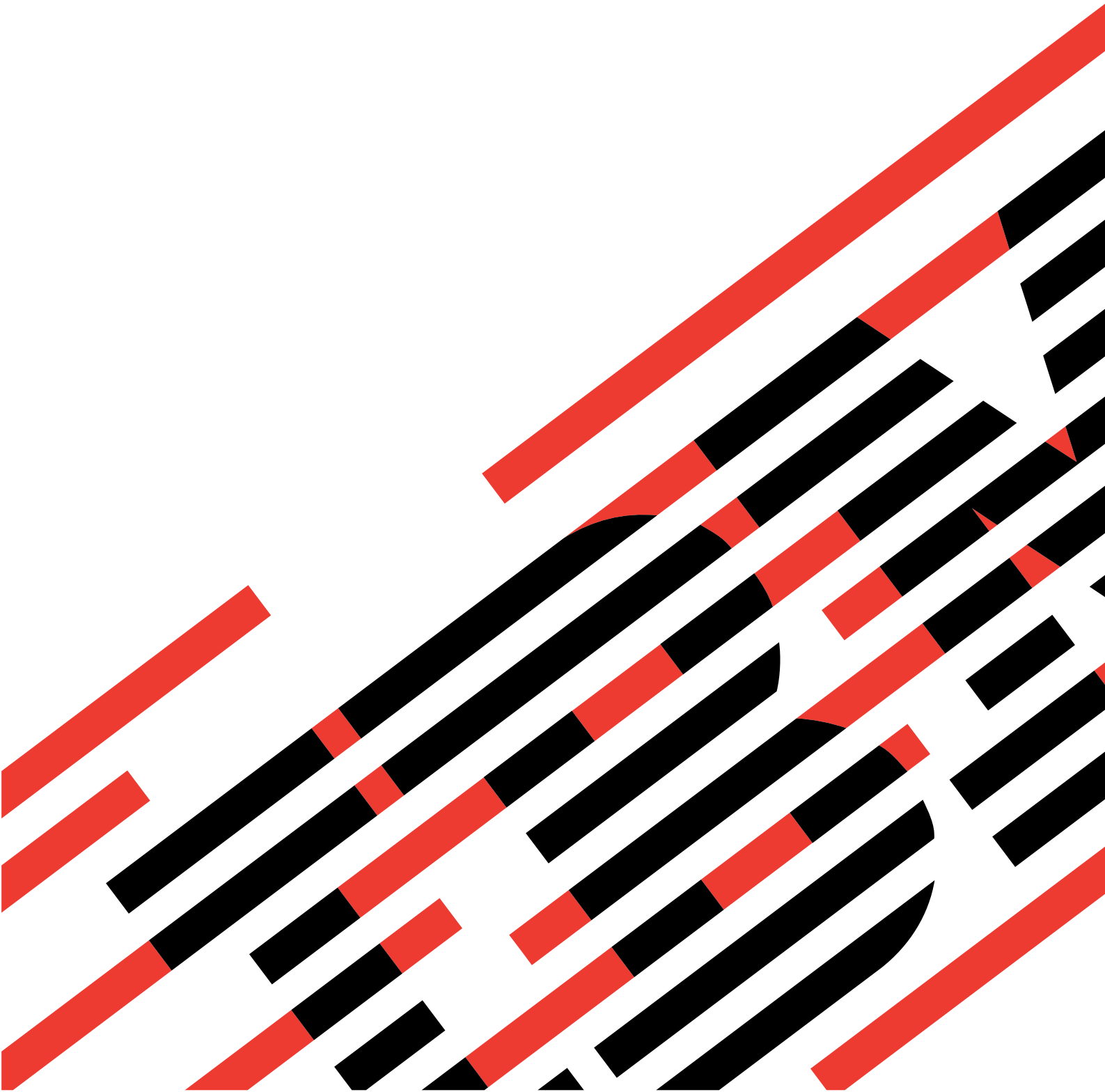
IBM

eserver

iSeries

Sieciowe usługi katalogowe (LDAP)



IBM

@server

iSeries

Sieciowe usługi katalogowe (LDAP)

Spis treści

Część 1. Usługi katalogowe (LDAP)

Produkt Usługi katalogowe udostępnia usługi serwera LDAP (Lightweight Directory Access Protocol) w serwerze iSeries. LDAP działa w oparciu o protokół TCP/IP i jest popularny jako usługa katalogowa dla aplikacji internetowych i nie tylko.

Jeśli produkt Usługi katalogowe jest znany, można rozpocząć czytanie od sekcji informującej o nowościach dla tej wersji. Można także wydrukować lub wyświetlić wersję PDF artykułu Usługi katalogowe.

Poniższe artykuły są wprowadzeniem do Usług katalogowych i zawierają informacje pomocne w administrowaniu serwerem LDAP na serwerach iSeries:

Aby uzyskać dodatkowe informacje dotyczące Usług katalogowych, należy odwiedzić stronę główną Directory Services  .

Usługi katalogowe udostępniają serwer LDAP IBM SecureWay Directory  .

Rozdział 1. Co nowego w wersji V5R2

Do Usług katalogowych dodano następujące rozszerzenia i nowe funkcje.

- Począwszy od wersji V5R1 Usługi katalogowe są częścią podstawowego systemu operacyjnego. W wersji V5R2 opcja 32 nie jest już dostępna.
- Zostały rozszerzone funkcje ochrony, w celu dodatkowego zabezpieczenia danych przechowywanych w serwerze katalogów.
- Serwer katalogów LDAP może być teraz używany jako kontroler domeny dla domeny Enterprise Identity Mapping (EIM).
- Dla administratorów dostępna jest nowa opcja, dostępna z poziomu aplikacji iSeries Navigator, która może być wykorzystywana do nadawania uprawnień dostępu do serwera katalogów na poziomie administratora tym użytkownikom, którzy mają dostęp do funkcji Directory Services Administrator (QIBM_DIRSRV_ADMIN) systemu operacyjnego.
- Można wybrać, czy serwer katalogów ma używać określonych adresów IP, czy też wszystkich skonfigurowanych. Więcej informacji na ten temat znajduje się w sekcji “Zmiana portu lub adresu IP” na stronie 21.
- W wersji V5R2 do funkcji API **ldap_set_option** dodano nową opcję śledzenia debugowania. Opcja LDAP_OPT_DEBUG może być używana do pomocy przy diagnozowaniu problemów z klientami korzystającymi z funkcji API języka C protokołu LDAP. Więcej informacji znajduje się w sekcji “Korzystanie z opcji LDAP_OPT_DEBUG do śledzenia błędów” na stronie 67 lub Funkcje API Usług katalogowych w Centrum informacyjnym iSeries  .

Co nowego, a co uległo zmianie:

Informacje o dokonanych technicznych zmianach są zaznaczone w następujący sposób:

- znak  oznacza początek informacji nowych lub zmienionych,
- znak  oznacza koniec informacji nowych lub zmienionych.

Rozdział 2. Drukowanie tego dokumentu

Aby przejrzeć lub pobrać wersję PDF, wybierz Directory Services (LDAP) (około 323 kB lub 66 stron).

Inne informacje

Można także przejrzeć lub wydrukować dowolny z następujących plików PDF:

- *LDAP Implementation Cookbook*  .
- *Understanding LDAP*  .
- *Using LDAP for Directory Integration: A Look at IBM SecureWay Directory, Active Directory, and Domino*

- *Implementation and Practical Use of LDAP on the iSeries Server*  .

Aby zapisać plik PDF na stacji roboczej w celu jego dalszego wykorzystania:
1. Otwórz PDF w przeglądarce (kliknij powyższy odsyłacz).
2. W menu przeglądarki kliknij **Plik**.
3. Kliknij **Zapisz jako**.
4. Przejdź do katalogu, w którym chcesz zapisać plik PDF.
5. Kliknij **Zapisz**.

Pobieranie programu Adobe Acrobat Reader

Program Adobe Acrobat Reader, potrzebny do przegądania i drukowania plików PDF, można pobrać z serwisu WWW firmy Adobe (www.adobe.com/products/acrobat/readstep.html)  .

Rozdział 3. Pierwsze kroki w Usługach katalogowych

Produkt Usługi katalogowe udostępnia usługi serwera LDAP (Lightweight Directory Access Protocol) w serwerze iSeries. LDAP działa w oparciu o protokół TCP/IP i jest coraz bardziej popularny jako usługa katalogowa dla aplikacji internetowych i nie tylko. Większość czynności związanych z konfigurowaniem i administrowaniem serwerem katalogów LDAP w systemie OS/400 wykonywanych jest za pomocą interfejsu GUI programu iSeries Navigator. Aby administrować produktem Usługi katalogowe, należy zainstalować program iSeries Navigator na komputerze PC, który jest połączony z serwerem iSeries. Usług katalogowych można używać z aplikacjami obsługującymi protokół LDAP, takimi jak aplikacje poczty, które wyszukują na serwerach LDAP adresy poczty elektronicznej.

Oprócz serwera LDAP elementem produktu Usługi katalogowe są także:

- Klient LDAP systemu OS/400. Zawiera on zestaw funkcji API, których można używać w programach OS/400 w celu tworzenia własnych aplikacji klientów. Więcej informacji o funkcjach API znajduje się w sekcji Usługi katalogowe w artykule Programowanie w Centrum informacyjnym iSeries.
- Wersja 3.2 IBM SecureWay Directory Client Software Development Kit (SDK). Zawiera ona klienta LDAP dla Windows i następujące narzędzia:
  - narzędzie IBM SecureWay Directory Management Tool, które udostępnia graficzny interfejs użytkownika do zarządzania zawartością katalogu;
  - narzędzia wiersza komend (ldapsearch, ldapadd itp.);
  - funkcje API C LDAP (zbiory bibliotek, nagłówkowe i przykłady kodu źródłowego);
  - dostawcę usług LDAP IBM JNDI (ibmjndi.jar);
  - dokumentację online dla powyższych narzędzi; miejsca położenia i nazwy tych zbiorów HTML są w zbiorze o nazwie readme.

Jeśli Usługi katalogowe były używane we wcześniejszej wersji systemu OS/400, należy przejść do sekcji “Migracja do wersji V5R2 z wcześniejszych wersji Usług katalogowych” na stronie 11.

Wstęp dotyczący protokołu LDAP zawiera sekcja “Podstawy LDAP” na stronie 8. Jeśli serwery LDAP były używane na innych platformach, dobrze jest przeczytać tę sekcję, gdyż zawiera informacje ważne dla systemu OS/400.

Po zapoznaniu się z podstawowymi informacjami należy przejść do sekcji “Planowanie serwera katalogów LDAP” na stronie 11.

Informacje na temat instalowania i konfigurowania serwera katalogów zawiera sekcja “Instalowanie i konfigurowanie Usług katalogowych” na stronie 14.

Dokumentacja

Artykuł Usługi katalogowe w Centrum informacyjnym zawiera przegląd informacji dotyczących protokołu LDAP oraz uwagi głównie na temat zarządzania serwerem katalogów LDAP w systemie OS/400. Zawiera także pełną dokumentację dla SecureWay Directory Client SDK. Aby uzyskać dodatkowe informacje dotyczące protokołu LDAP, należy zapoznać się z następującymi informacjami:

- *LDAP Implementation Cookbook* .
- *Understanding LDAP* .
- *Using LDAP for Directory Integration: A Look at IBM SecureWay Directory, Active Directory, and Domino*
- *Implementation and Practical Use of LDAP on the iSeries server* .

- *LDAP: Programming Directory-enabled Applications with Lightweight Directory Access Protocol* by Tim Howes and Mark Smith.
- *Understanding and Deploying LDAP Directory Services* by Mark C. Smith, Gordon S. Good, and Tim Howes.

Dodatkowe informacje na temat Usług katalogowych w serwerze iSeries są dostępne na stronie głównej iSeries server Directory Services .

Uwaga: Część materiału zawartego w tym dokumencie stanowi pochodną dokumentacji dotyczącej protokołu LDAP, wydanej przez University of Michigan. Copyright © 1992-1996, Regents of the University of Michigan. Wszystkie prawa zastrzeżone.

Podstawy LDAP

Protokół LDAP jest protokołem usług katalogowych działającym w oparciu o protokół TCP/IP. LDAP w wersji 2 jest zdefiniowany w Internet Engineering Task Force (IETF) Request for Comments (RFC) 1777, *Lightweight Directory Access Protocol*. LDAP w wersji 3 jest zdefiniowany w IETF RFC 2251, *Lightweight Directory Access Protocol (v3)*. Można je odnaleźć w Internecie pod adresem:

http://www.ietf.org

Usługa katalogowa LDAP opiera się na modelu klient/serwer. Jeden lub kilka serwerów LDAP zawiera dane katalogowe. Klient LDAP łączy się z serwerem LDAP i wysyła żądanie. Serwer wysyła odpowiedź lub wskaźnik (odwołanie) do innego serwera LDAP.

Użycie protokołu LDAP:

Ponieważ protokół LDAP jest usługą katalogową, a nie bazą danych, dane znajdujące się w katalogu LDAP są danymi opisowymi opartymi na atrybutach. Użytkownicy LDAP znacznie częściej czytają dane znajdujące się w katalogu niż je zmieniają. Aktualizacje polegają na prostej zmianie wszystkiego lub niezmienianiu niczego. Powszechnie używane katalogi LDAP to np. książki telefoniczne online lub książki adresów poczty elektronicznej.

Struktura katalogów LDAP:

Model usług katalogowych LDAP oparty jest na **pozycjach** (które nazywa się też **obiektami**). Każda pozycja składa się z jednego lub kilku **atrybutów**, takich jak nazwisko lub adres, oraz **typu**. Oznaczenia atrybutów tworzone są zwykle z mnemoników, takich jak cn (oznacza nazwę zwykłą) lub mail (oznacza adres poczty elektronicznej).

Rys. 1 na stronie 10 przedstawia przykładowy katalog zawierający pozycje dla osoby o nazwisku Tim Jones z atrybutami *mail* i *telephoneNumber*. Inne możliwe atrybuty to *fax*, *title* (tytuł), *sn* (oznaczający nazwisko, surname) oraz *jpegPhoto*.

Każdy katalog ma **schemat**, który jest zestawem reguł określających strukturę i zawartość katalogu. Do edycji plików schematów dla serwera LDAP powinno się używać narzędzia IBM SecureWay Directory Management Tool (DMT). Po zainstalowaniu Usług katalogowych pliki znajdują się w systemie w katalogu /QIBM/UserData/OS400/DirSrv.

Uwaga: Oryginalne kopie plików w schemacie domyślnym znajdują się w katalogu /QIBM/ProdData/OS400/DirSrv. Jeśli potrzebne jest zastąpienie plików w katalogu UserData, można je przekopiować do katalogu /QIBM/ProdData/OS400/DirSrv.

Każda pozycja katalogu ma specjalny atrybut o nazwie **objectClass**. Decyduje on, które atrybuty są wymagane, a które dozwolone. Innymi słowy, wartości atrybutu objectClass określają reguły schematu, które musi spełniać pozycja.

Każda pozycja katalogu ma także poniższe **atrybuty operacyjne**, które serwer LDAP obsługuje automatycznie:

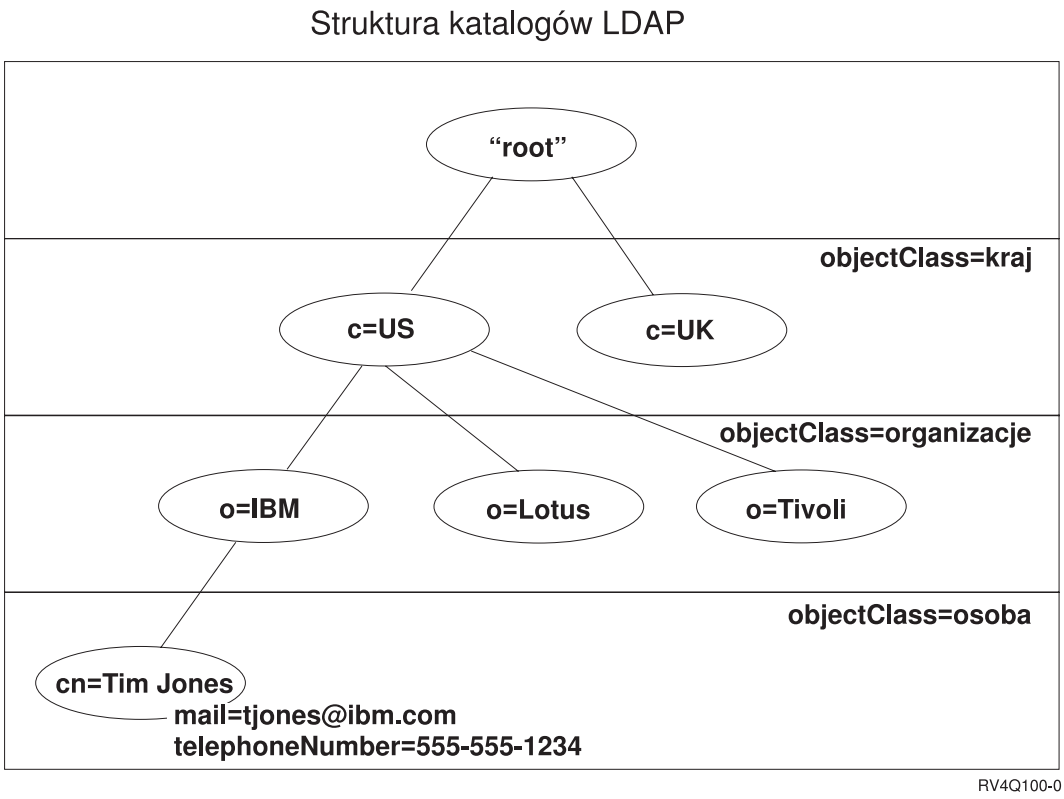
- CreatorsName zawiera nazwę wyróżniającą (DN) wiązania używaną podczas tworzenia pozycji.
- CreateTimestamp zawiera godzinę, o której pozycja została utworzona.
- modifiersName zawiera nazwę wyróżniającą, używaną podczas ostatniej modyfikacji (początkowo jego wartość jest taka sama jak CreatorsName).
- modifyTimestamp zawiera godzinę, o której pozycja została zmodyfikowana (początkowo jego wartość jest taka sama jak CreateTimestamp).

Tradycyjnie pozycje katalogu LDAP są ułożone hierarchicznie. Odzwierciedla to granice polityczne, geograficzne lub organizacyjne (patrz Rys. 1 na stronie 10). Pozycje przedstawiające kraje znajdują się jako pierwsze. Pozycje przedstawiające stany lub krajowe organizacje znajdują się jako drugie. Dalsze pozycje mogą reprezentować ludzi, jednostki organizacyjne, drukarki, dokumenty lub inne elementy.

Podczas tworzenia struktury katalogu użytkownik nie jest ograniczony do tradycyjnej hierarchii. Na przykład struktura ″według składników domeny″ cieszy się coraz większą popularnością. W tej strukturze pozycje składają się z części nazw domeny TCP/IP. Na przykład przypisanie dc=ibm,dc=com może być bardziej wskazane niż o=ibm,c=us.

Protokół LDAP odwołuje się do pozycji poprzez **nazwy wyróżniające (DN)**. Nazwy wyróżniające składają się z nazwy własnej pozycji, jak również nazw, w kolejności od dołu do góry, obiektów występujących wyżej w katalogu. Rys. 1 na stronie 10 przedstawia w lewym dolnym rogu przykładową pełną nazwę DN cn=Tim Jones, o=IBM, c=US. Każda pozycja ma przynajmniej jeden atrybut używany jako jej nazwa. Atrybut ten jest **względną nazwą wyróżniającą (RDN)** pozycji. Pozycja znajdująca się powyżej danej względnej nazwy wyróżniającej (RDN) jest nazywana jej **nadrzędną nazwą wyróżniającą**. W przedstawionym wyżej przykładzie cn=Tim Jones jest nazwą pozycji, a więc jest to RDN. o=IBM, c=US jest nadrzędną DN dla nazwy cn=Tim Jones.

Aby serwer LDAP zarządzał częścią katalogu LDAP, należy w konfiguracji serwera podać najwyższy poziom nadrzędnych nazw wyróżniających. Są one nazywane **przyrostkiem**. Serwer może uzyskać dostęp do wszystkich obiektów w katalogu, które w hierarchii katalogu znajdują się poniżej podanego przyrostka. Rys. 1 na stronie 10 przedstawia odpowiedni przykład: jeśli serwer LDAP zawierał katalog, to w konfiguracji będzie musiał mieć przyrostek o=ibm, c=us w celu umożliwienia klientowi odpowiadania na zapytania dotyczące Tim Jones.



Rysunek 1. Podstawowa struktura katalogu LDAP

Uwagi dotyczące LDAP i Usług katalogowych:

- Począwszy od wersji V4R5 zarówno serwer LDAP OS/400, jak i klient LDAP OS/400 opierają się na protokole LDAP w wersji 3. Możliwe jest używanie klienta V2 na serwerze V3. Nie można jednak użyć klienta V3 i serwera V2, chyba że zostanie on przypisany jako klient V2 i będzie korzystać tylko z funkcji API dla V2. Aby uzyskać dokładniejsze informacje, patrz Uwagi dla korzystających z protokołu LDAP V2/V3.
- Klient LDAP dla Windows również opiera się na protokole LDAP w wersji 3.
- Ponieważ protokół LDAP jest standardem, wszystkie serwery LDAP mają wiele wspólnych cech. Jednakże z powodu różnic w implementacji nie wszystkie są całkowicie zgodne ze sobą. Serwer LDAP udostępniony przez Usługi katalogowe jest zgodny z innymi serwerami katalogów LDAP w grupie produktów IBM SecureWay Directory i IBM Directory. Jednakże nie musi on być tak samo zgodny z innymi serwerami LDAP.
- Dane serwera LDAP, udostępnianego przez Usługi katalogowe, znajdują się w bazie danych OS/400.

Więcej informacji:

Przykłady użycia katalogów LDAP znajdują się w następujących sekcjach:

- Section 1.6 The Quick Start: A Public LDAP Example, w dokumentacji technicznej (redbook) *Understanding LDAP*.
- Section 3.3 Example Scenarios, w dokumentacji technicznej (redbook) Understanding LDAP.

Więcej informacji na temat założeń dotyczących LDAP zawiera Rozdział 5, “Pojęcia dotyczące Usług katalogowych” na stronie 35.

Uwagi dla korzystających z protokołu LDAP V2/V3

Począwszy od wersji V4R5 zarówno serwer LDAP OS/400, jak i klient LDAP OS/400 opierają się na protokole LDAP w wersji 3. Nie można używać klienta V3 na serwerze V2. Można jednak zmienić wersję klienta z V3 na V2 używając w tym celu funkcji API ldap_set_option(). Wówczas wysłanie zgłoszeń klienta do serwera V2 powiedzie się.

Można używać klienta V2 na serwerze V3. Należy jednak wziąć pod uwagę fakt, że przy żądaniu wyszukiwania serwer V3 może zwrócić dane w pełnym zakresie formatu UTF-8, podczas gdy klient V2 jest w stanie przetwarzać dane tylko w zestawach znaków IA5.

Uwaga: LDAP w wersji 2 jest zdefiniowany w Internet Engineering Task Force (IETF) Request for Comments (RFC) 1777, *Lightweight Directory Access Protocol*. LDAP w wersji 3 jest zdefiniowany w IETF RFC 2251, *Lightweight Directory Access Protocol (v3)*. Można je odnaleźć w Internecie pod adresem:

http://www.ietf.org 

Planowanie serwera katalogów LDAP

Przed zainstalowaniem Usług katalogowych i rozpoczęciem konfigurowania katalogu LDAP należy to zaplanować. Pomogą nam w tym następujące zagadnienia:

- **Zorganizowanie katalogu**. Należy zaplanować strukturę katalogu i określić przyrostki oraz atrybuty wymagane przez serwer.
- **Określenie wielkości katalogu**. Można wtedy oszacować, jak dużo pamięci potrzeba. Wielkość katalogu zależy od:
  - liczby atrybutów w schemacie serwera,
  - liczby pozycji na serwerze,
  - typu informacji przechowywanych na serwerze.

  Na przykład pusty katalog korzystający z domyślnego schematu produktu Usługi katalogowe wymaga około 10 MB przestrzeni pamięci. Katalog, który korzysta z domyślnego schematu i zawiera 1000 pozycji typowych informacji dotyczących pracowników, wymaga około 30 MB przestrzeni pamięci. Wielkość ta może się zmieniać w zależności od używanych atrybutów. Może ona znacznie wzrosnąć, jeśli w katalogu przechowuje się duże obiekty, takie jak obrazy.
- **Określenie potrzeb ochrony**. Usługi katalogowe dopuszczają używanie SSL oraz certyfikatów cyfrowych, a także TLS (Translation Layer Security) do ochrony komunikacji. Począwszy od wersji V5R1 obsługiwane jest także uwierzytelnianie protokołem Kerberos.
- Usługi katalogowe umożliwiają kontrolę dostępu do obiektów katalogu przy pomocy list kontroli dostępu (ACL). Do ochrony katalogu można także wykorzystać kontrolę ochrony OS/400.

Migracja do wersji V5R2 z wcześniejszych wersji Usług katalogowych

W wersji V5R2 OS/400 do Usług katalogowych dodano nowe opcje i możliwości. Zmiany te dotyczą zarówno serwera katalogów LDAP, jak i interfejsu GUI programu iSeries Navigator. Aby wykorzystywać nowe opcje interfejsu GUI, trzeba zainstalować iSeries Navigator na komputerze PC, który może komunikować się serwerem iSeries korzystając z protokołu TCP/IP. Program iSeries Navigator jest elementem iSeries Access for Windows. Jeśli na komputerze jest zainstalowana wcześniejsza wersja programu iSeries Navigator, należy dokonać jej aktualizacji do wersji V5R2.

Wersja V5R2 OS/400 obsługuje aktualizację z wersji V4R5 i V5R1. Podczas aktualizacji do wersji V5R2 OS/400, zarówno dane katalogu LDAP, jak i pliki schematów katalogów są automatycznie dostosowywane do formatów wersji V5R2. Jeśli migracji do wersji V5R2 ma podlegać serwer Usług katalogowych LDAP działający w wersji V4R3 lub V4R4 OS/400, to niezbędne jest wykonanie kilku dodatkowych działań związanych z migracją.

