



System i

Serwer katalogów

IBM Tivoli Directory Server for i5/OS (LDAP)

*Wersja 6 wydanie 1*







System i

Serwer katalogów

IBM Tivoli Directory Server for i5/OS (LDAP)

*Wersja 6 wydanie 1*

**Uwaga**

Przed skorzystaniem z tych informacji oraz z produktu, którego dotyczą, należy przeczytać informacje zawarte w sekcji "Uwagi", na stronie 319.

To wydanie dotyczy Wersji 6, Wydania 1, Modyfikacji 0 systemu operacyjnego IBM i5/OS (numer produktu 5761-SS1) oraz wszystkich kolejnych wydań i modyfikacji, o ile w nowych wydaniach nie określono inaczej. Wersja ta nie działa na wszystkich modelach komputerów z procesorem RISC ani na modelach z procesorem CISC.

© Copyright International Business Machines Corporation 1998, 2008. Wszelkie prawa zastrzeżone.

# Spis treści

## IBM Tivoli Directory Server for i5/OS (LDAP) . . . . . 1

Co nowego w wersji V6R1 . . . . .	1
Plik PDF z informacjami na temat produktu IBM Tivoli Directory Server for i5/OS (LDAP) . . . . .	3
Pojęcia dotyczące serwera Directory Server . . . . .	3
Katalogi . . . . .	4
Katalogi rozproszone . . . . .	7
Nazwy wyróżniające (DN) . . . . .	9
Przyrostek (kontekst nazwy) . . . . .	12
Schemat . . . . .	14
Zalecane procedury dla struktury katalogów . . . . .	34
Publikowanie . . . . .	36
Replikacja . . . . .	37
Dziedziny i szablony użytkowników . . . . .	46
Parametry wyszukiwania . . . . .	47
Uwagi dotyczące obsługi języków narodowych . . . . .	49
Znaczniki języka . . . . .	49
Odwołania do katalogu LDAP . . . . .	50
Transakcje . . . . .	51
Bezpieczeństwo serwera Directory Server . . . . .	51
Mechanizm rzutowania systemu operacyjnego . . . . .	84
Obsługa funkcji kronikowania systemu i5/OS w serwerze Directory Server . . . . .	90
Atrybuty unikalne . . . . .	90
Atrybuty operacyjne . . . . .	91
Pamięci podręczne serwera . . . . .	92
Elementy sterujące i rozszerzone operacje . . . . .	93
Uwagi na temat składowania i odtwarzania . . . . .	94
Pierwsze kroki z serwerem Directory Server . . . . .	95
Uwagi dotyczące migracji . . . . .	95
Planowanie serwera Directory Server . . . . .	100
Konfigurowanie serwera Directory Server . . . . .	101
Zapełnianie katalogu . . . . .	102
Administrowanie przez sieć WWW . . . . .	102
Scenariusze związane z serwerem Directory Server . . . . .	106
Scenariusz: konfigurowanie serwera Directory Server . . . . .	106
Scenariusz: kopiowanie użytkowników z listy sprawdzania serwera HTTP do serwera Directory Server . . . . .	114
Administrowanie serwerem Directory Server . . . . .	116

Ogólne zadania administrowania . . . . .	116
Zadania grupy administracyjnej . . . . .	134
Zadania związane z grupami ograniczonego wyszukiwania . . . . .	135
Zadania związane z grupami autoryzacji proxy . . . . .	138
Zadania związane z atrybutami unikalnymi . . . . .	141
Zadania związane z wydajnością . . . . .	143
Zadania związane z replikacją . . . . .	146
Zadania związane z topologią replikacji . . . . .	167
Zadania związane z właściwościami bezpieczeństwa . . . . .	176
Zadania związane ze schematem . . . . .	185
Zadania związane z pozycjami katalogu . . . . .	195
Zadania związane z użytkownikami i grupami . . . . .	203
Zadania związane z dziedziczeniami i szablonami użytkowników . . . . .	206
Zadania związane z listami kontroli dostępu . . . . .	214
Informacje dodatkowe . . . . .	218
Programy narzędziowe wiersza komend serwera Directory Server . . . . .	218
Format wymiany danych LDAP (LDIF) . . . . .	251
Schemat konfiguracji serwera Directory Server . . . . .	258
Identyfikatory obiektów (OID) . . . . .	298
Równoważność produktu IBM Tivoli Directory Server . . . . .	308
Konfiguracja domyślna serwera Directory Server . . . . .	308
Rozwiązywanie problemów z serwerem Directory Server . . . . .	309
Monitorowanie błędów i dostępu za pomocą protokołu zadania serwera Directory Server . . . . .	309
Odszukiwanie problemów za pomocą komendy TRCTCPAPP . . . . .	310
Używanie opcji LDAP_OPT_DEBUG do śledzenia błędów . . . . .	311
Identyfikatory komunikatów GLEnnnn . . . . .	312
Najczęstsze błędy klienta LDAP . . . . .	315
Błędy związane ze strategią haseł . . . . .	317
Rozwiązywanie problemów z funkcją API QGLDCPYVL . . . . .	317
Informacje pokrewne . . . . .	318

## Dodatek. Uwagi . . . . . 319

Znaki towarowe . . . . .	321
Warunki . . . . .	321



---

## IBM Tivoli Directory Server for i5/OS (LDAP)

Produkt IBM Tivoli Directory Server for i5/OS (zwany serwerem Directory Server) to funkcja systemu i5/OS, która udostępnia serwer LDAP (Lightweight Directory Access Protocol). LDAP działa w oparciu o protokół TCP/IP i jest popularny jako usługa katalogowa w zastosowaniach internetowych i nie tylko.

W tematach zawartych w tej publikacji znajdują się informacje ułatwiające korzystanie z serwera Directory Server oraz zrozumienie jego działania.

---

### Co nowego w wersji V6R1

Poniżej opisano nowe lub znacznie zmienione informacje w kolekcji tematów dotyczącej serwera IBM Tivoli Directory Server for i5/OS (LDAP).

### Rozstrzygnięcie konfliktów replikacji

W sieci z wieloma serwerami głównymi serwer IBM Tivoli® Directory Server ma możliwość automatycznego wykrywania i rozstrzygnięcia powodujących konflikt zmian, aby katalogi na wszystkich serwerach pozostawały spójne. Po wykryciu konfliktów replikacji zmiana powodująca konflikt jest zgłaszana w protokole serwera oraz rejestrowana w pliku protokołu niedokończonych operacji, aby administrator mógł odtworzyć utracone dane.

- Replikacja - przegląd
- Modyfikowanie ustawień protokołu niedokończonych operacji
- Wyświetlanie pliku protokołu niedokończonych operacji

### Komenda ldapmodify

Opcja -e plik\_błędu dodana do komendy ldapmodify umożliwia określenie pliku, do którego będą zapisywane odrzucone pozycje. Dodano opcję -n, aby zmiany, jakie zostałyby wprowadzone, były poprzedzane wykrzyknikiem i drukowane na standardowym wyjściu.

- ldapmodify i ldapadd
- Format wymiany danych LDAP (LDIF)

### Replikacja wielowątkowa

Można replikować dane przy użyciu wielu wątków, co zwiększa ogólną przepustowość replikacji.

- Replikacja wielowątkowa
- Umowy replikacji

### Szyfrowanie haseł

IBM Tivoli Directory Server udostępnia opcję konfiguracyjną umożliwiającą szyfrowanie danych hasła użytkownika przed zapisaniem ich w katalogu. Opcji szyfrowania można użyć w celu uniemożliwienia dostępu do danych hasła w postaci jawnego tekstu zarówno zwykłym użytkownikom katalogu, jak i administratorom.

- Szyfrowanie haseł
- Określanie właściwości strategii haseł

### Atrybut IBMAttributeTypes

IBM Tivoli Directory Server 6.0 umożliwia użycie pierwszych 128 znaków atrybutu do utworzenia nazwy tabeli.

