników. W większości platform i w wielu aplikacjach używane są rejestry użytkowników specyficzne dla danej platformy lub aplikacji.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

Utworzenie identyfikatora EIM i powiązanie go z różnymi tożsamościami użytkownika dla osoby lub jednostki ułatwia zbudowanie heterogenicznych, wielowarstwowych aplikacji, na przykład środowiska pojedynczego wpisywania się. 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 cztery tożsamości: jankowalski, jsk1, JANK i JKowalski.

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

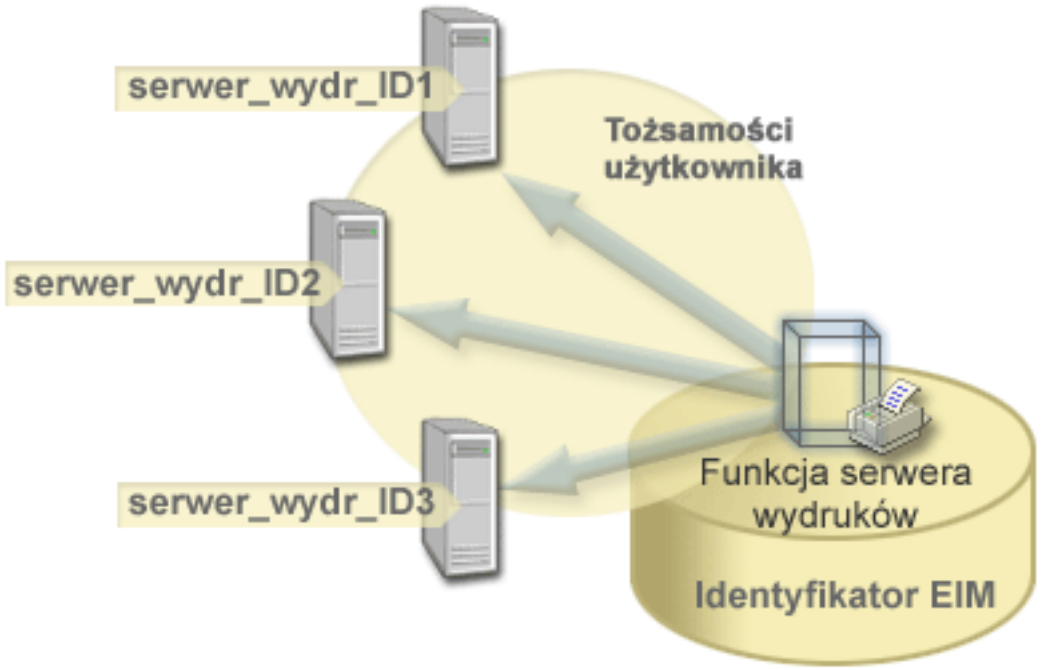


W EIM można tworzyć powiązania definiujące relacje między identyfikatorem Jan Kowalski a każdą z jego różnych tożsamości. Tworząc takie powiązania w celu zdefiniowania relacji, użytkownicy mogą pisać aplikacje używające funkcji API EIM do wyszukania potrzebnej, ale nieznanej tożsamości użytkownika w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

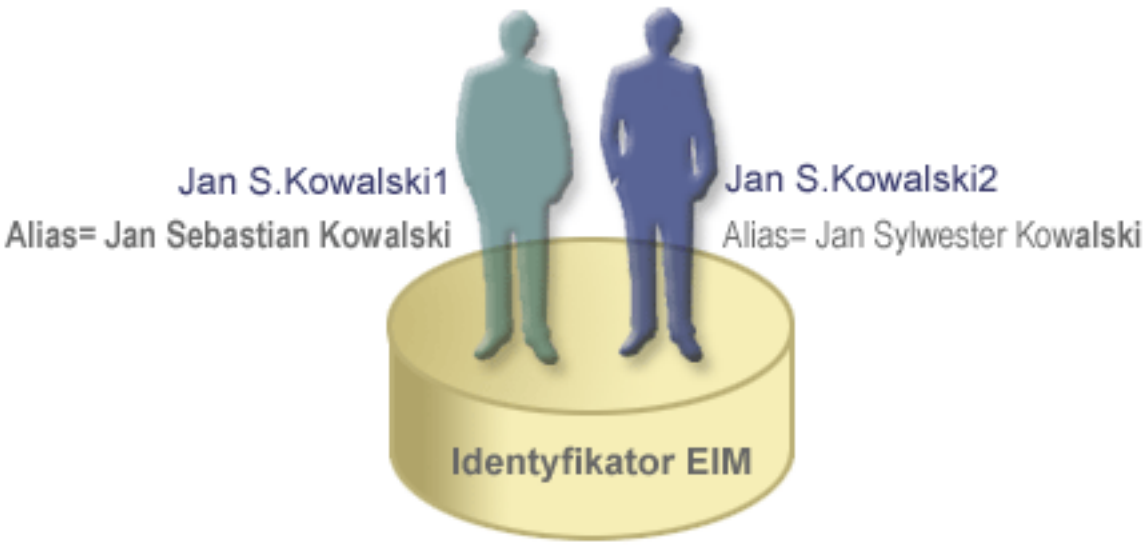
Identyfikatory EIM a używanie aliasów

Dla identyfikatorów EIM można tworzyć aliasy. 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.

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. Informacje te mogą być także wykorzystane podczas wykonywania operacji wyszukiwania EIM prowadzonej w celu odróżnienia użytkowników reprezentowanych przez identyfikator. Na przykład 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.

Każdy identyfikator EIM może mieć wiele aliasów służących do określenia, którego użytkownika *Jan S. Kowalski* ten identyfikator reprezentuje. Administrator EIM może dodać jeszcze jeden alias dla każdego identyfikatora EIM w celu pewniejszego ich odróżnienia. Dodatkowe aliasy mogą na przykład zawierać numery pracowników przypisane poszczególnym użytkownikom, numer wydziału, stanowisko lub inny wyróżniający atrybut.

Definicje rejestrów EIM

Definicja rejestru EIM reprezentuje rzeczywisty rejestr użytkowników istniejący 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$^{(R)}$). 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. Innymi przykładami często stosowanych rejestrów są centra dystrybucji kluczy Kerberos i rejestr profili użytkowników systemu OS/400.

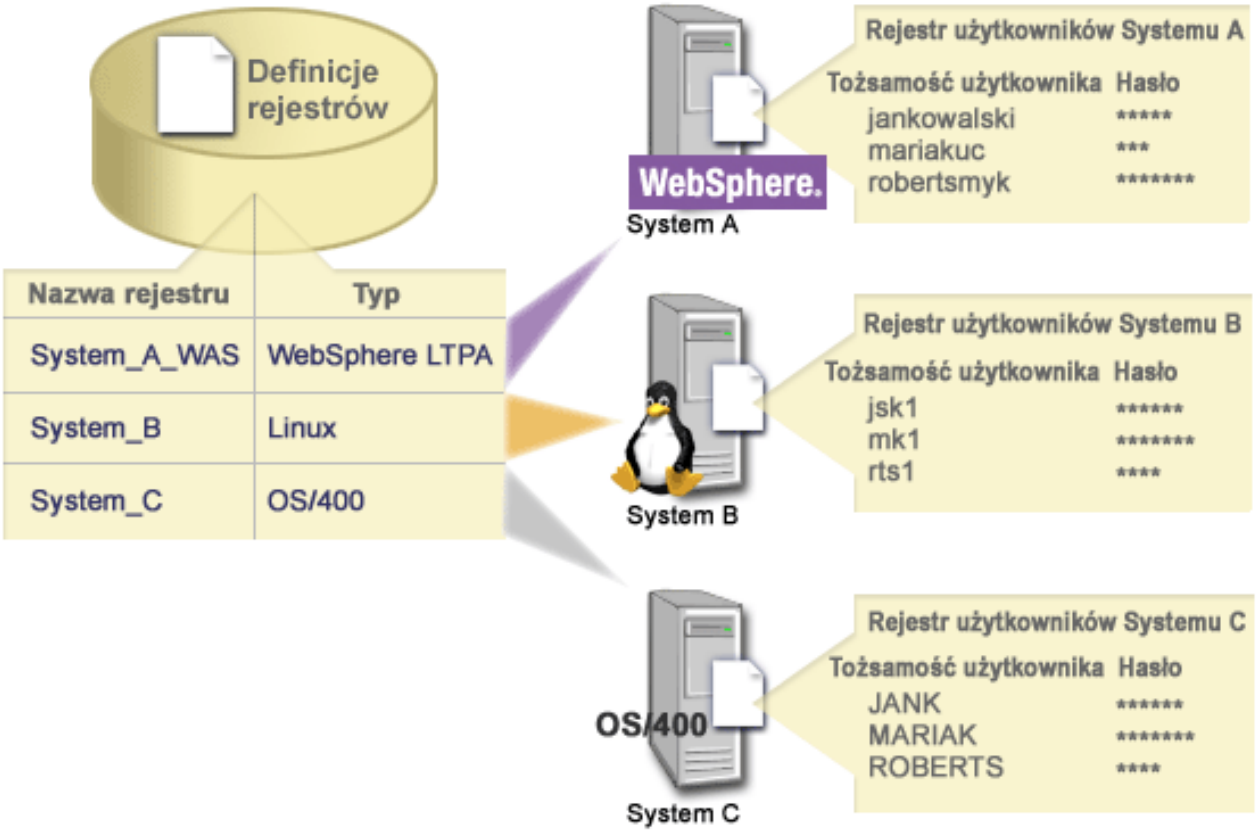
Definicje rejestrów EIM zawierają informacje dotyczące rejestrów użytkowników w przedsiębiorstwie. Administrator definiuje te rejestry w EIM, dostarczając następujące informacje:

- unikalna, arbitralna nazwa rejestru EIM,
- typ rejestru użytkowników.

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.

Na rysunku 6 administrator utworzył definicje rejestrów EIM dla rejestrów użytkowników reprezentujących system A, system B i system C. System A zawiera rejestr użytkowników dla WebSphere Lightweight Third-Party Authentication (LTPA). 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 podanym przykładzie administrator identyfikuje konkretną instancję rejestru użytkowników za pomocą System_A_WAS jako nazwy definicji rejestru. Oprócz nazwy administrator podaje także typ rejestru WebSphere LTPA.

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



Można także zdefiniować 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 RACF. Więcej szczegółów podano w przykładzie zawartym w temacie Definicje rejestrów systemu i aplikacji.

Definicje rejestrów EIM a używanie aliasów

Dla definicji rejestrów EIM można tworzyć aliasy. Można użyć predefiniowanego typu aliasu, można też zdefiniować własny typ aliasu. Do predefiniowanych typów aliasu należą:

- nazwa hosta systemu nazw domen (DNS),
- dziedzina Kerberos,
- nazwa wyróżniająca wystawcy,
- główna nazwa wyróżniająca,
- adres TCP/IP,
- nazwa hosta DNS LDAP.

Obsługa aliasów umożliwia programistom pisanie aplikacji nawet wtedy, gdy nie znają arbitralnej nazwy 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.

Gdy administrator dodaje alias do definicji rejestru EIM, aplikacja może wykonać wyszukiwania aliasu w celu znalezienia nazwy rejestru EIM podczas inicjowania. Wyszukanie aliasu pozwala aplikacji określić nazwę lub nazwy rejestrów EIM, które mają być używane jako dane wejściowe funkcji API wykonujących operacje wyszukiwania EIM.

Definicje rejestrów systemu i aplikacji

Niektóre aplikacje używają podzbioru tożsamości użytkownika w jednej instancji rejestru użytkowników. EIM pozwala administratorom na modelowanie tego scenariusza poprzez udostępnienie dwóch typów definicji rejestrów EIM: systemu i aplikacji.

Definicja rejestru systemu reprezentuje odrębny rejestr na stacji roboczej lub serwerze. Definicję rejestru systemu można utworzyć wtedy, gdy rejestr w przedsiębiorstwie ma jedną z następujących cech:

- jest on dostarczany przez system operacyjny, taki jak AIX(R), OS/400(R) lub produkt zarządzania ochroną, taki jak z/OS Security Server Resource Access Control Facility (RACF(R)),
- zawiera tożsamości użytkowników, które są unikalne dla konkretnej aplikacji, takie jak Lotus Notes(R),
- zawiera rozproszone tożsamości użytkowników, takie jak nazwy użytkowników protokołu Kerberos lub nazwy wyróżniające LDAP.