Podczas aktualizacji do wersji V5R2 OS/400 należy zwrócić uwagę na niektóre związane z nią aspekty:

- Podczas aktualizacji do wersji V5R2, Usługi katalogowe automatycznie wykonują migrację plików schematów do wersji V5R2, a stare pliki schematów są usuwane. Jeśli jednak pliki schematów zostały usunięte lub zmieniono ich nazwę, Usługi katalogowe nie mogą wykonać migracji. Może wtedy wystąpić błąd lub Usługi katalogowe mogą przyjąć, że wykonano już migrację plików.
- Usługi katalogowe wykonują migrację danych katalogowych do formatu V5R2 podczas pierwszego uruchomienia serwera lub imporcie pliku LDIF. Należy zarezerwować czas niezbędny na jej przeprowadzenie. Przy aktualizacji do wersji V5R2 z wersji V4R4 lub wcześniejszych należy zwrócić uwagę na fakt, iż dane katalogowe w wersji V5R2 będą wymagać około dwa razy więcej przestrzeni pamięci niż poprzednio. Dzieje się tak dlatego, że w wersji V4R4 i wcześniejszych Usługi katalogowe obsługiwały tylko zestaw znaków IA5 i przechowywały dane za pomocą CCSID=37 (format jednobajtowy). Usługi katalogowe obsługują pełny zestaw 10646 znaków ISO.

  Po uaktualnieniu do wersji V5R2, przed importem nowych danych, należy uruchomić serwer i przeprowadzić migrację istniejących danych. Próba importu danych przed uruchomieniem serwera może się nie powieść, jeśli nie ma się wystarczających uprawnień.
- Wersja V4R4 i wcześniejsze wersje Usług katalogowych nie uwzględniały stref czasowych podczas tworzenia pozycji datownika. Począwszy od wersji V4R5 strefa czasowa jest stosowana we wszystkich dodatkach i modyfikacjach katalogu. Dlatego podczas uaktualniania do wersji V5R2 z wersji V4R4 lub wcześniejszej, Usługi katalogowe dopasowują istniejące atrybuty createtimestamp i modifytimestamp do odpowiedniej strefy czasowej. Dokonują tego przez odjęcie strefy czasowej, aktualnie zdefiniowanej w systemie iSeries, od datowników składowanych w katalogu. Należy zauważyć, że jeśli bieżąca strefa czasowa nie jest taka sama, jak strefa czasowa aktywna podczas początkowego tworzenia lub modyfikacji pozycji, nowe wartości datowników nie odzwierciedlą pierwotnej strefy czasowej.
- Po migracji serwer katalogów LDAP będzie uruchamiany automatycznie w momencie uruchomienia protokołu TCP/IP. Jeśli nie chcesz, aby serwer katalogów uruchamiał się automatycznie, zmień to ustawienie za pomocą programu iSeries Navigator.

Migracja z wersji V4R3 lub V4R4 Usług katalogowych do V5R2

Wersja V5R2 OS/400 nie obsługuje bezpośredniej aktualizacji z wersji V4R3. Podczas migracji z wersji V4R3 lub V4R4 Usług katalogowych serwera LDAP do wersji V5R2, postępuj zgodnie z poniższymi procedurami:

- wykonaj aktualizację OS/400 z wersji V4R3 lub V4R4 do wydania pośredniego,
- zeskładuj bibliotekę bazy danych i następnie wykonaj migrację OS/400 z wersji V4R3 lub V4R4 do wersji V5R2.

Aktualizacja OS/400 z wersji V4R3 lub V4R4 do wydania pośredniego

Wprawdzie aktualizacje z wersji V4R3 i V4R4 OS/400 do wersji V5R2 nie są obsługiwane, jednak są obsługiwane następujące aktualizacje:

- wersja V4R3 i V4R4 aktualizowane do wersji V4R5
- wersja V4R4 i V4R5 aktualizowane do wersji V5R1
- wersja V4R5 i V5R1 aktualizowane do wersji V5R2

Jedyną metodą migracji z serwera Usług katalogowych jest aktualizacja do wydania pośredniego (V4R5 lub V5R1), a następnie do V5R2. Szczegółowe informacje o procedurach instalacji OS/400 zawiera podręcznik *Instalacja oprogramowania*  . Aby dokonać migracji, postępuj według poniższych punktów:

1. Zanotuj wszystkie zmiany wprowadzone w plikach schematów w katalogu /QIBM/UserData/OS400/DirSrv. Pliki schematów podlegają automatycznej migracji.
2. Dla wersji V4R4 lub V4R3 wykonaj instalację typu slip wersji V4R5 lub V5R1 OS/400.
3. Wykonaj instalację typu slip wersji V5R2 OS/400.
4. Uruchom serwer usług katalogowych (LDAP), jeśli jeszcze nie został uruchomiony.

5. Skorzystaj z narzędzia Directory Management, aby wprowadzić zmiany w plikach schematów dla wszystkich zmian użytkowników zanotowanych w punkcie 1 na stronie 12.
6. Uruchom ponownie serwer usług katalogowych (LDAP).

Składowanie biblioteki bazy danych i aktualizacja OS/400 w wersji V4R3 lub V4R4 do V5R2

Inną metodą migracji serwera Usług katalogowych jest zeskładowanie biblioteki bazy danych, z której korzystają Usługi katalogowe w wersji V4R3 lub V4R4, a następnie odtworzenie jej po zainstalowaniu od początku wersji V5R2. Oszczędza to instalacji wydania pośredniego. Jednak ustawienia serwera nie podlegają migracji i konieczne jest jego ponowne skonfigurowanie. Szczegółowe informacje o procedurach instalacji OS/400 zawiera podręcznik *Instalacja oprogramowania*  . Aby dokonać migracji, postępuj według poniższych punktów:

1. Zanotuj wszystkie zmiany wprowadzone w plikach schematów w katalogu /QIBM/UserData/OS400/DirSrv. Pliki schematów nie podlegają automatycznej migracji i jeśli chcesz zachować zmiany, należy je wprowadzić ponownie ręcznie.
2. Zanotuj ustawienia konfiguracji z właściwości serwera Usług katalogowych włącznie z nazwą biblioteki bazy danych.
3. Zeskładuj bibliotekę bazy danych, podaną w konfiguracji serwera Usług katalogowych.
4. Zanotuj konfigurację publikowania.
5. Zainstaluj od nowa system OS/400 w wersji V5R2.
6. Za pomocą programu EZ-Setup skonfiguruj serwer usług katalogowych (LDAP).
7. Odtwórz bibliotekę bazy danych, zeskładowaną w punkcie 3.
8. Skorzystaj z narzędzia Directory Management, aby wprowadzić w plikach schematów wszystkie zmiany użytkowników zanotowane w punkcie 1.
9. Skorzystaj z narzędzia iSeries Navigator, aby ponownie skonfigurować Usługi katalogowe (LDAP). Podaj bibliotekę bazy danych, która została zeskładowana i odtworzona.
10. Skorzystaj z narzędzia iSeries Navigator, aby ponownie skonfigurować publikowanie.
11. Uruchom ponownie serwer usług katalogowych (LDAP).

Zagadnienia związane z aktualizacją oprogramowania

Podczas aktualizacji z wersji V4R3 do dowolnej późniejszej wersji należy uwzględnić następujące elementy:

- **Migrowanie pliku kluczy do bazy danych kluczy:**

  Client Access w wersji V3R2 używał plików kluczy do nawiązywania połączeń SSL z serwerem katalogów LDAP. iSeries Access for Windows używa do nawiązywania połączeń SSL baz certyfikatów, które czasami nazywane są bazami danych kluczy. Aby używać połączeń SSL z serwerem katalogów LDAP, należy najpierw wykonać konwersję pliku kluczy do bazy danych kluczy. Pierwsza próba nawiązania połączenia SSL z serwerem katalogów LDAP spowoduje, że iSeries Navigator wyśle alert dotyczący tej zmiany. Jeśli klucz ma być poddany konwersji, należy najpierw określić pewne informacje dla bazy danych kluczy.

  Serwer katalogów LDAP w wersji V4R3 używał również pliku kluczy dla własnych połączeń SSL w wersji V4R3. Począwszy od wersji V4R4 używa on systemowej bazy certyfikatów. Jeśli serwer został skonfigurowany tak, aby używał SSL w wersji V4R3, zawartość pliku kluczy zostanie poddana migracji do systemowej bazy certyfikatów.
- **Zostały usunięte dwa pliki strumieniowe:**

  Następujące pliki strumieniowe używane przez Usługi katalogowe w wersji V4R3 nie są już potrzebne i są automatycznie usuwane podczas instalacji późniejszej wersji:

  ```
  /QIBM/ProdData/OS400/DirSrv/qgldcert.kyr
  /QIBM/ProdData/OS400/DirSrv/qgldcert.sth
  ```

  Nie są wymagane żadne dodatkowe czynności. Ta informacja uprzedza jedynie użytkownika o ich braku w systemie.

Należy również wziąć pod uwagę, że mogą wystąpić dodatkowe problemy związane z uaktualnieniem z innych wersji do bieżącej.

Instalowanie i konfigurowanie Usług katalogowych

Usługi katalogowe (LDAP) są automatycznie instalowane podczas instalacji OS/400. Serwer katalogów zawiera konfigurację domyślną, która uruchamia serwer katalogów podczas uruchamiania protokołu TCP/IP. Rozpoczyna on także publikowanie informacji z komputera OS/400 do serwera katalogów. Aby dostosować ustawienia serwera katalogów LDAP, należy uruchomić kreator konfiguracji Usług katalogowych. Aby skorzystać z kreatora, konieczne są uprawnienia specjalne *ALLOBJ i *IOSYSCFG.

Usługi katalogowe, począwszy od wersji V5R1, zostały zintegrowane z podstawowym systemem operacyjnym, tak więc Opcja 32 nie jest już dostępna począwszy od wersji V5R2.

Konfigurowanie serwera katalogów LDAP

Jeśli system nie zostanie skonfigurowany do rozpowszechnienia informacji dla innego serwera LDAP i serwer DNS sieci TCP/IP nie zna innych serwerów LDAP, to Usługi katalogowe zostają automatycznie zainstalowane w ograniczonej konfiguracji domyślnej. Usługi katalogowe udostępniają kreatora do pomocy podczas konfigurowania serwera katalogów LDAP dla określonych potrzeb. Można go uruchomić jako część programu EZ-Setup lub później z programu iSeries Navigator. Należy go użyć podczas początkowego konfigurowania serwera katalogów. Można go także użyć do zmiany konfiguracji serwera katalogów.

Uwaga: Użycie kreatora do ponownej konfiguracji serwera katalogów rozpoczyna konfigurację od nowa. Pierwotna konfiguracja jest usuwana, a nie zmieniana. Jednak dane katalogowe nie są usuwane, tylko składowane w bibliotece wybranej w trakcie instalacji (domyślnie QUSRDIRDB). Protokół zmian również pozostaje niezmieniony, domyślnie w bibliotece QUSRDIRCL.

Aby rozpocząć konfigurację od nowa, należy usunąć obie te biblioteki przed uruchomieniem kreatora.

Aby zmienić konfigurację serwera katalogów, ale nie usuwać jej zupełnie, należy kliknąć prawym przyciskiem myszy **Katalog** i wybrać **Właściwości**. Nie powoduje to usunięcia pierwotnej konfiguracji.

Do konfigurowania niezbędne są uprawnienia specjalne *ALLOBJ i *IOSYSCFG. Aby skonfigurować kontrolę ochrony OS/400, konieczne są uprawnienia specjalne *AUDIT.

Aby uruchomić kreator konfiguracji Usług katalogowych, wykonaj następujące czynności:
1. W programie iSeries Navigator rozwiń pozycję **Sieć**.
2. Rozwiń pozycję **Serwery**.
3. Kliknij **TCP/IP**.
4. Prawym przyciskiem myszy kliknij **Katalog** i wybierz **Konfiguracja**.

Uwaga: Jeśli serwer katalogów został już skonfigurowany, należy kliknąć **Rekonfiguruj**, a nie **Konfiguruj**.

Postępowanie zgodne z instrukcjami kreatora konfiguracji serwera LDAP prowadzi do skonfigurowania serwera Usług katalogowych.

Uwaga: Można również umieścić bibliotekę przechowującą dane katalogowe w puli pamięci dyskowej użytkowników (ASP), a nie w systemowej ASP. Jednak ta biblioteka nie może być przechowywana w niezależnej ASP, ponieważ każda próba konfigurowania, rekonfigurowania lub uruchomienia serwera z biblioteką, która znajduje się w niezależnej ASP, nie powiedzie się.

Po zakończeniu pracy kreatora serwer katalogów LDAP ma konfigurację podstawową. Jeśli w systemie jest uruchamiany Lotus Domino, to port 389 (domyślny port dla serwera LDAP) może być zajęty przez jego funkcję LDAP. Należy wykonać wtedy jedną z następujących czynności:

- zmienić port, którego używa Lotus Domino,
- zmienić port, którego używają Usługi katalogowe,
- użyć określonych adresów IP.

W tym momencie można uruchomić serwer. Jednak przedtem można wykonać niektóre lub wszystkie z podanych czynności:

- zaimportować dane do serwera,
- włączyć ochronę SSL (Secure Sockets Layer),
- włączyć uwierzytelnianie protokołem Kerberos,
- skonfigurować odwołanie.

Włączanie SSL na serwerze katalogów LDAP

Jeśli w systemie jest zainstalowany Menedżer certyfikatów cyfrowych, można użyć schematu ochrony SSL (Secure Sockets Layer) do ochrony dostępu do serwera katalogów LDAP. Przed włączeniem SSL na serwerze katalogów pomocne mogą okazać się informacje na temat używania SSL z Usługami katalogowymi.

Aby korzystać z połączeń SSL podczas administrowania serwerem katalogów LDAP z poziomu iSeries Navigator lub za pomocą klienta LDAP dla Windows, trzeba mieć zainstalowany na komputerze PC jeden z produktów Client Encryptions (5722CE2 lub 5722CE3).

Aby włączyć SSL na serwerze LDAP, należy użyć programu DCM. Można go uruchomić z folderu **Internet** w programie iSeries Navigator lub na stronie **Sieć** okna dialogowego **Właściwości** serwera katalogów.

Aby uruchomić program DCM ze strony **Sieć**, wykonaj następujące czynności:

1. W programie iSeries Navigator rozwiń pozycję **Sieć**.
2. Rozwiń pozycję **Serwery**.
3. Kliknij **TCP/IP**.
4. Prawym przyciskiem myszy kliknij **Katalog** i wybierz **Właściwości**.
5. Kliknij zakładkę **Sieć**.
6. Kliknij **Menedżer certyfikatów cyfrowych**.

   Program DCM zostanie uruchomiony w domyślnej przeglądarce WWW.

Aby dowiedzieć się, co trzeba zrobić, aby przypisać certyfikat cyfrowy do serwera katalogów, patrz sekcja Ochrona serwera katalogów LDAP.

Po udostępnieniu SSL można zmienić port używany przez serwer katalogów LDAP do połączeń chronionych.

Włączanie uwierzytelniania protokołem Kerberos na serwerze katalogów LDAP

Jeśli w systemie są skonfigurowane Sieciowe usługi uwierzytelniania, to serwer katalogów LDAP można skonfigurować, aby korzystał z uwierzytelniania protokołem Kerberos. Przed włączeniem protokołu Kerberos na serwerze katalogów pomocne mogą okazać się informacje na temat używania protokołu Kerberos z Usługami katalogowymi.

Aby włączyć uwierzytelnianie protokołem Kerberos, wykonaj następujące kroki:

1. W programie iSeries Navigator rozwiń pozycję **Sieć**.
2. Rozwiń pozycję **Serwery**.
3. Kliknij **TCP/IP**.
4. Prawym przyciskiem myszy kliknij **Katalog** i wybierz **Właściwości**.
5. Kliknij zakładkę **Kerberos**.
6. Zaznacz **Włącz uwierzytelnianie Kerberos**.

7. Na stronie **Kerberos** podaj inne ustawienia, odpowiednio do warunków. Informacje dotyczące poszczególnych pól można znaleźć w dokumentacji elektronicznej.

Konfiguracja domyślna Usług katalogowych

Serwer katalogów LDAP jest automatycznie instalowany podczas instalacji OS/400. Instalacja taka zawiera konfigurację domyślną. Serwer katalogów korzysta z konfiguracji domyślnej, jeśli spełnione są następujące warunki:

- administratorzy nie muszą uruchamiać kreatora konfiguracji Usług katalogowych lub zmieniać ustawień katalogu poprzez strony właściwości,
- nie jest skonfigurowane publikowanie Usług katalogowych,
- serwer katalogów LDAP nie może odnaleźć żadnych informacji o DNS LDAP.

Jeśli serwer katalogów LDAP korzysta z konfiguracji domyślnej, to:

- serwer katalogów LDAP uruchamia się automatycznie w momencie uruchamiania protokołu TCP/IP,
- system tworzy nowe konto administratora, cn=Administrator, oraz generuje używane wewnętrznie hasło; jeśli planujesz późniejsze użycie hasła administratora, możesz ustawić nowe hasło na stronie właściwości Usług katalogowych,
- w oparciu o nazwę IP systemu tworzony jest domyślny przyrostek; w oparciu o nazwę systemu tworzony jest także przyrostek obiektów systemu; na przykład, jeśli nazwa IP systemu to mary.acme.com, wtedy przyrostek wynosi dc=mary,dc=acme,dc=com,
- serwer katalogów LDAP korzysta z domyślnej biblioteki danych QUSRDIRDB, którą system tworzy w systemowej ASP,
- serwer korzysta z portu 389 do niechronionej komunikacji, a jeśli certyfikat cyfrowy został skonfigurowany dla LDAP, to włączony jest protokół SSL i do chronionej komunikacji używany jest port 636.

Dla publikowania Usług katalogowych przyjęte są następujące domyślne założenia:

- system publikuje informacje do lokalnego serwera katalogów LDAP,
- publikowanie nie korzysta z SSL,
- publikowanie korzysta z pojemników pod domyślnym przyrostkiem,
- do uwierzytelniania z serwerem katalogów system OS/400 używa identyfikatora cn=Administrator i wygenerowanego przez system hasła,
- system publikuje jedynie informacje systemowe.

Narzędzie IBM SecureWay Directory Management Tool

Narzędzie IBM SecureWay Directory Management Tool (DMT) udostępnia graficzny interfejs użytkownika do zarządzania zawartością katalogu LDAP. Za pomocą narzędzia DMT można wykonać między innymi następujące zadania:

- przeglądanie schematu katalogu,
- dodawanie, edytowanie i usuwanie klas obiektów,
- dodawanie, edytowanie i usuwanie atrybutów,
- przeglądanie i przeszukiwanie drzewa katalogów,
- dodawanie, edytowanie i przeglądanie pozycji,
- edytowanie pozycji RDNs,
- zarządzanie listami kontroli dostępu (ACL).

Narzędzie DMT jest częścią klienta LDAP dla Windows dołączonego do Usług katalogowych. Klient jest dostarczony w katalogu zintegrowanego systemu plików.

Aby zainstalować na komputerze PC klienta LDAP dla Windows, zawierającego narzędzie DMT, wykonaj następujące czynności:

1. W iSeries Navigator rozwiń **System plików**.
2. Wybierz **Pliki współużytkowane**.
3. Dwukrotnie kliknij **Qdirsrv**.
4. Dwukrotnie kliknij **UserTools**.
5. Dwukrotnie kliknij **Windows**.
6. Dwukrotnie kliknij **setup.exe**, aby rozpocząć instalację narzędzia DMT. Aby zakończyć instalację, postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

Dokumentacja narzędzia IBM SecureWay Directory Management Tool (DMT) znajduje się w pliku dparent.htm. Podczas instalacji klienta plik ten jest kopiowany do folderu programu IBM SecureWay na komputerze PC.

Rozdział 4. Zarządzanie serwerem katalogów LDAP

Aby zarządzać serwerem katalogów LDAP, użytkownik musi mieć niżej wymienione zestawy uprawnień:

- aby konfigurować serwer lub zmienić jego konfigurację: uprawnienia specjalne do wszystkich obiektów (All Object - *ALLOBJ) i do konfigurowania systemu (I/O System Configuration - *IOSYSCFG),
- aby uruchomić lub zamknąć serwer: uprawnienie Job Control (*JOBCTL) i uprawnienia do obiektów dla komend: Zakończenie protokołu TCP/IP (End TCP/IP - ENDTCP), Uruchomienie protokołu TCP/IP (Start TCP/IP - STRTCP), Uruchomienie serwera TCP/IP (Start TCP/IP Server - STRTCPSVR) oraz Zamknięcie serwera TCP/IP (End TCP/IP Server - ENDTCPSVR),
- aby skonfigurować kontrolę dla serwera katalogów: uprawnienie specjalne Audit (*AUDIT),
- aby obejrzeć protokół zadań serwera: uprawnienie specjalne do zarządzania wydrukami (Spool Control - *SPLCTL).

Aby zarządzać obiektami katalogów (takimi jak listy kontroli dostępu, prawa własności do obiektu oraz repliki), należy połączyć się z katalogiem przy pomocy nazwy wyróżniającej administratora lub innej nazwy wyróżniającej, do której przypisane są odpowiednie uprawnienia LDAP. Jeśli wykorzystywana jest integracja uprawnień, administratorem może być także użytkownik rzutowany, który ma uprawnienia do identyfikatora funkcji Directory Services Administrator (Administratora Usług katalogowych).

Zarządzanie serwerem katalogów obejmuje następujące zagadnienia:

Uruchamianie serwera katalogów LDAP

Aby uruchomić serwer katalogów LDAP, wykonaj następujące czynności:

1. W programie iSeries Navigator rozwiń pozycję **Sieć**.
2. Rozwiń pozycję **Serwery**.
3. Kliknij **TCP/IP**.
4. Prawym przyciskiem myszy kliknij opcję **Katalog** i wybierz **Uruchom**.

   Uruchomienie serwera katalogów może trochę potrwać. Jest to uzależnione od szybkości serwera i ilości dostępnej pamięci. Pierwsze uruchomienie serwera katalogów może trwać nieco dłużej niż zazwyczaj, ponieważ muszą być utworzone nowe pliki. Podobnie uruchamianie serwera katalogów po raz pierwszy po aktualizacji z wcześniejszych wersji Usług katalogowych, może zająć więcej czasu niż zwykle ponieważ serwer musi zaktualizować pliki. Istnieje możliwość regularnego sprawdzania statusu serwera, można więc sprawdzić, czy proces ten został już zakończony.

Uwaga: Serwer katalogów można także uruchomić z sesji 5250 przez wpisanie komendy STRTCPSVR *DIRSRV.

Dodatkowo, jeśli serwer katalogów został skonfigurowany tak, aby rozpoczynał działanie w momencie uruchamiania protokołu TCP/IP, można go także uruchomić przez wpisanie komendy STRTCP.

Zatrzymywanie serwera katalogów LDAP

Zatrzymanie serwera katalogów wpływa na działanie wszystkich aplikacji korzystających z serwera w czasie jego zatrzymania. Dotyczy to także aplikacji Enterprise Identity Mapping (EIM), które aktualnie używają serwera katalogów w operacjach EIM. Wszystkie aplikacje są odłączane od serwera katalogów, jednakże nie są zabronione próby ponownego podłączenia do niego.

Aby zatrzymać serwer katalogów LDAP, wykonaj następujące czynności:
1. W programie iSeries Navigator rozwiń pozycję **Sieć**.
2. Rozwiń pozycję **Serwery**.
3. Kliknij **TCP/IP**.
4. Prawym przyciskiem myszy kliknij **Katalog** i wybierz **Zatrzymaj**.

   Aby zakończyć pracę, serwer katalogów potrzebuje trochę czasu, w zależności od szybkości serwera, jego obciążenia oraz ilości dostępnej pamięci. Istnieje możliwość regularnego sprawdzania statusu serwera, można więc sprawdzić, czy proces ten został zakończony.

Uwaga: Serwer katalogów można także zatrzymać w sesji 5250 przez wpisanie komend ENDTCPSVR *DIRSRV, ENDTCPSVR *ALL lub ENDTCP. Komendy ENDTCPSVR *ALL oraz ENDTCP mają także wpływ na pozostałe serwery TCP/IP, które są uruchomione w systemie. Komenda ENDTCP zakończy także działanie protokołu TCP/IP.

Sprawdzanie statusu serwera katalogów

iSeries Navigator wyświetla status serwera katalogów w kolumnie **Status** w ramce po prawej stronie ekranu.

Aby sprawdzić status serwera katalogów, wykonaj następujące czynności:
1. W programie iSeries Navigator rozwiń pozycję **Sieć**.
2. Rozwiń pozycję **Serwery**.
3. Kliknij **TCP/IP**. iSeries Navigator wyświetla w kolumnie **Status** status wszystkich serwerów TCP/IP, w tym serwera katalogów. Aby zaktualizować status serwera, kliknij menu **Widok** i wybierz opcję **Odśwież**.
4. Aby uzyskać więcej informacji na temat statusu serwera katalogów, kliknij prawym przyciskiem myszy opcję **Katalog** i wybierz **Status**. Opcja ta wyświetli informacje o liczbie aktywnych połączeń, a także inne informacje, np. wcześniejsze i bieżące poziomy aktywności.

   Poza dostarczaniem dodatkowych informacji, sprawdzanie statusu serwera z użyciem tej opcji może oszczędzić czas. Informacje na temat statusu serwera można odświeżyć bez poświęcania dodatkowego czasu wymaganego do sprawdzenia statusu innych serwerów protokołu TCP/IP.

Sprawdzanie zadań na serwerze katalogów LDAP

Czasami konieczne jest monitorowanie zadań serwera katalogów LDAP. Aby sprawdzić zadania serwera, wykonaj następujące kroki:
1. W programie iSeries Navigator rozwiń pozycję **Sieć**.
2. Rozwiń pozycję **Serwery**.
3. Kliknij **TCP/IP**.
4. Kliknij prawym przyciskiem myszy opcję **Katalog** i wybierz opcję **Zadania serwera**.

Włączanie powiadamiania o zdarzeniach

Usługi katalogowe obsługują opcję powiadamiania o zdarzeniach, która umożliwia klientom zarejestrowanie w serwerze LDAP powiadamiania o wystąpieniu określonych zdarzeń, takich jak dodanie informacji do katalogu.