- Atrybut IBMAttributeTypes

## | **Niedozwolone zmiany schematu**

- | Kolumnę można zwiększyć, modyfikując schemat. Umożliwia to zwiększenie maksymalnej długości atrybutów
- | poprzez modyfikację schematu za pomocą narzędzi Web Administration lub ldapmodify.
- | • Niedozwolone zmiany schematu

## | **Katalog rozproszony**

- | IBM Tivoli Directory Server jest w założeniu katalogiem rozproszonym. W połączeniu z serwerem proxy funkcja katalogu rozproszonego umożliwia aplikacjom łączenie się z klastrem katalogów w taki sposób, jak gdyby był to jeden katalog. Funkcje katalogu rozproszonego i serwera proxy pozwalają wdrożyć infrastrukturę, w której można przechowywać miliony pozycji.
- | • Katalogi rozproszone

## | **Idapmodrdrn**

- | IBM Tivoli Directory Server obsługuje funkcję modifyDN z atrybutem newsuperior na węźle liścia.
- | • Idapmodrdrn

## | **Odszukiwanie problemów za pomocą komendy TRCTCPAPP**

- | Komendy TRCTCPAPP można użyć w celu śledzenia aktywnej instancji serwera.
- | • Odszukiwanie problemów za pomocą komendy TRCTCPAPP

## | **Dostęp do odczytu profili użytkowników rzutowanych**

- | Można uniemożliwić wszelkie operacje wyszukiwania skierowane do mechanizmu rzutowania użytkowników.
- | • Operacje LDAP
- | • Dostęp do odczytu profili użytkowników rzutowanych

## | **Wiele instancji serwerów**

- | W systemie i5/OS® może działać wiele serwerów katalogów. Każdy serwer jest nazywany instancją. Jeśli w poprzedniej wersji systemu i5/OS używany był serwer katalogów, zostanie przeprowadzona jego migracja do instancji o nazwie QUSRDIR. Na potrzeby obsługi aplikacji można tworzyć wiele instancji serwera katalogów.
- | • Zarządzanie instancjami
- | • Konfigurowanie serwera Directory Server

## | **Uwagi dotyczące migracji**

- | IBM Tivoli Directory Server jest aktualizowany do nowszych wersji przy pierwszym uruchomieniu.
- | • Migrowanie do wersji V6R1 z wersji V5R4 lub V5R3

## | **Strategia haseł**

- | Konta administratorów mogą być blokowane w wyniku nadmiernej ilości niepowodzeń uwierzytelniania. Opcja ta dotyczy tylko zdalnych połączeń klientów. Konto jest resetowane podczas uruchamiania serwera. Aby umożliwić blokowanie konta, zdefiniowano nowy atrybut.
- | • Ustawianie hasła administratora i strategii blokowania
- | • Określanie właściwości strategii haseł

- | Rozszerzona operacja żądania statusu konta umożliwia wczytanie statusu wybranego konta. Status może przyjmować wartość otwarte (włączone), zablokowane lub utraciło ważność.



- ldapexop



## Pozostałe informacje

**Równoważność serwera IBM® Tivoli® Directory Server:** serwer Directory Server w wersji V6R1 jest równoważny serwerowi IBM Tivoli Directory Server w wersji 6.0.

- Centrum informacyjne oprogramowania Tivoli

## Znajdowanie nowych lub zmienionych informacji

Aby ułatwić odnalezienie miejsc, w których wprowadzono zmiany techniczne, użyto następujących symboli:

- symbol  służący do zaznaczania początku nowego lub zmienionego fragmentu;
- symbol  służący do zaznaczania końca nowego lub zmienionego fragmentu.

Nowe i zmienione informacje w plikach PDF mogą być oznaczone symbolem | na lewym marginesie.

Więcej informacji na temat zmian i nowości w bieżącej wersji zawiera Wiadomość dla użytkowników.

---

## Plik PDF z informacjami na temat produktu IBM Tivoli Directory Server for i5/OS (LDAP)

Informacje na temat produktu IBM Tivoli Directory Server for i5/OS są dostępne w postaci pliku PDF, który można wyświetlić i wydrukować.

Aby przejrzeć lub pobrać dokument w formacie PDF, kliknij odsyłacz IBM Tivoli Directory Server for i5/OS (LDAP) (ok. 2700 KB).

## Inne informacje

Aby przejrzeć lub wydrukować wersje PDF podręczników pokrewnych i dokumentacji technicznej IBM (Redbooks), zapoznaj się z tematem “Informacje pokrewne” na stronie 318.

## Zapisywanie plików PDF

Aby zapisać plik PDF na stacji roboczej w celu jego przeglądania lub drukowania:

1. Kliknij prawym przyciskiem myszy odsyłacz do pliku PDF w przeglądarce.
2. Kliknij opcję zapisania pliku PDF lokalnie.
3. Przejdź do katalogu, w którym ma być zapisany plik PDF.
4. Kliknij opcję **Zapisz**.

## Pobieranie programu Adobe Reader

Do przeglądania i drukowania plików PDF potrzebny jest program Adobe Reader zainstalowany na komputerze. Jego nieodpłatną kopię można pobrać z serwisu WWW firmy Adobe ([www.adobe.com/products/acrobat/readstep.html](http://www.adobe.com/products/acrobat/readstep.html))



---

## Pojęcia dotyczące serwera Directory Server

Informacje na temat pojęć dotyczących serwera Directory Server.

Serwer Directory Server ma zaimplementowane specyfikacje IETF (Internet Engineering Task Force) LDAP V3. Zawiera również rozszerzenia dodane przez IBM w obszarach związanych z funkcjami i wydajnością. W tej wersji używana jest baza danych IBM DB2 Universal Database for iSeries jako pamięć pomocnicza zapewniająca

integralność transakcji w operacjach LDAP, wysoką wydajność operacji oraz możliwość składowania i odtwarzania w czasie działania serwera. Wersja ta współpracuje z klientami opartymi na specyfikacjach IETF LDAP V3.

## Katalogi

Serwer Directory Server umożliwia dostęp do bazy danych specjalnego typu, w której informacje są zapisywane w strukturze hierarchicznej podobnej do organizacji zintegrowanego systemu plików systemu i5/OS.

Jeśli nazwa obiektu jest znana, można pobrać jego charakterystykę. Jeśli nazwa konkretnego obiektu nie jest znana, można przeszukać katalog, tworząc listę obiektów spełniających określone wymagania. Katalogi można przeszukiwać według konkretnych kryteriów, nie tylko według z góry zdefiniowanego zestawu kategorii.

Katalog jest specjalną bazą danych o cechach odróżniających ją od relacyjnej bazy danych do zastosowań ogólnych. Różnica polega na tym, że odwołania do katalogu (odczyt lub wyszukiwanie), są znacznie częstsze niż aktualizacje (zapis). Ponieważ katalogi muszą obsługiwać duże ilości żądań odczytu, zwykle są zoptymalizowane do dostępu polegającego na odczycie. Ponieważ katalogi nie mają na celu udostępniania tylu funkcji, co bazy danych ogólnego zastosowania, można je optymalizować, aby w ekonomiczny sposób udostępniały więcej aplikacji o szybkim dostępie do danych katalogu w dużych środowiskach rozproszonych.

Katalog może być scentralizowany lub rozproszony. Jeśli katalog jest scentralizowany, to jeden serwer Directory Server (lub jeden klaster serwerów) w jednym miejscu umożliwia dostęp do katalogu. Jeśli katalog jest rozproszony, to dostęp do niego umożliwia wiele serwerów, zwykle o różnym położeniu geograficznym.

Jeśli katalog jest rozproszony, informacje w nim zapisane można dzielić lub replikować. Jeśli informacje zostały podzielone, każdy serwer katalogów zawiera unikalny zestaw informacji; zestawy na poszczególnych serwerach nie pokrywają się. Oznacza to, że każda pozycja katalogu jest przechowywana przez jeden i tylko jeden serwer. Technika dzielenia katalogu polega na używaniu odwołań LDAP. Umożliwiają one korzystanie z żądań LDAP (Lightweight Directory Access Protocol) w celu odwołania się do tego samego lub innego obszaru nazw zapisanego na innym (lub tym samym) serwerze. Podczas replikowania danych ta sama pozycja katalogu jest przechowywana na wielu serwerach. W katalogu rozproszonym niektóre informacje mogą być dzielone, a niektóre replikowane.