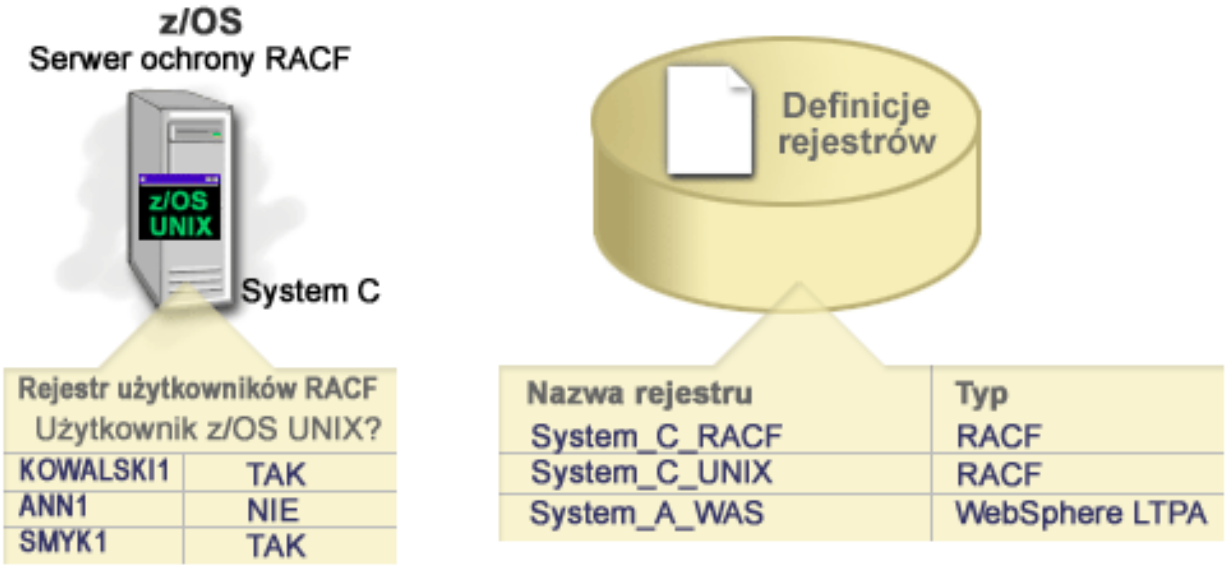
Definicja rejestru aplikacji reprezentuje podzbiór tożsamości użytkowników, które są zdefiniowane w rejestrze systemu. Tożsamości te współużytkują wspólny zbiór atrybutów lub cech, które umożliwiają im korzystanie z konkretnej aplikacji lub zbioru aplikacji. Definicję rejestru aplikacji można utworzyć wtedy, gdy tożsamości użytkowników mają następujące cechy:

- tożsamości użytkowników dla aplikacji lub zbioru aplikacji nie są przechowywane w rejestrze użytkowników specyficznym dla aplikacji lub zbioru aplikacji,
- tożsamości użytkowników dla aplikacji lub zbioru aplikacji są przechowywane w rejestrze systemu, który zawiera tożsamości użytkowników dla innych aplikacji.

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.

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 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



Powiązania EIM

Powiązanie EIM jest relacją między identyfikatorem EIM reprezentującym konkretną osobę a pojedynczą tożsamością użytkownika w rejestrze użytkowników 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. 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. Ten proces jest nazywany *odwzorowywaniem tożsamości*.

Przed utworzeniem powiązania 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.

Administrator może tworzyć różne typy powiązań między identyfikatorem EIM a tożsamością użytkownika w oparciu o sposób używania tożsamości użytkownika. 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 użytkowników w pojedynczym rejestrze użytkowników zarówno dla uwierzytelniania, jak i dla autoryzacji. Obecnie wykorzystując operacje wyszukiwania EIM aplikacje mogą używać do uwierzytelniania tożsamości

użytkowników zebranych w jednym rejestrze, podczas gdy do autoryzacji mogą używać powiązanych tożsamości użytkowników z innego rejestru użytkowników.

W EIM dostępne są trzy typy powiązań między identyfikatorem EIM a tożsamością użytkownika, które może zdefiniować administrator. Są to powiązania źródłowe, docelowe i administracyjne.

Powiązanie źródłowe

Jeśli tożsamość użytkownika jest używana do *uwierzytelniania*, powinna mieć powiązanie źródłowe z identyfikatorem EIM. 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 w operacji wyszukiwania EIM jako tożsamość docelowa zostanie użyta tożsamość użytkownika wyłącznie z powiązaniem źródłowym, nie zostaną zwrócone żadne powiązane tożsamości użytkownika.

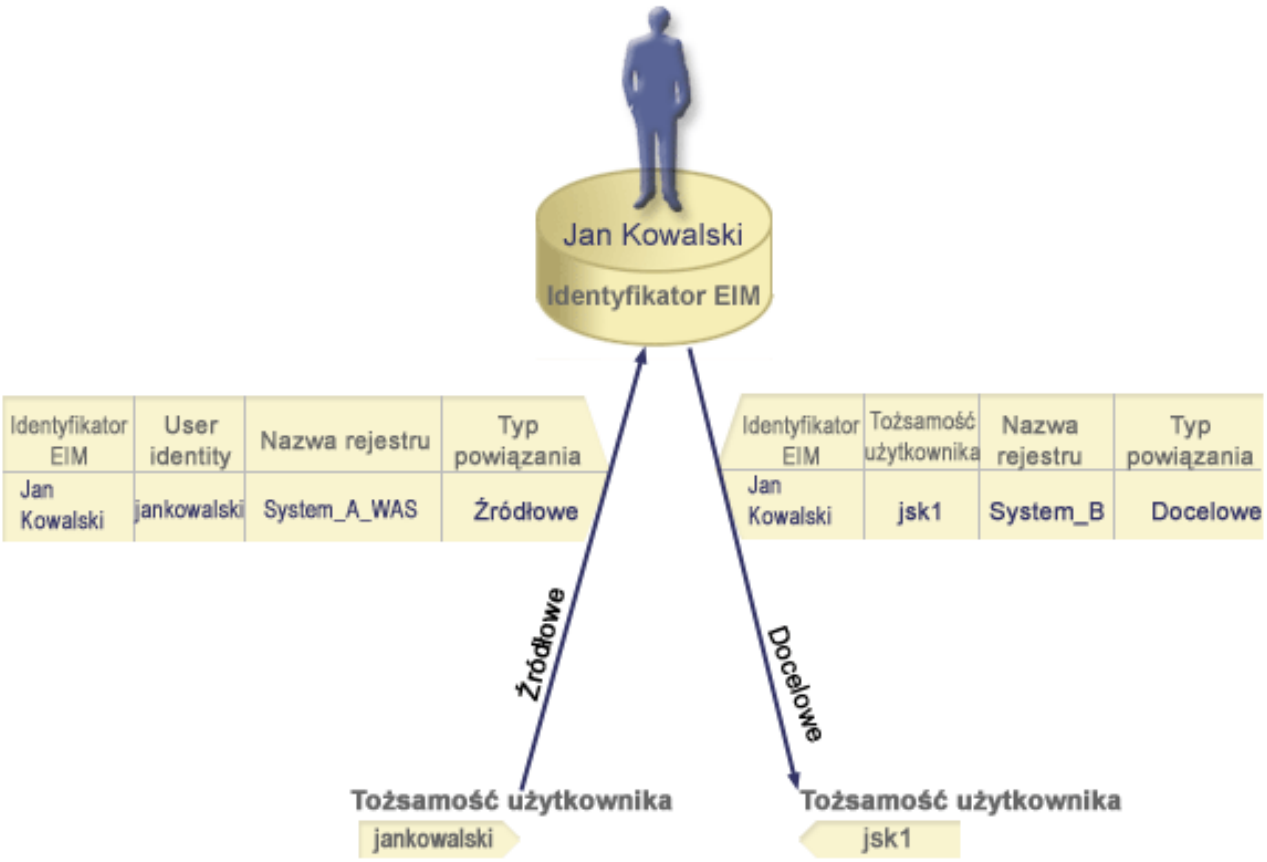
Powiązania docelowe

Jeśli tożsamość użytkownika jest używana do *autoryzacji*, a nie do uwierzytelniania, z identyfikatorem EIM powinna mieć ona powiązanie docelowe. Powiązanie docelowe umożliwia zwrócenie tożsamości użytkownika w wyniku wykonania operacji wyszukiwania EIM. Jeśli w operacji wyszukiwania EIM jako tożsamość źródłowa zostanie użyta tożsamość użytkownika wyłącznie z powiązaniem docelowym, nie zostaną zwrócone żadne powiązane tożsamości użytkownika.

Dla pojedynczej tożsamości użytkownika konieczne może być utworzenie zarówno powiązania docelowego, jak i źródłowego. 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 użytkownik zwykle uwierzytelnia się na platformie Windows i uruchamia aplikacje uzyskujące dostęp do serwera AIX. Ze względu na funkcję pełnioną przez danego użytkownika musi on czasami zalogować się bezpośrednio na serwerze AIX. W takiej sytuacji między tożsamością tego użytkownika systemu AIX a jego identyfikatorem EIM należy utworzyć zarówno powiązanie źródłowe, jak i docelowe. Tożsamości użytkowników reprezentujące użytkowników końcowych zwykle wymagają tylko powiązania docelowego.

Rysunek 6 przedstawia przykład powiązania źródłowego i docelowego. W tym przykładzie administrator utworzył dwa powiązania dla identyfikatora EIM Jan Kowalski, aby zdefiniować relację między tym identyfikatorem a dwoma powiązanymi tożsamościami użytkownika. Administrator utworzył powiązanie źródłowe dla jankowalski, tożsamość użytkownika WebSphere Lightweight Third-Party Authentication (LTPA) w rejestrze użytkowników System_A_WAS. Utworzył on także powiązanie docelowe dla jsk1, profil użytkownika OS/400 w rejestrze użytkowników systemu B. Powiązania te umożliwiają aplikacjom uzyskanie nieznanej tożsamości użytkownika (docelowa: jsk1) w oparciu o znaną tożsamość użytkownika (źródłowa: jankowalski) po wykonaniu operacji wyszukiwania EIM.

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



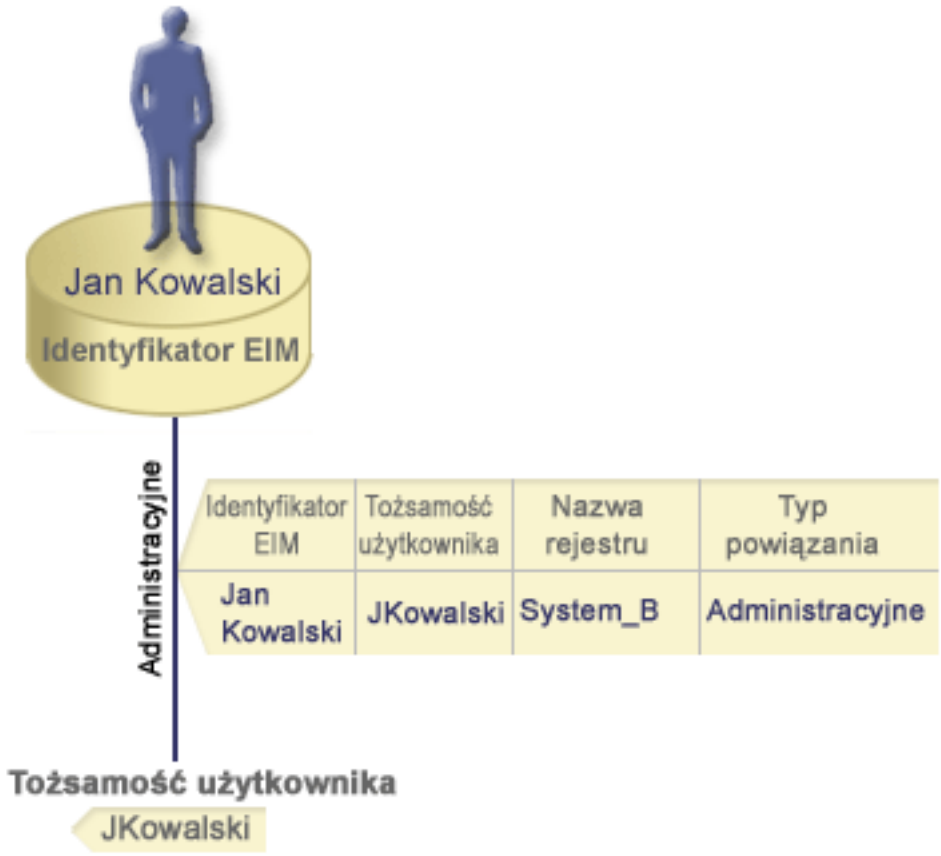
Powiązanie administracyjne

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.

Ze względu na charakter powiązania administracyjnego 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 Jan Kowalski ma jedną tożsamość użytkownika w systemie A i drugą tożsamość 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 obcego 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



Operacje wyszukiwania EIM

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.