Aby włączyć powiadamianie o zdarzeniach dla serwera, wykonaj następujące czynności:
1. W programie iSeries Navigator rozwiń pozycję **Sieć**.
2. Rozwiń pozycję **Serwery**.
3. Kliknij **TCP/IP**.
4. Prawym przyciskiem myszy kliknij **Katalog** i wybierz **Właściwości**.
5. Kliknij **Zdarzenia**.
6. Wybierz **Zezwól klientom na rejestrowanie powiadomień o zdarzeniach**.

Można również określić maksymalną liczbę rejestracji dla każdego połączenia i maksymalną łączną liczbę rejestracji dopuszczalnych przez serwer.

Więcej informacji na temat powiadamiania o zdarzeniach znajduje się w Dodatku C:Event Notification (Powiadamianie o zdarzeniach) w podręczniku IBM SecureWay Directory Version 3.2: Client SDK Programming Reference .

Konfigurowanie transakcji

Usługi katalogowe obsługują transakcje, które umożliwiają traktowanie grupy działań na katalogach LDAP jako jedną jednostkę. Więcej informacji znajduje się w sekcji “Transakcje” na stronie 40.

Aby skonfigurować transakcje serwera, wykonaj następujące czynności:
1. W programie iSeries Navigator rozwiń pozycję **Sieć**.
2. Rozwiń pozycję **Serwery**.
3. Kliknij **TCP/IP**.
4. Prawym przyciskiem myszy kliknij **Katalog** i wybierz **Właściwości**.
5. Kliknij **Transakcje**.
6. Określ swoje parametry transakcji.

Uwaga: Parametry transakcji mogą mieć wpływ na wydajność serwera LDAP, dlatego warto poeksperymentować z różnymi ustawieniami.

Zmiana portu lub adresu IP

Serwer katalogów LDAP udostępniony przez Usługi katalogowe używa następujących portów domyślnych:
- 389 dla połączeń niechronionych,
- 636 dla połączeń chronionych (jeśli używa się programu DCM do udostępniania Usług katalogowych jako aplikacji, która może używać portu chronionego).

Uwaga: Domyślnie wszystkie adresy IP, zdefiniowane w systemie lokalnym, są powiązane z serwerem.

Jeśli te porty są aktualnie wykorzystywane przez inną aplikację, Usługom katalogowym można albo przypisać inny port albo użyć różnych adresów IP dla dwóch serwerów, w przypadku gdy aplikacje obsługują opcję łączenia z określonym adresem IP.

Opis przykładowego konfliktu serwera LDAP Domino z serwerem LDAP Usług katalogowych iSeries znajduje się w sekcji Host Domino LDAP i Usługi katalogowe na tym samym serwerze iSeries

Aby zmienić porty używane przez serwer katalogów LDAP, wykonaj następujące czynności:
1. W programie iSeries Navigator rozwiń pozycję **Sieć**.

2. Rozwiń pozycję **Serwery**.
3. Kliknij **TCP/IP**.
4. Prawym przyciskiem myszy kliknij **Katalog** i wybierz **Właściwości**.
5. Kliknij zakładkę **Sieć**.
6. Wpisz odpowiednie numery portów, a następnie kliknij **OK**.

Aby zmienić adres IP na taki, za pomocą którego serwer katalogów akceptuje połączenia, wykonaj następujące czynności:

1. W programie iSeries Navigator rozwiń pozycję **Sieć**.
2. Rozwiń pozycję **Serwery**.
3. Kliknij **TCP/IP**.
4. Prawym przyciskiem myszy kliknij pozycję **Katalog** i wybierz opcję **Właściwości**.
5. Kliknij zakładkę **Sieć**.
6. Kliknij przycisk **Adresy IP...**.
7. Wybierz **Użyj wybrane adresy IP**, a następnie wybierz dla serwera adresy IP, które będą używane przy akceptowaniu połączeń.

Przenoszenie danych katalogów LDAP między systemami

Serwer katalogów LDAP Usług katalogowych może działać niezależnie od innych serwerów. Jednakże przydatne może okazać się rozwiązanie, w którym będzie on współpracował z innymi serwerami. Współpraca ta może obejmować:

- "Importowanie pliku LDIF"
- "Eksportowanie pliku LDIF"
- "Tworzenie nowej repliki serwera katalogów" na stronie 23
- "Publikowanie informacji w serwerze katalogów" na stronie 27

Importowanie pliku LDIF

Pomiędzy różnymi serwerami katalogów LDAP można przenosić informacje za pomocą plików w formacie LDIF (LDAP Data Interchange Format). Przed rozpoczęciem tej procedury należy przenieść plik LDIF do serwera iSeries jako plik strumieniowy.

Aby zaimportować plik LDIF do serwera katalogów LDAP, wykonaj następujące kroki:

1. Jeśli serwer katalogów jest uruchomiony, zatrzymaj go. Informacje o tym, jak zatrzymać serwer katalogów, zawiera sekcja "Zatrzymywanie serwera katalogów LDAP" na stronie 20.
2. W programie iSeries Navigator rozwiń pozycję **Sieć**.
3. Rozwiń pozycję **Serwery**.
4. Kliknij **TCP/IP**.
5. Prawym przyciskiem myszy kliknij opcję **Katalog** i wybierz **Narzędzia**, a następnie **Importuj plik**.

Uwaga: Aby importować pliki LDIF, możesz także użyć narzędzia ldapadd.

Eksportowanie pliku LDIF

Pomiędzy różnymi serwerami katalogów LDAP można przenosić informacje za pomocą plików w formacie LDIF (LDAP Data Interchange Format) (patrz sekcja "Format wymiany danych LDAP" na stronie 36). Do pliku LDIF można eksportować cały lub część katalogu LDAP.

Aby wyeksportować plik LDIF z serwera katalogów, wykonaj następujące kroki:

1. W programie iSeries Navigator rozwiń pozycję **Sieć**.
2. Rozwiń pozycję **Serwery**.
3. Kliknij **TCP/IP**.
4. Prawym przyciskiem myszy kliknij opcję **Katalog** i wybierz **Narzędzia**, a następnie **Eksportuj plik**.

Uwaga: Jeśli nie podasz miejsca, do którego plik LDIF ma być wyeksportowany, zostanie on zapisany w domyślnym katalogu podanym w profilu użytkownika OS/400. Jeśli nie zmieniłeś swojego katalogu domyślnego, jest nim katalog główny.

Uwagi:

1. Upewnij się, że ustawiłeś odpowiednie uprawnienia do pliku LDIF, co zapobiegnie nieuprawnionemu dostępowi do danych katalogu. Aby to zrobić, kliknij plik prawym przyciskiem myszy w programie iSeries Navigator, a następnie wybierz opcję **Uprawnienia**.
2. Można także utworzyć pełny lub częściowy plik LDIF, używając narzędzia ldapsearch (patrz sekcja “Narzędzie ldapsearch” na stronie 56). Użyj opcji -L i przekieruj dane wyjściowe do pliku.

Tworzenie nowej repliki serwera katalogów

W serwerach katalogów znajdujących się w innych serwerach iSeries można tworzyć repliki serwera katalogów LDAP. Usługi katalogowe używają do tworzenia repliki standardowego protokołu LDAP wersja 3.

Uwagi:

1. Nie można tworzyć replik serwerów pomiędzy protokołem LDAP wersja 3 a protokołem LDAP wersja 2. Dlatego replikowany system musi używać tej samej wersji LDAP co system, z którego tworzona jest replika. Wersje V4R3 i V4R4 OS/400 obsługują wersję 2 LDAP, wersja V4R5 i nowsze obsługują wersję 3 LDAP.
2. Możliwe jest tworzenie replik katalogu Usług katalogowych do serwerów IBM SecureWay V3.2 lub późniejszych na innych platformach. Do tego celu serwer katalogów OS/400 musi zostać skonfigurowany tak, aby korzystał z mechanizmu 3.2 ACI. Jeśli serwer napotka w trakcie próby tworzenia repliki na jakiś problem, zatrzyma operację. Jeśli to się zdarzy, replika będzie niepełna.

Aby utworzyć nową replikę serwera katalogów, wykonaj następujące kroki:

1. Skonfiguruj serwer główny i serwer replikę, jeśli jeszcze tego nie zrobiłeś.

   Uwaga: Upewnij się, że schematy i przyrostki w obu serwerach są zgodne.
2. Zatrzymaj serwer główny.
3. (opcjonalnie) Podaj dane LDAP do tworzenia początkowej repliki. Krok ten można pominąć, jeśli z serwera głównego do serwera repliki nie będą przenoszone żadne dane początkowe.
4. (opcjonalnie) Przenieś dane LDAP do serwera głównego. Pomiń ten krok, jeśli serwer replika spełnia jeden z następujących warunków:
   - jest to nowy serwer katalogów LDAP,
   - nie zawiera on danych, które mają być dalej obsługiwane.
5. Skonfiguruj serwer replikę.
6. Skonfiguruj w serwerze głównym nową replikę.
7. Upewnij się, że serwer główny umożliwia aktualizacje:
   a. W programie iSeries Navigator otwórz system, w którym działa główny serwer katalogów.
   b. Wybierz opcję **Sieć**.
   c. Rozwiń pozycję **Serwery**.
   d. Kliknij **TCP/IP**.
   e. Prawym przyciskiem myszy kliknij **Katalog** i wybierz **Właściwości**.
   f. Zaznacz pozycję **Możliwa aktualizacja katalogu**, jeśli nie jest zaznaczona.

Uwaga: Instrukcje te przyjmują, że serwer główny i serwery repliki działają w systemach zarządzanych z iSeries Navigator na tym samym komputerze osobistym. Jeśli zarządzasz systemami z oddzielnych komputerów osobistych, aby przeprowadzić te zadania możesz pracować na kilku komputerach jednocześnie. Jeśli serwer główny lub replika działa na systemie operacyjnym innym niż OS/400 firmy IBM, aby skonfigurować serwer, przeczytaj dokumentację dla tej platformy.

Konfigurowanie danych LDAP do replikacji początkowej

Na głównym serwerze katalogów LDAP mogą znajdować się dane, które można dodać do nowej repliki serwera. Aby to zrobić, trzeba najpierw wyeksportować katalog do pliku LDIF. Podczas eksportowania pliku LDIF trzeba zapobiec aktualizacji serwera głównego. Można to zrobić w jeden z następujących sposobów:

- Zatrzymaj serwer katalogów LDAP. W zależności od wielkości danych w katalogu może to wymagać zatrzymania serwera na dłuższy czas.
- Zmień właściwości serwera w taki sposób, żeby aktualizacja była niedozwolona. To pozwoli serwerowi kontynuować odpowiadanie na żądania przeszukiwania podczas eksportu pliku LDIF. Aby zastosować tę opcję, wykonaj następujące kroki:
  1. W programie iSeries Navigator otwórz system, w którym działa główny serwer katalogów.
  2. Wybierz opcję **Sieć**.
  3. Rozwiń pozycję **Serwery**.
  4. Kliknij **TCP/IP**.
  5. Prawym przyciskiem myszy kliknij **Katalog** i wybierz **Właściwości**.
  6. Jeśli pozycja **Możliwa aktualizacja katalogu**jest zaznaczona, usuń zaznaczenie. Zapobiegnie to aktualizowaniu katalogów w trakcie przeprowadzania replikacji.
  7. Kliknij **OK**.
  8. Zatrzymaj, a następnie zrestartuj serwer katalogów LDAP.

Po zatrzymaniu serwera lub zmianie jego właściwości dotyczących zabronienia aktualizacji katalogu, wykonaj następujące zadania

1. Wyeksportuj katalog do pliku LDIF.
2. Przenieś plik LDIF do systemu, na którym będzie działała replika serwera.

Po przeniesieniu pliku LDIF do systemu, na którym będzie uruchomiona replika serwera, należy zaimportować dane do repliki serwera.

1. W programie iSeries Navigator otwórz system, w którym działa replika serwera katalogów.
2. Jeśli replika serwera nie została jeszcze zatrzymana, zatrzymaj jej działanie. Odświeżaj status serwerów, aż serwer będzie miał status **Zatrzymany**.
3. Wybierz opcję **Sieć**.
4. Rozwiń pozycję **Serwery**.
5. Kliknij **TCP/IP**.
6. Prawym przyciskiem myszy kliknij **Katalog** i wybierz **Właściwości**.
7. Jeśli pozycja **Możliwa aktualizacja katalogu** nie jest zaznaczona, zaznacz ją. Umożliwi to importowanie danych.
8. Kliknij **OK**.
9. Zaimportuj plik LDIF, który został przeniesiony w kroku 2.
10. Prawym przyciskiem myszy kliknij **Katalog** i wybierz **Właściwości**.
11. Usuń zaznaczenie **Możliwa aktualizacja katalogu**.

Przenoszenie danych LDAP do serwera głównego

Gdy na serwerze utworzona zostanie replika serwera głównego LDAP, w serwerze repliki nie będzie można aktualizować danych serwera. Jeśli w serwerze, który ma zostać skonfigurowany jako replika serwera katalogów LDAP, znajdują się dane, które mają być skonfigurowane, prawdopodobnie trzeba będzie je przenieść do serwera głównego, aby mogły być dalej obsługiwane. Aby to zrobić, wykonaj następujące kroki:

1. W programie iSeries Navigator otwórz system, w którym działa replika serwera katalogów.
2. Wybierz opcję **Sieć**.
3. Rozwiń pozycję **Serwery**.
4. Kliknij **TCP/IP**.
5. Prawym przyciskiem myszy kliknij **Katalog** i wybierz **Właściwości**.
6. Jeśli pozycja **Możliwa aktualizacja katalogu**jest zaznaczona, usuń zaznaczenie. Zapobiegnie to aktualizowaniu katalogów w trakcie przeprowadzania replikacji.
7. Kliknij **OK**.
8. Zatrzymaj serwer katalogów LDAP.
9. Wyeksportuj katalog do pliku LDIF.
10. Przenieś plik LDIF do systemu, na którym będzie działał serwer główny.

Po przeniesieniu pliku LDIF do systemu, na którym będzie działał serwer główny, należy zaimportować dane do serwera głównego.

1. W programie iSeries Navigator otwórz system, w którym działa główny serwer katalogów.
2. Jeśli serwer główny nie został jeszcze zatrzymany, przerwij jego działanie. Odświeżaj status serwerów, aż serwer będzie miał status **Zatrzymany**.
3. Wybierz opcję **Sieć**.
4. Rozwiń pozycję **Serwery**.
5. Kliknij **TCP/IP**.
6. Prawym przyciskiem myszy kliknij **Katalog** i wybierz **Właściwości**.
7. Jeśli pozycja **Możliwa aktualizacja katalogu** nie jest zaznaczona, zaznacz ją. Umożliwi to importowanie danych.
8. Kliknij **OK**.
9. Zaimportuj plik LDIF, który został przeniesiony w kroku 10 na stronie 24.
10. Prawym przyciskiem myszy kliknij **Katalog** i wybierz **Właściwości**.
11. Usuń zaznaczenie **Możliwa aktualizacja katalogu**.

Konfigurowanie nowej repliki

Aby utworzyć nową replikę serwera, wykonaj następujące kroki:

Uwaga: Przed przeprowadzeniem tej procedury należy skonfigurować i zatrzymać replikę serwera.

1. W programie iSeries Navigator otwórz system, w którym działa replika serwera katalogów.
2. Wybierz opcję **Sieć**.
3. Rozwiń pozycję **Serwery**.
4. Kliknij **TCP/IP**.
5. Jeśli serwer nie został jeszcze zatrzymany, przerwij jego działanie. Odświeżaj status serwerów, aż serwer będzie miał status **Zatrzymany**.
6. Prawym przyciskiem myszy kliknij **Katalog** i wybierz **Właściwości**.
7. Kliknij zakładkę **Replikacje**.
8. Wybierz **Użyj jako serwera replik**.
9. W polu **Nazwa używana przez serwer główny do aktualizacji** wybierz nazwę dla serwera, której będzie używać podczas rejestracji repliki serwera w systemie, gdy wykonuje on aktualizację. Może to być nazwa wyróżniająca (DN) lub użytkownik protokołu Kerberos.

   Jeśli wybierzesz DN:

   - Kliknij przycisk **Hasło** obok pola **Nazwa używana do aktualizacji**. Wpisz hasło, którego serwer główny ma używać przy wpisywaniu się do repliki serwera w celu wprowadzenia aktualizacji.

     Uwaga: Hasło i nazwę wpisaną w kroku 9 należy zanotować. Będą one potrzebne w trakcie konfigurowania do replikacji serwera głównego.

   Jeśli wybierzesz **Dodanie użytkownika Kerberos**:

   - System poprosi o wprowadzenie nazwy Kerberos (w postaci LDAP/*nazwa_hosta*, gdzie *nazwa_hosta* to pełna nazwa hosta serwera głównego) i domyślnej dziedziny (takiej jak ACME.COM) serwera głównego.

     Uwaga: Aby używać protokołu Kerberos, zarówno na serwerze głównym, jak i na replikach serwera należy włączyć protokół Kerberos.
10. W polu **Użyj jako serwera głównego** wpisz nazwę serwera głównego w formacie adresu URL. Jeśli serwer główny używa innego portu niż domyślny, wpisz numer portu jako część adresu URL.
11. Kliknij zakładkę **Baza danych**/**Przyrostki**. Jeśli przyrostek, który ma być replikowany, nie znajduje się na liście, dodaj go.
12. (opcjonalnie) Jeśli do obsługi replikacji chcesz używać protokołu Secure Sockets Layer (SSL), użyj narzędzia DCM, aby włączyć obsługę SSL dla serwera. Program DCM można uruchomić z zakładki **Sieć**. Dodatkowe informacje o włączaniu obsługi SSL w serwerze katalogów zawiera sekcja “Włączanie SSL na serwerze katalogów LDAP” na stronie 15.
13. Kliknij **OK**.

Konfigurowanie nowej repliki w serwerze głównym

Aby skonfigurować nową replikę w serwerze głównym, wykonaj następujące kroki:

Uwaga: Zanim przeprowadzisz tę procedurę, powinieneś skonfigurować i uruchomić serwer główny.

1. W programie iSeries Navigator otwórz system, w którym działa główny serwer katalogów.
2. Wybierz opcję **Sieć**.
3. Rozwiń pozycję **Serwery**.
4. Kliknij **TCP/IP**.
5. Prawym przyciskiem myszy kliknij **Katalog** i wybierz **Właściwości**.
6. Zaznacz pozycję **Możliwa aktualizacja katalogu**, jeśli nie jest zaznaczona.
7. Kliknij **OK**.
8. Zatrzymaj, a następnie ponownie uruchom serwer katalogów LDAP. Odświeżaj status serwerów, aż serwer będzie miał status **Uruchomiony**.
9. Ponownie kliknij prawym przyciskiem myszy opcję **Katalog** i wybierz **Właściwości**.
10. Kliknij zakładkę **Replikacje**. iSeries Navigator może zażądać wpisania informacji wymaganych przy połączeniu. Wpisz te informacje i kliknij **OK**.
11. Kliknij **Dodaj**.
12. W polu **Serwer** wpisz nazwę repliki serwera w formacie adresu URL.
13. Wybierz metodę uwierzytelniania.

    Aby używać nazwy wyróżniającej i hasła:

    a. Wybierz **Używanie DN i hasła**.

    b. W polu **Połącz jako** wpisz nazwę podaną w kroku 9 na stronie 25, podczas konfigurowania repliki serwera.

    c. Kliknij pozycję **Hasło** i wpisz hasło, które podałeś w kroku 9 na stronie 25, podczas konfigurowania repliki serwera.

    Aby korzystać z protokołu Kerberos:

    - Wybierz **Używanie konta Kerberos serwera głównego**. Serwer główny do uwierzytelnienia będzie korzystał z nazwy głównej Kerberos.

      Uwaga: Aby używać protokołu Kerberos, zarówno na serwerze głównym, jak i na replikach serwera należy włączyć protokół Kerberos.
14. Jeśli do obsługi replikacji chcesz używać protokołu Secure Sockets Layer (SSL), użyj narzędzia DCM, aby włączyć obsługę SSL dla serwera. Program DCM można uruchomić z zakładki **Sieć**. Dodatkowe informacje o włączaniu obsługi SSL w serwerze katalogów zawiera sekcja “Włączanie SSL na serwerze katalogów LDAP” na stronie 15.
15. Jeśli serwer replik nie używa portu domyślnego, wpisz numer portu w polu **Port**.
16. Jeśli nie chcesz aktualizować repliki serwera przy każdej zmianie pozycji serwera głównego, wybierz opcję **Czas**. Następnie określ, jak często serwer główny ma aktualizować replikę.
17. Kliknij **OK**.
18. Kliknij zakładkę **Baza danych/Przyrostki**. Jeśli przyrostek, który ma być replikowany, nie znajduje się na liście, dodaj go.
19. Włącz aktualizację katalogów w każdym serwerze replice:
    a. W programie iSeries Navigator otwórz system, w którym działa replika serwera katalogów.
    b. Wybierz opcję **Sieć**.
    c. Rozwiń pozycję **Serwery**.
    d. Kliknij **TCP/IP**.
    e. Prawym przyciskiem myszy kliknij **Katalog** i wybierz **Właściwości**.
    f. Jeśli pozycja **Możliwa aktualizacja katalogu** nie jest zaznaczona, zaznacz ją.
    g. Kliknij **OK**.
20. Jeśli replika serwera nie została jeszcze uruchomiona, uruchom ją.

Uwaga: Jeden serwer nie może być jednocześnie serwerem głównym i repliką serwera.

Publikowanie informacji w serwerze katalogów

W systemie można skonfigurować opcję publikowania pewnych informacji w serwerze katalogów LDAP znajdującym się w tym samym lub w innym systemie. System OS/400 automatycznie publikuje te informacje wśród serwerów katalogów LDAP za każdym razem, gdy zostaną one zmienione w OS/400 za pomocą programu iSeries Navigator. Można publikować między innymi informacje o systemie (systemy i drukarki), współużytkowanych zasobach drukarkowych, o użytkownikach oraz o strategii usługi QoS protokołu TCP/IP. Więcej informacji na temat usługi QoS znajduje się w sekcji Konfiguracja protokołu LDAP i QoS .

Jeśli nadrzędna DN, do której publikowane są dane, nie istnieje, to Usługi katalogowe tworzą ją automatycznie. Można zainstalować także inne aplikacje OS/400, które będą publikowały informacje do katalogu LDAP. Dodatkowo, można wywoływać funkcje API z własnych programów w celu publikowania w katalogach LDAP innych typów informacji.

Uwagi:

1. Podczas konfigurowania systemu OS/400 do publikowania w serwerach katalogów LDAP informacji typu Użytkownicy, system automatycznie eksportuje pozycje katalogu dystrybucyjnego systemu do serwera LDAP. Używa wówczas funkcji API QGLDSSDD. Utrzymuje w ten sposób zgodność katalogu LDAP ze zmianami wprowadzonymi w katalogu dystrybucyjnym systemu. Więcej informacji na temat funkcji API QGLDSSDD API znajduje się w OS/400 Directory Services w sekcji Programming w Centrum informacyjnym iSeries. Zostały tam omówione następujące zagadnienia:
   - jak ręcznie wywołać funkcję API,
   - jak zapobiec eksportowaniu konkretnych użytkowników do serwera LDAP,
   - jak funkcja eksportuje pola katalogu dystrybucyjnego systemu.
2. Podczas konfigurowania systemu OS/400 do publikowania informacji typu System do serwera katalogów LDAP i wybierania jednej lub więcej drukarek do publikowania, system automatycznie dokonuje synchronizacji katalogu LDAP ze zmianami wprowadzonymi dla tych drukarek w systemie. Informacje o drukarkach, które mogą być publikowane, zawierają położenie drukarki, jej szybkość w stronach na minutę, dane o tym, czy obsługuje ona wydruk dupleksowy i kolorowy, jej rodzaj, model i opis. Informacje te są pobierane z opisu urządzenia w publikowanym systemie. W środowisku sieciowym użytkownicy mogą skorzystać z tych informacji przy wyborze drukarki.
3. Można także publikować informacje OS/400 do serwerów katalogów LDAP, które nie pracują w systemach OS/400, o ile zostaną one skonfigurowane do używania schematu IBM.

Aby skonfigurować publikowanie informacji OS/400 do serwerów katalogów LDAP, wykonaj następujące kroki:

1. W programie iSeries Navigator kliknij prawym przyciskiem myszy swój system i wybierz opcję **Właściwości**.
2. Kliknij zakładkę **Usługi katalogowe**.
3. Kliknij typy informacji, które mają być publikowane.

   Wskazówka:

   Jeśli zamierzasz publikować do tego samego serwera więcej niż jeden typ informacji, możesz zaoszczędzić czas wybierając jednoczesne konfigurowanie wielu typów informacji. iSeries Navigator użyje wówczas wartości wpisanych w trakcie konfigurowania jednego typu informacji jako domyślnych przy konfigurowaniu kolejnych typów.
4. Kliknij **Szczegóły**.
5. Kliknij pole wyboru **Publikuj informacje o systemie**.
6. Określ **Metodę uwierzytelniania**, której ma serwer używać i odpowiednie informacje uwierzytelnia jące.
7. Kliknij przycisk **Edytuj** obok pola **(Aktywny) Serwer LDAP**. W rozwiniętym oknie dialogowym wpisz nazwę serwera katalogów LDAP, do którego mają być publikowane informacje OS/400, a następnie kliknij **OK**.
8. W polu **Pod nazwą DN** wpisz nadrzędną nazwę wyróżniającą, pod którą informacje mają być dodane do serwera katalogów.
9. Wypełnij zgodnie ze swoją konfiguracją pola w ramce **Połączenie serwera**.

Uwaga: Aby rozpowszechnić informacje OS/400 do serwera katalogów za pomocą protokołu SSL lub Kerberos, konieczne jest uprzednie skonfigurowanie serwera katalogów tak, aby korzystał z odpowiedniego protokołu. Więcej informacji dotyczących protokołów SSL i Kerberos zawiera sekcja “Wykorzystywanie przez serwer LDAP uwierzytelniania protokołem Kerberos” na stronie 41.