Model serwera katalogów LDAP oparty jest na pozycjach (zwanych również 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 (common name - nazwa zwykła) lub mail (e-mail - adres poczty elektronicznej).

Rys. 1 na stronie 5 przedstawia przykładowy katalog zawierający pozycje dla osoby o nazwisku Tim Jones z atrybutami mail i telephoneNumber. Inne możliwe atrybuty to fax, title (tytuł), sn (surname - nazwisko) oraz jpegPhoto.

Każdy katalog ma schemat, który jest zestawem reguł określających strukturę i zawartość katalogu. Schemat można przeglądać za pomocą narzędzi administrowania WWW.

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.

Poza atrybutami zdefiniowanymi w schemacie pozycje zawierają również zestaw atrybutów obsługiwanych przez serwer. Atrybuty te są nazywane atrybutami operacyjnymi i obejmują informacje na temat miejsca utworzenia pozycji oraz kontroli dostępu.

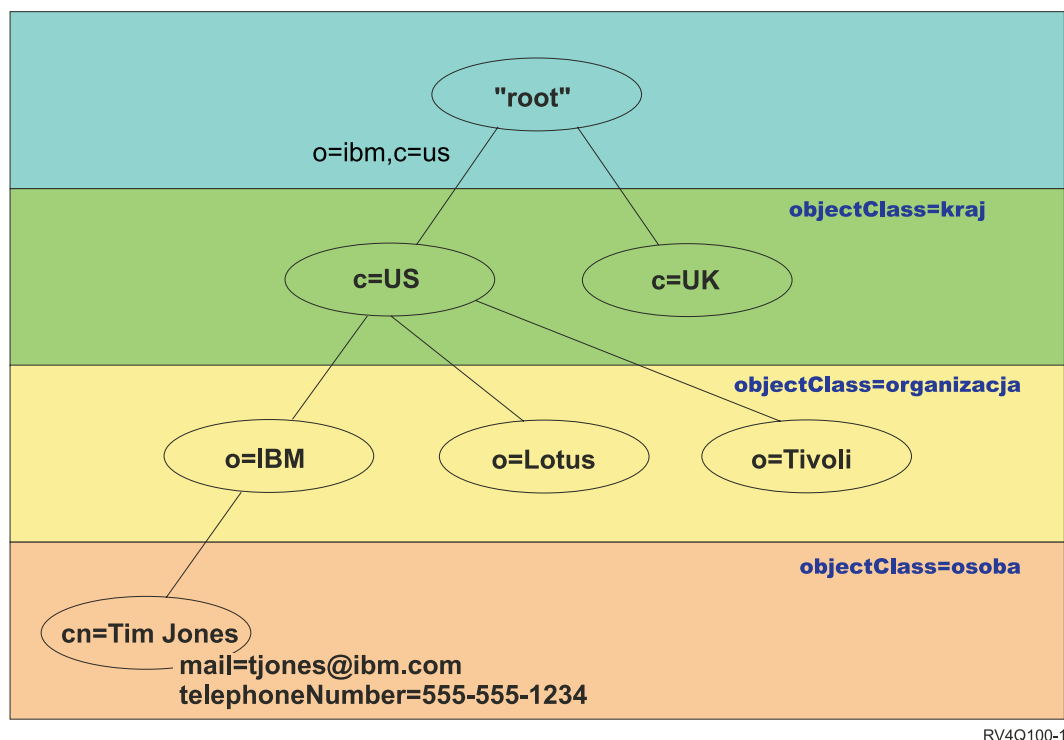
Tradycyjnie pozycje katalogu LDAP są ułożone hierarchicznie. Odzwierciedla to granice polityczne, geograficzne lub organizacyjne (patrz Rys. 1 na stronie 5). Pozycje odpowiadające krajom lub regionom znajdują się u góry hierarchii. Pozycje przedstawiające województwa lub organizacje krajowe znajdują się jako drugie. Dalsze pozycje mogą reprezentować osoby, jednostki organizacyjne, drukarki, dokumenty lub inne elementy.

Protokół LDAP odwołuje się do pozycji poprzez nazwy wyróżniające (DN). Nazwy wyróżniające składają się z nazwy pozycji, jak również nazw, w kolejności od dołu do góry, obiektów występujących wyżej w katalogu. Rys. 1 na stronie 5 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 nazwy 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 nazwą DN dla nazwy cn=Tim Jones.

Aby serwer LDAP zarządzał częścią katalogu LDAP, należy w jego konfiguracji podać najwyższy poziom nadrzędnych nazw wyróżniających. Są one nazywane przyrostkami. Serwer może uzyskać dostęp do wszystkich obiektów w katalogu, które w hierarchii znajdują się poniżej podanego przyrostka. Rys. 1 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 osoby o nazwisku Tim Jones.

## Struktura katalogów LDAP



Rysunek 1. Struktura katalogu LDAP

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

Załóżmy, że zadaniem jest utworzenie katalogu za pomocą struktury komponentu domeny, która będzie zawierała dane pracowników, takie jak nazwiska, numery telefonów i adresy poczty elektronicznej. Można użyć przyrostka lub kontekstu nazewnictwa opartego na domenie TCP/IP. Katalog ten można przedstawić w sposób podobny do poniższego:

```

/
|
+- ibm.com
  |
  +- employees
    |
    +- Tim Jones
      |
      | 555-555-1234
      | tjones@ibm.com
  
```

```
|
+- John Smith
   555-555-1235
   jsmith@ibm.com
```

Po wprowadzeniu do serwera Directory Server dane te mogą wyglądać podobnie do przedstawionych poniżej:

```
# przyrostek ibm.com
dn: dc=ibm,dc=com
objectclass: top
objectclass: domain
dc: ibm

# katalog pracowników
dn: cn=employees,dc=ibm,dc=com
objectclass: top
objectclass: container
cn: employees

# pracownik Tim Jones
dn: cn=Tim Jones,cn=employees,dc=ibm,dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
objectclass: publisher
objectclass: ePerson
cn: Tim Jones
cn: "Jones, Tim"
sn: Jones
givenname: Tim
telephonenumber: 555-555-1234
mail: tjones@ibm.com

# pracownik John Smith
dn: cn=John Smith,cn=employees,dc=ibm,dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
objectclass: publisher
objectclass: ePerson
cn: John Smith
cn: "Smith, John"
sn: Smith
givenname: John
telephonenumber: 555-555-1235
mail: jsmith@ibm.com
```

Można zauważyć, że każda pozycja zawiera wartości atrybutów o nazwie objectclass. Wartości objectclass definiują atrybuty dozwolone w tej pozycji, takie jak telephonenumber lub givenname. Dozwolone klasy obiektu są zdefiniowane w schemacie. Schemat jest zestawem reguł definiujących typ pozycji dozwolonych w bazie danych.

## Klienci i serwery katalogu

Katalogi są zwykle dostępne dzięki komunikacji klient/serwer. Procesy klienta i serwera mogą działać na tym samym komputerze, ale nie muszą. Serwer może obsługiwać wielu klientów. Aplikacja, która chce odczytać lub zapisać informacje w katalogu, nie ma do niego bezpośredniego dostępu. Zamiast tego wywołuje funkcję lub funkcję API powodującą wysłanie komunikatu do innego procesu. Drugi proces uzyskuje dostęp do informacji w imieniu aplikacji wysyłającej żądanie. Wyniki operacji odczytu lub zapisu są następnie zwracane do aplikacji wysyłającej żądanie.

Funkcja API definiuje interfejs programistyczny używany przez konkretny język programowania w celu uzyskania dostępu do usługi. Format i zawartość komunikatów wymienianych między klientem i serwerem musi być zgodna z odpowiednim protokołem. LDAP definiuje protokół komunikatów używany przez klientów i serwery katalogów.

Istnieje również powiązana funkcja API LDAP dla języka C oraz sposoby dostępu do katalogu z aplikacji w języku Java przy użyciu interfejsu JNDI (Java Naming and Directory Interface).