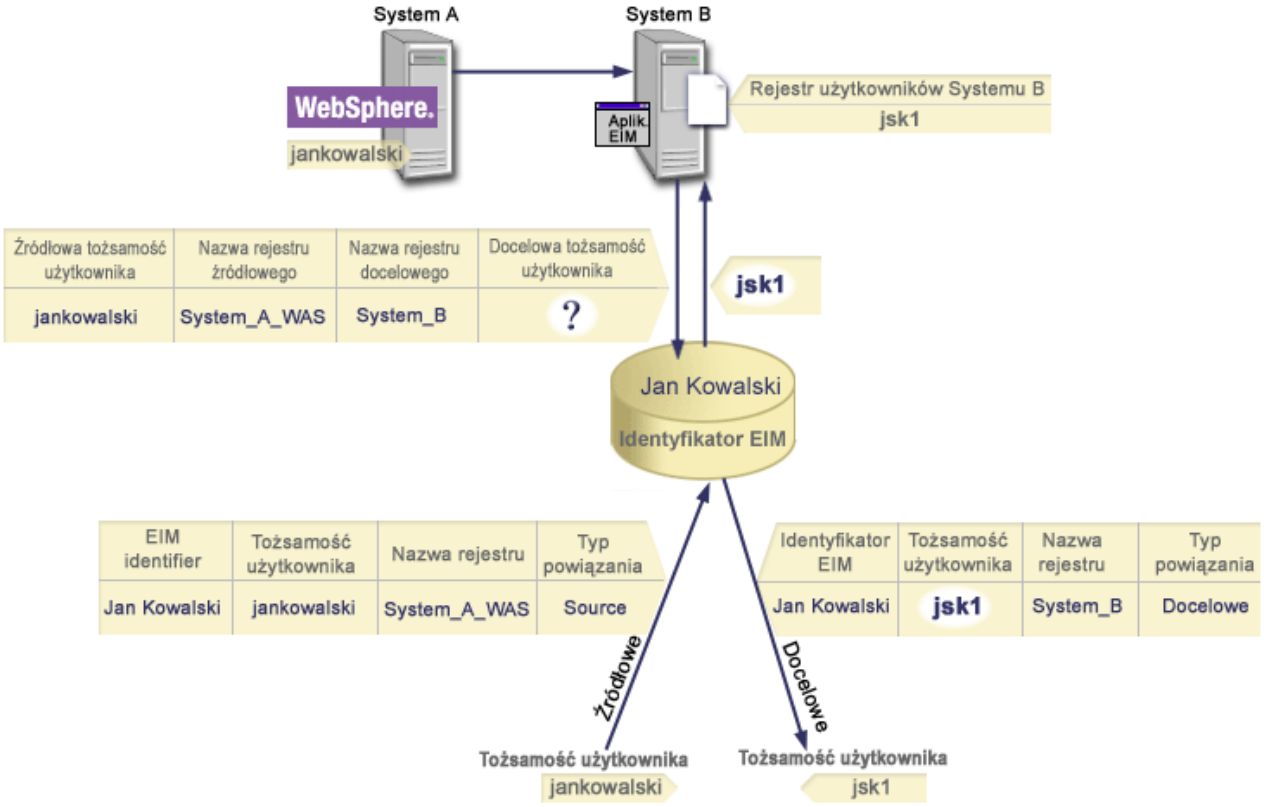
Gdy aplikacja dostarcza *tożsamość użytkownika jako źródło*, aplikacja ta musi także dostarczyć nazwę definicji rejestru EIM dla źródłowej tożsamości użytkownika i nazwę definicji rejestru EIM, który jest celem operacji wyszukiwania EIM. Aby tożsamość użytkownika mogła być używana jako źródło w operacji wyszukiwania EIM, musi ona mieć zdefiniowane powiązanie źródłowe.

Gdy aplikacja dostarcza *identyfikator EIM jako źródło* dla operacji wyszukiwania EIM, aplikacja ta musi także dostarczyć nazwę definicji rejestru EIM, który jest celem tej operacji wyszukiwania EIM. Aby tożsamość użytkownika została zwrócona jako cel dowolnego typu z operacji wyszukiwania EIM, dla tej tożsamości użytkownika musi być zdefiniowane powiązanie docelowe.

Dostarczone informacje są przekazywane do kontrolera domeny EIM, gdzie wszystkie informacje EIM są przechowywane, a operacja wyszukiwania EIM wyszukuje powiązania źródłowe odpowiadające podanym informacjom. W oparciu o identyfikator EIM (podany w funkcji API lub określony na podstawie informacji o powiązaniach źródłowych) operacja wyszukiwania EIM przeszukuje następnie powiązanie docelowe, aby znaleźć identyfikator zgodny z nazwą definicji docelowego rejestru EIM.

Na rysunku 10 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 rodzimy program w systemie B w celu uzyskania dostępu do danych w systemie B. Program rodzimy używa funkcji API EIM do wykonania operacji wyszukiwania EIM w oparciu o tożsamość użytkownika w systemie A będąca 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. Te informacje dotyczące źródła są przekazywane do kontrolera domeny EIM, a operacja wyszukiwania EIM znajduje powiązanie źródłowe zgodne z podanymi informacjami. Za pomocą nazwy identyfikatora EIM operacja wyszukiwania EIM odnajduje powiązanie docelowe dla identyfikatora Jan Kowalski, które jest zgodne z nazwą definicji rejestru EIM celu dla System_B. Jeśli zgodne powiązanie docelowe zostanie znalezione, operacja wyszukiwania EIM zwraca tożsamość użytkownika jsk1 do aplikacji.

Rysunek 10: Operacja wyszukiwania EIM działająca w oparciu o znaną tożsamość użytkownika jankowalski



Uprawnienia EIM

Uprawnienia EIM umożliwiają użytkownikowi wykonanie konkretnych zadań administracyjnych lub operacji wyszukiwania EIM. Nadawanie i odbieranie uprawnień innym użytkownikom jest zarezerwowane tylko dla użytkowników o uprawnieniach administratora EIM. Uprawnienia EIM są nadawane tylko tożsamościom użytkowników, które są znane kontrolerowi domeny EIM.

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

- **Administrator LDAP.** Użytkownik mający to uprawnienie może konfigurować nową domenę EIM. Może on wykonywać następujące zadania:
  - tworzenie domeny,
  - usuwanie domeny,

  - tworzenie i usuwanie identyfikatorów EIM,
  - tworzenie i usuwanie definicji rejestrów EIM,
  - tworzenie i usuwanie powiązań źródłowych, docelowych i administracyjnych,
  - wykonywanie operacji wyszukiwania EIM,
  - pobieranie powiązań, identyfikatorów EIM, definicji rejestrów EIM,
  - dodawanie, usuwanie i wyświetlanie informacji o uprawnieniach EIM.
- **Administrator EIM.** Użytkownik mający to uprawnienie może zarządzać wszystkimi danymi EIM w domenie EIM. Może on wykonywać następujące zadania:
  - usuwanie domeny,
  - tworzenie i usuwanie identyfikatorów EIM,
  - tworzenie i usuwanie definicji rejestrów EIM,
  - tworzenie i usuwanie powiązań źródłowych, docelowych i administracyjnych,
  - wykonywanie operacji wyszukiwania EIM,
  - pobieranie powiązań, identyfikatorów EIM, definicji rejestrów EIM,
  - dodawanie, usuwanie i wyświetlanie informacji o uprawnieniach EIM.
- **Administrator identyfikatorów EIM.** Użytkownik mający to uprawnienie może dodawać i zmieniać identyfikatory EIM i zarządzać powiązaniami źródłowymi i administracyjnymi. Może on wykonywać następujące zadania:
  - tworzenie identyfikatora EIM,
  - dodawanie i usuwanie powiązań źródłowych,
  - dodawanie i usuwanie powiązań administracyjnych,
  - wykonywanie operacji wyszukiwania EIM,
  - pobieranie powiązań, identyfikatorów EIM, definicji rejestrów EIM.
- **Wyszukiwanie odwzorowań EIM.** Użytkownik mający to uprawnienie może wykonywać operacje wyszukiwania EIM. Może on wykonywać następujące zadania:
  - wykonywanie operacji wyszukiwania EIM,
  - pobieranie powiązań, identyfikatorów EIM, definicji rejestrów EIM.
- **Administrator rejestrów EIM.** Użytkownik mający to uprawnienie może zarządzać wszystkimi definicjami rejestrów EIM. Może on wykonywać następujące zadania:
  - dodawanie i usuwanie powiązań docelowych,
  - wykonywanie operacji wyszukiwania EIM,
  - pobieranie powiązań, identyfikatorów EIM, definicji rejestrów EIM.
- **Administrator rejestru X EIM.** Użytkownik mający to uprawnienie może zarządzać konkretną definicją rejestru EIM. Może on wykonywać następujące zadania:
  - dodawanie i usuwanie powiązań docelowych dla definicji rejestru EIM,
  - wykonywanie operacji wyszukiwania EIM,
  - pobieranie powiązań, identyfikatorów EIM, definicji rejestrów EIM.

Poniższe tabele zostały pogrupowane według zadań EIM, które wykonują dane funkcje API. Na poszczególne tabele składają się funkcje API EIM, różne uprawnienia EIM i zakres dostępu do pewnych funkcji EIM, który mają użytkownicy o tych uprawnieniach.

Tabela 1: Praca z domenami

Funkcja API EIM	Administrator LDAP	Administrator EIM	Administrator identyfika-torów EIM	Wyszukiwanie odwzorowań EIM	Administrator rejestrów EIM	Administrator rejestru X EIM
eimChangeDomain	X	X	-	-	-	-

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

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
eimAddApplicationRegistry	X	X	-	-	-	-
eimAddSystemRegistry	X	X	-	-	-	-
eimChangeRegistry	X	X	-	-	X	X
eimChangeRegistryUser	X	X	-	-	X	X
eimChgRegistryAlias	X	X	-	-	X	X
eimGetRegistryFromAlias	X	X	X	X	X	X
eimListRegistries	X	X	X	X	X	X
eimListRegistryAliases	X	X	X	X	X	X
eimListRegistryUsers	X	X	X	X	X	X
eimRemoveRegistry	X	X	-	-	-	-

Tabela 4: Praca z powiązaniami

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 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 6: 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	-	-	-	-

Koncepcje dotyczące LDAP w kontekście EIM

Do przechowywania danych EIM używa serwera LDAP jako kontrolera domeny EIM. Nazw wyróżniających LDAP można użyć podczas konfigurowania EIM dla serwera iSeries oraz podczas uwierzytelniania w kontrolerze domeny EIM.

Aby używać nazw wyróżniających LDAP podczas konfigurowania i administrowania EIM, należy zapoznać się z następującymi koncepcjami dotyczącymi LDAP:

- Nazwa wyróżniająca LDAP
- Nadrzędna nazwa wyróżniająca LDAP

Nazwa wyróżniająca LDAP

Nazwa wyróżniająca LDAP jest pozycją LDAP identyfikującą i opisującą autoryzowanego użytkownika serwerowi LDAP. Do skonfigurowania serwera LDAP tak, aby przechowywał informacje domeny EIM można użyć kreatora konfiguracji EIM. Nazw wyróżniających LDAP można użyć jako sposobu na uzyskiwanie dostępu i pobieranie tych danych EIM, dzięki czemu serwer iSeries może należeć do środowiska pojedynczego wpisywania się.

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 LDAP 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 LDAP. 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. Więcej informacji na temat sposobu używania tych nazw przez EIM zawiera temat Nadrzędna nazwa wyróżniająca LDAP.

Ponieważ EIM używa serwera LDAP do przechowywania danych EIM, nazwy wyróżniające LDAP można wykorzystywać jako sposób uwierzytelniania w kontrolerze domeny EIM. Nazwy wyróżniające LDAP mogą być także wykorzystane podczas konfigurowania EIM dla serwera iSeries. Nazw wyróżniających LDAP można używać na przykład podczas:

- konfigurowania serwera LDAP tak, aby był kontrolerem domeny EIM; zadanie to wykonuje się, tworząc i używając nazwy wyróżniającej LDAP identyfikującej administratora LDAP w serwerze LDAP; jeśli serwer LDAP 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 LDAP musi reprezentować użytkownika, który ma uprawnienia do tworzenia obiektów w lokalnej przestrzeni nazw serwera LDAP,
- stosowania kreatora konfiguracji EIM do wybrania typu użytkownika w celu wykonania operacji EIM w imieniu funkcji systemu operacyjnego; do operacji tych należą wyszukiwania odwzorowań i usuwanie powiązań podczas usuwania lokalnego profilu użytkownika OS/400; 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.

Więcej informacji na temat nazw wyróżniających i sposobu ich używania przez LDAP zawiera temat dotyczący podstaw LDAP.

Nadrzędna nazwa wyróżniająca LDAP

Nadrzędna nazwa wyróżniająca LDAP 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 zajmuje najwyższy poziom w przestrzeni nazw serwera LDAP.

Przykładem pełnej nazwy wyróżniającej LDAP 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.

Ponieważ EIM używa serwera LDAP do przechowywania danych EIM, nazwy wyróżniające LDAP można wykorzystywać jako sposób uwierzytelniania w kontrolerze domeny EIM. Nazw wyróżniających LDAP można także używać podczas konfigurowania EIM dla serwera iSeries. Na przykład 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 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.

Więcej informacji na temat nazw wyróżniających i sposobu ich używania zawiera temat dotyczący podstaw LDAP.