10. Jeśli serwer katalogów nie używa portu domyślnego, wpisz poprawny numer portu w polu **Port**.
11. Kliknij opcję **Sprawdź**, aby upewnić się, czy nadrzędna nazwa wyróżniająca istnieje w danym serwerze i czy informacje o połączeniu są poprawne. Jeśli potrzebna ścieżka nie istnieje w katalogu, zostanie wyświetlone okno dialogowe, w którym będzie trzeba ją utworzyć.

    Uwaga: Jeśli nadrzędna nazwa wyróżniająca nie istnieje i nie zostanie utworzona, wówczas publikowanie zakończy się błędem.
12. Kliknij **OK**.

Uwaga: Można także publikować informacje OS/400 do serwera katalogów LDAP pracującego na innej platformie. Niezbędne jest publikowanie informacji o użytkownikach i systemie do serwera katalogów, który korzysta ze schematu zgodnego ze schematem Usług katalogowych. Definicje schematów IBM SecureWay Directory, które obejmują Usługi katalogowe iSeries, można znaleźć na stronie WWW Directory Services.

Współużytkowane zasoby drukarkowe muszą być publikowane do serwera katalogów, który obsługuje schemat Active Directory firmy Microsoft. Publikowanie współużytkowanych zasobów drukarkowych do Active Directory umożliwia użytkownikom konfigurowanie drukarek iSeries bezpośrednio ze swoich pulpitów Windows 2000 za pomocą kreatora dodawania drukarek Windows 2000. Aby skonfigurować drukarkę w kreatorze dodawania drukarek, należy uruchomić jej wyszukiwanie w Active Directory w Windows 2000.

Funkcje API do publikowania w serwerze katalogów informacji o systemie OS/400

Usługi katalogowe udostępniają obsługę wbudowanej opcji publikowania informacji o użytkownikach i systemie. Lista opcji znajduje się na stronie **Usługi katalogowe** w oknie dialogowym **Właściwości**. Aby umożliwić własnym programom OS/400 publikowanie innych typów informacji, można użyć funkcji API serwera LDAP, służących do konfigurowania i publikowania. Te typy informacji także mogą być wyświetlane na stronie **Usługi katalogowe**. Tak jak użytkownicy i systemy, pierwotnie nie są one dostępne i można je skonfigurować za pomocą tej samej procedury. Program, który dodaje dane do katalogu LDAP, nazywany jest agentem publikującym. Typ informacji, które są publikowane, takie jak widoczne na stronie **Usługi katalogowe**, określa się jako nazwę agenta.

Włączenie obsługi publikowania do własnych programów umożliwiają następujące funkcje API:

QgldChgDirSvrA
: Aplikacja używa formatu CSVR0500, aby początkowo dodać nazwę agenta, zaznaczoną jako pozycja nieaktywna. Instrukcje dla użytkowników aplikacji powinny informować, że aby skonfigurować agenta publikacji (publishing agent), należy korzystać z programu iSeries Navigator, w celu przejścia na stronę właściwości Usług katalogowych. Przykładami nazw agentów są nazwy agentów systemów i użytkowników automatycznie dostępne na stronie **Usługi katalogowe**.

QgldLstDirSvrA
: Format LSVR0500 tej funkcji API służy do wyświetlania listy agentów aktualnie dostępnych w systemie.

QgldPubDirObj
: Ta funkcja API służy do przeprowadzania faktycznego publikowania informacji.

Szczegółowe informacje dotyczące funkcji API zawiera sekcja Lightweight Directory Access Protocol (LDAP) w artykule Programming w Centrum informacyjnym iSeries.

Określanie serwera odwołań

Aby przypisać serwery odwołań do serwera katalogów, wykonaj następujące kroki:
1. W programie iSeries Navigator rozwiń pozycję **Sieć**.
2. Rozwiń pozycję **Serwery**.
3. Kliknij **TCP/IP**.
4. Prawym klawiszem myszy kliknij **Katalog** i wybierz **Właściwości**.
5. Kliknij **Dodaj**.
6. W wierszu komend podaj nazwę serwera odwołań w formacie adresu URL. Poniżej znajdują się przykłady akceptowalnych adresów URL LDAP:
   - ldap://test.server.com
   - ldap://test.server.com:400
   - ldap://9.9.99.255

   Uwaga: Jeśli serwer odwołań nie korzysta z portu domyślnego, należy podać poprawny numer portu jako część adresu URL, podobnie do określenia portu 400 w drugim przykładzie powyżej.
7. Kliknij **OK**.

Dodawanie przyrostków do serwera katalogów LDAP

Dodanie przyrostka do serwera katalogów LDAP umożliwia serwerowi zarządzanie odpowiednią częścią drzewa katalogu.

Uwaga: Nie można dodać przyrostka, który znajduje się pod przyrostkiem istniejącym już w serwerze. Na przykład jeśli o=ibm, c=us są przyrostkami istniejącymi w serwerze, nie można dodać przyrostka ou=rochester, o=ibm, c=us.

Aby dodać przyrostek do serwera katalogów, wykonaj następujące czynności:
1. W programie iSeries Navigator rozwiń pozycję **Sieć**.
2. Rozwiń pozycję **Serwery**.
3. Kliknij **TCP/IP**.
4. Prawym przyciskiem myszy kliknij **Katalog** i wybierz **Właściwości**.
5. Kliknij zakładkę **Baza danych**/**Przyrostki**.
6. W polu **Nowy przyrostek** wpisz nazwę nowego przyrostka.
7. Kliknij **Dodaj**.
8. Kliknij **OK**.

Uwaga: Dodanie przyrostka wskazuje serwerowi sekcję katalogu, ale nie powoduje utworzenia żadnego obiektu. Jeśli wcześniej nie istniał obiekt odpowiadający nowemu przyrostkowi, to trzeba go utworzyć podobnie jak każdy inny obiekt.

Usuwanie przyrostków z serwera katalogów

Aby usunąć przyrostek z serwera katalogów LDAP, wykonaj następujące kroki:
1. W programie iSeries Navigator rozwiń pozycję **Sieć**.
2. Rozwiń pozycję **Serwery**.
3. Kliknij **TCP/IP**.
4. Prawym przyciskiem myszy kliknij **Katalog** i wybierz **Właściwości**.
5. Kliknij zakładkę **Baza danych**/**Przyrostki**.
6. Kliknij przyrostek, który ma zostać usunięty, aby go zaznaczyć.
7. Kliknij przycisk **Usuń**.

   Uwaga: Można wybrać usuwanie przyrostka bez usuwania obiektów katalogowych znajdujących się pod nim. Spowoduje to, że dane będą niedostępne z serwera katalogów. Potem można jednak odzyskać dostęp do danych przez ponowne dodanie przyrostka.

Składowanie i odzyskiwanie informacji Usług katalogowych

Usługi katalogowe przechowują informacje w następujących miejscach:

- w bibliotece bazy danych (domyślnie QUSRDIRDB), która przechowuje zawartość serwera katalogów,
- w bibliotece QDIRSRV2 używanej do przechowywania publikowanych informacji,
- w bibliotece QUSRSYS, która przechowuje różne pozycje w obiektach zaczynających się na QGLD (aby je składować, należy podać QUSRSYS/QGLD*).
- Jeśli serwer katalogów jest konfigurowany do protokołowania zmian katalogowych, biblioteka baz danych, wywoływana QUSRDIRCL, używa protokołu zmian.

Jeśli zawartość katalogu zmienia się regularnie, należy składować bibliotekę baz danych i jej obiekty regularnie. Dane konfiguracyjne są przechowywane również w następującym katalogu:

```
/QIBM/UserData/OS400/Dirsrv/
```

Pliki znajdujące się w tym katalogu należy składować po każdej zmianie konfiguracji lub zastosowaniu poprawek PTF.

Informacje na temat składowania i odzyskiwania danych OS/400 znajdują się w podręczniku Składowanie i odtwarzanie, SA12-7269 .

Zarządzanie prawami własności i dostępem do danych w katalogach

Zarządzanie prawami własności i dostępem do danych w katalogach obejmuje następujące zagadnienia:

- “Praca z prawami własności do obiektów katalogu”
- “Praca z listami kontroli dostępu (ACL)”
- “Praca z grupami list kontroli dostępu (ACL)” na stronie 31

Praca z prawami własności do obiektów katalogu

Aby skonfigurować prawa własności do obiektów katalogu, wykonaj następujące kroki:

1. W programie iSeries Navigator rozwiń pozycję **Sieć**.
2. Rozwiń pozycję **Serwery**.
3. Kliknij **TCP/IP**.
4. Prawym przyciskiem myszy kliknij **Katalog** i wybierz **Uprawnienie**.

   Jeśli nie jesteś jeszcze połączony z serwerem katalogów, zostanie wyświetlone okno dialogowe **Połącz z serwerem katalogów**. Połącz się jako administrator serwera lub właściciel obiektu, z którego prawami własności chcesz pracować.
5. W drzewie katalogów wybierz obiekt, z którego prawami własności chcesz pracować, i kliknij **OK**.

Praca z listami kontroli dostępu (ACL)

Praca z listami ACL obejmuje przypisywanie obiektom w katalogach jawnych i niejawnych list ACL, dodawanie użytkowników do ACL, usuwanie użytkowników z ACL i przeglądanie obiektów w katalogach. Należy zauważyć, że począwszy od wersji V5R1 Usługi katalogowe obsługują nowy model ACL, co oznacza, że jeśli listy ACL były stosowane wcześniej, to należy ponownie się z nimi zapoznać.

Aby pracować z listami kontroli dostępu, wykonaj następujące kroki:

1. W programie iSeries Navigator rozwiń pozycję **Sieć**.
2. Rozwiń pozycję **Serwery**.
3. Kliknij **TCP/IP**.
4. Prawym przyciskiem myszy kliknij **Katalog** i wybierz **Uprawnienia**.

   Jeśli nie jesteś jeszcze połączony z serwerem katalogów, zostanie wyświetlone okno dialogowe **Połącz z serwerem katalogów**. Połącz się jako administrator serwera lub właściciel obiektu, z którego listą ACL chcesz pracować.
5. W drzewie katalogów wybierz obiekt, z którego listą ACL chcesz pracować, i kliknij **OK**.

6. Kliknij zakładkę **ACL**.

Praca z grupami list kontroli dostępu (ACL)

Aby pracować z grupami ACL, wykonaj następujące kroki:
1. W programie iSeries Navigator wybierz opcję **Sieć**.
2. Wybierz opcję **Serwery**.
3. Kliknij **TCP/IP**.
4. Prawym przyciskiem myszy kliknij **Katalog** i wybierz **Grupy ACL**.

Praca z dostępem administratora dla upoważnionych użytkowników

Począwszy od wersji V5R2 można nadać dostęp administratora profilom użytkowników, które mają dostęp do idetyfikatora funkcji Directory Services Administrator (QIBM_DIRSRV_ADMIN).

Na przykład jeśli profil użytkownika JOHNSMITH ma nadany dostęp do identyfikatora funkcji Directory Services Administrator oraz w oknie dialogowym Właściwości katalogu wybrana jest opcja Nadanie dostępu administratora uprawnionym użytkownikom, profil JOHNSMITH ma wtedy uprawnienia administratora LDAP. Kiedy ten profil używany jest do połączenia z serwerem katalogów za pomocą następującej nazwy wyróżniającej (DN) os400-profile=JOHNSMTH,cn=accounts,os400-sys=systemA.acme.com, użytkownik ma uprawnienia administratora. Przyrostek obiektów systemu w tym przykładzie wygląda następująco: os400-sys=systemA.acme.com. Więcej informacji na temat użytkowników rzutowanych znajduje się w sekcji “Postprocesor rzutowania systemu operacyjnego” na stronie 43.

Aby wybrać tę opcję, wykonaj następujące kroki:
1. W programie iSeries Navigator rozwiń pozycję **Sieć**.
2. Wybierz opcję **Serwery**.
3. Prawym przyciskiem myszy kliknij pozycję **Katalog** i wybierz opcję **Właściwości**.
4. Na zakładce **Ogólne** w **Informacjach administratora** wybierz opcję **Nadaj administratorowi dostęp do użytkowników autoryzowanych**.

Aby ustawić identyfikator funkcji uprawniającej Directory Services Administrator w profilu użytkownika, wykonaj następujące kroki:
1. W programie iSeries Navigator prawym przyciskiem myszy kliknij nazwę systemu i wybierz **Application Administration (Administrowanie aplikacji)**.
2. Kliknij zakładkę **Host Applications (Aplikacje udostępniane)**.
3. Rozwiń **Operating System/400**.
4. Kliknij **Directory Services Administrator**, aby wyróżnić opcję.
5. Kliknij przycisk **Customize (Dostosuj)**.
6. Rozwiń pozycję **Users (Użytkownicy)**, **Groups (Grupy)** lub **Uses not in a group (Użytkownicy spoza grup)**, która jest odpowiednia dla danego użytkownika.
7. Wybierz użytkownika lub grupę, która ma być dodana do listy **Access allowed (Dostęp zezwolony)**.
8. Kliknij przycisk **Dodaj**.
9. Kliknij przycisk **OK**, aby zastosować zmiany.
10. W oknie dialogowym **Application Administration (Administrowanie aplikacji)** kliknij przycisk **OK**.

Śledzenie dostępu i zmian w katalogu LDAP

Dostęp i zmiany w katalogu LDAP można śledzić. Do śledzenia zmian w katalogu można używać protokołu zmian katalogów LDAP. Protokół zmian znajduje się pod specjalnym przyrostkiem cn=changelog. Jest on przechowywany w bibliotece QUSRDIRCL.

Aby uaktywnić protokół zmian, wykonaj następujące kroki:

1. W programie iSeries Navigator rozwiń pozycję **Sieć**.
2. Rozwiń pozycję **Serwery**.
3. Kliknij **TCP/IP**.
4. Prawym przyciskiem myszy kliknij **Katalog** i wybierz **Właściwości**.
5. Kliknij zakładkę **Baza danych/Przyrostki**.
6. Wybierz **Protokół zmian katalogu**.
7. (opcjonalnie) W pozycji **Maksymalna liczba pozycji** podaj maksymalną liczbę pozycji, jaką może przechowywać protokół zmian.

   Uwaga: Jest to wprawdzie parametr opcjonalny, ale zaleca się określanie maksymalnej liczby pozycji. Jeśli nie zostanie podana, protokół zmian będzie przechowywał wszystkie pozycje i może stać się bardzo duży.

Klasa obiektów changeLogEntry jest wykorzystywana do przedstawiania zmian zastosowanych w serwerze katalogów. Zestaw zmian jest podany w postaci uporządkowanego zestawu wszystkich pozycji znajdujących się w pojemniku protokołu zmian, określonego przez parametr changeNumber (liczba zmian). Informacja protokołu zmian jest ″tylko do odczytu″.

Użytkownik, znajdujący się na liście ACL dla przyrostka cn=changelog, może przeszukiwać pozycje w protokole zmian. Można wykonywać tylko przeszukiwania według przyrostka protokołu zmian cn=changelog. Nie należy próbować dodawać, zmieniać ani usuwać przyrostka protokołu zmian nawet wtedy, gdy posiada się stosowne uprawnienia. Może to wywołać nieprzewidywalne skutki.

Przykład:

Poniższy przykład korzysta z programu narzędziowego wiersza komend ldapsearch, aby wczytać wszystkie pozycje protokołu zmian zarejestrowanych na serwerze:

```
ldapsearch -h host_ldap  -D cn=administrator -w hasło -b cn=changelog  (changetype=*)
```

Włączanie kontrolowania obiektu dla serwera katalogów

Usługi katalogowe obsługują kontrolowanie ochrony OS/400. Jeśli wartość systemowa QAUDCTL ma wartość *OBJAUD, to kontrolowanie obiektu można włączyć za pomocą programu iSeries Navigator.

Aby włączyć kontrolowanie obiektu dla Usług katalogowych, wykonaj następujące czynności:
1. W programie iSeries Navigator rozwiń pozycję **Sieć**.
2. Rozwiń pozycję **Serwery**.
3. Kliknij **TCP/IP**.
4. Prawym przyciskiem myszy kliknij **Katalog** i wybierz **Właściwości**.
5. Kliknij zakładkę **Kontrola**.
6. Wybierz ustawienia kontroli dla serwera.

Zmiany ustawień kontroli odniosą skutek natychmiast po kliknięciu **OK**, nie trzeba restartować serwera katalogów LDAP. Więcej informacji znajduje się w sekcji “Ochrona Usług katalogowych” na stronie 40

Regulowanie wydajności serwera katalogów LDAP

Wydajność serwera katalogów LDAP można regulować zmieniając jedną z następujących charakterystyk:
- wielkość operacji przeszukiwania,
- maksymalny czas dozwolony dla przeszukiwania,
- ustawienia transakcji serwera,
- liczbę połączeń baz danych i wątków serwera.

Aby dostosować wartości związane z wydajnością serwera katalogów, wykonaj następujące kroki:
1. W programie iSeries Navigator rozwiń pozycję **Sieć**.
2. Rozwiń pozycję **Serwery**.

3. Kliknij **TCP/IP**.
4. Prawym przyciskiem myszy kliknij **Katalog** i wybierz **Właściwości**.
5. Kliknij zakładkę **Wydajność**.

Można także dopasować wydajność serwera katalogów przez zmianę liczby połączeń baz danych oraz wątków serwera wykorzystywanych przez niego. Aby zmienić tę wartość, wykonaj następujące kroki:
1. W programie iSeries Navigator rozwiń pozycję **Sieć**.
2. Rozwiń pozycję **Serwery**.
3. Kliknij **TCP/IP**.
4. Prawym przyciskiem myszy kliknij **Katalog** i wybierz **Właściwości**.
5. Kliknij zakładkę **Baza danych**/**Przyrostki**.

Rozdział 5. Pojęcia dotyczące Usług katalogowych

Poniższe informacje będą pomocne podczas zdobywania wiedzy na temat serwera LDAP Usług katalogowych i uruchamiania go:

Informacje na temat podstaw LDAP oraz planowania serwera LDAP zawiera także Rozdział 3, "Pierwsze kroki w Usługach katalogowych" na stronie 7.

Listy kontroli dostępu LDAP

W wielu przypadkach może zaistnieć potrzeba ograniczenia dostępu do danych na serwerze katalogów LDAP. Na przykład serwer LDAP w sieci wewnętrznej przedsiębiorstwa może zawierać książkę telefoniczną pracowników. Być może konieczne będzie umożliwienie wszystkim pracownikom przeglądania danych w tym katalogu.

Jednak pani prezes firmy nie chce, aby wszyscy pracownicy mieli dostęp do jej numeru telefonu. W tym przypadku można utworzyć **listę ACL**. Przy jej pomocy można ograniczyć dostęp do tej pozycji tylko do tych pracowników, od których prezes chce otrzymywać telefony.

Przy pomocy list ACL można sterować uprawnieniami do dodawania i usuwania obiektów katalogu. Można także określić, czy użytkownicy mogą czytać, pisać, przeszukiwać i porównywać atrybuty katalogu. Listy ACL mogą być dziedziczone lub jawne. Oznacza to, że można korzystać z list ACL na dwa sposoby:

- jawnie skonfigurować listę ACL dla konkretnych obiektów,
- określić, czy obiekty dziedziczą listy ACL od obiektów znajdujących się wyżej w hierarchii katalogu LDAP.

Być może prezes w poprzednim przykładzie nie chciała, aby wszyscy pracownicy mieli dostęp do jej numeru telefonu. Chciała jednak, aby wszyscy menedżerowie mieli do niego dostęp. W tym przypadku można użyć **Grupy ACL**, aby uprościć nadawanie uprawnień dla menedżerów. Grupy ACL umożliwiają nadawanie uprawnień dostępu konkretnym grupom użytkowników, zamiast nadawania ich indywidualnie. Jest to szczególnie użyteczne, jeśli ta sama grupa osób wymaga dostępu do więcej niż jednego zestawu obiektów. Jeśli na przykład ci sami menedżerowie, którzy mieli dostęp do numeru telefonu pani prezes, będą potrzebowali później dostępu do pozycji finansowych, można ponownie użyć grupy ACL.

Modele ACL

Wszystkie wersje Usług katalogowych obsługują model uprawnień na poziomie klasy dostępu. W modelu tym każdy typ atrybutu LDAP ma klasyfikację Normal (zwykły), Sensitive (wrażliwy) lub Critical (krytyczny). Klasyfikacje te określone są w plikach schematów atrybutów. Podczas dodawania użytkownika do listy ACL obiektu określa się, dla których klasyfikacji użytkownik ma prawo odczytu, zapisu, przeszukiwania, porównywania. W większości schematów numer telefonu będzie sklasyfikowany jako atrybut Normal (zwykły). Dlatego, aby menedżerom w powyższym przykładzie udostępnić numer telefonu pani prezes, można im nadać prawa odczytu do atrybutu Normal w obiekcie katalogu zawierającym jej dane. Nie będą oni nadal mieli dostępu do danych z atrybutem Sensitive i Critical. Wszystkie wersje Usług katalogowych obsługują ustawianie uprawnień na poziomie klasy dostępu.

Usługi katalogowe obsługują także model uprawnień na poziomie atrybutów. W modelu tym możliwe jest podanie uprawnień do odczytu, zapisu, przeszukiwania i porównywania dla określonych atrybutów, bez względu na ich klasę dostępu. Wróćmy do powyższego przykładu. W modelu uprawnień na poziomie atrybutów można nadać menedżerom dostęp do odczytu atrybutu telephoneNumber(numer telefonu) nawet jeśli nie mają oni dostępu do atrybutów Normal.

Model uprawnień na poziomie atrybutów jest zgodny tylko z serwerami Usług katalogowych SecureWay w wersji 3.2 i nowszych. Domyślnie nie jest włączony. Opcję jego uaktywnienia można znaleźć podczas pracy z listami kontroli dostępu. Po włączeniu model można wyłączyć tylko rekonfigurując serwer i odtwarzając bazę danych katalogów. Przed podjęciem decyzji o włączeniu tego modelu należy zdać sobie sprawę z tego, że nie będzie możliwości administrowania nim z dowolnego klienta V2 LDAP (włącznie z iSeries Navigator w wersjach przed V5R1), a próba takiego administrowania może spowodować uszkodzenie pozycji listy ACL.

Specjalne wartości ACL

Początkowo wszystkie obiekty w serwerze katalogów Usług katalogowych mają listę ACL, która zawiera specjalną grupę ACL, CN=Anybody, obejmującą wszystkich użytkowników katalogu. Domyślnie grupa ta ma prawo do odczytu, przeszukiwania i porównywania atrybutów klasy Normal dla wszystkich obiektów.

Można nadać kilku obiektom takie same prawa dostępu dla wszystkich użytkowników, którzy połączą się z serwerem katalogów połączeniem innym niż anonimowe. Aby to zrobić, należy użyć specjalnej grupy list kontroli dostępu (ACL) cn=Authenticated.

Aby określić, jakie prawa dostępu ma obiekt, można skorzystać ze specjalnej nazwy wyróżniającej (DN) cn=this. W ten sposób pozycje potomne, dziedziczące listy ACL, są automatycznie uprawnione do wykonywania operacji na swoich własnych obiektach.

Dodatkowe informacje

Aby administrować listami ACL przy pomocy programu iSeries Navigator, nie jest potrzebna znajomość szczegółów dotyczących sposobu, w jaki Usługi katalogowe implementują listy ACL. Jednak jeśli chcesz zmieniać atrybuty dotyczące list ACL podczas przetwarzania plików LDIF lub używać list ACL z poziomu wiersza komend LDAP, koniecznie zapoznaj się z atrybutami list ACL. Więcej informacji na temat atrybutów list ACL znajduje się w dokumencie Access Control Lists (Listy kontroli dostępu) w dokumentacji The IBM SecureWay Directory Management Tool.

Aby uzyskać więcej informacji na temat konfigurowania i zmieniania list ACL i grup ACL, należy przejść do następujących tematów:

“Praca z listami kontroli dostępu (ACL)” na stronie 30
“Praca z grupami list kontroli dostępu (ACL)” na stronie 31

Format wymiany danych LDAP

Format LDIF (LDAP data interchange format) umożliwia łatwe przesyłanie danych z katalogu pomiędzy serwerami katalogów LDAP. Pliki LDIF zawierają pozycje katalogów LDAP w prostym formacie tekstowym. Format LDIF używany przez serwer katalogów zmienił się począwszy od wersji V4R5 Usług katalogowych. Pliki LDIF składają się z sekwencji wierszy opisujących pozycję katalogu lub zestaw zmian dla pozycji katalogu. Nie mogą opisywać obu rzeczy jednocześnie.

Ogólnym formatem pozycji LDIF jest:

```
version: 1
dn: nazwa wyróżniająca
typatr1: wartośćatr1
...
```

gdzie:

- *version* oznacza wersję formatu pliku LDIF. Numerem wersji musi być 1. Jeśli brakuje numeru wersji, plik LDIF jest traktowany jako zbiór w starszym formacie. Gdy plik LDIF jest w wersji 1, jego zawartość MUSI być kodowana w formacie UTF-8.
- *nazwa wyróżniająca* jest nazwą wyróżniającą pozycji katalogu.
- *typatr1* jest typem atrybutu LDAP (takim jak cn lub ou).
- *wartośćatr1* jest wartością atrybutu.

Każda pozycja może mieć kilka atrybutów. Każdy atrybut występuje w osobnym wierszu. Jeśli wartość atrybutu jest dłuższa niż jeden wiersz, może być kontynuowana w następnym wierszu i jest poprzedzona znakiem spacji lub tabulatorem.

Pozycje z tego samego pliku LDIF rozdzielone są przez puste wiersze. Każdy wiersz rozpoczynający się haszem (#) jest wierszem komentarza i musi być ignorowany podczas analizowania pliku LDIF.

Każda nazwa wyróżniająca lub wartość atrybutu powinna być zakodowana w formacie base-64, jeśli wystąpi jeden z warunków:

- zawiera znaki końca wiersza lub wysuwu o wiersz,
- zaczyna się od dwukropka (:), spacji lub znaku mniejszości (<),
- kończy się spacją.

Atrybuty kodowane w formacie base-64 są oznaczone przez użycie dwóch dwukropków między nazwą atrybutu a jego wartością.

Zewnętrzne odniesienia znajdują się w pliku:// URL format. Pomiędzy typem atrybutu a wartością zewnętrznego odniesienia powinien się znajdować dwukropek i znak mniejszości (″:<″).