## Ochrona katalogu

Katalog powinien obsługiwać podstawowe możliwości wymagane do zaimplementowania strategii ochrony. Nie musi udostępniać bezpośrednio funkcji ochrony, ale może być zintegrowany z zaufaną usługą ochrony sieci udostępniającą podstawowe usługi ochrony. Po pierwsze potrzebna jest metoda uwierzytelniania użytkowników. Uwierzytelnianie polega na sprawdzeniu, czy użytkownicy są tymi, za których się podają. Nazwa użytkownika i hasło to podstawowy schemat uwierzytelniania. Po uwierzytelnieniu użytkowników należy określić, czy mają oni uprawnienia do wykonywania żądanych operacji na konkretnych obiektach.

Autoryzacja często opiera się na listach kontroli dostępu (ACL). Lista ACL to lista autoryzacji, którą można podłączyć do obiektów i atrybutów w katalogu. Lista ACL określa zezwolenie na określony typ dostępu lub zablokowanie go dla użytkowników i grup użytkowników. Aby skrócić listy ACL i ulepszyć zarządzanie nimi, użytkowników o tym samym prawach dostępu często łączy się w grupy.

### Pojęcia pokrewne

“Schemat” na stronie 14

Schemat jest zestawem reguł określających sposób przechowywania danych w katalogu. Schemat definiuje typ dozwolonych pozycji oraz strukturę i składnię atrybutów.

“Atrybuty operacyjne” na stronie 91

Istnieje szereg atrybutów o specjalnym znaczeniu dla serwera katalogów znanych jako atrybuty operacyjne. Są to atrybuty obsługiwane przez serwer i odzwierciedlające zarządzane przez serwer informacje o pozycji lub wywierające wpływ na działanie serwera.

“Nazwy wyróżniające (DN)” na stronie 9

Każda pozycja w katalogu ma nazwę wyróżniającą (DN). Nazwa DN jednoznacznie identyfikuje pozycję w katalogu. Pierwszy komponent nazwy DN jest nazywany względną nazwą wyróżniającą (RDN).

Funkcje API protokołu LDAP

Temat Funkcje API protokołu LDAP zawiera więcej informacji o funkcjach API serwera katalogów.

“Bezpieczeństwo serwera Directory Server” na stronie 51

Informacje o funkcjach służących do zabezpieczania serwera Directory Server.

### Informacje pokrewne



Serwis WWW The Java Naming and Directory Interface (JNDI) Tutorial

## Katalogi rozproszone

Katalog rozproszony to środowisko, w którym dane są rozdzielone na wiele serwerów katalogów. Aby katalog rozproszony wyglądał dla aplikacji klienckich jak pojedynczy katalog, wykorzystuje się jeden lub wiele serwerów proxy, które mają informacje o wszystkich serwerach i znajdujących się na nich danych.

Serwery proxy rozdzielają żądania przychodzące między właściwe serwery i zbierają wyniki w celu zwrócenia jednolitej odpowiedzi do klienta. Zestaw serwerów zaplecza zawiera właściwe części katalogu rozproszonego. Te serwery zaplecza są standardowymi serwerami LDAP z dodatkową obsługą serwera proxy na potrzeby wysyłania żądań w imieniu użytkownika, który może być zdefiniowany na innym serwerze lub należeć do grup zdefiniowanych na innych serwerach.

Serwer IBM Tivoli Directory Server w wersjach 6.0 i nowszych (na platformach rozproszonych) udostępnia taki katalog rozproszony wraz z serwerami proxy, serwerami zaplecza i narzędziami do konfigurowania katalogu. Katalog taki można skalować do wielu milionów pozycji.

## Obsługa katalogów rozproszonych przez serwer IBM Directory Server for i5/OS

Serwer IBM Directory Server for i5/OS może działać jako serwer zaplecza w katalogu rozproszonym IBM Tivoli. Serwer katalogów systemu operacyjnego i5/OS nie może działać jako serwer proxy i nie zawiera narzędzi wymaganych

l do skonfigurowania katalogu rozproszonego. Serwer proxy może działać na innej platformie, podczas gdy rzeczywiste dane znajdują się na jednym lub wielu serwerach katalogów systemu i5/OS lub jednocześnie na serwerach katalogów i5/OS i Tivoli.

l Aby można było podzielić istniejące dane katalogu z serwera katalogów i5/OS w celu ich użycia w topologii katalogu rozproszonego, należy wyeksportować dane do pliku LDIF z katalogu i5/OS, uruchomić narzędzie konfigurowania katalogu rozproszonego dostępne na platformach Tivoli i załadować do niego plik LDIF, a następnie przeładować dane na serwerach katalogów i5/OS i Tivoli, które będą uczestniczyły w katalogu rozproszonym jako serwery zaplecza. Proces ten jest taki sam na serwerach i5/OS i Tivoli, a użytkownicy mają już narzędzie do konfigurowania rozproszonego katalogu, ponieważ mają serwer proxy na platformie Tivoli.

## l **Elementy sterujące i rozszerzone operacje obsługujące katalogi rozproszone**

l Ponieważ grupy oraz przypisanych im użytkowników można rozproszyć na wielu serwerach, serwer IBM Tivoli Directory Server ma zdefiniowany zestaw elementów sterujących i rozszerzonych operacji obsługujących członkostwo w grupach i kontrolę dostępu w katalogu rozproszonym. Dostępny jest także mechanizm zapisu kontrolnego pozwalający określić klienta, od którego pochodzi zapytanie.

l **Uwaga:** Pozycja katalogu znajduje się na jednym serwerze i na jego replikach. Jednakże w katalogu rozproszonym użytkownik może należeć do jednej lub wielu grup na jednym serwerze, a także do innych grup zdefiniowanych na innym serwerze. Ponadto użytkownik może nie być zdefiniowany na serwerze zaplecza, który przetwarza dane żądanie.

## l **Audit (Kontrola)**

l Audit (Kontrola) to mechanizm wykorzystywany przez serwer proxy do wysyłania unikalnego identyfikatora żądania klienta zainicjowanego przez serwer proxy na serwerach zaplecza. Oprócz unikalnego identyfikatora w ramach kontroli wysyłany jest także adres IP klienta, który utworzył żądanie. Unikalny identyfikator służy do dopasowywania pozycji kontroli na serwerze proxy do pozycji kontroli na serwerze zaplecza. Jeśli żądanie przechodzi przez wiele serwerów, dodawane są informacje o adresie IP każdego serwera, dzięki czemu zachowywana jest informacja o ścieżce prowadzącej przez poszczególne serwery do klienta.

## l **Group Membership Evaluation (Wartościowanie członkostwa w grupach)**

l Ta rozszerzona operacja umożliwia autoryzowanemu klientowi (serwerowi proxy) wysyłanie informacji o użytkowniku do serwera zaplecza oraz żądanie listy grup (statycznych, zagnieżdżonych lub dynamicznych), do których użytkownik należy na serwerze zaplecza.

## l **Group Membership (Członkostwo w grupach)**

l Ten element sterujący umożliwia autoryzowanemu klientowi (serwerowi proxy) wysyłanie listy grup, która będzie służyć do kontroli dostępu. Kontrola dostępu podlega wartościowaniu na podstawie tej listy grup, a nie na podstawie listy grup, jaką serwer normalnie utworzyłby przy użyciu lokalnych informacji o grupach. W typowym scenariuszu ta lista grup jest gromadzona przez serwer proxy z każdego serwera zaplecza na pomocą rozszerzonej operacji Group Membership Evaluation (Wartościowanie członkostwa w grupach).

## l **Obsługa kontroli katalogów rozproszonych**

l Funkcje kontroli bezpieczeństwa systemu i5/OS zostały rozszerzone o obsługę katalogów rozproszonych.