Obsługa pojedynczego wpisywania się za pomocą EIM

EIM udostępnia niedrogi mechanizm służący do obsługi pojedynczego wpisywania się w całym przedsiębiorstwie. Implementacja EIM i Kerberos dla systemu operacyjnego OS/400 zapewnia prawdziwe wielowarstwowe, heterogeniczne środowisko pojedynczego wpisywania się. Poniżej przedstawiono korzyści płynące z pojedynczego wpisywania się w przedsiębiorstwie. Mogą z nich czerpać użytkownicy, administratorzy i programiści aplikacji.

Korzyści dla użytkowników
W środowisku pojedynczego wpisywania się uwierzytelnianie odbywa się za każdym razem, gdy użytkownicy próbują uzyskać dostęp do nowego systemu, tu jednak nie będą proszeni o podanie haseł. EIM zwalnia użytkowników z obowiązku pamiętania i zarządzania wieloma nazwami oraz hasłami używanymi do uzyskania dostępu do innych systemów w sieci. Po jednokrotnym uwierzytelnieniu użytkownika może on uzyskać dostęp do usług i aplikacji w przedsiębiorstwie bez potrzeby korzystania z wielu haseł w innych systemach.

Korzyści dla administratorów
Pojedyncze wpisywanie się ułatwia administratorom zarządzanie ochroną przedsiębiorstwa. Bez stosowania pojedynczego wpisywania się, użytkownicy i aplikacje mogą umieszczać hasła w pamięciach podręcznych w różnych systemach, co naraża na niebezpieczeństwo ochronę całej sieci. Administratorzy spędzają wiele czasu i wydają spore sumy pieniędzy na implementację rozwiązań ograniczających takie niebezpieczeństwa dotyczące ochrony. Pojedyncze wpisywanie się ogranicza nakład pracy administratora potrzebny podczas zarządzania uwierzytelnianiem przy jednoczesnym zapewnieniu ochrony sieci. Ponadto pojedyncze wpisywanie się ogranicza koszty poniesione w związku z resetowaniem zapomnianych haseł.

Korzyści dla programistów aplikacji
Programistom aplikacji, które muszą być uruchamiane w sieciach heterogenicznych, EIM udostępnia infrastrukturę tworzenia aplikacji działających na wielu platformach. Za pomocą funkcji API EIM programiści mogą w celu zapewnienia uwierzytelniania pisać aplikacje korzystające z najodpowiedniejszego istniejącego rejestru użytkowników, podczas gdy do autoryzacji mogą oni korzystać z innego rejestru użytkowników. Programiści aplikacji nie muszą w tworzonych aplikacjach obsługiwać specyficznych dla danej platformy rejestrów użytkowników, ponieważ EIM dostarcza infrastrukturę do tworzenia aplikacji odwzorowujących tożsamości użytkowników w tych rejestrach użytkowników na pojedyncze identyfikatory EIM. Ponadto EIM umożliwia programistom obsługę tych

aplikacji bez konieczności zmiany powiązanych semantyk ochrony, a ochrona na poziomie aplikacji znacząco obniża koszty implementowania wielowarstwowych aplikacji międzyplatformowych.

Obsługa pojedynczego wpisywania się w iSeries
W celu zapewnienia środowiska pojedynczego wpisywania się IBM używa jednocześnie dwóch technologii: EIM i usługi uwierzytelniania sieciowego, która jest implementacją IBM protokołu Kerberos i funkcji API GSS. Konfigurując te dwie technologie administrator może aktywować środowisko pojedynczego wpisywania się. Protokół Kerberos jest używany do uwierzytelniania użytkowników w sieci przez systemy Windows 2000, XP, AIX i zSeries. Protokół ten obejmuje użycie opartego na sieci, bezpiecznego centrum dystrybucji kluczy, który uwierzytelnia nazwy użytkowników (użytkownicy Kerberos) w sieci. Użytkownik odbiera bilet Kerberos od centrum dystrybucji kluczy. Bilet ten uwierzytelnia użytkownika w innej usłudze w przedsiębiorstwie. Bilet może być przekazany od użytkownika do usługi, która akceptuje bilety. Usługa akceptująca bilet używa go do określenia, za kogo podaje się użytkownik (w rejestrze użytkowników Kerberos i dziedzinie) i czy w rzeczywistości jest on tą osobą, za którą się podaje.

Podczas gdy usługa uwierzytelniania sieciowego umożliwia serwerowi iSeries należenie do dziedziny Kerberos, EIM dostarcza mechanizm do powiązania nazw użytkowników Kerberos z pojedynczym identyfikatorem EIM, który reprezentuje danego użytkownika w całym przedsiębiorstwie. Inne tożsamości użytkowników, takie jak nazwa użytkownika w systemie OS/400, również mogą być powiązane z tym identyfikatorem EIM. W oparciu o te powiązania EIM dostarcza systemowi operacyjnemu OS/400 i aplikacjom mechanizm służący do określenia, który profil użytkownika OS/400 odpowiada danej osobie lub jednostce reprezentowanej przez daną nazwę użytkownika protokołu Kerberos. Informacje przechowywane w EIM można sobie wyobrazić jako strukturę drzewiastą z identyfikatorem EIM będącym korzeniem i listą tożsamości użytkowników powiązanych z identyfikatorem EIM będących gałęziami.

Używając poniższego rysunku, wyobraźmy sobie, że użytkownik, taki jak Jan Kowalski wpisuje się do sieci za pomocą komputera PC z systemem Windows i uzyskuje dostęp do instancji systemu operacyjnego OS/400 w celu dotarcia do aplikacji z obsługą protokołu Kerberos. Użytkownik ten nie jest proszony o podanie nazwy użytkownika OS/400. Aplikacje mogą wyszukać powiązanie z identyfikatorem EIM tego użytkownika w celu znalezienia nazwy użytkownika OS/400. Użytkownik Jan Kowalski nie potrzebuje hasła w profilu użytkownika OS/400, ponieważ profil ten nie jest używany do uwierzytelnienia, a jedynie do autoryzacji.

Rysunek 1. Środowisko pojedynczego wpisywania się

Temat Scenariusz: Włączenie pojedynczego wpisywania się zawiera przykład sposobu konfigurowania przez administratora usługi uwierzytelniania sieciowego i EIM w celu aktywowania środowiska pojedynczego wpisywania się.

Za pomocą pojedynczego wpisywania się można uzyskać dostęp do następujących aplikacji:

- iSeries Navigator,
- Emulator PC5250,
- Distributed Relational Database Architecture (TM)(DRDA)(R),
- NetServer,
- QFileSvr.400.

Planowanie EIM

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 wpisywania się.

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 wpisywania się.

W poniższym arkuszu planowania podano usługi, które należy zainstalować przed konfigurowaniem EIM.

Arkusz planowania	**Odpowiedź**
Czy system OS/400 jest w wersji V5R2 (5722-SS1) lub nowszej?	
Czy na serwerach iSeries zainstalowano oprogramowanie Cryptographic Access Provider (5722-AC3)?	
Czy na odpowiednich komputerach PC w sieci (komputery PC używane do pracy z serwerami iSeries) i na serwerach iSeries zainstalowano oprogramowanie iSeries Access for Windows (5722-XE1)?	
Czy na wszystkich komputerach PC w sieci i w systemie iSeries zainstalowano składnik Sieć oprogramowania iSeries Navigator?	
Jeśli serwer LDAP jest obecnie zainstalowany i chcesz go używać jako kontrolera domeny EIM, czy znasz nazwę wyróżniającą i hasło administratora LDAP?	
Jeśli serwer LDAP jest skonfigurowany, czy można go tymczasowo zatrzymać? (Będzie to wymagane w celu zakończenia procesu konfigurowania EIM.)	
Czy masz uprawnienia specjalne *SECADM, *ALLOBJ i *IOSYSCFG?	
Czy zostały zastosowane najnowsze poprawki PTF?	

Jeśli do uwierzytelniania użytkowników planujesz używać protokołu Kerberos, musisz także skonfigurować usługę uwierzytelniania sieciowego. Pełny arkusz planowania usługi uwierzytelniania sieciowego dostępny jest w temacie Planowanie usługi uwierzytelniania sieciowego.

Jeśli konfigurujesz usługę uwierzytelniania sieciowego i EIM do aktywowania pojedynczego wpisywania się, skorzystaj z tematu Scenariusz: Aktywowanie pojedynczego wpisywania się przedstawiającego sposób konfiguracji obu tych produktów w przedsiębiorstwie.

Instalowanie wymaganych opcji programu iSeries Navigator

Aby aktywować środowisko pojedynczego wpisywania się za pomocą 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 pracy z serwerem iSeries.

Aby zainstalować opcję Sieć:

1. Kliknij **Start —> Programy —> IBM iSeries Access for Windows —> Konfiguracja 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.

Konfigurowanie usługi uwierzytelniania sieciowego

Usługa uwierzytelniania sieciowego umożliwia użycie uwierzytelniania Kerberos na serwerze iSeries. Usługa ta nie stanowi wymagania wstępnego dotyczącego używania EIM na serwerze, jednak wykorzystanie uwierzytelniania Kerberos w celu zapewnienia ochrony sieci niesie wiele korzyści.

Usługa uwierzytelniania sieciowego używana razem z EIM umożliwia aktywowanie środowiska pojedynczego wpisywania się. Środowisko pojedynczego wpisywania przynosi korzyści zarówno użytkownikom, jak i administratorom. Użytkownicy mogą posługiwać się mniejszą liczbą nazw i haseł, a administratorzy mogą śledzić mniejszą ilość informacji dotyczących poszczególnych użytkowników. Ponieważ środowisko pojedynczego wpisywania się pomaga również pokonać różnice między wieloma platformami i różnymi systemami, które mogą znajdować się w używanej sieci, koszty programowania aplikacji i ogólne koszty administracyjne zostają zredukowane.

Jeśli na serwerze iSeries lub na wszystkich serwerach w sieci nie jest obecnie skonfigurowana usługa uwierzytelniania sieciowego, zapoznaj się z informacjami dotyczącymi planowania tej usługi dostępnymi w temacie o planowaniu usługi uwierzytelniania sieciowego. Jeśli posiadasz wiedzę dotyczącą usługi uwierzytelniania sieciowego, przejdź do tematu o konfigurowaniu usługi uwierzytelniania sieciowego, aby rozpocząć proces konfigurowania.

Konfigurowanie EIM

Aby aktywować środowisko pojedynczego wpisywania się na wielu platformach bez zmiany istniejących strategii ochrony, należy skonfigurować EIM oraz usługę uwierzytelniania sieciowego. Skonfigurowanie i używanie usługi uwierzytelniania sieciowego nie stanowi jednak wymagania wstępnego dotyczącego konfigurowania i używania EIM.

Aby rozpocząć proces konfigurowania EIM w celu włączenia serwera iSeries do środowiska pojedynczego wpisywania się, należy użyć kreatora konfigurowania EIM. W zależności od potrzeb kreatora tego można użyć do przyłączenia do nowej domeny lub utworzenia i przyłączenia nowej domeny.

Kreator konfigurowania EIM umożliwia proste wykonanie podstawowej konfiguracji EIM. Na przykład jeśli nie jest jeszcze skonfigurowany serwer LDAP lub usługa uwierzytelniania sieciowego, kreator konfigurowania EIM pomoże wykonać te zadania.

Po użyciu kreatora do wykonania podstawowej konfiguracji EIM, a przed użyciem środowiska pojedynczego wpisywania się należy wykonać dodatkowe kroki konfiguracyjne. Przykład ilustrujący konfigurowanie środowiska pojedynczego wpisywania się za pomocą usługi uwierzytelniania sieciowego i EIM w fikcyjnym przedsiębiorstwie zawiera temat Scenariusz: aktywowanie pojedynczego wpisywania się.

Przed użyciem kreatora konfigurowania EIM należy wykonać wszystkie kroki konfigurowania w celu dokładnego określenia sposobu używania zarówno EIM, jak i usługi uwierzytelniania sieciowego do aktywowania środowiska pojedynczego wpisywania się. Po zakończeniu planowania można użyć kreatora do skonfigurowania EIM dla używanego serwera iSeries za pomocą jednego z następujących sposobów: utworzenie nowych domen lub przyłączenie domen już istniejących. Konfigurowanie EIM opisano w poniższych tematach:

Utworzenie i przyłączenie nowej domeny
Wykonanie tego zadani spowoduje utworzenie domeny EIM w używanej sieci i skonfigurowanie serwera iSeries tak, aby do niej należał. Kreator tworzy nową domenę i konfiguruje lokalny serwer LDAP tak, aby był kontrolerem domeny EIM dla nowej domeny. Ponadto, jeśli na serwerze iSeries nie skonfigurowano protokołu Kerberos, kreator wyświetla zachętę do uruchomienia kreatora konfigurowania usługi uwierzytelniania sieciowego. Po wykonaniu tego zadania można skonfigurować inne serwery iSeries tak, aby należały do tej domeny. W tym celu należy połączyć się z każdym z nich i użyć kreatora konfigurowania EIM do skonfigurowania serwera w celu włączenia go do istniejącej domeny EIM.