Poniżej zamieszczono kilka przykładów plików LDIF:

Przykład 1: prosty plik LDAP zawierający dwie pozycje

```
version: 1
   dn: cn=Barbara Jensen, ou=Rochester, o=Big Company, c=US
   objectclass: top
   objectclass: person
   objectclass: organizationalPerson
   cn: Barbara Jensen
   cn: Barbara J Jensen
   cn: Babs Jensen
   sn: Jensen
   uid: bjensen
   telephonenumber: +1 408 555 1212
   description: Wielka miłośniczka żeglarstwa.

   dn: cn=Bjorn Jensen, ou=Rochester, o=Big Company, c=US
   objectclass: top
   objectclass: person
   objectclass: organizationalPerson
   cn: Bjorn Jensen
   sn: Jensen
   telephonenumber: +1 408 555 1212
   description:Babs jest wielkim miłośnikiem żeglarstwa i dużo pływa
   poszukując doskonałych warunków do żeglowania.
   title:Product Manager, Rod and Reel Division
```

Przykład 2: plik zawierający wartość zakodowaną w formacie base-64

```
version: 1
   dn: cn=Gern Jensen, ou=Rochester, o=Big Company, c=US
   objectclass: top
   objectclass: person
   objectclass: organizationalPerson
```

```
   cn: Gern Jensen
   cn: Gern O Jensen
   sn: Jensen
   uid: gernj
   telephonenumber: +1 408 555 1212
   description:: V2hhdCBhIGNhcmVmdWwgcmVhZGVyIHlvdSBhcmUhICBUaGlzIHZhbHVlIGlzIGJ
    hc2UtNjQtZW5jb2RlZCBiZWNhdXNlIGl0IGhhcyBhIGNvbnRyb2wgY2hhcmFjdGVyIGluIGl0ICh
    hIENSKS4NICBCeSB0aGUgd2F5LCB5b3Ugc2hvdWxkIHJlYWxseSBnZXQgb3V0IG1vcmUu
```

Przykład 3: plik zawierający serie rekordów zmian i komentarzy

Uwaga: Pliki LDIF z rekordami zmian nie mogą być importowane bezpośrednio do serwera. Natomiast są one obsługiwane przez programy użytkowe powłoki LDAP.

```
version: 1
   # Dodanie nowej pozycji
   dn: cn=Fiona Jensen, ou=Rochester, o=Big Company, c=US
   changetype: add
   objectclass: top
   objectclass: person
   objectclass: organizationalPerson
   cn: Fiona Jensen
   sn: Jensen
   uid: fiona
   telephonenumber: +1 408 555 1212
   jpegphoto:< file:///usr/local/directory/photos/fiona.jpg

   # Usunięcie istniejącej pozycji
   dn: cn=Robert Jensen, ou=Rochester, o=Big Company, c=US
   changetype: delete

   # Zmodyfikowanie względnej nazwy wyróżniającej pozycji
   dn: cn=Paul Jensen, ou=Rochester, o=Big Company, c=US
   changetype: modrdn
   newrdn: cn=Paula Jensen
   deleteoldrdn: 1
```

Kolejność pozycji w pliku LDIF jest ważna. Pozycja nadrzędna musi już istnieć w katalogu, aby pomyślnie dodać pozycję, która jest podana w pliku LDIF do katalogu LDAP. W podanym przykładzie druga i trzecia pozycja nie zostaną dodane, jeśli pierwsza pozycja nie istnieje.

Podobnie, aby można było zaimportować plik LDIF do serwera, który obsługuje pewne przyrostki, musi on zawierać pozycje dla tych przyrostków. Na przykład, jeśli serwer miał przyrostek ou=Rochester, o=Big Company, c=US, plik LDIF przedstawiony powyżej mógł być zaimportowany. Ale jeśli serwer miał przyrostek o=Big Company, c=US, musi istnieć pozycja dla tego przyrostka, określona jako pierwsza w pliku LDIF w następujący sposób:

```
dn: o=Big Company, c=US
objectclass: organization
o: Big Company
```

Konkretny format i zawartość plików LDIF są określone przez schemat serwera, z którego są eksportowane. Można importować plik LDIF do każdego serwera LDAP używającego takiego samego schematu, jak serwer, z którego plik był eksportowany. Serwery LDAP różnych producentów używają różnych schematów (z innymi klasami obiektów i atrybutami). Dlatego nie można importować pliku LDIF, który został utworzony na jednym serwerze, do innego serwera.

Specyfikacje plików LDIF w postaci RFC są dostępne pod następującym adresem URL:

http://www.ietf.org/rfc/rfc2849.txt

Procedury pokrewne:

“Importowanie pliku LDIF” na stronie 22
“Eksportowanie pliku LDIF” na stronie 22

Uwagi na temat obsługi języków narodowych (NLS)

Począwszy od wersji V4R5 zarówno serwer LDAP OS/400 Directory Services jaki i klient LDAP OS/400 opierają się na protokole LDAP w wersji 3. Wiąże się to z następującymi zagadnieniami dotyczącymi NLS:

- dane są przesyłane pomiędzy serwerami LDAP a klientami w formacie UTF-8; wszystkie znaki ISO 10646 są dozwolone,
- serwer usług katalogowych LDAP w celu wprowadzenia danych do bazy danych korzysta z metody odwzorwującej UTF-16,
- serwer i klient dokonują porównań ciągów znaków bez rozróżniania wielkich i małych liter; algorytmy wykorzystujące wielkie litery nie działają poprawnie dla wszystkich języków (ustawień narodowych).

Więcej informacji dotyczących UCS-2 zawiera sekcja Globalization w artykule Planning w Centrum informacyjnym iSeries.

Prawa własności do obiektów w katalogach LDAP

Każdy obiekt w katalogu LDAP ma przynajmniej jednego właściciela. Właściciele obiektów mają prawo do ich usuwania. Właściciele i administrator serwera są jedynymi użytkownikami, którzy mogą zmieniać atrybuty prawa własności oraz listy ACL obiektu. Prawa własności do obiektu mogą być dziedziczone lub nadawane w sposób jawny. Oznacza to, że aby nadać prawa własności, można wykonać jedną z poniższych czynności:

- nadać w sposób jawny prawa własności do konkretnego obiektu,
- określić, że obiekty dziedziczą prawa własności z obiektów na wyższych poziomach w hierarchii katalogów LDAP.

Usługi katalogowe pozwalają na określnie kilku właścicieli dla tego samego obiektu. Można także określić, czy obiekt jest właścicielem samego siebie. Aby to zrobić, należy dołączyć wartość specjalną DN cn=this do listy właścicieli obiektu. Na przykład przyjmijmy, że właścicielem obiektu cn=A jest cn=this. Każdy użytkownik będzie miał dostęp do obiektu cn=A na prawach właściciela, jeśli połączy się on z serwerem jako cn=A.

Procedura pokrewna:

“Praca z prawami własności do obiektów katalogu” na stronie 30

Odwołania do katalogu LDAP

Odwołania umożliwiają serwerom katalogów LDAP pracę w grupach. Jeśli nazwy DN żądanej przez klienta nie ma w jednym katalogu, serwer może automatycznie wysłać żądanie (odwołać się) do innego serwera LDAP.

Usługi katalogowe umożliwiają użycie dwóch różnych typów odwołań. Można określić domyślne serwery odwołań, gdzie serwer LDAP będzie odnosił się do klientów, zawsze, gdy nazwy DN nie będzie w katalogu. Można także użyć klienta LDAP do dodania do serwera katalogów pozycji, których parametrem jest odwołanie objectClass. Umożliwia to określanie odwołań zależnych od żądanej nazwy DN.

Uwaga: W przypadku Usług katalogowych obiekty odwołania muszą zawierać tylko nazwę wyróżniającą (dn), klasę obiektów (objectClass) i atrybut odniesienia (ref). Sekcja “Narzędzie ldapsearch” na stronie 56 zawiera przykład ilustrujący te ograniczenia.

Serwery odwołań są ściśle powiązane z serwerami replik. Ponieważ dane na serwerach replik nie mogą być zmieniane przez klientów, serwer replik przekazuje wszystkie żądania zmiany danych katalogu do serwera głównego.

Transakcje

Systemowy serwer katalogów LDAP można tak skonfigurować, aby programy typu klient mogły korzystać z transakcji. Transakcja to grupa działań na katalogach LDAP, traktowana jak jedna jednostka. Żadne z pojedynczych działań LDAP, stanowiących część transakcji, nie zostanie wprowadzone na stałe dopóki wszystkie działania w transakcji nie zostaną pomyślnie zakończone i nie zostanie ona zatwierdzona. Jeśli jakiekolwiek działanie się nie powiedzie lub transakcja zostanie anulowana, to pozostałe działania zostaną cofnięte. Umożliwia to utrzymanie porządku w działaniach LDAP. Użytkownik może na przykład skonfigurować w swoim kliencie transakcję, która będzie usuwała kilka pozycji katalogu. Jeśli klient utraci połączenie z serwerem, to dzięki transakcji żadna z pozycji nie zostanie usunięta. Użytkownik może po prostu uruchomić transakcję ponownie, bez sprawdzania, które pozycje zostały pomyślnie usunięte.

Częścią transakcji mogą być następujące działania LDAP:

- dodawanie,
- modyfikowanie,
- modyfikowanie nazwy RDN,
- usuwanie.

Uwaga: Nie należy umieszczać w transakcjach zmian w schemacie katalogu (cn=przyrostek schematu). Można je brać pod uwagę, ale nie zostaną one wycofane, jeśli transakcja się nie powiedzie. Może to spowodować wystąpienie nieprzewidywalnych problemów w serwerze katalogów.

Dodatkowe informacje na temat transakcji znajdują się w dodatku Limited Transaction Support dokumentacji IBM SecureWay Directory Client SDK Programming Reference .

Repliki serwerów katalogów LDAP

Dane znajdujące się na replikach serwerów katalogów LDAP są takie same, jak dane na głównym serwerze katalogów LDAP (master server). Istnieją dwie główne zalety posiadania jednej lub kilku replik katalogu LDAP:

- Repliki powodują zwiększenie szybkości przeszukiwania katalogów. Zamiast bezpośredniego wyszukiwania przez klientów żądań na jednym głównym serwerze, można je podzielić pomiędzy główny serwer i serwery replik.
- Repliki zapewniają kopię zapasową serwera głównego. Jeśli główny serwer nie jest dostępny, serwer replik może nadal w pełni realizować żądania przeszukiwania i umożliwiać dostęp do danych katalogu.

Serwery replik przeznaczone są tylko do odczytu. Jeśli uprawniony użytkownik próbuje zmienić pozycję na serwerze replik, przesyła on żądanie do głównego serwera katalogów.

Procedura pokrewna:

“Tworzenie nowej repliki serwera katalogów” na stronie 23

Ochrona Usług katalogowych

Kontrola działania ochrony

Począwszy od wersji V5R1, Usługi katalogowe obsługują kontrolę ochrony OS/400. Kontrola obejmuje następujące elementy:

- łączenie i odłączanie się od serwera katalogów,
- zmiany w uprawnieniach do obiektów katalogu LDAP,
- zmiany praw własności obiektów katalogu LDAP,
- tworzenie, usuwanie, przeszukiwanie i zmiany obiektów katalogu LDAP,

- zmiany hasła administratora i aktualizacje nazw wyróżniających (DN),
- zmiany haseł użytkowników,
- import i eksport zbiorów.

Zanim kontrola pozycji katalogu zacznie działać, potrzebne może się okazać wprowadzenie kilku zmian do ustawień kontroli systemu OS/400. Jeśli wartość systemowa QAUDCTL ma wartość *OBJAUD, to można włączyć kontrolowanie obiektu za pomocą programu iSeries Navigator. Więcej informacji dotyczących kontroli znajduje się w artykule *Security - Reference*  lub Kontrola ochrony w Centrum informacyjnym iSeries.

Uwierzytelnianie i ochrona połączenia

Usługi katalogowe dostarczają następującego mechanizmu, który można rozszerzyć na ochronę komunikacji pomiędzy klientami LDAP i serwerem katalogów LDAP:

- połączenia Secure Sockets Layer (SSL),
- uwierzytelnianie protokołem Kerberos,
- szyfrowanie haseł CRAM-MD5.

Używanie ochrony SSL (Secure Sockets Layer) i TLS (Translation Layer Security) na serwerze katalogów LDAP

Aby komunikacja z serwerem katalogów LDAP była lepiej chroniona, Usługi katalogowe mogą używać ochrony SSL (Secure Sockets Layer).

Aby używać SSL z Usługami katalogowymi, należy zainstalować w systemie jeden z produktów Cryptographic Access Provider (5722-ACx). Jeśli ochrona SSL ma być używana poprzez iSeries Navigator, należy zainstalować na komputerze PC jeden z produktów Client Encryption (5722-CEx). Oprogramowanie to jest potrzebne do:

- Skonfigurowania i administrowania Usług katalogowych ze stacji roboczej za pomocą połączenia SSL. Obejmuje to czynności wykonywane za pomocą iSeries Navigator.
- Używania połączenia SSL z aplikacjami utworzonymi za pomocą interfejsów API klienta Windows.

Ochrona SSL jest standardem dla ochrony w Internecie. SSL można używać do komunikowania się zarówno z klientami LDAP, jak i z serwerami replik LDAP. Aby zapewnić dodatkową ochronę połączeń SSL, można korzystać z uwierzytelniania klienta oprócz uwierzytelniania systemu. Uwierzytelnianie klienta wymaga od klienta LDAP przedstawienia certyfikatu cyfrowego, który potwierdza tożsamość klienta w serwerze przed ustanowieniem połączenia.

Aby używać SSL, należy zainstalować w systemie produkt DCM, opcja 34 systemu OS/400. Program DCM zawiera interfejs, który umożliwia tworzenie i zarządzanie certyfikatami cyfrowymi i bazami certyfikatów. Aby uzyskać informacje na temat certyfikatów cyfrowych i używania programu DCM, patrz sekcja Zarządzanie certyfikatami cyfrowymi. Aby uzyskać informacje na temat ochrony SSL na serwerach iSeries, patrz sekcja Ochrona aplikacji z użyciem SSL. Aby uzyskać informacje na temat ochrony TLS na serwerach iSeries, patrz sekcja Supported SSL and Transport Layer Security (TLS) protocols.

Wykorzystywanie przez serwer LDAP uwierzytelniania protokołem Kerberos

Usługi katalogowe umożliwiają takie skonfigurowanie serwera katalogów LDAP, aby korzystał on z uwierzytelniania protokołem Kerberos. Protokół Kerberos jest sieciowym protokołem uwierzytelniania, korzystającym z kryptografii klucza tajnego i obsługującym uwierzytelnianie aplikacji typu klient/serwer.

Aby włączyć uwierzytelnianie protokołem Kerberos, należy zainstalować w systemie jeden z produktów Cryptographic Service Provider products (5722AC2 lub 5722AC3). Konieczne jest także skonfigurowanie sieciowych usług uwierzytelniania.

Protokół Kerberos dla Usług katalogowych zapewnia obsługę mechanizmu GSSAPI SASL. Umożliwia to klientom LDAP, zarówno SecureWay, jak i Windows 2000 korzystanie z uwierzytelniania Kerberos z serwerem katalogów LDAP.

Używana przez serwer **nazwa główna Kerberos** ma następującą postać:

```
nazwa-usługi/nazwa-hosta@dziedzina
```

nazwa-usługi to LDAP, nazwa-hosta to pełna nazwa systemu w sieci TCP/IP, zaś dziedzina jest to domyślna dziedzina podawana w konfiguracji protokołu Kerberos systemu.

Na przykład dla systemu o nazwie mój-as400, w domenie TCP/IP acme.com, z domyślną dziedziną Kerberos ACME.COM, nazwa główna Kerberos serwera LDAP powinna brzmieć LDAP/mój-as400.acme.com@ACME.COM. Domyślna dziedzina protokołu Kerberos jest podana w pliku konfiguracyjnym protokołu (domyślnie jest to /QIBM/UserData/OS400/NetworkAuthentication/krb5.conf) z dyrektywą default_realm (default_realm = ACME.COM). Przyjęto konwencję stosowania wielkich liter dla nazw dziedzin protokołu Kerberos i małych dla nazw hostów. LDAP/ musi być napisane wielkimi literami. Jeśli domyślna dziedzina nie zostanie skonfigurowana, nie będzie możliwe skonfigurowanie serwera katalogów tak, aby korzystał z uwierzytelniania protokołem Kerberos.

Jeśli używane jest uwierzytelnianie protokołem Kerberos, to serwer katalogów LDAP wiąże nazwę wyróżniającą (DN) z połączeniem, określając w ten sposób dostęp do danych katalogu. Nazwę wyróżniającą serwera można wybrać za pomocą jednej z przedstawionych metod:

- Serwer może utworzyć nazwę wyróżniającą w oparciu o identyfikator protokołu Kerberos. Po wybraniu tej opcji tożsamość protokołu Kerberos w postaci główny@dziedzina generuje nazwę wyróżniającą w postaci ibm-nk=główny@dziedzina, ibm-kn= jest równoznaczne z ibm-kerberosName=.
- Serwer szuka w katalogu nazwy wyróżniającej (DN), która zawiera pozycje dla jednostki głównej i dziedziny protokołu Kerberos. Po wybraniu tej opcji serwer przeszukuje katalog, aby znaleźć pozycję, która określa protokół Kerberos:
  - Serwer szuka w katalogu obiektu krbRealm-V2, który ma atrybut krbRealmName-V2 odpowiadający dziedzinie protokołu Kerberos. Jeśli znajdzie taką pozycję, to przeszukuje nazwy wyróżniające podane dla atrybutu princSubtree, które są zgodne z nazwą główną oraz nazwą dziedziny. Nazwa wyróżniająca, skonfigurowana w atrybucie krbAliasedObjectName, jest używana jeśli zawiera nazwę wyróżniającą wcześniej znalezionej pozycji. W przeciwnym przypdku używana jest nazwa wyróżniająca pozycji. Metoda ta jest zazwyczaj używana, gdy KDC protokołu Kerberos przechowuje informacje jednostki głównej w katalogu LDAP.
  - Jeśli przedstawione powyżej wyszukiwanie nie powiedzie się, wtedy serwer rozpocznie szukanie pozycji katalogu, która używa klasy pomocniczej ibm-securityIdentities a jej wartością atrybutu altSecurityIdentities jest KERBEROS:principal@realm. Metody tej można użyć do powiązania tożsamości protokołu Kerberos gdy KDC nie przechowuje jednostek głównych w katalogu.

Niezbędny jest plik tabeli kluczy (keytab), zawierający klucz dla jednostki głównej usługi LDAP. Więcej informacji, na temat używania protokołu Kerberos na serwerach iSeries, znajduje się w Centrum informacyjnym w temacie Network authentication service (Sieciowe usługi uwierzytelniania) w sekcji Security (Ochrona). Sekcja Konfigurowanie sieciowych usług uwierzytelniania omawia dodawanie informacji do plików tabel kluczy.

Postprocesor rzutowania systemu operacyjnego

Postprocesor rzutowania systemu ma możliwość odwzorowywania obiektów OS/400 jako pozycji wewnątrz drzewa katalogów dostępnego z LDAP. Obiekty rzutowane są reprezentacjami LDAP obiektów OS/400 bieżących pozycji przechowywanych w bazie danych serwera LDAP. Począwszy od wersji V5R2 profile użytkowników OS/400 są jedynymi obiektami odwzorowywanymi lub rzutowanymi jako pozycje wewnątrz drzewa katalogowego. Odwzorowywanie profilu użytkownika odnosi się do postprocesora użytkownika rzutowanego systemu OS/400.

Operacje LDAP są odwzorowywane na obiektach bazowych (underlying) systemu OS/400 i wykonują funkcje systemu operacyjnego, w celu uzyskania dostępu do tych obiektów. Wszystkie operacje LDAP, przeprowadzane na profilach użytkowników, są dokonywane za pomocą uprawnień profilu użytkownika, który jest związany z połączeniem klienta.

Więcej informacji na temat postprocesora rzutowania systemu operacyjnego znajduje się w następujących sekcjach:

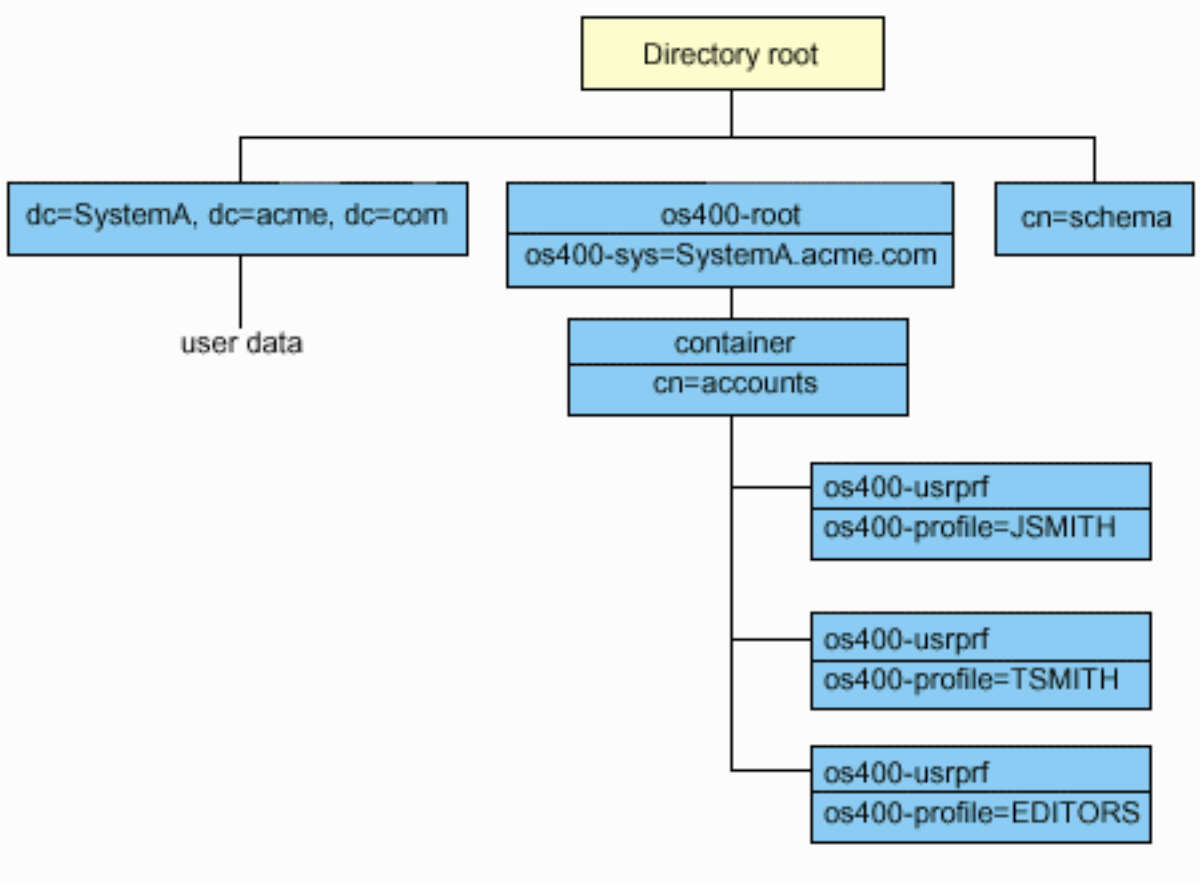
- “Drzewo informacji katalogu rzutowanych użytkowników systemu OS/400”
- “Operacje LDAP” na stronie 44
- “Administrator i nazwa wyróżniająca łącząca z repliką” na stronie 48
- “Schematy użytkowników rzutowanych systemu OS/400” na stronie 49

Drzewo informacji katalogu rzutowanych użytkowników systemu OS/400

Poniższy rysunek przedstawia przykładowe Drzewo informacji katalogu (DIT) dla postprocesora użytkownika rzutowanego. Rysunek przedstawia zarówno pojedyncze profile jak i grupy profili. Na tym rysunku JSMITH i TSMITH są profilami użytkowników, co jest wewnętrznie oznaczone przez identyfikator grupy (GID), GID=*NONE (lub 0); EDITORS jest profilem grupy, co jest wewnętrznie oznaczone przez niezerowy identyfikator GID.

Przyrostek dc=SystemA,dc=acme,dc=com został dołączony w celu pokazania odniesienia. Ten przyrostek przedstawia bieżący postprocesor bazy danych, zarządzanej przez inne pozycje LDAP. Przyrostek

cn=schema jest aktualnie używanym schematem serwera rozległego.



Korzeń drzewa jest przyroskiem, którego wartością domyślną jest os400-sys=*SystemA.acme.com*, gdzie *SystemA.acme.com* jest nazwą systemu. Klasą obiektu (objectclass) jest os400-root. Chociaż DIT nie może być modyfikowane lub usunięte, jednak można przekonfigurować przyrostek obiektu systemowego. Aby to zrobić, należy się upewnić, czy bieżący przyrostek nie jest używany na listach ACL lub gdzie indziej w systemie. Jeśli tak, należy zmodyfikować wszystkie miejsca, w których przyrostek jest używany.

Na poprzednim rysunku pojemnik cn=accounts został umieszczony poniżej korzenia. Ten obiekt nie może być modyfikowany. Pojemnik został umieszczony na tym poziomie w celu poprzedzania innego rodzaju informacji lub obiektów, które mogą być w przyszłości rzutowane przez system operacyjny. Poniżej pojemnika cn=accounts znajdują się profile użytkowników, które są rzutowane jako objectclass=os400-usrprf. Profile użytkowników odnoszą się do profili użytkowników rzutowanych i są znane protokołowi LDAP w postaci os400-profile=JSMITH,cn=accounts,os400-sys=SystemA.acme.com.

Operacje LDAP

Poniżej przedstawione są operacje LDAP, które mogą być przeprowadzone za pomocą profili użytkowników rzutowanych.

Łączenie

Klient LDAP może się łączyć (uwierzytelniać) z serwerem LDAP za pomocą profilu użytkownika rzutowanego. Łączenie polega na podaniu nazwy wyróżniającej (DN) profilu uzytkownika dla nazwy wyróżniającej połączenia oraz prawidłowego hasła uwierzytelniającego profilu użytkownika systemu OS/400. Przykładem użycia nazwy wyróżniającej przy żądaniu połączenia jest: os400-profile=jsmith,cn=accounts,os400-sys=systemA.acme.com.