- l • **Audit (Kontrola):** śledzenie ścieżki żądania wstecz do klienta, który je utworzył, jest przydatne. System I5/OS prowadzi kontrolę, dodając pole "routing" do istniejącej pozycji w kronice kontroli bezpieczeństwa DI. Choć treści nie można zweryfikować, pochodzą one od klienta, który ma uprawnienie do korzystania z autoryzacji proxy, dlatego powinien być zaufanym klientem.
- l • **Group membership (Członkostwo w grupach):** obecność tego elementu sterującego jest kontrolowana dwuczłoniowo. Do pozycji kroniki kontroli bezpieczeństwa DI dodano jednoznakowe pole "uznania członkostwa w

grupie" (group membership assertion). Serwer można także skonfigurować, aby opcjonalnie kontrolował listę grup przesyłaną przez klienta. Po skonfigurowaniu tej opcji serwer kontroluje również pole "odniesienie XD" (XD cross reference) w pozycji kroniki DI oraz tworzy jedną lub więcej pozycji w kronice kontroli bezpieczeństwa z pasującym polem "odniesienie XD" oraz listą grup (do 5 grup w jednej pozycji kroniki).

Temat dotyczący bezpieczeństwa, do którego odsyłacz znajduje się poniżej, zawiera szczegółowe informacje o funkcji kontroli bezpieczeństwa w systemie i5/OS. Można także przejść do serwisu WWW grupy wykonawczej Internet Engineering Task Force i wyszukać dokumentu *RFC 4648* w celu uzyskania dalszych informacji o konfigurowaniu kontroli na serwerze katalogów.

Więcej informacji o katalogach rozproszonych i ich konfigurowaniu zawiera temat Distributed Directories w Centrum informacyjnym oprogramowania Tivoli.

#### **Pojęcia pokrewne**

"Kontrola" na stronie 51

Kontrola umożliwia śledzenie szczegółów określonych transakcji serwera Directory Server.

#### **Informacje pokrewne**

Kontrolowanie bezpieczeństwa

Więcej informacji dotyczących kontroli zawiera temat Kontrolowanie bezpieczeństwa.

Object Identifiers (OIDs) for extended operations and controls

## **Nazwy wyróżniające (DN)**

Każda pozycja w katalogu ma nazwę wyróżniającą (DN). Nazwa DN jednoznacznie identyfikuje pozycję w katalogu. Pierwszy komponent nazwy DN jest nazywany względną nazwą wyróżniającą (RDN).

Składa się ona z par atrybut=wartość, oddzielonych przecinkami, na przykład:

```
cn=Ben Gray,ou=editing,o=New York Times,c=US
cn=Lucille White,ou=editing,o=New York Times,c=US
cn=Tom Brown,ou=reporting,o=New York Times,c=US
```

Na nazwę wyróżniającą (DN) mogą się składać wszystkie atrybuty zdefiniowane w schemacie katalogu. Kolejność par wartości atrybutu komponentu jest istotna. Nazwa DN zawiera jeden komponent dla każdego poziomu hierarchii katalogu od najwyższego szczebla do poziomu, na którym znajduje się pozycja. Nazwy DN LDAP zaczynają się od najbardziej szczegółowego atrybutu (zwykle rodzaju nazwy) i zawierają atrybuty o coraz większym zakresie, często kończąc się na atrybucie kraju. Pierwszy komponent nazwy DN jest nazywany względną nazwą wyróżniającą (RDN). Odróżnia pozycję od innych pozycji mających tę samą pozycję nadrzędną. W powyższych przykładach RDN "cn=Ben Gray" oddziela pierwszą pozycję od drugiej (z RDN "cn=Lucille White"). W przeciwnym przypadku te dwa przykłady nazw DN są równoważne. W pozycji musi także znajdować się para atrybut=wartość składająca się na RDN dla tej pozycji. (Nie jest to prawdą w przypadku innych komponentów DN).

Poniższe przykłady przedstawiają tworzenie pozycji dla osoby:

```
dn: cn=Tim Jones,o=ibm,c=us
objectclass: top
objectclass: person
cn: Tim Jones
sn: Jones
telephonenumber: 555-555-1234
```

## **Reguły używania znaków specjalnych w nazwach wyróżniających**

Niektóre znaki w nazwie DN mają specjalne znaczenie. Na przykład "=" (znak równości) oddziela nazwę atrybutu i wartość, a ",", (przecinek) oddziela parę atrybut=wartość. Znaki specjalne to: , (przecinek), = (znak równości), + (plus), < (mniejsze niż), > (większe niż), # (hash), ; (średnik), \ (ukośnik odwrotny) i " (cudzysłów, ASCII 34).

Znak specjalny można umieścić w wartości atrybutu, usuwając specjalne znaczenie. Aby te znaki specjalne lub inne znaki umieścić w wartości atrybutu w łańcuchu DN, należy użyć następujących metod:

1. Jeśli jest to znak specjalny, należy go poprzedzić ukośnikiem odwrotnym (`\` ASCII 92). Ten przykład przedstawia sposób użycia przecinka w nazwie organizacji:  
`CN=L. Eagle,O=Sue\, Grabbit and Runn,C=GB`  
 Ta metoda jest preferowana.
2. W przeciwnym razie należy zastąpić ten znak ukośnikiem odwrotnym i dwiema cyframi w kodzie szesnastkowym, które tworzą pojedynczy bajt kodu znaku. Kod znaku **musi** być w zestawie kodowym UTF-8.  
`CN=L. Eagle,O=Sue\2C Grabbit and Runn,C=GB`
3. Otocz całą wartość atrybutu cudzysłowami ("", ASCII 34), które nie będą traktowane jako część wartości. Między parą znaków cudzysłowu wszystkie znaki są traktowane tak, jak zostały wpisane, z wyjątkiem znaku \ (ukośnika odwrotnego). Znak \ (ukośnik odwrotny) można używać podczas korzystania ze znaków ukośnika odwrotnego (ASCII 92) lub znaków cudzysłowu (ASCII 34), wszystkich wspomnianych wcześniej znaków specjalnych lub par cyfr szesnastkowych, jak w przypadku metody 2. Na przykład, aby wprowadzić znak cudzysłowu w ciągu `cn=xyz"qrs"abc`, należy wpisać `cn=xyz\"qrs\"abc` lub w celu użycia znaku \:  
`"pojedynczy znak ukośnika odwrotnego należy wpisać w ten sposób \\"`  
 Inny przykład, `"\Zoo"` jest nieprawidłowy, ponieważ `Z` w tym kontekście nie wymaga użycia znaku ukośnika.

## Pseudo nazwy DN

Pseudo nazwy DN są używane w definicji kontroli dostępu i podczas wartościowania. Katalog LDAP obsługuje szereg pseudo nazw wyróżniających (na przykład "group:CN=THIS" i "access-id:CN=ANYBODY"), które odwołują się do dużej ilości nazw wyróżniających o wspólnych cechach charakterystycznych w odniesieniu do wykonywanej operacji lub obiektu, na którym operacja jest wykonywana.

Directory Server obsługuje trzy pseudo nazwy DN:

- access-id: CN=THIS

Podana jako część listy ACL, ta nazwa wyróżniająca odwołuje się do bindDN zgodnej z nazwą wyróżniająca, na której wykonywana jest operacja. Na przykład jeśli operacja jest wykonywana na obiekcie "cn=osobaA, ou=IBM, c=US", a bindDN to "cn=osobaA, ou=IBM, c=US", nadane uprawnienia są połączeniem uprawnień nadanych dla "CN=THIS" i dla "cn=osobaA, ou=IBM, c=US".

- group: CN=ANYBODY

Określona jako część listy ACL, ta nazwa wyróżniająca odwołuje się do wszystkich użytkowników, nawet tych, którzy nie zostali uwierzytelnieni. Użytkowników nie można usuwać z tej grupy, a tej grupy nie można usunąć z bazy danych.

- group: CN=AUTHENTICATED

Ta nazwa wyróżniająca odwołuje się do każdej nazwy wyróżniającej, która została uwierzytelniona przez katalog. Metoda uwierzytelniania nie jest brana pod uwagę.