Przyłączenie istniejącej domeny
Po użyciu kreatora konfigurowania EIM do skonfigurowania kontrolera domeny i domeny EIM należy wybrać to zadanie po to, aby skonfigurować inne serwery iSeries tak, żeby należały do danej domeny. To zadanie należy wykonać dla każdego działającego w sieci serwera iSeries, który będzie używał EIM. Po zakończeniu pracy z kreatorem należy podać informacje dotyczące przyłączanej domeny, w tym informacje o połączeniu (takie jak numer portu i określenie, czy będą używane Transport Layer Security (TLS)/Secure Sockets Layer (SSL)) z kontrolerem domeny EIM. Jeśli na serwerze iSeries nie skonfigurowano protokołu Kerberos, kreator wyświetla zachętę do uruchomienia kreatora konfigurowania usługi uwierzytelniania sieciowego.

Dostęp do kreatora konfigurowania EIM

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 —> Enterprise Identity Mapping**.
4. Prawym przyciskiem myszy kliknij **Konfiguracja** i wybierz **Konfiguruj...**, aby uruchomić kreator konfigurowania EIM.
5. Wybierz **Przyłącz do istniejącej domeny** lub **Utwórz i przyłącz do nowej domeny**.

Po użyciu kreatora do utworzenia kontrolera domeny i skonfigurowania serwerów iSeries w domenie, aby zakończyć konfigurowanie EIM, musisz wykonać następujące zadania:

1. Dodawanie rejestrów EIM do domeny EIM dla innych niż iSeries aplikacji i serwerów, które mają należeć do danej domeny EIM.
2. Tworzenie identyfikatorów EIM w domenie dla każdego unikalnego użytkownika lub jednostki dla systemów należących do domeny EIM.
3. Tworzenie powiązań między różnymi tożsamościami osoby lub jednostki a identyfikatorami EIM.

Tworzenie i przyłączanie nowej domeny

Do skonfigurowania serwera LDAP na serwerze iSeries, tak aby był on kontrolerem domeny EIM dla nowej domeny, można użyć kreatora konfiguracji EIM. Jeśli to konieczne, kreator konfiguracji EIM sprawdza, czy podano podstawowe informacje konfiguracyjne dla serwera LDAP.

Ponadto, jeśli na serwerze iSeries nie skonfigurowano protokołu Kerberos, kreator wyświetla zachętę do uruchomienia kreatora konfigurowania usługi uwierzytelniania sieciowego. Po zakończeniu pracy w tym kreatorze, nowa domena EIM zostaje skonfigurowana, system iSeries zostaje skonfigurowany do przyłączenia nowej domeny, a podane rejestry użytkowników zostają dodane do tej domeny.

Do wykonania tego zadania za pomocą kreatora należy mieć uprawnienia specjalne Security Administrator (*SECADM), All Object (*ALLOBJ) i System Configuration (*IOSYSCFG).

Aby uruchomić kreator konfiguracji EIM i jego używać w celu utworzenia i przyłączenia nowej domeny EIM, w programie iSeries Navigator należy wykonać następujące kroki:

Uwaga: Kreator dodatkowo konfiguruje lokalny serwer LDAP jako nowego kontrolera domeny EIM.

1. Rozwiń gałąź **Sieć** —> **Enterprise Identity Mapping**.
2. Prawym przyciskiem myszy kliknij **Konfiguracja** i wybierz **Konfiguruj...**, aby uruchomić kreator konfigurowania EIM.
3. Na stronie **Witamy** wybierz opcję **Utwórz i przyłącz nową domenę** i kliknij przycisk **Dalej**.

4. Jeśli usługa uwierzytelniania sieciowego nie jest skonfigurowana na serwerze iSeries, zostanie wyświetlone okno dialogowe **Konfigurowanie usługi uwierzytelniania sieciowego**. W tym oknie można określić, czy konfigurować usługę uwierzytelniania sieciowego. Jeśli wybierzesz **Tak**, zostanie uruchomiony kreator konfiguracji usługi uwierzytelniania sieciowego. Po zakończeniu konfigurowania usługi uwierzytelniania sieciowego można kontynuować pracę w kreatorze konfiguracji EIM.
5. Jeśli lokalny serwer LDAP nie jest skonfigurowany, zostanie wyświetlone okno dialogowe **Konfiguruj serwer katalogów**. Aby skonfigurować lokalny serwer LDAP, w oknie dialogowym podaj następujące informacje:
   - W polu **Port** pozostaw domyślny numer portu **389** lub zmień go, aby z serwerem katalogów używać niechronionej komunikacji EIM.
   - W polu **Nazwa wyróżniająca** wpisz nazwę wyróżniającą LDAP identyfikującą administratora LDAP w serwerze LDAP. Kreator konfiguracji EIM tworzy nazwę wyróżniającą administratora LDAP i używa jej do skonfigurowania serwera LDAP jako kontrolera tworzonej domeny.
   - W polu **Hasło** wpisz hasło administratora LDAP.
   - W polu **Potwierdź hasło** wpisz ponownie hasło.
   - Kliknij przycisk **Dalej**.
6. W oknie dialogowym **Podaj kontroler domeny** wpisz następujące informacje:
   - 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: = + < > , # ; \ ani *.
   - W polu **Opis** wpisz opis domeny.
   - Kliknij przycisk **Dalej**.
7. W oknie dialogowym **Podaj nadrzędną nazwę wyróżniającą domeny** określ, czy chcesz podawać nadrzędną nazwę wyróżniającą dla tworzonej domeny. 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.
8. W oknie dialogowym **Podaj użytkownika połączenia** wybierz **typ użytkownika**, który ma być używany podczas połączenia. Dostępne są następujące typy użytkowników: Nazwa wyróżniająca i hasło, Plik kluczy Kerberos i nazwa użytkownika oraz Nazwa użytkownika Kerberos 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:
   - Wybierając opcję **Nazwa wyróżniająca i hasło**, musisz podać następujące informacje:
     - W polu **Nazwa wyróżniająca** wpisz nazwę wyróżniającą LDAP identyfikującą użytkownika, który ma uprawnienia do tworzenia obiektów w lokalnej przestrzeni nazw serwera LDAP. Jeśli we wcześniejszym kroku użyto kreatora do skonfigurowania serwera LDAP, musisz wprowadzić Nazwę wyróżniającą administratora LDAP utworzonego w tym kroku.
     - W polu **Hasło** wpisz hasło użytkownika.
     - W polu **Potwierdź hasło** wpisz ponownie hasło.
   - Wybierając opcję **Plik kluczy Kerberos i nazwa użytkownika**, musisz podać następujące informacje:
     - W polu **Plik kluczy** wpisz nazwę pliku kluczy na serwerze iSeries identyfikującą użytkownika, który ma uprawnienia do tworzenia obiektów w lokalnej przestrzeni nazw serwera LDAP. Możesz też kliknąć przycisk **Przeglądaj**, aby wybrać plik kluczy.
     - W polu **Nazwa użytkownika** wpisz nazwę użytkownika Kerberos, która ma być używana do zidentyfikowania użytkownika.

- W polu **Dziedzina** wpisz nazwę dziedziny Kerberos dla nazwy użytkownika. Nazwy użytkownika i dziedziny jednoznacznie identyfikują użytkowników Kerberos w pliku kluczy. Na przykład nazwa użytkownika jkowalski w dziedzinie ordept.firma.com jest reprezentowana w pliku kluczy jako jkowalski@ordept.firma.com.

  - Wybierając opcję **Nazwa użytkownika Kerberos i hasło**, musisz podać następujące informacje:
    - W polu **Nazwa użytkownika** wpisz nazwę użytkownika Kerberos identyfikującą użytkownika, który ma uprawnienia do tworzenia obiektów w lokalnej przestrzeni nazw serwera LDAP.
    - W polu **Dziedzina** wpisz nazwę dziedziny Kerberos dla nazwy użytkownika.
    - W polu **Hasło** wpisz hasło użytkownika.
    - W polu **Potwierdź hasło** wpisz ponownie hasło. Nazwy użytkownika i dziedziny jednoznacznie identyfikują użytkowników Kerberos w pliku kluczy. Na przykład nazwa użytkownika jkowalski w dziedzinie ordept.firma.com jest reprezentowana w pliku kluczy jako jkowalski@ordept.firma.com.
  - Kliknij przycisk **Sprawdź połączenie**, aby przetestować informacje konfiguracyjne użytkownika, łącząc się z kontrolerem domeny.
  - Kliknij przycisk **Dalej**.

9. W oknie dialogowym **Informacje o rejestrze** wybierz typ rejestrów użytkowników, który chcesz dodać do tej domeny EIM. Wybierz jeden lub oba poniższe typy rejestrów użytkowników:
   - Wybierz **OS400**, aby dodać do domeny EIM rejestr użytkowników reprezentujący rejestr lokalny. W dostępnym polu wpisz nazwę rejestru, który ma zostać utworzony w domenie. Nazwa rejestru EIM jest arbitralnym łańcuchem reprezentującym typ rejestru i konkretną instancję tego rejestru.
   - Wybierz **Kerberos**, aby do domeny EIM dodać rejestr użytkowników Kerberos. W dostępnym polu wpisz nazwę rejestru, który ma zostać utworzony w domenie, i jeśli to konieczne, wybierz opcję **Rozróżnianie wielkości liter w tożsamościach użytkowników Kerberos**.
   - Kliknij przycisk **Dalej**.
10. W oknie dialogowym **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 wyszukiwania odwzorowań i usuwanie powiązań podczas usuwania lokalnego profilu użytkownika OS/400. Dostępne są następujące typy użytkowników: Nazwa wyróżniająca i hasło, Plik kluczy Kerberos i nazwa użytkownika oraz Nazwa użytkownika Kerberos i hasło. Od wybranego typu użytkownika zależą inne informacje, które należy podać w tym oknie:

Uwaga: 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 wpisywaniem się i usuwaniem profili użytkowników mogą się nie powieść.

11. Wybierając opcję **Nazwa wyróżniająca i hasło**, musisz podać następujące informacje:
    - W polu **Nazwa wyróżniająca** wpisz nazwę wyróżniającą LDAP identyfikującą użytkownika w systemie OS/400, która to nazwa ma być używana podczas łączenia się z kontrolerem domeny EIM.
    - W polu **Hasło** wpisz hasło użytkownika.
    - W polu **Potwierdź hasło** wpisz ponownie hasło.
12. Wybierając opcję **Nazwa użytkownika Kerberos i hasło**, musisz podać następujące informacje:
    - W polu **Nazwa użytkownika** wpisz nazwę użytkownika Kerberos identyfikującą użytkownika w systemie OS/400, która to nazwa ma być używana podczas łączenia się z kontrolerem domeny EIM.
    - W polu **Dziedzina** wpisz nazwę dziedziny Kerberos dla nazwy użytkownika.
    - W polu **Hasło** wpisz hasło użytkownika.
    - W polu **Potwierdź hasło** wpisz ponownie hasło. Nazwy użytkownika i dziedziny jednoznacznie identyfikują użytkowników Kerberos w pliku kluczy. Na przykład nazwa użytkownika jkowalski w dziedzinie ordept.firma.com jest reprezentowana w pliku kluczy jako jkowalski@ordept.firma.com.
13. Wybierając opcję **Plik kluczy Kerberos i nazwa użytkownika**, musisz podać następujące informacje:

- W polu **Plik kluczy** wpisz nazwę pliku kluczy na serwerze iSeries identyfikującą użytkownika w systemie OS/400, która to nazwa ma być używana podczas łączenia się z kontrolerem domeny EIM. Możesz też kliknąć przycisk **Przeglądaj**, aby wybrać plik kluczy.
- W polu **Nazwa użytkownika** wpisz nazwę użytkownika Kerberos, która ma być używana do zidentyfikowania użytkownika.
- W polu **Dziedzina** wpisz nazwę dziedziny Kerberos dla nazwy użytkownika. Nazwy użytkownika i dziedziny jednoznacznie identyfikują użytkowników Kerberos w pliku kluczy. Na przykład nazwa użytkownika jkowalski w dziedzinie ordept.firma.com jest reprezentowana w pliku kluczy jako jkowalski@ordept.firma.com.

14. Kliknij przycisk **Sprawdź połączenie**, aby przetestować połączenie z kontrolerem domeny dla utworzonego użytkownika systemu.
15. Kliknij przycisk **Dalej**.
16. Przejrzyj podane informacje konfiguracyjne na panelu **Podsumowanie**. Jeśli wszystkie podane informacje są poprawne, kliknij przycisk **Zakończ**.