Aby mieć dostęp do informacji postprocesora rzutowania systemu, klient musi połączyć się jako użytkownik rzutowany. Serwer przeprowadza wszystkie operacje korzystając z uprawnień tego profilu użytkownika. Nazwa wyróżniająca profilu użytkownika rzutowanego może być wykorzystywana w listach ACL LDAP, tak jak inne nazwy wyróżniające pozycji LDAP. Prosta metoda łączenia jest jedyną dozwoloną metodą łączenia, kiedy w żądaniu łączenia określony został użytkownik rzutowany.

Wyszukiwanie

Postprocesor rzutowanego systemu obsługuje kilka podstawowych filtrów wyszukiwania. W tych filtrach można określić atrybuty klasy obiektu os400-profile oraz os400-gid. Atrybut os400-profile obsługuje znaki zastępcze. Atrybut os400-gid jest ograniczony do określania (os400-gid=0) co jest pojedynczym profiem użytkownika, a co jest grupą profili !(os400-gid=0). Użytkownik możne odtworzyć wszystkie atrybuty profilu użytkownika, z wyjątkiem hasła i podobnych.

W przypadku niektórych filtrów zwracana jest jedynie klasa obiektu nazwy wyróżniającej oraz wartość atrybutu os400-profile. Jednakże, aby uzyskać bardziej szczegółowe informacje, można przeprowadzić dalsze wyszukiwania.

Poniższa tabela opisuje zachowanie postprocesora rzutowanego systemu w przypadku operacji wyszukiwania.

Tabela 1. Zachowanie postprocesora rzutowanego systemu dla operacji wyszukiwania

Żądanie wyszukiwania	**Podstawa wyszukiwania**	**Zasięg wyszukiwania**	**Filtr wyszukiwania**	**Komentarz**
Zwróć informacje dla os400-sys=SystemA, (opcjonalnie) dla pojemników znajdujących się pod nim i (opcjonalnie) dla obiektów w tych pojemnikach.	os400-sys=SystemA.acme.com	podstawowy, w poddrzewie lub jednopoziomowy	objectclass=* objectclass=os400-root objectclass=container objectclass=os400-usrprf	Zwraca odpowiednie atrybuty oraz ich wartości w oparciu o określony zasięg oraz filtr. Zwracane są atrybuty zestawu hardcoded oraz ich wartości dla przyrostka obiektu systemu i znajdującego się pod nim pojemnika.
Zwróć wszystkie profile użytkowników.	cn=accounts, os400-sys=SystemA.acme.com	jednopoziomowy lub w poddrzewie	os400-gid=0	Dla profili rzutowanych użytkowników zwracane są jedynie wartości nazwy wyróżniającej (DN), klasy obiektu oraz atrybutu os400-profile. Jeśli określony został inny filtr, zwracany jest LDAP_UNWILLING_TO_PERFORM.

Tabela 1. Zachowanie postprocesora rzutowanego systemu dla operacji wyszukiwania (kontynuacja)

Żądanie wyszukiwania	**Podstawa wyszukiwania**	**Zasięg wyszukiwania**	**Filtr wyszukiwania**	**Komentarz**
Zwróć wszystkie profile grup.	cn=accounts, os400-sys=SystemA.acme.com	jednopoziomowy lub w poddrzewie	(!(os400-gid=0))	Dla profili rzutowanych użytkowników zwracane są jedynie wartości nazwy wyróżniającej (DN), klasy obiektu oraz atrybutu os400-profile. Jeśli określony został inny filtr, zwracany jest LDAP_UNWILLING_TO_PERFORM.
Zwróć wszystkie profile użytkowników i grup.	cn=accounts, os400-sys=SystemA.acme.com	jednopoziomowy lub w poddrzewie	os400-profile=*	Dla profili rzutowanych użytkowników zwracane są jedynie wartości nazwy wyróżniającej (DN), klasy obiektu oraz atrybutu os400-profile. Jeśli określony został inny filtr, zwracany jest LDAP_UNWILLING_TO_PERFORM.
Zwróć informacje dla określonego użytkownika lub grupy, takich jak profil użytkownika JSMITH.	cn=accounts, os400-sys=SystemA.acme.com	jednopoziomowy lub w poddrzewie	os400-profile=JSMITH	Mogą byc określone inne atrybuty do zwrócenia.
Zwróć informacje dla określonego użytkownika lub grupy, takich jak profil użytkownika JSMITH.	os400-profile=JSMITH, cn=accounts, os400-sys=SystemA.acme.com	podstawowy, w poddrzewie lub jednopoziomowy	objectclass=os400-usrprf objectclass=* os400-profile=JSMITH	Można określić, że mają być zwracane inne atrybuty. Chociaż można określić zasięg jednopoziomowy, rezultaty wyszukiwania nie zwrócą wartości, ponieważ w drzewie DIT poniżej profilu użytkownika JSMITH nic nie ma.
Zwróć wszystkie profile użytkowników i grup zaczynające się na A.	cn=accounts, os400-sys=SystemA.acme.com	jednopoziomowy lub w poddrzewie	os400-profile=A*	Dla profili rzutowanych użytkowników zwracane są jedynie wartości nazwy wyróżniającej (DN), klasy obiektu oraz atrybutu os400-profile. Jeśli określony został inny filtr, zwracany jest LDAP_UNWILLING_TO_PERFORM.

Tabela 1. Zachowanie postprocesora rzutowanego systemu dla operacji wyszukiwania (kontynuacja)

Żądanie wyszukiwania	Podstawa wyszukiwania	Zasięg wyszukiwania	Filtr wyszukiwania	Komentarz
Zwróć wszystkie profile grup zaczynające się na G.	cn=accounts, os400-sys=SystemA.acme.com	jednopoziomowy lub w poddrzewie	(&(!(os400-gid=0)) (os400-profile=G*))	Dla profili rzutowanych użytkowników zwracane są jedynie wartości nazwy wyróżniającej (DN), klasy obiektu oraz atrybutu os400-profile. Jeśli określony został inny filtr, zwracany jest LDAP_UNWILLING_ TO_PERFORM.
Zwróć wszystkie profile użytkowników zaczynające się na A.	cn=accounts, os400-sys=SystemA.acme.com	jednopoziomowy lub w poddrzewie	(&(os400-gid=0) (os400-profile=A*))	Dla profili rzutowanych użytkowników zwracane są jedynie wartości nazwy wyróżniającej (DN), klasy obiektu oraz atrybutu os400-profile. Jeśli określony został inny filtr, zwracany jest LDAP_UNWILLING_ TO_PERFORM.

Porównywanie

Operacja porównywania LDAP może być użyta do porównania wartości atrybutu profilu użytkownika rzutowanego. Atrybuty os400-aut oraz os400-docpwd nie mogą być porównywane.

Dodawanie i modyfikowanie

Za pomocą operacji dodawania LDAP można tworzyć profile użytkowników, a za pomocą operacji modyfikowania LDAP - modyfikować je.

Usuwanie

Profile użytkowników można usuwać za pomocą operacji usuwania LDAP. Aby określić zachowanie parametrów DLTUSRPRF OWNOBJOPT i PGPOPT, dostarczono teraz dwa elementy kontrolne serwera LDAP. Te elementy kontrolne mogą być określone przy operacji usuwania LDAP. Więcej informacji na temat zachowania tych parametrów znajduje się w pomocy komendy Usuwanie profilu użytkownika (Delete User Profile - DLTUSRPRF).

Poniżej przedstawione są elementy kontrolne i ich identyfikatory obiektu (OID), które można określić podczas operacji usuwania klienta.

- os400-dltusrprf-ownobjopt 1.3.18.0.2.10.8

  Poniżej przedstawiona jest wartość sterująca:
  - controlValue ::= ownObjOpt [newOwner]
  - ownObjOpt ::= *NODLT / *DLT / *CHGOWN

Wartość sterująca ownObjOpt określa rodzaj działania w przypadku, gdy profil użytkownika ma jakieś obiekty. Wartość *NODLT oznacza, że profil użytkownika nie zostanie usunięty, jeśli jest właścicielem istniejących obiektów. Wartość *DLT oznacza usunięcie posiadanych obiektów, a wartość *CHGOWN przeniesienie prawa własności do innego profilu.

Wartość newOwner określa profil, do którego ma być przeniesione prawo własności. Ta wartość jest wymagana, jeśli ownObjOpt jest ustawione na *CHGOWN.

Przykłady wartości kontrolnych są następujące:

- *NODLT: określa, że profil nie może być usunięty, jeśli ma jakiś obiekt,
- *CHGOWN SMITH: określa przeniesienie prawa własności jakichkolwiek obiektów do profilu użytkownika SMITH.

- Identyfikator obiektu (OID) jest określony w pliku ldap.h jako LDAP_OS400_OWNOBJOPT_CONTROL_OID.
  - os400-dltusrprf-pgpopt 1.3.18.0.2.10.9

    Wartość kontrolna jest zdefiniowana następująco:

    controlValue ::=pgpOpt [newPgp [newPgpAut]]
    pgpOpt ::= *NOCHG / *CHGPGP
    newPgp ::= *NONE / nazwa-profilu-użytkownika
    newPgpAut ::= *OLDPGP / *PRIVATE / *ALL / *CHANGE / *USE / *EXCLUDE

    Wartość pgpOpt określa rodzaj działania w przypadku, gdy usuwany profil jest grupą pierwotną dla innych obiektów. Jeśli określono *CHGPGP, trzeba także określić wartość newPgp. Wartość newPgp określa nazwę profilu pierwotnej grupy lub *NONE. Jeśli określony jest nowy profil pierwotnej grupy, można także określić wartość newPgpAut. Wartość newPgpAut określa uprawnienia do obiektów, które są nadawane nowej grupie pierwotnej.

  Przykłady wartości kontrolnych są następujące:

  - *NOCHG: określa, że profil nie może być usunięty jeśli jest pierwotną grupą dla jakichkolwiek obiektów
  - *CHGPGP *NONE: określa usuwanie pierwotnej grupy obiektów
  - *CHGPGP SMITH *USE: określa zmianę grupy pierwotnej na profil użytkownika SMITH i przydziela uprawnienia *USE grupie pierwotnej

  Jeśli żaden z tych elementów kontrolnych nie zostanie określony podczas usuwania, używane są aktualne wartości domyślne dla komendy QSYS/DLTUSRPRF.

ModRDN

Nie można zmienić nazwy profili użytkowników rzutowanych, ponieważ opcja ta nie jest obsługiwana przez system operacyjny.

Imoprtowanie i eksportowanie list API

Funkcje API QgldImportLdif i QgldExportLdif nie obsługują opcji importowania lub eksportowania danych wewnątrz postprocesora rzutowanego systemu.

Administrator i nazwa wyróżniająca łącząca z repliką

Jako skonfigurowanego administratora lub nazwę wyróżniającą łączącą z repliką można określić profil użytkownika rzutowanego. Użyte zostanie wtedy hasło profilu użytkownika. Profile użytkowników rzutowanych mogą stać się także administratorami LDAP, jeśli mają uprawnienia do identyfikatora funkcji Directory Server Administrator (QIBM_DIRSRV_ADMIN). Dostęp administratora może być nadany wielu profilom użytkowników.

Więcej informacji znajduje się w sekcji “Praca z dostępem administratora dla upoważnionych użytkowników” na stronie 31.

Schematy użytkowników rzutowanych systemu OS/400

Klasy obiektów oraz atrybuty z postprocesora rzutowanego można znaleźć w schemacie serwera rozległego. Nazwy atrybutów LDAP mają format os400–*nnn*, gdzie *nnn* jest typowym słowem kluczowym atrybutu (takim jak CRTUSRPRF lub CHGUSRPRF) komend profilu użytkownika. Więcej informacji znajduje się w sekcji “Drzewo informacji katalogu rzutowanych użytkowników systemu OS/400” na stronie 43.

Obsługa kronikowania w Usługach katalogowych i systemie OS/400

Do przechowywania danych katalogów Usługi katalogowe używają baz danych systemu OS/400. Do przechowywania pozycji katalogów w bazach danych Usługi katalogowe używają kontroli transakcji. Wymaga to obsługi kronikowania OS/400.

Gdy serwer lub narzędzie LDIF do importu jest uruchamiane po raz pierwszy, są tworzone następujące elementy:

- kronika,
- dziennik,
- potrzebne na początku tabele baz danych.

Kronika QSQJRN jest wbudowana w bibliotekę baz danych podaną w konfiguracji. Dziennik QSQJRN0001 jest początkowo tworzony w tej bibliotece.

Środowisko, wielkość i struktura katalogu lub strategia składowania i odtwarzania mogą różnić się nieco od domyślnych, np. sposobem zarządzania tymi obiektami lub różnymi wielkościami progowymi. Jeśli jest to konieczne, można zmienić parametry komend kronikowania. Kronikowanie LDAP jest domyślnie skonfigurowane na usuwanie poprzednich dzienników. Jeśli został skonfigurowany protokół zmian i wymagane jest zachowanie poprzednich dzienników, należy wykonać następującą komendę z poziomu wiersza komend systemu OS/400:

```
JRN(QUSRDIRCL/QSQJRN) DLTRCV(*NO)
```

Jeśli został skonfigurowany protokół zmian, za pomocą następującej komendy można usunąć jego dzienniki:

```
CHGJRN JRN(QUSRDIRCL/QSQJRN)  DLTRCV(*YES)
```

Więcej informacji dotyczących komend kronikowania można znaleźć w sekcji OS/400 commands w artykule Programming w Centrum informacyjnym iSeries.

Rozdział 6. Narzędzia wiersza komend LDAP

Usługi katalogowe zawierają pięć narzędzi, które umożliwiają wykonywanie operacji na serwerze katalogów LDAP ze środowiska komend Qshell w systemie OS/400. Narzędzia te używają funkcji API protokołu LDAP. Można ich używać z wiersza komend qsh lub wywoływać je z programów. Mogą one także być pomocne jako przykłady programów. Podczas instalacji klienta LDAP dla Windows, wchodzącego w skład Usług katalogowych, instalowany jest także kod, który jest bardzo podobny do kodu źródłowego programów użytkowych powłoki.

Poniżej wymieniono wspomniane narzędzia:
- "Narzędzia ldapmodify i ldapadd" dodają i modyfikują pozycje katalogu LDAP.
- "Narzędzie ldapdelete" na stronie 54 usuwa pozycje z katalogu LDAP.
- "Narzędzie ldapsearch" na stronie 56 przeszukuje pozycje katalogu LDAP.
- "Narzędzie ldapmodrdn" na stronie 61 zmienia względną nazwę wyróżniającą pozycji katalogu LDAP.

Sekcja "Uwagi na temat używania SSL z narzędziami wiersza komend LDAP" na stronie 63 zawiera informacje na temat używania SSL przy pomocy narzędzi wiersza komend.

Narzędzia ldapmodify i ldapadd

Narzędzie ldapmodify umożliwia zmianę lub dodawanie pozycji do serwera katalogów LDAP z powłoki komend QSH w systemie. Korzysta ono z następujących interfejsów API (Application program interfaces) ldap_modify, ldap_add oraz ldap_delete. Narzędzie ldapadd działa prawie tak samo, jak narzędzie ldapmodify, z tym wyjątkiem, że flaga -a jest włączana automatycznie.

Format:

ldapmodify [-a] [-V] [-b] [-c] [-r] [-M] [-n] [-v] [-F] [-R] [-C *zestaw_znaków***] [-d** *poziom_debugowania***] [-D** *naz_wyr_powiązania***] [-w** *hasło* **] [-m** *mechanizm***] [-O***liczba_przeskoków***] [-h** *host_ldap***] [-p** *port_ldap***] [-f** *zbiór***] [-Z] [-K** *zbiór_kluczy***] [-P** *hasło_zbioru_kluczy***] [-N** *nazwa_certyfikatu***]**

ldapadd [-V] [-b] [-c] [-r] [-M] [-n] [-v] [-F] [-R] [-C *zestaw_znaków***] [-d** *poziom_debugowania***] [-D** *naz_wyr_powiązania* **] [-w** *hasło***] [-m** *mechanizm***] [-O***liczba_przeskoków***] [-h** *host_ldap***] [-p** *port_ldap***] [-f** *zbiór***] [-Z] [-K** *zbiór_kluczy***] [-P** *hasło_zbioru_kluczy***] [-N** *nazwa_certyfikatu***]**

Uwaga: Jeśli dane wejściowe nie zostaną pobrane z pliku *zbiór* przy pomocy opcji **-f**, narzędzie będzie czekać na podanie ich poprzez standardowe wejście. Aby przerwać oczekiwanie, naciśnij klawisz SysReq, a następnie wybierz 2. Zakończ poprzednie żądanie.

Diagnostyka:

Jeśli nie wystąpiły żadne błędy, statusem wyjścia jest 0. Wystąpienie błędu powoduje powstanie niezerowego statusu wyjścia, a do standardowego wyjścia dla błędów zapisywany jest komunikat diagnostyczny.

Kliknij tutaj, aby wyświetlić przykład użycia tego narzędzia.

Parametry:

-V	Określa, z której wersji LDAP korzysta narzędzie, aby połączyć się z serwerem LDAP. Domyślnie używane jest połączenie LDAP V3. Aby jawnie wybrać LDAP V3, należy podać wartość ″-V 3″. Aby uruchomić jako aplikację LDAP V2, należy podać ″-V 2″.

-a	Parametr ten używany jest tylko przez narzędzie ldapmodify. Wskazuje, że narzędzie domyślnie doda pozycje, a nie zmodyfikuje je. Użycie tego parametru jest równoważne użyciu narzędzia ldapadd.
-b	Przyjmuje, że wszystkie wartości zaczynające się od `/' są wartościami binarnymi i że rzeczywista wartość znajduje się w pliku, którego ścieżka została podana w miejscu, w którym normalnie pojawia się wartość.
-c	Tryb działania ciągłego. Błędy są zgłaszane, ale narzędzia ldapmodify lub ldapadd nadal działają i wykonują operacje zmiany lub dodawania. Domyślnie po wystąpieniu błędu następuje przerwanie pracy.
-r	Wszystkie wartości zastępuje wartościami domyślnymi.
-M	Zarządza obiektami odwołania tak jak pozycjami regularnymi.
-n	Pokazuje, co byłoby wykonane, ale nie aktualizuje pozycji. Użyteczny podczas debuggowania w połączeniu z parametrem -v.
-v	Używa trybu szczegółowego z wieloma komunikatami diagnostycznymi zapisanymi w standardowym wyjściu.
-F	Wymusza zastosowanie wszystkich zmian bez względu na zawartość wierszy wejściowych zaczynających się od replica: (domyślnie wiersze replica: porównywane są z hostem serwera LDAP i używanym portem w celu określenia, czy powinien zostać zastosowany rekord protokołu replikacji).
-R	Określa, że odwołania nie mają następować automatycznie.
-C *zestaw_znaków*	Określa, że łańcuchy dostarczone do narzędzia jako wejściowe są reprezentowane w lokalnym zestawie znaków (*zestaw_znaków*) i muszą być konwertowane do formatu UTF-8. Opcji zestaw_znaków **-C** używa się, gdy wejściowa strona kodowa łańcucha znaków różni się od wartości strony kodowej zadania. Aby zobaczyć dozwolone wartości *zestaw_znaków*, patrz dokumentacja funkcji API ldap_set_iconv_local_charset().
-d *poziom_debugowania*	Ustawia poziom debugowania na *poziom_debugowania*.
-D *naz_wyr_powiązania*	Używa *naz_wyr_powiązania* do powiązania z katalogiem LDAP. *naz_wyr_powiązania* powinien być nazwą DN w postaci łańcucha znaków.
-w *hasło*	Używa *hasło* jako hasła podczas uwierzytelniania.
-m *mechanizm*	Parametr *mechanizm* określa mechanizm SASL używany przez klienta do połączenia z serwerem. Zostanie użyta funkcja API ldap_sasl_bind_s(). Dostępne mechanizmy to między innymi CRAM-MD5 (szyfrowane hasło), EXTERNAL (używane z SSL) i GSSAPI (Kerberos). Parametr **-m** jest ignorowany przez komendę, jeśli jest ustawiony parametr **-V 2**. Jeśli nie zostanie określony parametr **-m**, używane jest proste uwierzytelnianie.
-O*liczba_przeskoków*	Parametr *liczba_przeskoków* określa maksymalną liczbę przeskoków, którą wykona biblioteka klienta w czasie gdy przegląda odwołania. Domyślna liczba przeskoków jest równa 10.
-h *host_ldap*	Określa alternatywny host, na którym działa serwer LDAP.
-p *port_ldap*	Określa alternatywny port TCP, na którym serwer LDAP prowadzi nasłuch. Domyślnym portem LDAP jest 389. Jeśli go nie podano i podano parametr **-Z**, używany jest domyślny port 636 SSL LDAP.
-f *zbiór*	Odczytuje informacje dotyczące modyfikacji pozycji z pliku LDIF zamiast ze standardowego wejścia. Jeśli plik LDIF nie jest określony, do podania zmodyfikowanych rekordów w formacie LDIF trzeba użyć standardowego wejścia.
-Z	Używa chronionego połączenia SSL w komunikacji z serwerem LDAP. Opcja **-Z** jest obsługiwana tylko przez wersje tego narzędzia, które obsługują SSL.

-K *zbiór_kluczy*	Określa nazwę zbioru bazy danych kluczy SSL. Jeśli zbiór bazy danych kluczy nie znajduje się w bieżącym katalogu, podaj pełną nazwę zbioru bazy danych kluczy. Jeśli narzędzie nie może znaleźć bazy danych kluczy, użyje zestawu ″hard-codced″ domyślnie uwierzytelnionych certyfikatem administratorów. Zbiór bazy danych kluczy zwykle zawiera jeden lub więcej certyfikatów ośrodków certyfikacji (CA) respektowanych przez klienta. Tego typu certyfikaty X.509 zwane są także użytkownikami zaufanymi. Parametr ten odblokowuje przełącznik **-Z**.
-P *hasło_zbioru_kluczy*	Określa hasło bazy danych kluczy. Hasło to jest wymagane przy dostępie do szyfrowanych informacji w zbiorach bazy danych kluczy (włącznie z prywatnym kluczem). Jeśli hasło zeskładowanego zbioru haseł jest związane ze zbiorem bazy danych kluczy, hasło jest otrzymywane z zeskładowanego zbioru i ten parametr nie jest wymagany. Parametr jest ignorowany, gdy są podane parametry **-Z** i/lub **-K**.
-N *nazwa_certyfikatu*	Określa poziom związany z certyfikatem klienta w zbiorze bazy danych kluczy. Jeśli serwer LDAP jest skonfigurowany tylko do uwierzytelniania serwera, certyfikat klienta nie jest wymagany. Jeśli serwer LDAP jest skonfigurowany do uwierzytelniania klienta i serwera, wymagany jest certyfikat klienta. Parametr *nazwa_certyfikatu* nie jest wymagany, jeśli pewna para certyfikat/klucz prywatny została określona jako domyślna. Podobnie parametr *nazwa_certyfikatu* nie jest wymagany, jeśli w wyznaczonej bazie danych kluczy znajduje się pojedyncza para certyfikat/klucz prywatny. Parametr jest ignorowany, gdy nie zostanie podany parametr **-Z** ani parametr **-K**.

Alternatywny format wejścia:

Narzędzie ldapmodify obsługuje alternatywny format wejścia w celu zapewnienia zgodności ze starszymi wersjami narzędzia. Format ten składa się z jednej lub kilku pozycji, które oddzielone są od siebie pustymi wierszami. Każda pozycja ma następujący format:

```
Distinguished Name (DN)
atrybut=wartość
[atrybut=wartość ...]
```

gdzie *atrybut* jest nazwą atrybutu, a *wartość* jest wartością. Domyślnie wartości są dodawane. Jeśli zostanie podana flaga wiersza komend **-r**, domyślnym ustawieniem jest zastępowanie istniejących wartości nowymi. Dany atrybut może występować więcej niż raz (na przykład można dodać więcej niż jedną wartość atrybutu). W celu kontynuacji wartości w kilku wierszach, można użyć odwrotnego ukośnika (\) jako pierwszego znaku w wierszach kontynuacji. Aby usunąć wartość, należy wartość *atrybut* poprzedzić myślnikiem (-). Aby usunąć cały atrybut, należy pominąć znak równości (=) i wartość. Parametr *atrybut* powinien być poprzedzony znakiem plus (+), aby dodać wartość w przypadku flagi **-r**.

Przykłady: ldapmodify i ldapadd

Przykład 1:

Przyjmijmy, że plik **/tmp/entrymods** istnieje i ma następującą zawartość:

```
dn: cn=Modify Me, o=University of Higher Learning, c=US
changetype: modify
replace: mail
mail: modme@student.of.life.edu
-
add: title
title: Grand Poobah
-
add: jpegPhoto
jpegPhoto:< file:///tmp/modme.jpeg
-
delete: description
-
```

Komenda ldapmodify -b -r -f /tmp/entrymods będzie działała w następujący sposób:

- zastąpi zawartość atrybutu poczty (mail) pozycji ″Modify Me″ wartością modme@student.of.life.edu,
- doda tytuł (title) Grand Poobah,
- doda zawartość pliku /**tmp**/**modme.jpeg** jako jpegPhoto,
- całkowicie usunie atrybut description.

Te same zmiany można wykonać w starszym formacie wejściowym ldapmodify:

```
cn=Modify Me, o=University of Higher Learning, c=US
mail=modme@student.of.life.edu
+title=Grand Poobah
+jpegPhoto=/tmp/modme.jpeg
-description
```

Komendą używającą starego formatu będzie:

```
ldapmodify -b -r -f /tmp/entrymods
```

Przykład 2:

Przyjmijmy, że plik /**tmp**/**newentry** istnieje i ma następującą zawartość:

```
dn: cn=John Doe, o=University of Higher Learning, c=US
objectClass: person
cn: John Doe
cn: Johnny
sn: Doe
title: Manager
mail: johndoe@student.of.life.edu
uid: jdoe
```

Komenda ldapadd -f /tmp/entrymods doda nową pozycję John Doe, używając wartości z pliku /tmp/newentry.

Przykład 3:

Przyjmijmy, że plik /**tmp**/**newentry** istnieje i ma następującą zawartość:

```
dn: cn=John Doe, o=University of Higher Learning, c=US
changetype: delete
```

Komenda ldapmodify -f /tmp/entrymods usunie pozycję John Doe.