**Uwaga:** "CN=AUTHENTICATED" odwołuje się do nazwy wyróżniającej uwierzytelnionej w dowolnym miejscu na serwerze, bez względu na miejsce, w którym znajduje się obiekt reprezentujący nazwę wyróżniająca. Jednak należy jej używać ostrożnie. Na przykład pod jednym przyrostkiem "cn=Secret" może znajdować się węzeł o nazwie "cn=Confidential Material", który ma pozycję aclentry "group:CN=AUTHENTICATED:normal:rsc". Pod innym przyrostkiem "cn=Common" może znajdować się węzeł "cn=Public Material". Jeśli te dwa drzewa znajdują się na tym samym serwerze, powiązanie z "cn=Public Material" będzie uważane za uwierzytelnione i uzyska uprawnienia do klasy normal w obiekcie "cn= Confidential Material".

Niektóre przykłady pseudo nazw DN:

### Przykład 1

Przyjmując następującą listę ACL dla obiektu: cn=osobaA, c=US

```
AclEntry: access-id: CN=THIS:critical:rwc
AclEntry: group: CN=ANYBODY: normal:rsc
AclEntry: group: CN=AUTHENTICATED: sensitive:rsc
```



Użytkownik powiązany jako	Otrzyma
cn=osobaA, c=US	normal:rsc:sensitive:rcs:critical:rwsc
cn=osobaB, c=US	normal:rsc:sensitive:rsc
Anonimowy	normal:rsc

W tym przykładzie osobaA przyjmuje uprawnienia nadane identyfikatorowi "CN=THIS" i uprawnienia nadane pseudo grupom nazw wyróżniających zarówno "CN=ANYBODY", jak i "CN=AUTHENTICATED".

## Przykład 2

Przyjmując następującą listę ACL dla obiektu: cn=osobaA, c=US AclEntry: access-id:cn=osobaA, c=US: object:ad

AclEntry: access-id: CN=THIS:critical:rwsc  
 AclEntry: group: CN=ANYBODY: normal:rsc  
 AclEntry: group: CN=AUTHENTICATED: sensitive:rcs

Dla operacji wykonywanej na cn=osobaA, c=US:

Użytkownik powiązany jako	Otrzyma
cn=osobaA, c=US	object:ad:critical:rwsc
cn=osobaB, c=US	normal:rsc:sensitive:rsc
Anonimowy	normal:rsc

W tym przykładzie osobaA przyjmuje uprawnienia nadane identyfikatorowi "CN=THIS" oraz te nadane nazwie wyróżniającej "cn=osobaA, c=US". Należy zauważyć, że uprawnienia grupy nie są nadawane, ponieważ istnieje bardziej szczegółowa pozycja aclentry ("access-id:cn=osobaA, c=US") dla nazwy wyróżniającej łączenia ("cn=osobaA, c=US").

## Rozszerzone przetwarzanie DN

Złożona nazwa RDN nazwy wyróżniającej może składać się z wielu komponentów połączonych operatorami '+'. W serwerze rozszerzono obsługę wyszukiwania pozycji o takiej nazwie DN. Złożoną nazwę RDN można określić w dowolnej kolejności jako podstawę dla operacji wyszukiwania.

```
ldapsearch -b "cn=mike+ou=austin,o=ibm,c=us" "(objectclass=*)"
```

Serwer obsługuje rozszerzoną operację normalizacji nazwy wyróżniającej. Rozszerzone operacje normalizacji nazwy wyróżniającej normalizują nazwy wyróżniające, używając schematu serwera. Rozszerzona operacja może być przydatna dla aplikacji korzystających z nazw wyróżniających.

## Składnia nazwy wyróżniającej

Formalna składnia nazwy wyróżniającej opiera się na standardzie RFC 2253. Składnia w notacji BNF (Backus Naur Form) jest następująca:

```
<nazwa> ::= <komponent_nazwy> ( <separator> )
          | <komponent_nazwy> <separator> <nazwa>

<separator> ::= <opcjonalna_spacja>
               <separator>
               <opcjonalna_spacja>

<separator> ::= ", " | "; "

<opcjonalna_spacja> ::= ( <CR> ) *( " " )

<komponent_nazwy> ::= <atrybut>
                    | <atrybut> <opcjonalna_spacja> "+"
                    <opcjonalna_spacja> <komponent_nazwy>
```

```

<atrybut> ::= <łańcuch>
           | <klucz> <opcjonalna_spacja> "=" <opcjonalna_spacja> <łańcuch>

<klucz> ::= 1*( <znak_klucza> ) | "OID." <oid> | "oid." <oid>
<znak_klucza> ::= litery, cyfry i spacja

<oid> ::= <łańcuch_cyfr> | <łańcuch_cyfr> "." <oid>
<łańcuch_cyfr> ::= 1*<cyfra>
<cyfra> ::= cyfry 0-9

<łańcuch> ::= *( <znak_łańcucha> | <para> )
           | "'" *( <znak_łańcucha> | <specjalny> | <para> ) "'"
           | "#" <wartość_szesnastkowa>

<specjalny> ::= "," | "=" | <CR> | "+" | "<" | ">"
             | "#" | ";"

<para> ::= "\" ( <specjalny> | "\" | "'" )
<znak_łańcucha> ::= dowolny znak z wyjątkiem <specjalnego>, "\" lub "'"

<wartość_szesnastkowa> ::= 2*<znak_szesnastkowy>
<znak_szesnastkowy> ::= 0-9, a-f, A-F

```

Znaku średnika (;) można używać do oddzielania nazw RDN w nazwach wyróżniających, choć w takich przypadkach używa się zwykle przecinka (,).

Obok przecinka lub średnika mogą występować znaki niewidoczne (spacje). Znaki niewidoczne są ignorowane, a średnik jest zastępowany przecinkiem.

Poza tym spacje ( ' ' ASCII 32) mogą się znajdować przed znakami '+' i '=' lub po nich. Podczas analizowania są one ignorowane.

Poniższy przykład jest nazwą wyróżniającą zapisaną w notacji używanej w typowych formach nazw. Pierwsza jest nazwą zawierającą trzy komponenty. Pierwszy z elementów jest złożoną nazwą RDN. Złożona nazwa RDN zawiera wiele par atrybut:wartość i można jej używać do identyfikowania konkretnych pozycji w przypadkach, gdy prosta nazwa CN może być niejednoznaczna:

```
OU=Sales+CN=J. Smith,O=Widget Inc.,C=US
```

### Pojęcia pokrewne

“Katalogi” na stronie 4

Serwer Directory Server umożliwia dostęp do bazy danych specjalnego typu, w której informacje są zapisywane w strukturze hierarchicznej podobnej do organizacji zintegrowanego systemu plików systemu i5/OS.

“Bezpieczeństwo serwera Directory Server” na stronie 51

Informacje o funkcjach służących do zabezpieczania serwera Directory Server.

“Elementy sterujące i rozszerzone operacje” na stronie 93

Elementy sterujące i rozszerzone operacje umożliwiają zwiększanie możliwości protokołu LDAP bez jego modyfikowania.

## Przyrostek (kontekst nazwy)

Przyrostek (znany również jako kontekst nazwy) to nazwa DN identyfikująca najwyższą pozycję w lokalnej hierarchii katalogu.

Ze względu na schemat względnego nazewnictwa stosowany w LDAP ta nazwa DN jest także przyrostkiem każdej innej pozycji w ramach danej hierarchii katalogu. Serwer katalogów może mieć wiele przyrostków, reprezentujących lokalnie przechowywane hierarchie katalogu, np. o=ibm,c=us.

Pozycję zgodną z przyrostkiem należy dodać do katalogu. Tworzona pozycja musi używać klasy obiektu zawierającej używany atrybut nazewnictwa. Aby utworzyć pozycję odpowiadającą temu przyrostkowi, można użyć narzędzia Web Administration lub programu ldapadd dla interpretera Qshell.

Istnieje pojęcie globalnego obszaru nazw LDAP. Może on zawierać następujące nazwy DN:

- cn=John Smith,ou=Rochester,o=IBM
- cn=Jane Doe,o=My Company,c=US
- cn=system administrator,dc=myco,dc=com

Przyrostek "o=IBM" informuje serwer, że tylko pierwsza nazwa DN znajduje się w obszarze nazw obsługiwanych przez serwer. Próby odwołania do obiektów nienależących do jednego z przedrostków powodują wystąpienie błędu braku obiektu lub odwołanie do innego serwera katalogów.