Zakończenie pracy kreatora jest jednoznaczne z zakończeniem podstawowej konfiguracji EIM. Jednak aby sfinalizować konfigurację EIM dla tego serwera, należy wykonać następujące zadania:

1. Dodawanie domeny, która została utworzona, do folderu zarządzania domenami EIM.
2. Dodawanie rejestrów EIM do domeny EIM dla innych aplikacji i serwerów, które mają należeć do danej domeny EIM.
3. Tworzenie identyfikatorów EIM w domenie dla każdego unikalnego użytkownika lub jednostki dla systemów należących do domeny EIM.
4. Tworzenie powiązań między różnymi tożsamościami osoby lub jednostki a identyfikatorami EIM.

Ponadto można użyć Secure Sockets Layer (SSL) lub Transport Layer Security (TLS) do skonfigurowania chronionego połączenia z kontrolerem domeny.

Konfigurowanie chronionego połączenia z kontrolerem domeny EIM

Po użyciu kreatora do utworzenia i podłączenia nowej domeny można zdecydować się na wykorzystanie Secure Sockets Layer (SSL) lub Transport Layer Security Protocol (TLS) w celu ustanowienia chronionego połączenia z kontrolerem domeny EIM. Aby skonfigurować SSL lub TLS dla EIM:

1. Włącz SSL dla kontrolera domeny serwera LDAP.
2. Użyj programu Digital Certificate Manager (DCM), aby utworzyć certyfikat wymagany przez serwer LDAP do wykorzystania SSL.
3. Użyj programu DCM, aby przypisać certyfikat do serwera LDAP.
4. Zaktualizuj właściwości konfiguracji EIM, określając, że serwer iSeries używa chronionego połączenia SSL.
5. Zaktualizuj właściwości domeny EIM dla każdej domeny EIM, podając, że EIM używa połączenia SSL podczas zarządzania domeną za pomocą programu iSeries Navigator.

Przyłączenie istniejącej domeny

Do przyłączenia istniejącej domeny EIM można użyć kreatora konfiguracji EIM. Kreatora tego można użyć, gdy domena EIM i kontroler domeny zostały już skonfigurowane w sieci. Podczas pracy w kreatorze należy podać informacje na temat domeny, w tym informacje o połączeniu z kontrolerem domeny EIM. Kreator przechowuje te informacje na serwerze iSeries i używa ich do połączenia z kontrolerem domeny EIM. Ponadto kreator tworzy na tym serwerze iSeries rejestr użytkowników EIM reprezentujący rejestr profili użytkowników OS/400.

Do wykonania tego zadania za pomocą kreatora należy mieć uprawnienia specjalne Security Administrator (*SECADM) i All Object (*ALLOBJ).

Aby uruchomić i używać kreatora konfiguracji EIM w celu przyłączenia istniejącej domeny EIM:

1. Rozwiń gałąź **Sieć —> Enterprise Identity Mapping**.
2. Prawym przyciskiem myszy kliknij **Konfiguracja** i wybierz **Konfiguruj...**, aby uruchomić kreator konfigurowania EIM. Po uruchomieniu kreatora w wyświetlanych oknach dialogowych podaj wymagane informacje.
3. W oknie dialogowym **Witamy** wybierz **Przyłącz istniejącą domenę** i kliknij przycisk **Dalej**.
4. Jeśli usługa uwierzytelniania sieciowego nie jest skonfigurowana na serwerze iSeries, zostanie wyświetlone okno dialogowe **Konfigurowanie usługi uwierzytelniania sieciowego**. W tym oknie można określić, czy usługa uwierzytelniania sieciowego ma być konfigurowana. Jeśli wybierzesz **Tak**, zostanie uruchomiony kreator konfiguracji usługi uwierzytelniania sieciowego. Po zakończeniu konfigurowania usługi uwierzytelniania sieciowego można kontynuować pracę w kreatorze konfiguracji EIM.
5. W oknie dialogowym **Podaj kontroler domeny** wpisz następujące informacje:
   - W polu **Nazwa kontrolera domeny** wpisz nazwę systemu będącego kontrolerem domeny EIM, która ma być przyłączona do serwera iSeries.
   - Jeśli chcesz, aby do ochrony transmisji danych EIM przesyłanych podczas ich pobierania z kontrolera domeny był używany protokół SSL, kliknij **Użyj SSL**.
   - Kliknij **Sprawdź połączenie**, aby przetestować informacje konfiguracyjne kontrolera domeny.

Uwaga: Jeśli wybrano Użyj SSL i wyświetlany jest komunikat o błędzie, może on sygnalizować, że serwer LDAP nie został skonfigurowany do obsługi SSL.

   - Kliknij przycisk **Dalej**.
6. W oknie dialogowym **Podaj użytkownika połączenia** wybierz **typ użytkownika**, który ma być używany podczas połączenia. Dostępne są następujące typy użytkowników: Nazwa wyróżniająca i hasło, Plik kluczy Kerberos i nazwa użytkownika oraz Nazwa użytkownika Kerberos 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:
   - Wybierając opcję **Nazwa wyróżniająca i hasło**, musisz podać następujące informacje:
     - W polu **Nazwa wyróżniająca** wpisz nazwę wyróżniającą LDAP identyfikującą użytkownika, który ma uprawnienia do tworzenia obiektów w lokalnej przestrzeni nazw serwera LDAP.
     - W polu **Hasło** wpisz hasło użytkownika.
     - W polu **Potwierdź hasło** wpisz ponownie hasło.
   - Wybierając opcję **Plik kluczy Kerberos i nazwa użytkownika**, musisz podać następujące informacje:
     - W polu **Plik kluczy** wpisz nazwę pliku kluczy na serwerze iSeries identyfikującą użytkownika, który ma uprawnienia do tworzenia obiektów w lokalnej przestrzeni nazw serwera LDAP. Możesz też kliknąć przycisk **Przeglądaj**, aby wybrać plik kluczy.
     - W polu **Nazwa użytkownika** wpisz nazwę użytkownika Kerberos, która ma być używana do zidentyfikowania użytkownika.
     - W polu **Dziedzina** wpisz nazwę dziedziny Kerberos dla nazwy użytkownika. Nazwy użytkownika i dziedziny jednoznacznie identyfikują użytkowników Kerberos w pliku kluczy. Na przykład nazwa użytkownika jkowalski w dziedzinie ordept.firma.com jest reprezentowana w pliku kluczy jako jkowalski@ordept.firma.com.
   - Wybierając opcję **Nazwa użytkownika Kerberos i hasło**, musisz podać następujące informacje:
     - W polu **Nazwa użytkownika** wpisz nazwę użytkownika Kerberos identyfikującą użytkownika, który ma uprawnienia do tworzenia obiektów w lokalnej przestrzeni nazw serwera LDAP.
     - W polu **Dziedzina** wpisz nazwę dziedziny Kerberos dla nazwy użytkownika.
     - W polu **Hasło** wpisz hasło użytkownika.

- W polu **Potwierdź hasło** wpisz ponownie hasło. Nazwy użytkownika i dziedziny jednoznacznie identyfikują użytkowników Kerberos w pliku kluczy. Na przykład nazwa użytkownika jkowalski w dziedzinie ordept.firma.com jest reprezentowana w pliku kluczy jako jkowalski@ordept.firma.com.

- Kliknij przycisk **Sprawdź połączenie**, aby przetestować informacje konfiguracyjne użytkownika, łącząc się z kontrolerem domeny.
- Kliknij przycisk **Dalej**.

7. Na stronie **Podaj domenę** wybierz nazwę domeny, którą chcesz przyłączyć, i kliknij przycisk **Dalej**.
8. Na stronie **Informacje o rejestrze** wybierz typ rejestrów użytkowników, który chcesz dodać do tej domeny EIM. Wybierz jeden lub oba poniższe typy rejestrów użytkowników:
   - Wybierz **OS400**, aby dodać do domeny EIM rejestr użytkowników reprezentujący rejestr lokalny. W dostępnym polu wpisz nazwę rejestru, który ma zostać utworzony w domenie. Nazwa rejestru EIM jest arbitralnym łańcuchem reprezentującym typ rejestru i konkretną instancję tego rejestru.
   - Wybierz **Kerberos**, aby do domeny EIM dodać rejestr użytkowników Kerberos. W dostępnym polu wpisz nazwę rejestru, który ma zostać utworzony w domenie, i jeśli to konieczne, wybierz opcję **Rozróżnianie wielkości liter w tożsamościach użytkowników Kerberos**. Możesz zaakceptować wartość domyślną; nazwa rejestru Kerberos jest wtedy taka sama jak nazwa dziedziny. Używając identycznych nazw rejestru Kerberos i dziedziny, możesz zwiększyć wydajność pobierania informacji z rejestru. Więcej informacji na temat definiowania rejestrów użytkowników w EIM zawiera temat Definicje rejestrów EIM.
   - Kliknij przycisk **Dalej**.
9. W oknie dialogowym **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 wyszukiwania odwzorowań i usuwanie powiązań podczas usuwania lokalnego profilu użytkownika OS/400. Dostępne są następujące typy użytkowników: Nazwa wyróżniająca i hasło, Plik kluczy Kerberos i nazwa użytkownika oraz Nazwa użytkownika Kerberos i hasło. Od wybranego typu użytkownika zależą inne informacje, które należy podać w tym oknie:
   - Wybierając opcję **Nazwa wyróżniająca i hasło**, musisz podać następujące informacje:
     - W polu **Nazwa wyróżniająca** wpisz nazwę wyróżniającą LDAP identyfikującą użytkownika w systemie OS/400, która to nazwa ma być używana podczas łączenia się z kontrolerem domeny EIM.
     - W polu **Hasło** wpisz hasło użytkownika.
     - W polu **Potwierdź hasło** wpisz ponownie hasło.
   - Wybierając opcję **Nazwa użytkownika Kerberos i hasło**, musisz podać następujące informacje:
     - W polu **Nazwa użytkownika** wpisz nazwę użytkownika Kerberos identyfikującą użytkownika w systemie OS/400, która to nazwa ma być używana podczas łączenia się z kontrolerem domeny EIM.
     - W polu **Dziedzina** wpisz nazwę dziedziny Kerberos dla nazwy użytkownika.
     - W polu **Hasło** wpisz hasło użytkownika.
     - W polu **Potwierdź hasło** wpisz ponownie hasło. Nazwy użytkownika i dziedziny jednoznacznie identyfikują użytkowników Kerberos w pliku kluczy. Na przykład nazwa użytkownika jkowalski w dziedzinie ordept.firma.com jest reprezentowana w pliku kluczy jako jkowalski@ordept.firma.com.
   - Wybierając opcję **Plik kluczy Kerberos i nazwa użytkownika**, musisz podać następujące informacje:
     - W polu **Plik kluczy** wpisz nazwę pliku kluczy na serwerze iSeries identyfikującą użytkownika w systemie OS/400, która to nazwa ma być używana podczas łączenia się z kontrolerem domeny EIM. Możesz też kliknąć przycisk **Przeglądaj**, aby wybrać plik kluczy.
     - W polu **Nazwa użytkownika** wpisz nazwę użytkownika Kerberos, która ma być używana do zidentyfikowania użytkownika.
     - W polu **Dziedzina** wpisz nazwę dziedziny Kerberos dla nazwy użytkownika.

- Kliknij przycisk **Sprawdź połączenie**, aby przetestować połączenie dla utworzonego użytkownika systemu.
- Kliknij przycisk **Dalej**.

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

Zakończenie pracy kreatora jest jednoznaczne z zakończeniem podstawowej konfiguracji EIM. Jednak aby sfinalizować konfigurację EIM dla tego serwera, należy wykonać następujące zadania:

1. Dodawanie domeny, która została podłączona, do folderu zarządzania domenami EIM.
2. Dodawanie rejestrów EIM do domeny EIM dla innych niż iSeries aplikacji i serwerów, które mają należeć do danej domeny EIM.
3. Tworzenie identyfikatorów EIM w domenie dla każdego unikalnego użytkownika lub jednostki dla systemów należących do domeny EIM.
4. Tworzenie powiązań między różnymi tożsamościami osoby lub jednostki a identyfikatorami EIM.

Ponadto, aby aktywować środowisko pojedynczego wpisywania się, należy skonfigurować usługę uwierzytelniania sieciowego dla serwera iSeries.

Zarządzanie EIM

Po skonfigurowaniu EIM na serwerze iSeries udostępnionych zostaje wiele zadań służących do zarządzania domeną EIM oraz informacjami. W podanych niżej tematach opisano poszczególne zadania używane do zarządzania EIM na serwerze iSeries i w sieci przedsiębiorstwa.

Zarządzanie domenami EIM
Podaje informacje EIM zawarte w domenie EIM i właściwościach tej domeny.

Zarządzanie powiązaniami
Zarządza powiązaniami tożsamości użytkowników z identyfikatorami EIM wszystkich użytkowników w przedsiębiorstwie.

Zarządzanie identyfikatorami EIM
Obsługuje identyfikatory EIM powiązane z użytkownikami w przedsiębiorstwie.