Narzędzie ldapdelete

Narzędzie ldapdelete pozwala usunąć jedną lub więcej pozycji z serwera katalogów LDAP. Działa za pomocą powłoki komend QSH na OS/400. Używa funkcji API ldap_delete.

Format:

ldapdelete [-V] [-M] [-n] [-v] [-c] [-R] [-C *zestaw_znaków***] [-d** *poziom_debugowania***] [-f** *zbiór***] [-D** *naz_wyr_powiązania***] [-w** *hasło***] [-m** *mechanizm***] [-O** *liczba_przeskoków***] [-h** *host_ldap***] [-p** *port_ldap***] [-Z] [-K** *zbiór_kluczy***] [-P** *hasło_zbioru_kluczy***] [-N** *nazwa_certyfikatu***] [***dn***]...**

Uwaga: Jeśli nie są udostępnione argumenty *dn*, komenda ldapdelete będzie oczekiwać na odczyt listy nazw DN ze standardowego wejścia. Aby przerwać oczekiwanie, naciśnij klawisz SysReq, a następnie wybierz 2. Zakończ poprzednie żądanie.

Diagnostyka:

Jeśli nie wystąpiły żadne błędy, statusem wyjścia jest 0. Wystąpienie błędu powoduje powstanie niezerowego statusu wyjścia, a do standardowego wyjścia dla błędów zapisywany jest komunikat diagnostyczny.

Kliknij tutaj, aby wyświetlić przykłady użycia narzędzia ldapdelete.

Parametry:

-V	Określa, z której wersji LDAP korzysta narzędzie, aby połączyć się z serwerem LDAP. Domyślnie używane jest połączenie LDAP V3. Aby jawnie wybrać LDAP V3, należy podać wartość ″-V 3″. Aby uruchomić jako aplikację LDAP V2, należy podać ″-V 2″.
-M	Zarządza obiektami odwołania tak jak pozycjami regularnymi.
-n	Pokazuje, co byłoby wykonane, ale nie usunie pozycji. Użyteczny podczas debugowania w połączeniu z parametrem **-v**.
-v	Używa trybu szczegółowego z wieloma komunikatami diagnostycznymi zapisanymi w standardowym wyjściu.
-c	Tryb działania ciągłego. Błędy są zgłaszane, ale ldapdelete będzie kontynuować operacje usuwania. Domyślnie po wystąpieniu błędu następuje przerwanie pracy.
-R	Określa, że odwołania nie mają następować automatycznie.
-C *zestaw_znaków*	Określa, że nazwy wyróżniające (DN), dostarczone do narzędzia ldapdelete jako wejściowe, są reprezentowane w lokalnym zestawie znaków (*zestaw_znaków*). Użycie parametru **-C** *zestaw_znaków* spowoduje zastąpienie domyślnego, w którym łańcuchy muszą być dostarczone w formacie UTF-8. Opcji zestaw_znaków **-C** używa się, gdy wejściowa strona kodowa łańcucha znaków różni się od wartości strony kodowej zadania. Aby zobaczyć dozwolone wartości *zestaw_znaków*, patrz dokumentacja funkcji API ldap_set_iconv_local_charset().
-d *poziom_debugowania*	Ustawia poziom debugowania na *poziom_debugowania*.
-f *zbiór*	Odczytuje serie wierszy ze *zbioru*, wykonując jedno usuwanie LDAP dla każdego wiersza w zbiorze. Każdy wiersz powinien zawierać pojedynczą nazwę wyróżniającą.
-D *naz_wyr_powiązania*	Używa *naz_wyr_powiązania* do powiązania z katalogiem LDAP. *naz_wyr_powiązania* powinien być nazwą DN w postaci łańcucha znaków.
-w *hasło*	Używa *hasło* jako hasła podczas uwierzytelniania.
-m *mechanizm*	Parametr *mechanizm* określa mechanizm SASL, używany do połączenia z serwerem. Zostanie użyta funkcja API ldap_sasl_bind_s(). Dostępne mechanizmy to CRAM-MD5 (szyfrowane hasło), EXTERNAL (używane z SSL) i GSSAPI (Kerberos). Parametr -m jest ignorowany, jeśli jest ustawiony parametr -V 2. Jeśli parametr **-m** nie jest określony, używa się prostego uwierzytelniania.
-O *liczba_przeskoków*	Parametr *liczba_przeskoków* określa maksymalną liczbę przeskoków, którą wykona biblioteka klienta podczas przeglądania odwołań. Domyślna liczba przeskoków jest równa 10.
-h *host_ldap*	Określa alternatywny host, na którym działa serwer LDAP.
-p *port_ldap*	Określa alternatywny port TCP, na którym serwer LDAP prowadzi nasłuch. Domyślnym portem LDAP jest 389. Jeśli go nie podano i podano parametr **-Z**, używany jest domyślny port 636 SSL LDAP.
-Z	Używa chronionego połączenia SSL w komunikacji z serwerem LDAP. Opcja **-Z** jest obsługiwana tylko przez wersje tego narzędzia, które obsługują SSL.
-K *zbiór_kluczy*	Określa nazwę zbioru bazy danych kluczy SSL. Jeśli zbiór bazy danych kluczy nie znajduje się w bieżącym katalogu, podaj pełną nazwę zbioru bazy danych kluczy. Jeśli narzędzie nie może znaleźć bazy danych kluczy, użyje zestawu ″hard-coded″ domyślnie uwierzytelnionych certyfikatem administratorów. Zbiór bazy danych kluczy zwykle zawiera jeden lub więcej certyfikatów ośrodków certyfikacji (CA) respektowanych przez klienta. Tego typu certyfikaty X.509 zwane są także użytkownikami zaufanymi. Parametr ten odblokowuje przełącznik **-Z**.

-P *hasło_zbioru_kluczy*	Określa hasło bazy danych kluczy. Hasło to jest wymagane przy dostępie do szyfrowanych informacji w zbiorach bazy danych kluczy (włącznie z prywatnym kluczem). Jeśli hasło zeskładowanego zbioru haseł jest związane ze zbiorem bazy danych kluczy, hasło jest otrzymywane z zeskładowanego zbioru i ten parametr nie jest wymagany. Parametr jest ignorowany, gdy są podane parametry **-Z** i/lub **-K**.
-N *nazwa_certyfikatu*	Określa poziom związany z certyfikatem klienta w zbiorze bazy danych kluczy. Jeśli serwer LDAP jest skonfigurowany tylko do uwierzytelniania serwera, certyfikat klienta nie jest wymagany. Jeśli serwer LDAP jest skonfigurowany do uwierzytelniania klienta i serwera, wymagany jest certyfikat klienta. Parametr *nazwa_certyfikatu* nie jest wymagany, jeśli pewna para certyfikat/klucz prywatny została określona jako domyślna. Podobnie parametr *nazwa_certyfikatu* nie jest wymagany, jeśli w wyznaczonej bazie danych kluczy znajduje się pojedyncza para certyfikat/klucz prywatny. Parametr jest ignorowany, gdy nie zostanie podany parametr **-Z** ani parametr **-K**.
dn	Określa jeden lub więcej argumentów *dn*. Każdy parametr *dn* powinien być nazwą DN reprezentowaną przez łańcuch znaków.

Przykład: ldapdelete

Poniższa komenda będzie próbowała usunąć pozycję oznaczoną commonName Delete Me bezpośrednio pod pozycją organizacji University of Life:

```
ldapdelete cn=Delete Me, o=University of Life, c=US
```

Może okazać się konieczne podanie parametrów *naz_wyr_powiązania* i *hasło* (patrz opcje **-D** i **-w**).

Narzędzie ldapsearch

Narzędzie ldapsearch umożliwia wyszukiwanie pozycji na serwerze katalogów LDAP za pomocą powłoki komend QSH na OS/400. Używa funkcji API ldap_search.

Wyszukiwanie używa filtra zgodnego z reprezentacją łańcuchów dla filtrów LDAP. Więcej informacji na temat filtrów wyszukiwania LDAP znajduje się w sekcji na temat funkcji API ldap_search w OS/400 Directory Services w artykule Programowanie w Centrum informacyjnym iSeries.

Jeśli narzędzie ldapsearch odnajdzie jedną lub kilka pozycji, pobiera atrybuty określone przez *atrybuty* i drukuje pozycje i wartości do standardowego wyjścia. Jeśli lista atrybutów nie zostanie wyświetlona, narzędzie zwraca wszystkie atrybuty.

Format:

ldapsearch [-V] [-n] [-v] [-t] [-A] [-B] [-L] [-M] [-R] [-C *zestaw_znaków***] [-d** *poziom_debugowania***] [-F** *separator***] [-f** *zbiór***] [-D** *naz_wyr_powiązania***] [-w** *hasło_powiązania***] [-m** *mechanizm***] [-O** *liczba_przeskoków***] [-h** *host_ldap***] [-p** *port_ldap***] [-Z] [-K** *zbiór_kluczy***] [-P** *hasło_zbioru_kluczy***] [-N** *nazwa_certyfikatu***] [-b** *baza_wyszukiwania***] [-s** *zasięg* **] [-a** *podstawianie_aliasów***] [-l** *limit_czasu***] [-z** *limit_wielkości***]** *filtr* **[***atrybuty...***]**

Diagnostyka:

Jeśli nie wystąpiły żadne błędy, statusem wyjścia jest 0. Wystąpienie błędu powoduje powstanie niezerowego statusu wyjścia, a do standardowego wyjścia dla błędów zapisywany jest komunikat diagnostyczny.

Format wyjściowy:

Jeśli ldapsearch odnajdzie jedną lub kilka pozycji, zapisuje każdą pozycję do standardowego wyjścia w formie:

```
Distinguished Name (DN)
nazwa_atrybutu=wartość
nazwa_atrybutu=wartość
nazwa_atrybutu=wartość
...
```

Pozycje oddzielane są od siebie pojedynczym pustym wierszem. Jeśli określono znak separatora poprzez podanie opcji **-F**, będzie on wyświetlany zamiast znaku równości (=). Jeśli używana jest opcja **-t**, rzeczywista wartość zastępowana jest przez nazwę pliku tymczasowego. Jeśli podano opcję **-A**, zapisywana jest tylko część nazwa_atrybutu.

Kliknij tutaj, aby wyświetlić przykłady używania narzędzia ldapsearch.

Parametry:

-V	Określa, z której wersji LDAP korzysta narzędzie, aby połączyć się z serwerem LDAP. Domyślnie używane jest połączenie LDAP V3. Aby jawnie wybrać LDAP V3, należy podać wartość ″-V 3″. Aby uruchomić jako aplikację LDAP V2, należy podać ″-V 2″.
-n	Pokazuje, co byłoby wykonane, ale nie wykonuje żadnej operacji wyszukiwania. Użyteczny podczas debugowania w połączeniu z parametrem **-v**.
-v	Używa trybu szczegółowego z wieloma komunikatami diagnostycznymi zapisanymi w standardowym wyjściu.
-t	Zapisuje pobrane wartości do zestawu plików tymczasowych. Jest to użyteczne podczas pracy z wartościami binarnymi, takimi jak jpegPhoto lub danymi dźwiękowymi.
-A	Pobiera tylko atrybuty (nie wartości). Jest to użyteczne do sprawdzania, czy pozycja zawiera ten atrybut, gdy nie jest potrzebna konkretna wartość.
-B	Wyświetla wartości binarne. Jest to użyteczne w przypadku pracy z wartościami, które występują w innych zestawach znaków, takich jak ISO-8859.1. Opcja ta jest implikowana przez parametr **-L**
-L	Wyświetla wyniki wyszukiwania w formacie LDIF. Opcja ta włącza także opcję **-B** i powoduje ignorowanie opcji **-F**.
-M	Zarządza obiektami odwołania tak jak pozycjami regularnymi.
-R	Określa, że odwołania nie mają następować automatycznie.
-C *zestaw_znaków*	Określa, że łańcuchy znaków dostarczone do narzędzia ldapsearch jako wejściowe są reprezentowane w lokalnym zestawie znaków (*zestaw_znaków*). Łańcuch wejściowy zawiera filtr, nawiązanie do nazwy DN i podstawową nazwę DN. Podobnie, podczas wyświetlania danych narzędzie ldapsearch konwertuje otrzymane z serwera LDAP dane do określonych znaków. Opcji zestaw_znaków **-C** używa się, gdy wejściowa strona kodowa łańcucha znaków różni się od wartości strony kodowej zadania. Aby zobaczyć dozwolone wartości *zestaw_znaków*, patrz dokumentacja funkcji API ldap_set_iconv_local_charset(). Również jeśli obie opcje: -C i -L są określone, przyjmuje się, że dane wejściowe są zestawem określonych znaków, ale dane wyjściowe narzędzia ldapsearch są zawsze zabezpieczone w reprezentacji UTF-8 lub w podstawowej reprezentacji 64-kodowej danych, gdy wykryto znaki niemożliwe do wydrukowania. Sytuacja ta ma miejsce odkąd standardowe pliki LDIF zawierają reprezentacje danych łańcuchowych tylko w formacie UTF-8 (lub opartym na 64-kodowym formacie UTF-8).
-d *poziom_debugowania*	Ustawia poziom debugowania na *poziom_debugowania*.
-F *separator*	Używa *separator* jako pola separującego pomiędzy nazwami i wartościami atrybutów. Separatorem domyślnym jest '=', chyba że została określona flaga **-L**, wówczas opcja ta jest ignorowana.
-f *zbiór*	Odczytuje wiersz z pliku wykonując operację wyszukiwania LDAP dla każdego wiersza. Każdy wiersz powinien zawierać pojedynczą nazwę wyróżniającą.
-D *naz_wyr_powiązania*	Używa *naz_wyr_powiązania* do powiązania z katalogiem LDAP. *naz_wyr_powiązania* powinien być nazwą DN w postaci łańcucha znaków.

-w *hasło*	Używa *hasło* jako hasła podczas uwierzytelniania.
-m *mechanizm*	Parametr *mechanizm* określa mechanizm SASL używany do połączenia z serwerem. Zostanie użyta funkcja API ldap_sasl_bind_s(). Dostępne mechanizmy to CRAM-MD5 (szyfrowane hasło), EXTERNAL (używane z SSL) i GSSAPI (Kerberos). Parametr **-m** jest ignorowany, jeśli parametr **-V** zostanie ustawiony na 2. Jeśli parametr **-m** nie jest określony, używa się prostego uwierzytelniania.
-O *liczba_przeskoków*	Parametr *liczba_przeskoków* określa maksymalną liczbę przeskoków, którą wykona biblioteka klienta podczas przeglądania odwołań. Domyślna liczba przeskoków jest równa 10.
-h *host_ldap*	Określa alternatywny host, na którym działa serwer LDAP.
-p *port_ldap*	Określa alternatywny port TCP, na którym serwer LDAP prowadzi nasłuch. Domyślnym portem LDAP jest 389. Jeśli go nie podano i podano parametr **-Z**, używany jest domyślny port 636 SSL LDAP.
-Z	Używa chronionego połączenia SSL w komunikacji z serwerem LDAP. Opcja **-Z** jest obsługiwana tylko przez wersje tego narzędzia, które obsługują SSL.
-K *zbiór_kluczy*	Określa nazwę zbioru bazy danych kluczy SSL. Jeśli zbiór bazy danych kluczy nie znajduje się w bieżącym katalogu, podaj pełną nazwę zbioru bazy danych kluczy. Jeśli narzędzie nie może znaleźć bazy danych kluczy, użyje zestawu ″hard-codced″ domyślnie uwierzytelnionych certyfikatem administratorów. Zbiór bazy danych kluczy zwykle zawiera jeden lub więcej certyfikatów ośrodków certyfikacji (CA) respektowanych przez klienta. Tego typu certyfikaty X.509 zwane są także użytkownikami zaufanymi. Parametr ten odblokowuje przełącznik **-Z**.
-P *hasło_zbioru_kluczy*	Określa hasło bazy danych kluczy. Hasło to jest wymagane przy dostępie do szyfrowanych informacji w zbiorach bazy danych kluczy (włącznie z prywatnym kluczem). Jeśli hasło zeskładowanego zbioru jest związane ze zbiorem bazy danych kluczy, hasło jest otrzymywane z zeskładowanego zbioru i ten parametr nie jest wymagany. Parametr jest ignorowany, gdy są podane parametry **-Z** i/lub **-K**.
-N *nazwa_certyfikatu*	Określa poziom związany z certyfikatem klienta w zbiorze bazy danych kluczy. Jeśli serwer LDAP jest skonfigurowany tylko do uwierzytelniania serwera, certyfikat klienta nie jest wymagany. Jeśli serwer LDAP jest skonfigurowany do uwierzytelniania klienta i serwera, wymagany jest certyfikat klienta. Parametr *nazwa_certyfikatu* nie jest wymagany, jeśli pewna para certyfikat/klucz prywatny została określona jako domyślna. Podobnie parametr *nazwa_certyfikatu* nie jest wymagany, jeśli w wyznaczonej bazie danych kluczy znajduje się pojedyncza para certyfikat/klucz prywatny. Parametr jest ignorowany, gdy nie zostanie podany parametr **-Z** ani parametr **-K**.
-b *baza_wyszukiwania*	Używa *baza_wyszukiwania* jako początkowego punktu wyszukiwania zamiast domyślnego. Jeśli parametr **-b** nie zostanie określony, narzędzie będzie sprawdzać, czy zmienna środowiskowa LDAP_BASEDN zawiera definicję *baza_wyszukiwania*.
-s *zasięg*	Określa zakres wyszukiwania. Parametrem *zasięg* powinno być base, one lub sub, aby określić, czy wyszukiwanie ma być podstawowe, jednopoziomowe lub w poddrzewie. Wartością domyślną jest sub.
-a *podstawianie_aliasów*	Określa, w jaki sposób są podstawiane aliasy. Parametr *podstawianie_aliasów* powinien mieć wartość never, always, search lub find, określającą odpowiednio, że aliasy mają być podstawiane: nigdy, zawsze, podczas przeszukiwania lub tylko podczas umiejscawiania obiektu podstawowego dla wyszukiwania. Wartością domyślną jest never.
-l *limit_czasu*	Czeka maksymalnie *limit_czasu* sekund na zakończenie wyszukiwania.
-z *limit_wielkości*	Ogranicza wyniki wyszukiwania do maksymalnie *limit_wielkości* pozycji. Umożliwia to określenie górnej granicy liczby pozycji zwracanych podczas operacji wyszukiwania.
filtr	Określa nazwę filtra używanego przez funkcję wyszukiwania (search).
atrybuty...	Określa atrybuty pobrane przez narzędzie, jeśli funkcja wyszukiwania (search) znajdzie jedną lub więcej pozycji. Jeśli nie zostaną podane żadne wartości dla *atrybuty*, narzędzie zwraca wszystkie atrybuty.

Przykład: ldapsearch

Przykład 1:

Komenda ldapsearch cn=john doe cn telephoneNumber wykonuje operację wyszukiwania w poddrzewie (używając domyślnej podstawy wyszukiwania) pozycji z nazwiskiem commonName o wartości john doe. Podczas operacji wyszukiwania wartości nazwiska (commonName) i numeru telefonu (telephoneNumber) są pobierane i przesyłane do standardowego wyjścia. Jeśli podczas wyszukiwania odnalezione zostaną dwie pozycje, dane wyjściowe będą podobne do przedstawionych poniżej:

```
cn=John E Doe, ou=College of Literature, Science, and the Arts,
ou=Students, ou=People, o=University of Higher Learning, c=US
cn=John Doe
cn=John Edward Doe
cn=John E Doe 1
cn=John E Doe
telephoneNumber=+1 313 555-5432

cn=John B Doe, ou=Information Technology Division,
ou=Faculty and Staff,
ou=People, o=University of Higher Learning, c=US
cn=John Doe
cn=John B Doe 1
cn=John B Doe
telephoneNumber=+1 313 555-1111
```

Przykład 2:

Komenda ldapsearch -t uid=jed jpegPhoto audio przeprowadza wyszukiwanie w poddrzewie za pomocą domyślnej podstawy wyszukiwania dla pozycji o ID użytkownika równym jed. Podczas operacji wyszukiwania pobierane są wartości jpegPhoto i dźwiękowe i zapisywane do plików tymczasowych. Jeśli podczas operacji wyszukiwania odnaleziona zostanie jedna wartość dla każdego żądanego atrybutu, dane wyjściowe są podobne do przedstawionych poniżej:

```
cn=John E Doe,
ou=Information Technology Division,
ou=Faculty and Staff,
ou=People, o=University of Higher Learning, c=US
audio=/tmp/ldapsearch-audio-a19924
jpegPhoto=/tmp/ldapsearch-jpegPhoto-a19924
```

Przykład 3:

Komenda ldapsearch -L -s one -b c=US o=university* o description przeprowadza jednopoziomową operację wyszukiwania na poziomie c=US. Ta operacja wyszukiwania szuka wszystkich instytucji, których nazwa (organizationName) zaczyna się od university. Wyniki wyszukiwania wyświetlane są w formacie LDIF. Komenda ta pobiera wartość atrybutu nazwy instytucji (organizationName) i wartości atrybutów (description) i drukuje je do standardowego wyjścia w przedstawiony poniżej sposób:

```
dn: o=University of Alaska Fairbanks, c=US
o: University of Alaska Fairbanks
description: Preparing Alaska for a brave new tomorrow
description: leaf node only

dn: o=University of Colorado at Boulder, c=US
o: University of Colorado at Boulder
description: No personnel information
description: Institution of education and research

dn: o=University of Colorado at Denver, c=US
o: University of Colorado at Denver
o: UCD
o: CU/Denver
o: CU-Denver
description: Institute for Higher Learning and Research
```

```
dn: o=University of Florida, c=US
o: University of Florida
o: UFl
description: Shaper of young minds
...
```

Przykład 4:

Jak to opisano w sekcji “Odwołania do katalogu LDAP” na stronie 39, katalogi LDAP Usług katalogowych mogą zawierać obiekty odwołań, które zawierają tylko:

- nazwę wyróżniającą (dn),
- klasę obiektu (objectClass),
- atrybut odwołania (ref).

Przykład ten przedstawia wyszukiwanie, w którym bierze udział obiekt odwołania.

Przyjmijmy, że System_A zawiera pozycję odwołania:

```
dn: cn=Barb Jensen, ou=Rochester, o=Big Company, c=US
ref: ldap://System_B:389/cn=Barb Jensen,
  ou=Rochester, o=Big Company, c=US
objectclass: referral
```

Wszystkie atrybuty powiązane z pozycją powinny znajdować się w Systemie_B.

System_B zawiera pozycję:

```
dn: cn=Barb Jensen, ou=Rochester, o=Big Company, c=US
cn: Barb Jensen
objectclass: organizationalPerson
sn: Jensen
telephonenumber: (800) 555 1212
```

Kiedy klient wysyła żądanie do Systemu_A i nie dodaje elementu sterującego manageDsaIT, wtedy serwer zwraca odwołanie. Na przykład przez użycie flagi -M narzędzia ldapsearch serwer LDAP w Systemie_A wysyła do klienta odpowiedź zawierającą adres URL:

```
ldap://System_B:389/cn=Barb Jensen,  ou=Rochester, o=Big Company, c=US
```

Klient używa tej informacji do wysłania żądania do Systemu_B. Jeśli pozycja w Systemie_A zawiera jakieś atrybuty oprócz dn, objectclass i ref, serwer ignoruje je.

Gdy klient odbierze z serwera odpowiedź na odwołanie, wysyła ponownie żądanie, tym razem do serwera, na który wskazuje zwrócony adres URL. Jeśli wyszukiwanie było przeprowadzone z jednopoziomowym zasięgiem, zgłoszenie odwołania używa podstawowego zasięgu. Wyniki tego wyszukiwania zależą od wartości podanej jako zakres wyszukiwania (**-b**).

Jeśli podano parametr -s sub, jak poniżej:

```
ldapsearch -h System_A -b ou=Rochester, o=Big Company, c=US -s sub sn=Jensen
```

operacja wyszukiwania zwraca wszystkie atrybuty dla wszystkich pozycji zawierających sn=Jensen, które znajdują się w lub poniżej ou=Rochester, o=Big Company, c=US zarówno w Systemie_A i Systemie_B. Klient otrzymuje odwołanie z Systemu_A i przeszukuje System_B, zwracając cn=Barb Jense,ou=Rochester,o=Big Company,c=US.

Jeśli podano parametr -s one, jak poniżej:

```
ldapsearch -h System_A -b ou=Rochester, o=Big Company, c=US-s one sn=Jensen
```

operacja wyszukiwania nie zwraca żadnych pozycji w żadnym z systemów. Zamiast tego serwer zwraca adres URL odwołania do klienta:

```
ldap://System_B:389/cn=Barb Jensen,
  ou=Rochester, o=Big Company, c=US??base
```

Klient z kolei wysyła żądanie:

```
 ldapsearch -h System_B -b cn=Barb Jensen, ou=Rochester, o=Big Company, c=US
     -s base sn=Jensen
```

Zwraca to pozycję cn=Barb Jensen,ou=Rochester,o=Big Company,c=US.

Narzędzie ldapmodrdn

Narzędzie ldapmodrdn umożliwia zmianę względnej nazwy wyróżniającej pozycji na serwerze katalogów LDAP. Jest ono używane z powłoki komend QSH na OS/400. Używa funkcji API ldap_modrdn.

Format:

ldapmodrdn [-V] [-r] [-M] [-n] [-v] [-c] [-R] [-C *zestaw_znaków***] [-d** *poziom_debugowania***] [-D** *naz_wyr_powiązania***] [-w** *hasło***] [-m** *mechanizm***] [-O** *liczba_przeskoków***] [-h** *host_ldap***] [-p** *port_ldap***] [-Z] [-K** *zbiór_kluczy***] [-P** *hasło_zbioru_kluczy***] [-N** *nazwa_certyfikatu***] [-f** *zbiór* **] [***nazwa-wyróżn_wzgl-nazwa-wyróżn***]**

Uwagi:

1. Jeśli podane zostaną argumenty wiersza komend *dn* i *rdn*, parametr *rdn* zastąpi względną nazwę wyróżniającą pozycji określonej przez nazwę DN, *dn*. W przeciwnym razie zawartość pliku (lub standardowego wejścia, jeśli nie zostanie podana flaga **-f**) powinna składać się z jednej lub kilku pozycji.