Serwer Directory Server zawiera wiele przyrostków. Serwer Directory Server zawiera kilka predefiniowanych przedrostków określających dane specyficzne dla konkretnej implementacji:

- cn=schema zawiera reprezentację schematu dostępną przez LDAP
- cn=changelog przechowuje protokół zmian serwera, jeśli został włączony
- cn=localhost zawiera niereplikowane informacje sterujące niektórymi aspektami działania serwera, na przykład obiekty konfiguracji replikacji
- cn=IBMpolicies zawiera informacje o działaniu serwera, które *jest* replikowane
- cn=pwdpolicy zawiera strategię haseł dla całego serwera
- przyrostek "os400-sys=system-name.mydomain.com" zapewnia dostęp do obiektów systemu i5/OS za pośrednictwem protokołu LDAP, obecnie ograniczony do profili użytkowników i grup

Serwer Directory Server jest wstępnie skonfigurowany z domyślnym przyrostkiem dc=system-name,dc=domain-name, aby ułatwić rozpoczęcie pracy z serwerem. Używanie tego przyrostka nie jest konieczne. Można dodawać własne przyrostki i usunąć wstępnie skonfigurowany przyrostek.

Trzy konwencje nazewnictwa przyrostków są używane najczęściej. Jedna jest oparta na domenie TCP/IP organizacji. Druga jest oparta na nazwie i położeniu organizacji.

Na przykład dla domeny TCP/IP mojafirma.com można wybrać następujący przyrostek dc=mojafirma,dc=com, gdzie atrybut dc odnosi się do komponentu domeny. W tym przypadku najwyższa pozycja utworzona w katalogu może wyglądać następująco (używając LDIF, formatu pliku tekstowego do reprezentacji pozycji LDAP):

```
dn: dc=mojafirma,dc=com
objectclass: domain
dc: mojafirma
```

Klasa obiektu domain ma również atrybuty opcjonalne, których można użyć. Aby sprawdzić dodatkowe atrybuty, należy przejrzeć schemat lub przeprowadzić edycję utworzonej pozycji za pomocą narzędzia Web Administration.

Jeśli nazwą firmy jest Moja firma i znajduje się ona w Stanach Zjednoczonych, można wybrać przyrostek podobny do poniższego:

```
o=Moja firma
o=Moja firma,c=US
ou=Widget Division,o=Moja firma,c=US
```

Gdzie ou jest nazwą klasy obiektu organizationalUnit, o jest nazwą organizacji, a c jest standardowym dwukierunkowym skrótem kraju używanym w klasie obiektu kraju. W tym przypadku tworzona pozycja najwyższego poziomu może być następująca:

```
dn: o=Moja firma,c=US
objectclass: organization
o: Moja firma
```

Używane aplikacje mogą wymagać zdefiniowania konkretnych przyrostków lub korzystania z konkretnej konwencji nazewnictwa. Na przykład, jeśli katalog jest używany do zarządzania certyfikatami cyfrowymi, konieczne może być określenie struktury części katalogu, w której nazwy pozycji są zgodne z nazwami wyróżniającymi organizacji dla certyfikatów, które zawierają.

Pozycje dodawane do katalogu muszą mieć przyrostki zgodne z wartością nazwy DN, np. `ou=Marketing,o=ibm,c=us`. Jeśli zapytanie zawiera przyrostek, który nie jest zgodny z żadnym przyrostkiem skonfigurowanym w lokalnej bazie danych, przekazywane jest ono do serwera LDAP, który jest identyfikowany przez domyślne odwołanie. Jeśli nie określono żadnego domyślnego odwołania LDAP, zwracany jest rezultat informujący, że obiekt nie istnieje.

#### **Pojęcia pokrewne**

“Zadania związane z pozycjami katalogu” na stronie 195

Ten temat zawiera informacje dotyczące zarządzania pozycjami katalogu.

“Zadania związane ze schematem” na stronie 185

Ten temat zawiera informacje dotyczące zarządzania schematem.

#### **Zadania pokrewne**

“Dodawanie i usuwanie przyrostków serwera Directory Server” na stronie 124

W tym temacie opisano dodawanie i usuwanie przyrostków serwera Directory Server.

#### **Odsyłacze pokrewne**

“`ldapmodify` i `ldapadd`” na stronie 218

Programy narzędziowe wiersza komend służące do dodawania i modyfikowania pozycji w katalogu LDAP.

## **Schemat**

Schemat jest zestawem reguł określających sposób przechowywania danych w katalogu. Schemat definiuje typ dozwolonych pozycji oraz strukturę i składnię atrybutów.

Dane są przechowywane w katalogu za pomocą pozycji katalogu. Pozycja składa się z klasy obiektu, która jest wymagana, i jej atrybutów. Atrybuty mogą być wymagane lub opcjonalne. Klasa obiektu określa rodzaj informacji opisywanych przez pozycję i definiuje zestaw atrybutów, które zawiera. Każdy atrybut ma przynajmniej jedną przypisaną wartość.

Więcej informacji dotyczących schematu znajduje się w następujących sekcjach:

#### **Pojęcia pokrewne**

“Katalogi” na stronie 4

Serwer Directory Server umożliwia dostęp do bazy danych specjalnego typu, w której informacje są zapisywane w strukturze hierarchicznej podobnej do organizacji zintegrowanego systemu plików systemu i5/OS.

“Zadania związane z pozycjami katalogu” na stronie 195

Ten temat zawiera informacje dotyczące zarządzania pozycjami katalogu.

“Zadania związane ze schematem” na stronie 185

Ten temat zawiera informacje dotyczące zarządzania schematem.

## **Schemat serwera Directory Server**

Schemat serwera Directory Server jest predefiniowany, jednak można go zmienić zgodnie z dodatkowymi wymaganiami.

Serwer Directory Server obsługuje dynamiczne schematy. Schemat jest publikowany jako część danych katalogu i jest dostępny w pozycji podschematu (`DN="cn=schema"`). Można zadać zapytanie w schemacie, używając funkcji `API ldap_search()` i zmienić go, używając funkcji `ldap_modify()`.

Schemat zawiera więcej opcji konfiguracji, niż opisano w dokumencie LDAP Version 3 Request For Comments (RFC) oraz standardowych specyfikacjach. Na przykład dla danego atrybutu można określić, które indeksy mają być obsługiwane. Te dodatkowe informacje konfiguracyjne są obsługiwane w odpowiedniej pozycji podschematu. Dodatkowa klasa obiektu jest zdefiniowana dla pozycji podschematu `IBMSubschema` zawierającej atrybuty `"MAY"`, w których znajdują się rozszerzone informacje na temat schematu.

Serwer Directory Server definiuje pojedynczy schemat dla całego serwera, dostępny dzięki specjalnej pozycji katalogu "cn=schema". Pozycja zawiera cały schemat zdefiniowany dla serwera. Aby pobrać dane schematu, można wywołać funkcję ldap\_search, używając:

```
DN: "cn=schema", search scope: base, filter: objectclass=subschema
lub objectclass=*
```

Schemat zawiera wartości następujących typów atrybutów:

- objectClass,
- attributeType,
- IBMAttributeType,
- reguł sprawdzania zgodności,
- składni poleceń LDAP.

Składnia tych definicji schematu jest oparta na standardzie RFC LDAP wersja 3.