Zarządzanie uprawnieniami użytkowników EIM
Chroni informacje EIM, pracując z uprawnieniami EIM podczas sterowania operacjami i funkcjami EIM, które mogą wykonywać użytkownicy.

Zarządzanie rejestrami użytkowników
Obsługuje rejestry użytkowników, które zostały dodane do domeny EIM.

Zarządzanie domenami EIM

Do zarządzania wszystkimi domenami EIM można użyć programu iSeries Navigator. Aby można było zarządzać daną domeną EIM, musi ona znajdować się na liście domen w folderze Zarządzanie domenami dostępnym w gałęzi Sieć w programie iSeries Navigator lub należy ją do tej listy dodać. Po utworzeniu i skonfigurowaniu nowej domeny EIM aby móc nią zarządzać, należy ją dodać do folderu Zarządzanie domenami.

Do zarządzania domeną EIM istniejącą w dowolnym miejscu w tej samej sieci można użyć dowolnego połączenia iSeries. Serwer iSeries, który został podłączony w programie iSeries Navigator, nie musi należeć do danej domeny, aby mógł nią zarządzać.

Zarządzanie domenami EIM obejmuje następujące zadania:

- Dodawanie domeny do zarządzania domenami

- Połączenie się z domeną
- Usuwanie domeny
- Usuwanie domeny z zarządzania domenami

Dodawanie domeny do zarządzania domenami

Aby dodać domenę, należy mieć uprawnienia specjalne *SECADM. Aby do zarządzania domenami dodać istniejącą domenę EIM:

1. Rozwiń gałąź **Sieć —> Enterprise Identity Mapping**.
2. Prawym przyciskiem myszy kliknij **Zarządzanie domenami** i wybierz **Dodaj domenę...**
3. Podaj informacje o domenie i połączeniu.
4. Kliknij przycisk **OK**, aby dodać domenę.

Połączenie się z domeną

Jeśli w tej chwili nie masz połączenia z domeną EIM, w której chcesz pracować, musisz się najpierw z nią połączyć. Z daną domeną EIM możesz połączyć się nawet wtedy, gdy używany serwer iSeries nie jest skonfigurowany w tej domenie.

Aby połączyć się z domeną EIM:

1. Rozwiń gałąź **Sieć —> Enterprise Identity Mapping —> Zarządzanie domenami**.
2. Wybierz domenę, z którą chcesz się połączyć. Jeśli domeny, z którą chcesz pracować, nie ma na liście, musisz dodać domenę EIM do zarządzania domenami.
3. Prawym przyciskiem myszy kliknij domenę EIM, z którą chcesz się połączyć, i wybierz **Połącz...**
4. Podaj typ użytkownika i wymagane informacje o użytkowniku, które mają być używane do połączenia się z kontrolerem domeny EIM.
5. Kliknij przycisk **OK**.

Usuwanie domeny

Do wykonania tego zadania niezbędne są uprawnienia administratora LDAP lub uprawnienia administratora EIM. Przed usunięciem domeny EIM należy najpierw usunąć z niej wszystkie rejestry i informacje o identyfikatorach EIM.

Aby usunąć domenę EIM:

1. Rozwiń gałąź **Sieć —> Enterprise Identity Mapping —> Zarządzanie domenami**.
2. Z wybranej domeny EIM usuń wszystkie rejestry użytkowników.
3. Z wybranej domeny EIM usuń wszystkie identyfikatory EIM.
4. Prawym przyciskiem myszy kliknij domenę, którą chcesz usunąć, i kliknij przycisk **Usuń...**
5. W oknie dialogowym **Potwierdzenie usunięcia** kliknij **Tak**.

Usuwanie domeny z zarządzania domenami

Chociaż nie jest to konieczne, po wprowadzeniu zmian daną domenę można usunąć z zarządzania domenami.

Aby usunąć domenę:

1. Rozwiń gałąź **Sieć —> Enterprise Identity Mapping**.
2. Prawym przyciskiem myszy kliknij **Zarządzanie domenami** i wybierz **Usuń domenę...**
3. Wybierz domenę EIM, którą chcesz usunąć z zarządzania domenami.
4. Kliknij przycisk **OK**, aby usunąć domenę.

Zarządzanie powiązaniami

Powiązanie definiuje relację między identyfikatorem EIM a tożsamością użytkownika w rejestrze. Na przykład można utworzyć powiązanie między profilem użytkownika OS/400 lub nazwą użytkownika

protokołu Kerberos a identyfikatorem EIM. Można je następnie użyć do określenia, który identyfikator EIM odpowiada lokalnemu profilowi użytkownika iSeries lub nazwie użytkownika protokołu Kerberos.

Obsługa powiązań tożsamości użytkowników wraz z odpowiednimi identyfikatorami EIM umożliwia uproszczenie zadań administracyjnych wymaganych do śledzenia, którzy użytkownicy mają konta w różnych systemach w danej sieci.

Zarządzanie powiązaniami umożliwia wykorzystanie zalet obsługi pojedynczego wpisywania się w sieci. Implementując chronioną sieć z pojedynczym wpisywaniem się, należy regularnie aktualizować powiązania.

Istnieją trzy typy powiązań, które można utworzyć: źródłowe, docelowe i administracyjne. Do utworzenia lub obsługi powiązań między tożsamościami użytkowników a odpowiednimi identyfikatorami EIM, można użyć następujących zadań:

- Tworzenie powiązania
- Usuwanie powiązania

Tworzenie powiązania

W celu aktywowania środowiska pojedynczego wpisywania się należy utworzyć powiązania między różnymi tożsamościami użytkowników, którymi mogą być osoby lub jednostki, a pojedynczymi identyfikatorami EIM tych użytkowników. Można utworzyć powiązania docelowe, źródłowe i administracyjne.

Aby utworzyć powiązanie administracyjne, należy mieć uprawnienie administratora identyfikatorów lub uprawnienie administratora EIM. Aby utworzyć powiązanie docelowe, należy mieć uprawnienie administratora wszystkich rejestrów, uprawnienie administratora konkretnego rejestru lub uprawnienie administratora EIM.

Aby utworzyć powiązanie dla identyfikatora EIM:

1. Rozwiń gałąź **Sieć —> Enterprise Identity Mapping —> Zarządzanie domenami**.
2. Uzyskaj połączenie z domeną 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. Rozwiń domenę EIM, z którą masz połączenie.
4. Kliknij **Identyfikatory**, aby wyświetlić listę identyfikatorów EIM.
5. Prawym przyciskiem myszy kliknij odpowiedni identyfikator EIM i wybierz **Właściwości...**
6. Kliknij zakładkę **Powiązania**.
7. Kliknij przycisk **Dodaj...**, aby wyświetlić okno dialogowe **Dodaj powiązanie**.
8. Kliknij przycisk **Pomoc**, jeśli podczas wypełniania pól potrzebujesz więcej informacji.
9. Po podaniu wymaganych informacji, kliknij przycisk **OK**.

Usuwanie powiązania

Aby usunąć powiązanie administracyjne lub źródłowe, należy mieć uprawnienia administratora identyfikatorów lub uprawnienia administratora EIM. Aby usunąć powiązanie docelowe, należy mieć uprawnienia administratora dla wybranych rejestrów (w tym dla rejestru, z którym chcesz pracować), uprawnienia administratora rejestrów lub uprawnienia administratora EIM.

Aby usunąć powiązanie:

1. Rozwiń gałąź **Sieć —> Enterprise Identity Mapping —> Zarządzanie domenami**.
2. Uzyskaj połączenie z domeną 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 domeną EIM.

3. Rozwiń domenę EIM, z którą masz połączenie.
4. Kliknij **Identyfikatory**.
5. Prawym przyciskiem myszy kliknij identyfikator EIM, a następnie wybierz **Właściwości...**
6. Kliknij zakładkę **Powiązania**, aby wyświetlić bieżące powiązania dla tego identyfikatora EIM.
7. Wybierz powiązanie, które chcesz usunąć.
8. Kliknij przycisk **Usuń**, aby usunąć powiązanie.
9. Kliknij przycisk **OK**.

Zarządzanie identyfikatorami EIM

Obsługa identyfikatorów EIM reprezentujących użytkowników w sieci jest bardzo ważna ze względu na właściwą ochronę. Użytkownicy w przedsiębiorstwie prawie zawsze zmieniają się. Jedni przychodzą, drudzy odchodzą, a jeszcze inni są przenoszeni między działami. Zachodzące zmiany wymagają śledzenia kont użytkowników i dostępu, który mają oni do systemów w sieci. Utworzenie identyfikatorów EIM i powiązanie ich z tożsamościami odpowiednich użytkowników ułatwia to śledzenie.

Obsługa pojedynczego wpisywania się powoduje, że wykonywanie zadań przez użytkowników jest znacznie łatwiejsze, zwłaszcza gdy są oni przenoszeni między działami lub innymi obszarami przedsiębiorstwa. Uprawnienia dostępu i potrzeby dostępu do systemu takich użytkowników również mogą się zmienić. Dzięki obsłudze pojedynczego wpisywania się użytkownicy ci nie muszą pamiętać nowych nazw i haseł w nowych systemach.

Zarządzanie identyfikatorami EIM użytkowników w przedsiębiorstwie obejmuje wiele rutynowych zadań. Do zarządzania identyfikatorami EIM w sieci i domenach służą następujące zadania:

- Tworzenie identyfikatora EIM
- Dodawanie aliasu do identyfikatora EIM
- Usuwanie identyfikatora EIM

Informacje na temat zarządzania powiązaniami zawiera temat Zarządzanie powiązaniami.

Tworzenie identyfikatora EIM

Aby utworzyć identyfikator EIM, należy mieć uprawnienia administratora identyfikatorów lub uprawnienia administratora EIM.

Aby utworzyć identyfikator EIM dla wybranej osoby lub jednostki:

1. Rozwiń gałąź **Sieć —> Enterprise Identity Mapping —> Zarządzanie domenami**.
2. Uzyskaj połączenie z domeną 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 domeną.
3. Rozwiń domenę EIM, z którą masz połączenie.
4. Prawym przyciskiem myszy kliknij **Identyfikatory** i wybierz **Nowy identyfikator...**
5. Kliknij przycisk **Pomoc**, jeśli potrzebujesz więcej informacji na temat poszczególnych pól.
6. Po podaniu wymaganych informacji, kliknij przycisk **OK**.

Dodawanie aliasu do identyfikatora EIM

Aby udostępnić dodatkowe informacje wyróżniające, dla identyfikatora EIM można utworzyć alias. Alias ten może być następnie używany przez użytkowników do odróżnienia identyfikatorów EIM. 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.

Aby do identyfikatora dodać alias, należy mieć uprawnienia administratora identyfikatorów lub uprawnienia administratora EIM.

Aby do identyfikatora EIM dodać alias:

1. Rozwiń gałąź **Sieć —> Enterprise Identity Mapping —> Zarządzanie domenami**.
2. Uzyskaj połączenie z domeną 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. Rozwiń domenę EIM, z którą masz połączenie.
4. Prawym przyciskiem myszy kliknij identyfikator EIM, który chcesz wybrać, a następnie wybierz **Właściwości**. Jeśli nie ma żadnych identyfikatorów EIM, patrz temat Tworzenie identyfikatora EIM.
5. Podaj nazwę aliasu, który chcesz dodać do tego identyfikatora EIM i kliknij przycisk **Dodaj**.
6. Kliknij przycisk **OK**, aby zapisać zmiany.

Usuwanie identyfikatora EIM

Aby usunąć identyfikator EIM, należy mieć uprawnienia administratora EIM.

Aby usunąć identyfikator EIM:

1. Rozwiń gałąź **Sieć —> Enterprise Identity Mapping —> Zarządzanie domenami**.
2. Uzyskaj połączenie z domeną 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. Rozwiń domenę EIM, z którą masz połączenie.
4. Kliknij **Identyfikatory**.
5. Wybierz jeden lub więcej identyfikatorów przeznaczonych do usunięcia.
6. Prawym przyciskiem myszy kliknij wybrane identyfikatory EIM i wybierz **Usuń**.
7. Aby usunąć wybrane identyfikatory EIM, w oknie dialogowym **Potwierdzenie usunięcia** kliknij **Tak**.

Zarządzanie uprawnieniami użytkowników EIM

EIM definiuje wielorakie uprawnienia EIM potrzebne do wykonania różnych operacji w domenie. Do operacji tych należą funkcje zarządzania domeną, takie jak tworzenie identyfikatorów, wyświetlanie rejestrów i wykonywanie operacji wyszukiwania odwzorowania. Nadawanie i odbieranie uprawnień innym użytkownikom jest zarezerwowane tylko dla użytkowników o uprawnieniach administratora EIM.

Krótki opis poszczególnych grup uprawnień oraz szczegóły dotyczące dostępu do niektórych funkcji EIM, który można uzyskać za pomocą tych uprawnień, zawiera temat Uprawnienia EIM.