   ```
   Distinguished Name (DN)

   Relative Distinguished Name (RDN)
   ```

   Każda para DN/RDN oddzielona jest jednym lub kilkoma pustymi wierszami.
2. Jeśli nie dostarczono informacji wejściowych ze *zbioru* przez użycie opcji **-f** (lub z wiersza komend przez podanie pary *dn* i *rdn*), komenda ldapmodrdn będzie oczekiwać na odczytanie pozycji z wejścia standardowego. Aby przerwać oczekiwanie, naciśnij klawisz SysReq, a następnie wybierz 2. Zakończ poprzednie żądanie.

Diagnostyka:

Jeśli nie wystąpiły żadne błędy, statusem wyjścia jest 0. Wystąpienie błędu powoduje powstanie niezerowego statusu wyjścia, a do standardowego wyjścia dla błędów zapisywany jest komunikat diagnostyczny.

Kliknij tutaj, aby wyświetlić przykład użycia narzędzia ldapmodrdn.

Parametry:

-V	Określa, z której wersji LDAP korzysta narzędzie, aby połączyć się z serwerem LDAP. Domyślnie używane jest połączenie LDAP V3. Aby jawnie wybrać LDAP V3, należy podać wartość ″-V 3″. Aby uruchomić jako aplikację LDAP V2, należy podać ″-V 2″.
-r	Usuwa z pozycji stare wartości względnej nazwy wyróżniającej. Domyślnie stare wartości są zachowywane.
-M	Zarządza obiektami odwołania tak jak pozycjami regularnymi.
-n	Pokazuje, co zostałoby wykonane, ale nie zmienia pozycji. Użyteczny podczas debugowania w połączeniu z parametrem **-v**.

-v	Używa trybu szczegółowego z wieloma komunikatami diagnostycznymi zapisanymi w standardowym wyjściu.
-c	Tryb działania ciągłego. Błędy są zgłaszane, ale ldapmodrdn będzie kontynuować operacje zmian. Domyślnie po wystąpieniu błędu następuje zakończenie pracy.
-R	Określa, że odwołania nie mają następować automatycznie.
-C *zestaw_znaków*	Określa, że łańcuchy dostarczone do narzędzia jako wejściowe są reprezentowane w lokalnym zestawie znaków (*zestaw_znaków*) i muszą być konwertowane do formatu UTF-8. Opcji zestaw_znaków **-C** używa się, gdy wejściowa strona kodowa łańcucha znaków różni się od wartości strony kodowej zadania. Aby zobaczyć dozwolone wartości *zestaw_znaków*, patrz dokumentacja funkcji API ldap_set_iconv_local_charset().
-d *poziom_debugowania*	Ustawia poziom debugowania na *poziom_debugowania*.
-D *naz_wyr_powiązania*	Używa *naz_wyr_powiązania* do powiązania z katalogiem LDAP. *naz_wyr_powiązania* powinien być nazwą DN w postaci łańcucha znaków.
-w *hasło*	Używa *hasło* jako hasła podczas uwierzytelniania.
-m *mechanizm*	Parametr *mechanizm* określa mechanizm SASL, używany do połączenia z serwerem. Zostanie użyta funkcja API ldap_sasl_bind_s(). Dostępne mechanizmy to CRAM-MD5 (szyfrowane hasło), EXTERNAL (używane z SSL) i GSSAPI (Kerberos). Parametr -m jest ignorowany, jeśli jest ustawiony parametr -V 2. Jeśli parametr **-m** nie jest określony, używa się prostego uwierzytelniania.
-O *liczba_przeskoków*	Parametr *liczba_przeskoków* określa maksymalną liczbę przeskoków, którą wykona biblioteka klienta podczas przeglądania odwołań. Domyślna liczba przeskoków jest równa 10.
-h *host_ldap*	Określa alternatywny host, na którym działa serwer LDAP.
-p *port_ldap*	Określa alternatywny port TCP, na którym serwer LDAP prowadzi nasłuch. Domyślnym portem LDAP jest 389. Jeśli go nie podano i podano parametr **-Z**, używany jest domyślny port 636 SSL LDAP.
-Z	Używa chronionego połączenia SSL w komunikacji z serwerem LDAP. Opcja **-Z** jest obsługiwana tylko przez wersje tego narzędzia, które obsługują SSL.
-K *zbiór_kluczy*	Określa nazwę zbioru bazy danych kluczy SSL. Jeśli zbiór bazy danych kluczy nie znajduje się w bieżącym katalogu, podaj pełną nazwę zbioru bazy danych kluczy. Jeśli narzędzie nie może znaleźć bazy danych kluczy, użyje zestawu ″hard-coded″ domyślnie uwierzytelnionych certyfikatem administratorów. Zbiór bazy danych kluczy zwykle zawiera jeden lub więcej certyfikatów ośrodków certyfikacji (CA) respektowanych przez klienta. Tego typu certyfikaty X.509 zwane są także użytkownikami zaufanymi. Parametr ten odblokowuje przełącznik **-Z**.
-P *hasło_zbioru_kluczy*	Określa hasło bazy danych kluczy. Hasło to jest wymagane przy dostępie do szyfrowanych informacji w zbiorach bazy danych kluczy (włącznie z prywatnym kluczem). Jeśli hasło zeskładowanego zbioru haseł jest związane ze zbiorem bazy danych kluczy, hasło jest otrzymywane z zeskładowanego zbioru i ten parametr nie jest wymagany. Parametr jest ignorowany, gdy są podane parametry **-Z** i/lub **-K**.
-N *nazwa_certyfikatu*	Określa poziom związany z certyfikatem klienta w zbiorze bazy danych kluczy. Jeśli serwer LDAP jest skonfigurowany tylko do uwierzytelniania serwera, certyfikat klienta nie jest wymagany. Jeśli serwer LDAP jest skonfigurowany do uwierzytelniania klienta i serwera, wymagany jest certyfikat klienta. Parametr *nazwa_certyfikatu* nie jest wymagany, jeśli pewna para certyfikat/klucz prywatny została określona jako domyślna. Podobnie parametr *nazwa_certyfikatu* nie jest wymagany, jeśli w wyznaczonej bazie danych kluczy znajduje się pojedyncza para certyfikat/klucz prywatny. Parametr jest ignorowany, gdy nie zostanie podany parametr **-Z** ani parametr **-K**.
-f *zbiór*	Odczytuje dane na temat modyfikacji pozycji z pliku LDIF zamiast ze standardowego wejścia lub z wiersza komend (parametr *dn* i nowa wartość *rdn*). Standardowe wejście można także uzupełnić z pliku (< zbiór).
nazwa-wyróżn_wzgl-nazwa-wyróżn	Określa wyróżniającą nazwę pozycji, która ma być zmieniona, oraz nową względną nazwę wyróżniającą pozycji.

Przykład: ldapmodrdn

Przyjmijmy, że utworzony został plik tekstowy /**tmp**/**entrymods** i że ma następującą zawartość:

```
cn=Modify Me, o=University of Life, c=US
cn=The New Me
```

Poniższa komenda:

```
ldapmodrdn -r -f /tmp/entrymods
```

spowoduje zmianę względnej nazwy wyróżniającej pozycji Modify Me z Modify Me na The New Me. Poprzednia wartość cn, Modify Me, zostanie usunięta.

Uwagi na temat używania SSL z narzędziami wiersza komend LDAP

Aby użyć opcji SSL (Secure Sockets Layer) w narzędziach wiersza komend, należy mieć zainstalowany jeden z produktów Cryptographic Access Provider Products (5722-ACx).

Sekcja “Używanie ochrony SSL (Secure Sockets Layer) i TLS (Translation Layer Security) na serwerze katalogów LDAP” na stronie 41 omawia używanie SSL z Usługami katalogowymi serwera LDAP. Informacje te obejmują zarządzanie i tworzenie ośrodków certyfikacji dla programu DCM.

Niektóre serwery LDAP dostępne dla klienta używają wyłącznie uwierzytelniania serwera. W przypadku tych serwerów należy tylko zdefiniować jeden lub kilka certyfikatów zaufanych użytkowników w bazie certyfikatów. W przypadku uwierzytelniania serwera klient może być pewny, że docelowy serwer LDAP otrzyma certyfikat z jednego z zaufanych ośrodków certyfikacji (CA). Oprócz tego wszystkie transakcje LDAP, które mają miejsce poprzez połączenie SSL z serwerem, są szyfrowane. Dotyczy to funkcji uwierzytelniania LDAP, dostarczanych w funkcjach API, które są używane do nawiązania połączenia z serwerem katalogów. Na przykład jeśli serwer LDAP używa certyfikatu Verisign o wysokim zaufaniu, należy:

1. Uzyskać z Verisign certyfikat CA.
2. Użyć DCM do zaimportowania go do bazy certyfikatów.
3. Użyć DCM do zaznaczenia go jako zaufanego.

Jeśli serwer LDAP używa prywatnych certyfikatów serwera, administrator serwera może dostarczyć kopię pliku żądanych certyfikatów serwera. Należy zaimportować plik żądanych certyfikatów do bazy certyfikatów i zaznaczyć go jako zaufany.

Jeśli w celu uzyskania dostępu do serwerów LDAP, które używają uwierzytelniania zarówno klientów, jak i serwerów, używane są narzędzia powłoki, należy:

- Zdefiniować w bazie certyfikatów jeden lub kilka certyfikatów zaufanych użytkowników. Daje to klientowi pewność, że jeden z zaufanych ośrodków certyfikacji wydał certyfikat dla docelowego serwera LDAP. Oprócz tego wszystkie transakcje LDAP, które mają miejsce poprzez połączenie SSL z serwerem, są szyfrowane. Znajdują się tu uwierzytelnienia LDAP, dostarczone w funkcjach API, które są używane do konsolidacji z serwerem katalogów.
- Utworzyć parę kluczy i zażądać certyfikatu klienta z CA. Po otrzymaniu podpisanego certyfikatu z CA, należy go przesłać do pliku kluczy w systemie kliencie.

Rozdział 7. Rozwiązywanie problemów z Usługami katalogowymi

Niestety, nawet wiarygodne serwery, takie jak serwer Usług katalogowych LDAP, czasami powodują problemy. Gdy serwer katalogów LDAP wykaże błąd, w określeniu jego przyczyny i sposobów rozwiązania mogą pomóc następujące informacje:

- “Podstawowa procedura rozwiązywania problemów z Usługami katalogowymi”
- “Najczęstsze błędy klienta LDAP” na stronie 68

Więcej informacji na temat najczęstszych problemów z Usługami katalogowymi zawiera strona główna Directory Services znajdująca się pod następującym adresem URL:

`http://www.iseries.ibm.com/ldap`

Podstawowa procedura rozwiązywania problemów z Usługami katalogowymi

Kody powrotu dla błędów LDAP znajdują się w pliku ldap.h, znajdującym się w systemie w katalogu QSYSINC/H.LDAP.

Jeśli po wystąpieniu błędu na serwerze katalogów LDAP istnieje potrzeba uzyskania dokładniejszych informacji, można przejrzeć protokół zadania QDIRSRV. W przypadku powtarzających się błędów można uruchomić komendę śledzenia aplikacji TCP/IP (TRCTCPAPP APP(*DIRSRV)), aby uruchomić śledzenie błędów. Więcej informacji na ten temat znajduje się w sekcji “Korzystanie z komendy TRCTCPAPP podczas szukania problemów” na stronie 66.

Usługi katalogowe używają kilku serwerów SQL (Structured Query Language). Gdy wystąpi błąd SQL, protokół zadania QDIRSRV zawiera zazwyczaj następujący komunikat:

```
SQL error -1 occurred (wystąpił  błąd -1 SQL)
```

W takich wypadkach protokół zadania QDIRSRV zawiera odsyłacz do protokołów zadań serwera SQL. Jednakże czasami QDIRSRV może nie zawierać tego komunikatu ani odsyłacza, nawet jeśli przyczyną problemu jest serwer SQL. Wtedy pomocne będzie ustalenie serwerów SQL, które powinny zostać uruchomione, i sposobów ich wykorzystania przez Usługi katalogowe.

Gdy serwer katalogów LDAP jest normalnie uruchamiany, generuje komunikat podobny do następującego:

Uwaga: Komunikaty i liczba zadań uruchomionych na serwerze SQL mogą być różne w następujących sytuacjach:

- uruchomienie serwera po raz pierwszy,
- potrzebne jest dokonanie migracji,
- serwer użytkownika używa protokołu zmian,
- serwer użytkownika umożliwia większą liczbę połączeń do bazy danych.

```
                                                        System:   WARMERS
Zadanie :   QDIRSRV   Użytkownik . . :   QDIRSRV   Numer . . :   174440

  >> CALL PGM(QSYS/QGLDSVR)
     Job 057448/QUSER/QSQSRVR used for SQL server mode processing.
     Job 057340/QUSER/QSQSRVR used for SQL server mode processing.
     Job 057448/QUSER/QSQSRVR used for SQL server mode processing.
     Job 057166/QUSER/QSQSRVR used for SQL server mode processing.
     Job 057279/QUSER/QSQSRVR used for SQL server mode processing.
   Job 057288/QUSER/QSQSRVR used for SQL server mode processing.
     Serwer usług katalogowych (LDAP) został pomyślnie uruchomiony.
```

Usługi katalogowe podczas uruchamiania serwera LDAP używają pierwszego serwera SQL, 057448/QUSER/QSQSRVR. Usługi katalogowe mogą w razie konieczności uruchomić dodatkowe serwery SQL podczas uruchamiania serwera LDAP, jeśli serwer jest uruchamiany po raz pierwszy, potrzebne jest wykonanie migracji lub serwer użytkownika używa protokołu zmian. Po uruchomieniu serwery SQL są usuwane.

W tym przykładzie nie został użyty żaden dodatkowy serwer SQL, w celu migracji lub uruchomienia serwera, tak więc protokół zmian nie został skonfigurowany. Następny serwer SQL (057340/QUSER/QSQSRVR) jest używany przez Usługi katalogowe tylko do replikacji.

Ostatnie połączenie w tym przykładzie (057288/QUSER/QSQSRVR) jest używane do operacji add, modify, modrdn oraz delete. Pozostałe połączenia są używane do operacji search, bind oraz compare.

Łączną liczbę używanych serwerów SQL, które używają Usługi katalogowe dla operacji katalogów po uruchomieniu serwera, podaje się na stronie Właściwości serwera katalogów na zakładce **Database**/**Suffixes** w iSeries Navigator. Dodatkowo jeden serwer SQL jest zawsze konfigurowany do replikacji.

Monitorowanie błędów i dostępu do serwera za pomocą protokołu zadania Usług katalogowych

Przeglądanie protokołu zadania serwera LDAP może pomóc w wykrywaniu błędów i w monitorowaniu dostępu do serwera.

Jeśli serwer został uruchomiony, aby przejrzeć protokół zadania QDIRSRV, wykonaj następujące kroki:
1. W programie iSeries Navigator rozwiń pozycję **Sieć**.
2. Rozwiń pozycję **Serwery**.
3. Kliknij **TCP**/**IP**.
4. Kliknij prawym przyciskiem myszy opcję **Katalog** i wybierz opcję **Zadania serwera**.
5. Z menu **Plik** wybierz opcję **Protokół zadania**.

Jeśli serwer został zatrzymany, aby przejrzeć protokół zadania QDIRSRV, wykonaj następujące kroki:
1. W programie iSeries Navigator rozwiń pozycję **Operacje podstawowe**.
2. Kliknij opcję **Wydruk**.
3. W kolumnie **Użytkownik**, w prawym panelu iSeries Navigator zostaje wyświetlony QDIRSRV. Aby przejrzeć protokół zadania, kliknij dwukrotnie **Qpjoblog** po lewej stronie pozycji QDIRSRV, w tym samym wierszu.

   Uwaga: iSeries Navigator można skonfigurować tak, aby wyświetlał jedynie pliki wydruku. Jeśli QDIRSRV nie znajduje się na liście, kliknij opcję **Wydruk**, następnie wybierz **Dołącz** z menu **Opcje**. W polu **Użytkownik** podaj wartość **Wszyscy**, a następnie kliknij **OK**.

Uwaga: Do przeprowadzenia niektórych zadań Usługi katalogowe używają innych zasobów systemu. Jeśli błąd wystąpi w jednym z tych zasobów, protokół zadania wskaże źródło dalszych informacji. W niektórych przypadkach Usługi katalogowe mogą mieć problemy z określeniem źródła informacji. Należy wówczas przejrzeć protokół zadania serwerów SQL (Structured Query Language) i sprawdzić, czy błąd nie jest związany z serwerami SQL.

Korzystanie z komendy TRCTCPAPP podczas szukania problemów

Serwer udostępnia śledzenie komunikacji w celu zbierania danych na liniach komunikacyjnych, takich jak interfejsy sieci lokalnych (LAN) lub sieci rozległych (WAN). Przeciętny użytkownik może nie zrozumieć całej zawartości danych śledzenia. Jednakże pozycje śledzenia można wykorzystać do określenia, czy pomiędzy dwoma punktami następuje wymiana danych.

Komenda Śledzenie aplikacji TCP/IP (Trace TCP/IP Application - TRCTCPAPP) z opcją *DIRSRV, może być użyta na serwerze katalogów LDAP, aby pomóc w rozwiązaniu problemów z klientami lub aplikacjami.

Więcej informacji na temat używania komendy TRCTCPAPP z protokołem LDAP, a także ograniczenia, co do wymaganych uprawnień znajdują się w sekcji Opis komendy TRCTCPAPP (Śledzenie aplikacji TCP/IP (Trace TCP/IP Application - TRCTCPAPP)).

Więcej ogólnych informacji na temat śledzenia komunikacji znajduje się w sekcji Śledzenie komunikacji (Communications trace).

Korzystanie z opcji LDAP_OPT_DEBUG do śledzenia błędów

Począwszy od wersji V5R2 można używać opcji LDAP_OPT_DEBUG funkcji API **ldap_set_option()**, w celu śledzenia problemów z klientami używającymi funkcji API języka C protokołu LDAP. Opcja debugowania ma wiele ustawień poziomu debugowania, które można używać do pomocy przy rozwiązywaniu problemów z tymi aplikacjami.

Poniżej przedstawiony jest przykład włączania podczas opcji debugowania śledzenia klienta.

```
int  debugvalue=  LDAP_DEBUG_TRACE  |  LDAP_DEBUG_PACKETS;
ldap_set_option(    1d,  LDAP_OPT_DEBUG,  &debugvalue);
```

Kolejnym sposobem ustawiania poziomu debugowania jest skonfigurowanie numerycznej wartości zmiennej środowiskowej LDAP_DEBUG dla zadania, w którym aplikacja kliencka jest uruchamiana, na tę samą, którą zmienna debugvalue przyjęłaby, gdyby użyta została funkcja API **ldap_set_option()**.

Przykład włączania śledzenia klienta, za pomocą zmiennej środowiskowej LDAP_DEBUG, wygląda następująco:

```
ADDENVVAR  ENVVAR(LDAP_DEBUG)  VALUE(0x0003)
```

Po uruchomieniu klienta, który powoduje problem, należy w wierszu poleceń iSeries wpisać następującą komendę:

```
DMPUSRTRC    NumerZadaniaKlienta
```

gdzie NumerZadaniaKlienta jest numerem zadania klienta.

Aby te informacje były wyświetlane interaktywnie, należy w wierszu poleceń iSeries wpisać następującą komendę:

```
DSPPFM  QAPOZDMP  QPOZnnnnnn
```

gdzie nnnnnn jest numerem zadania.

Aby zapisać te informacje, w celu wysłania ich do obsługi, wykonaj następujące czynności:

1. Utwórz plik SAVF za pomocą komendy CRTSAVF.
2. Wpisz następujące polecenie w wierszu komend iSeries.

   ```
   SAVOBJ  OBJ(QAPOZDMP  LIB(QTEMP)  DEV(*SAVF)  SAVF(xxx)
   ```

   gdzie *xxx* jest nazwą pliku SAVF.

Najczęstsze błędy klienta LDAP

Znajomość przyczyn występowania najczęstszych błędów klienta LDAP może pomóc w rozwiązywaniu problemów z serwerem. Aby przejrzeć pełną listę błędów klienta LDAP, patrz OS/400 Directory Services w sekcji ″Programming″ w Centrum informacyjnym iSeries.

Komunikaty o błędach klienta mają następujący format:

```
[Operacja LDAP wykazująca błąd]:[stany błędów klienta LDAP API]
```

Uwaga: W objaśnieniach błędów założono, że klient komunikuje się z serwerem LDAP znajdującym się w systemie OS/400. Klient komunikujący się z serwerem na innej platformie może otrzymywać podobne błędy, lecz przyczyny i rozwiązania najprawdopodobniej będą inne.

Najczęstsze komunikaty zawierają następujące informacje:

- “ldap_search: Timelimit exceeded”
- “[Failing LDAP operation]: Operations error”
- “ldap_bind: No such object”
- “ldap_bind: Inappropriate authentication”
- “[Failing LDAP operation]: Insufficient access” na stronie 69
- “[Failing LDAP operation]: Cannot contact LDAP server” na stronie 69
- “[Failing LDAP operation]: Failed to connect to ssl server” na stronie 69

ldap_search: Timelimit exceeded

ldap_search: Przekroczono limit czasu. Błąd ten występuje, gdy operacje ldapsearches przeprowadzane są zbyt wolno. Aby naprawić ten błąd, można:

- Zwiększyć limit czasu wyszukiwania dla serwera katalogów LDAP. Informacje dotyczące tej operacji zawiera sekcja “Regulowanie wydajności serwera katalogów LDAP” na stronie 32.
- Zmniejszyć aktywność w systemie. Można także zmniejszyć liczbę aktywnych zadań klientów LDAP.

[Failing LDAP operation]: Operations error

[Błędna operacja LDAP]: Błąd podczas działania. Błąd ten może być spowodowany kilkoma przyczynami. Aby uzyskać informacje o przyczynie tego błędu dla konkretnego przypadku, przejrzyj protokoły zadań QDIRSRV i serwera SQL, które opisano w sekcji “Podstawowa procedura rozwiązywania problemów z Usługami katalogowymi” na stronie 65.

ldap_bind: No such object

ldap_bind: Brak takiego obiektu. Najczęstszą przyczyną tego błędu jest niepoprawne wpisanie przez użytkownika informacji podczas wykonywania operacji. Inną częstą przyczyną jest usiłowanie nawiązania połączenia przez klienta z nazwą DN, która nie istnieje. To się często zdarza, gdy użytkownik błędnie poda administratora DN. Na przykład użytkownik może podać QSECOFR lub Administrator, podczas gdy faktyczny administrator DN może być czymś w rodzaju cn=Administrator.

Szczegóły na temat tego błędu zawiera protokół zadania QDIRSRV, który opisano w sekcji “Podstawowa procedura rozwiązywania problemów z Usługami katalogowymi” na stronie 65.

ldap_bind: Inappropriate authentication

ldap_bind: Niewłaściwe uwierzytelnienie. Serwer zwraca komunikat Invalid credentials (Niepoprawne uwierzytelnienie), kiedy hasło lub połączona nazwa DN są niepoprawne. Serwer zwraca komunikat o niewłaściwym uwierzytelnieniu, kiedy klient próbuje połączenia w jednym z następujących przypadków:

- z pozycji, która nie ma atrybutu userpassword (hasło użytkownika),

- z pozycji, która reprezentuje użytkownika systemu OS/400 mającego atrybut UID, a nie atrybut userpassword (hasło użytkownika); powoduje to próbę porównania pomiędzy określonym hasłem a hasłem użytkownika systemu OS/400, które nie są zgodne,
- z pozycji, która reprezentuje użytkownika rzutowanego i wymagana jest metoda połączenia inna niż prosta.

Błąd ten generowany jest zazwyczaj, gdy klient usiłuje nawiązać połączenie z niepoprawnym hasłem. Szczegóły na temat tego błędu zawiera protokół zadania QDIRSRV, który opisano w sekcji “Podstawowa procedura rozwiązywania problemów z Usługami katalogowymi” na stronie 65.

[Failing LDAP operation]: Insufficient access

[Błędna operacja LDAP]: Niewłaściwy dostęp. Błąd ten jest zazwyczaj generowany, gdy nazwa DN, pod którą nawiązuje się połączenie, nie ma odpowiednich uprawnień do wykonania zażądanej przez klienta operacji (takiej jak dodanie lub usunięcie). Szczegóły na temat tego błędu zawiera protokół zadania QDIRSRV, który opisano w sekcji “Podstawowa procedura rozwiązywania problemów z Usługami katalogowymi” na stronie 65.

[Failing LDAP operation]: Cannot contact LDAP server

[Błędna operacja LDAP]: Nie można nawiązać opłączenia z serwerem LDAP. Najczęstsze powody wystąpienia tego błędu to:

- Klient LDAP wysyła żądanie, zanim serwer LDAP podanego systemu zostanie uruchomiony i przyjmie status oczekiwania.
- Użytkownik podaje niepoprawny numer portu. Na przykład, serwer korzysta z portu 386, ale żądanie klienta usiłuje użyć portu 387.

Aby uzyskać informacje o błędzie, przejrzyj protokół zadania QDIRSRV opisany w sekcji “Podstawowa procedura rozwiązywania problemów z Usługami katalogowymi” na stronie 65. Jeśli serwer usług katalogowych (LDAP) został pomyślnie uruchomiony, w protokole zadania QDIRSRV zostanie zapisany komunikat Directory Services server started successfully (Serwer usług katalogowych został pomyślnie uruchomiony).

[Failing LDAP operation]: Failed to connect to ssl server

[Błędna operacja LDAP]: Połączenie z serwerem ssl nie powiodło się. Błąd ten występuje, gdy serwer LDAP odmawia połączenia z klientem, ponieważ nie można nawiązać połączenia SSL. Może to być spowodowane jedną z poniżej wymienionych przyczyn:

- obsługa Certificate Management odmówi połączenia klienta z serwerem, należy wtedy użyć programu DCM, aby upewnić się, czy certyfikaty zostały poprawnie skonfigurowane, a następnie wykonać restart serwera i ponowić próbę połączenia,
- użytkownik może nie mieć dostępu do odczytu bazy certyfikatów *SYSTEM (domyślnie /QIBM/userdata/ICSS/Cert/Server/default.kdb).

Dla aplikacji C systemu OS/400 dostępne są dodatkowe informacje o błędach SSL. Szczegóły zawarte są w dokumentacji konkretnych funkcji API Usług katalogowych.