Aby zmienić uprawnienia EIM użytkownika:

1. W programie iSeries Navigator rozwiń gałąź **Sieć —> Enterprise Identity Mapping —> Zarządzanie domenami**.
2. Rozwiń domenę EIM, w której chcesz pracować. Jeśli nie masz z nią połączenia, zostanie wyświetlona zachęta do nawiązania połączenia. Pamiętaj o połączeniu się z domeną za pomocą identyfikatora użytkownika o uprawnieniach administratora EIM.
3. Prawym przyciskiem myszy kliknij domenę EIM i wybierz **Uprawnienie...**

4. W oknie dialogowym **Edycja uprawnienia EIM** podaj użytkownika, którego uprawnienia EIM chcesz zmienić.
5. Kliknij przycisk **OK**.
6. W oknie dialogowym **Edycja uprawnienia EIM** wprowadź niezbędne zmiany w uprawnieniach użytkownika.
7. Kliknij przycisk **OK**, aby zapisać zmiany w uprawnieniach.

Zarządzanie rejestrami użytkowników

Przed utworzeniem powiązań między tożsamościami dostępnymi w rejestrach użytkowników a odpowiednimi identyfikatorami EIM w domenie EIM należy zdefiniować rejestr użytkowników.

Poniższe zadania dotyczą zarządzania rejestrami użytkowników w domenie EIM.

- Dodawanie rejestru użytkowników
- Dodawanie aliasu do rejestru użytkowników
- Definiowanie prywatnego typu rejestru użytkowników w EIM
- Usuwanie rejestru użytkowników
- Usuwanie aliasu z rejestru użytkowników

Dodawanie rejestru użytkowników

Aby dodać rejestr użytkowników, należy mieć uprawnienie administratora EIM. Szczegóły dotyczące tego uprawnienia i opis możliwości użytkownika, który je ma, znajdują się w temacie Uprawnienia EIM.

Aby dodać rejestr użytkowników do domeny EIM:

1. Rozwiń gałąź **Sieć —> Enterprise Identity Mapping —> Zarządzanie domenami**.
2. Połącz się z domeną EIM, używając identyfikatora użytkownika, który ma uprawnienie administratora EIM.
   - 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. Rozwiń domenę EIM, z którą masz połączenie.
4. Prawym przyciskiem myszy kliknij **Rejestry użytkowników** i wybierz **Dodaj rejestr...**.
5. Podaj wymagane informacje o rejestrze użytkowników. Możesz także podać informacje o aliasie dla tego rejestru użytkowników.
6. Kliknij **OK**, aby zapisać podane informacje i dodać rejestr użytkowników do wybranej domeny EIM.

Dodawanie aliasu do rejestru użytkowników

Użytkownik lub programista aplikacji może utworzyć alias, aby dostarczyć dodatkowe informacje wyróżniające dla rejestru użytkowników. Alias ten może być następnie używany przez użytkowników do rozróżniania rejestrów użytkowników. Na przykład programiści aplikacji i administratorzy używają aliasu w rejestrze użytkowników do określenia, które rejestry EIM powinny być używane przez aplikacje. Informacje na temat sposobu używania aliasów z rejestrami użytkowników zawiera temat dotyczący definicji rejestrów EIM.

Aby dodać alias do rejestru użytkowników, należy użyć jednego z następujących uprawnień: administrator EIM, administrator wszystkich rejestrów lub administrator wybranego rejestru, którego dotyczy dane zadanie.

Aby dodać alias do rejestru użytkowników w domenie EIM:

1. Rozwiń gałąź **Sieć —> Enterprise Identity Mapping —> Zarządzanie domenami**.
2. Uzyskaj połączenie z domeną 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. Rozwiń domenę EIM, z którą masz połączenie.
4. Kliknij **Rejestry użytkowników**, aby wyświetlić listę rejestrów w tej domenie.
5. Prawym przyciskiem myszy kliknij rejestr użytkowników, do którego dodajesz alias, i wybierz **Właściwości...**.
6. W oknie dialogowym **Właściwości** kliknij zakładkę **Alias**.
7. Podaj nazwę i typ aliasu, który chcesz dodać. Możesz podać typ aliasu, którego nie ma na liście typów.
8. Kliknij przycisk **Dodaj**.
9. Kliknij przycisk **OK**, aby zapisać zmiany.

Definiowanie prywatnego typu rejestru użytkowników w EIM

Aby zdefiniować typ rejestru użytkowników, który nie jest domyślnie rozpoznawany przez EIM, należy 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 dla systemu OS/400 może być 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). Formularz fact sheet z odsyłaczami do formularzy zgłoszeniowych znajduje się w serwisie WWW instytutu ANSI: http://web.ansi.org/public/services/reg_org.html

  . 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), tworząc nowy łuk identyfikatorów obiektów: 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.
- Innym punktem początkowym jest międzynarodowy rejestr schematów ISO DCC NSAP. NSAP (Network Service Access Point) to punkt dostępu do usługi. Skrót ten jest używany w wielu standardach międzynarodowych. Rejestr schematów jest dostępny pod adresem http://www.fei.org.uk po wybraniu nagłówka ISO DCC NSAP

  . W tym serwisie dostępna jest lista zawierająca informacje kontaktowe trzynastu ośrodków nadawania nazw, spośród których niektóre przypisują także identyfikatory obiektów.
- 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/

  .

Więcej informacji na temat identyfikatorów obiektów dla strategii certyfikatów można znaleźć pod adresem http://csrc.nist.gov/csor/pkireg.htm

.

Usuwanie rejestru użytkowników

Usunięcie rejestru użytkowników z domeny EIM powoduje utratę wszystkich powiązań z identyfikatorami EIM dla tożsamości użytkowników w danym ich rejestrze. Dodanie z powrotem rejestru użytkowników do domeny EIM po jego uprzednim usunięciu nie resetuje relacji powiązań.

Aby usunąć rejestr użytkowników, należy mieć uprawnienia administratora EIM.

Aby usunąć rejestr użytkowników:

1. Rozwiń gałąź **Sieć —> Enterprise Identity Mapping —> Zarządzanie domenami**.
2. Uzyskaj połączenie z domeną 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. Rozwiń domenę EIM, z którą masz połączenie.
4. Kliknij **Rejestry użytkowników**, aby wyświetlić listę rejestrów w tej domenie.
5. Prawym przyciskiem myszy kliknij rejestr użytkowników, który chcesz usunąć, i kliknij przycisk **Usuń...**
6. W oknie dialogowym **Potwierdzenie** kliknij przycisk **Tak**, aby usunąć wybrany rejestr użytkowników.

Usuwanie aliasu z rejestru użytkowników

Aby usunąć alias z rejestru użytkowników, należy mieć uprawnienia administratora rejestrów i uprawnienia administratora wybranych rejestrów (dotyczy to także rejestru, z którym chcemy pracować) lub uprawnienia administratora EIM.

Aby usunąć alias z rejestru użytkowników w domenie EIM:

1. Rozwiń gałąź **Sieć —> Enterprise Identity Mapping —> Zarządzanie domenami**.
2. Uzyskaj połączenie z domeną 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. Rozwiń domenę EIM, z którą masz połączenie.
4. Kliknij **Rejestry użytkowników**, aby wyświetlić listę rejestrów w tej domenie.
5. Prawym przyciskiem myszy kliknij rejestr użytkowników, z którego usuwasz alias i wybierz **Właściwości**.
6. W oknie dialogowym **Właściwości** kliknij zakładkę **Alias**.
7. Wybierz alias, który chcesz usunąć, i kliknij **Usuń**.
8. Kliknij przycisk **OK**, aby zapisać zmiany.

Funkcje API EIM

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.

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.

Pełną listę funkcji API dla EIM dostępnych dla serwera iSeries wraz ze szczegółowymi informacjami można znaleźć w temacie Funkcje API Enterprise Identity Mapping (EIM).

Rozwiązywanie problemów dotyczących EIM

W EIM zawarto wiele technologii, aplikacji i funkcji. Ponieważ do uporania się z problemami można wykorzystać wiele metod, poniższe tematy zawierają szczegółowe informacje i instrukcje dotyczące sposobów rozwiązywania często występujących problemów, takich jak:

- Nie można połączyć się z kontrolerem domeny
- Wyświetlenie identyfikatorów EIM trwa długo
- Kreator konfigurowania EIM zawiesza się pod koniec przetwarzania
- Uchwyt EIM nie jest poprawny
- Uwierzytelnianie Kerberos i komunikaty diagnostyczne

Nie można połączyć się z kontrolerem domeny

Problemy z nawiązaniem połączenia z kontrolerem domeny mogą być spowodowane wieloma czynnikami. Aby znaleźć przyczynę problemu:

- Sprawdź, czy informacje podane dla następujących pozycji są poprawne:
  - nazwa kontrolera domeny,
  - port,
  - ID i hasło użytkownika.
- Sprawdź, czy kontroler domeny jest aktywny. Jeśli kontrolerem domeny jest serwer iSeries, możesz użyć programu iSeries Navigator:
  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 aktywowaniu domeny spróbuj nawiązać z nią połączenie.

1. Rozwiń gałąź **Sieć —> Enterprise Identity Mapping —> Zarządzanie domenami**.
2. Wybierz domenę, z którą chcesz się połączyć. Jeśli domena EIM, z którą chcesz pracować, nie została wyświetlona w folderze Zarządzanie domenami lub brak jakichkolwiek domen, musisz dodać domenę EIM do zarządzania domenami.
3. Prawym przyciskiem myszy kliknij domenę EIM, z którą chcesz się połączyć, i wybierz **Połącz...**
4. Podaj typ użytkownika i wymagane informacje o użytkowniku, które mają być używane do połączenia się z kontrolerem domeny EIM.
5. Kliknij przycisk **OK**.

Wyświetlenie identyfikatorów EIM trwa długo

Podczas otwierania folderu Identyfikatory w programie iSeries Navigator może okazać się, że trzeba czekać bardzo długo na wyświetlenie listy identyfikatorów. Jeśli w domenie jest duża liczba identyfikatorów EIM, do ich wyświetlenia korzystne może być zawężenie kryteriów wyszukiwania.

Aby dostosować wyświetlanie identyfikatorów EIM:

1. W programie iSeries Navigator rozwiń gałąź **Sieć —> Enterprise Identity Mapping —> Zarządzanie domenami**.
2. Rozwiń domenę, dla której chcesz wyświetlić identyfikatory EIM.
3. Prawym przyciskiem myszy kliknij **Identyfikator** i wybierz **Dostosuj ten widok —> Pokaż...**
4. Podaj kryteria wyświetlania. Jako znaku zastępczego można użyć gwiazdki (*).

5. Kliknij przycisk OK.

Kolejne kliknięcie pozycji **Identyfikatory** spowoduje wyświetlenie tylko tych identyfikatorów EIM, które spełniają podane kryteria. Jeśli chcesz wyświetlić wszystkie identyfikatory EIM, wykonaj powyższe kroki, aby wybrać dostosowaną opcję wyświetlania **Wszystkie identyfikatory**.

Kreator konfigurowania EIM zawiesza się pod koniec przetwarzania

Jeśli kreator zawiesi się pod koniec przetwarzania, być może czeka on na uruchomienie kontrolera domeny. Sprawdź, czy podczas uruchamiania serwera LDAP 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 gałąź **Zarządzanie pracą —> Podsystemy —> Qsyswrk**.
2. Prawym przyciskiem myszy kliknij **Qdirsrv** i wybierz **Protokół zadania**.

Uchwyt EIM nie jest poprawny

Jeśli podczas zarządzania EIM za pomocą programu iSeries Navigator użytkownik otrzymuje błąd wskazujący, że uchwyt EIM nie jest poprawny, oznacza to, że połączenie z kontrolerem domeny zostało utracone.

Aby ponownie nawiązać połączenie z kontrolerem domeny:

1. W programie iSeries Navigator rozwiń gałąź **Sieć —> Enterprise Identity Mapping —> 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**.

Uwierzytelnianie Kerberos i komunikaty diagnostyczne

Podczas używania protokołu Kerberos do uwierzytelniania w EIM, komunikat diagnostyczny CPD3E3F jest zapisywany do protokołu zadania za każdym razem, gdy uwierzytelnianie lub operacje odwzorowywania tożsamości nie powiodą się. 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.

Informacje pokrewne dotyczące EIM

Aby lepiej poznać inne technologie dotyczące EIM, można zapoznać się z następującymi tematami zamieszczonymi w Centrum informacyjnym:

- **Usługa uwierzytelniania sieciowego**
  Informacje dotyczące konfigurowania usługi uwierzytelniania sieciowego na serwerze iSeries. Usługa ta umożliwia serwerowi iSeries należenie do istniejącej sieci Kerberos. Użycie usługi uwierzytelniania sieciowego wraz z EIM umożliwia aktywowanie pojedynczego wpisywania się w sieci.
- **Directory Services (LDAP)**
  Informacje dotyczące konfigurowania oraz informacje konceptualne na temat Directory Services (LDAP). EIM używa serwera LDAP do przechowywania danych EIM i odwzorowywania powiązań.