Przykładowa pozycja schematu może zawierać:

```
objectclasses=( 1.3.6.1.4.1.1466.101.120.111
                NAME 'extensibleObject'
                SUP top AUXILIARY )

objectclasses=( 2.5.20.1
                NAME 'subschema'
                AUXILIARY MAY
                ( dITStructureRules
                  $ nameForms
                  $ ditContentRules
                  $ objectClasses
                  $ attributeTypes
                  $ matchingRules
                  $ matchingRuleUse ) )

objectclasses=( 2.5.6.1
                NAME 'alias'
                SUP top STRUCTURAL
                MUST aliasedObjectName )

attributeTypes=( 2.5.18.10
                 NAME 'subschemaSubentry'
                 EQUALITY distinguishedNameMatch
                 SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
                 NO-USER-MODIFICATION
                 SINGLE-VALUE USAGE directoryOperation )

attributeTypes=( 2.5.21.5 NAME 'attributeTypes'
                 EQUALITY objectIdentifierFirstComponentMatch
                 SYNTAX 1.3.6.1.4.1.1466.115.121.1.3
                 USAGE directoryOperation )

attributeTypes=( 2.5.21.6 NAME 'objectClasses'
                 EQUALITY objectIdentifierFirstComponentMatch
                 SYNTAX 1.3.6.1.4.1.1466.115.121.1.37
                 USAGE directoryOperation
                 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
                 USAGE directoryOperation )

ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.5 DESC 'Binary' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.7 DESC 'Boolean' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.12 DESC 'DN' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.15 DESC 'Directory String' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.24 DESC 'Generalized Time' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.26 DESC 'IA5 String' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.27 DESC 'INTEGER' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.50 DESC 'Telephone Number' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.53 DESC 'UTC Time' )
```

```

matchingRules=( 2.5.13.2 NAME 'caseIgnoreMatch'
                 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
matchingRules=( 2.5.13.0 NAME 'objectIdentifierMatch'
                 SYNTAX 1.3.6.1.4.1.1466.115.121.1.38 )
matchingRules=( 2.5.13.30 NAME 'objectIdentifierFirstComponentMatch'
                SYNTAX 1.3.6.1.4.1.1466.115.121.1.38 )
matchingRules=( 2.5.13.4 NAME 'caseIgnoreSubstringsMatch'
                SYNTAX 1.3.6.1.4.1.1466.115.121.1.58 )

```

Dane schematu można zmieniać za pomocą funkcji API ldap\_modify. Za pomocą nazwy wyróżniającej "cn=schema" można dodawać, usuwać lub zmieniać typ atrybutu lub klasę obiektu. Można również podać pełny opis. Dodając lub zastępując pozycję w schemacie można używać definicji LDAP wersji 3, definicji rozszerzenia atrybutu IBM lub obu rodzajów definicji.

### Pojęcia pokrewne

“Zadania związane ze schematem” na stronie 185

Ten temat zawiera informacje dotyczące zarządzania schematem.

Funkcje API protokołu LDAP

Temat Funkcje API protokołu LDAP zawiera więcej informacji o funkcjach API serwera katalogów.

“Klasy obiektu” na stronie 17

Klasa obiektu określa zbiór atrybutów używanych do opisanie obiektu.

“Atrybuty” na stronie 18

Każda pozycja katalogu ma zestaw atrybutów powiązanych z nią poprzez jej klasę obiektu.

### Odsyłacze pokrewne

“Atrybut IBMAttributeTypes” na stronie 20

Atrybutu IBMAttributeTypes można używać do definiowania danych schematu, które nie są ujęte w standardzie LDAP wersja 3 dla atrybutów.

“Reguły sprawdzania zgodności” na stronie 21

Reguła sprawdzania zgodności stanowi wytyczne do porównywania ciągów znaków podczas wyszukiwania.

“Składnia atrybutu” na stronie 24

Składnia atrybutu definiuje jego dozwolone wartości.

“Schemat dynamiczny” na stronie 27

Możliwe jest dynamiczne modyfikowanie schematu.

## Obsługa typowych schematów

Katalog IBM Directory obsługuje standardowy schemat katalogów.

Katalog IBM Directory obsługuje standardowy schemat katalogów zdefiniowany w następujących dokumentach:




- Dokumenty RFC grupy wykonawczej Internet Engineering Task Force (IETF) dotyczące protokołu LDAP w wersji 3, na przykład RFC 2252 i 2256.
- Model CIM (Common Information Model) grupy wykonawczej Desktop Management Task Force (DMTF).
- Schemat LIPS (Lightweight Internet Person Schema) konsorcjum Network Application Consortium.

Ta wersja LDAP obejmuje schemat zdefiniowany w LDAP w wersji 3 skonfigurowany domyślnie. Obejmuje również definicje schematów DEN.

IBM udostępnia także zestaw rozszerzonych wspólnych definicji schematu, których używają inne produkty IBM, kiedy korzystają z katalogu LDAP. Obejmują one:

- Obiekty dla aplikacji raportowania, takich jak osoba, grupa, kraj, jednostka organizacyjna i rola, położenie, województwo itd.
- Obiekty dla innych podsystemów, takie jak konta, usługi i punkty dostępu, autoryzacja, uwierzytelnianie, strategia bezpieczeństwa itd.

### Informacje pokrewne

-  Internet Engineering Task Force (IETF)
-  Desktop Management Task Force (DMTF)
-  Network Application Consortium

## Klasy obiektu

Klasa obiektu określa zbiór atrybutów używanych do opisanego obiektu.

Na przykład, gdyby utworzyć klasę obiektu **tymczPracownik**, mogłaby ona zawierać atrybuty skojarzone z tymczasowo zatrudnionym pracownikiem, takie jak **identyfikator**, **dataZatrudnienia** lub **długośćPrzypisania**. Można dodawać własne klasy obiektu w celu dostosowania katalogu do wymagań własnej organizacji. IBM Directory Server udostępnia kilka podstawowych typów klas obiektu, takich jak:

- Grupy
- Położenia
- Organizacje
- Osoby

**Uwaga:** Klasy obiektu specyficzne dla serwera Directory Server mają przedrostek 'ibm-'.

Klasy obiektu są definiowane na podstawie charakterystyki typu, dziedziczenia i atrybutów.

## Typ klasy obiektu

Klasa obiektu może być w jednym z trzech typów:

### Strukturalna:

Każda pozycja musi należeć do jednej i tylko jednej klasy obiektu, która definiuje podstawową zawartość pozycji. Ta klasa obiektu przedstawia rzeczywisty obiekt. Ponieważ wszystkie pozycje muszą należeć do strukturalnej klasy obiektu, jest to najbardziej powszechny typ klasy obiektu.

### Abstrakcyjna:

Ten typ jest używany jako klasa nadrzędna lub szablon dla innych (strukturalnych) klas obiektu. Definiuje zestaw atrybutów wspólnych dla zestawu strukturalnych klas obiektu. Te klasy obiektu, jeśli zostały zdefiniowane jako klasy podrzędne względem klasy abstrakcyjnej, dziedziczą zdefiniowane atrybuty. Atrybutów nie trzeba definiować dla każdej podrzędnej klasy obiektu.

### Pomocnicza:

Ten typ określa dodatkowe atrybuty, które można powiązać z pozycją należącą do konkretnej strukturalnej klasy obiektu. Mimo iż pozycja może należeć tylko do jednej strukturalnej klasy obiektu, to może należeć do wielu pomocniczych klas obiektu.

## Dziedziczenie klasy obiektu

Ta wersja serwera Directory Server obsługuje dziedziczenie klas obiektu i definicji atrybutów. Nową klasę obiektu można zdefiniować w oparciu o klasy nadrzędne (wielokrotne dziedziczenie) i dodatkowe lub zmienione atrybuty.

Każda pozycja jest przypisana do pojedynczej strukturalnej klasy obiektu. Wszystkie klasy obiektu dziedziczą atrybuty z abstrakcyjnej klasy obiektu **top**. Mogą również dziedziczyć z innych klas obiektu. Struktura klasy obiektu określa listę wymaganych i dozwolonych atrybutów dla konkretnej pozycji. Dziedziczenie klas obiektu zależy od kolejności definicji klas obiektu. Klasa obiektu może dziedziczyć tylko z klas obiektu, które ją poprzedzają. Na przykład struktura klasy obiektu dla pozycji osoby może być zdefiniowana w pliku LDIF w następujących sposób:

```
objectClass: top
objectClass: person
objectClass: organizationalPerson
```

W tej strukturze klasa `organizationalPerson` dziedziczy z klas obiektu `person` i `top`, a klasa obiektu `person` dziedziczy tylko z klasy obiektu `top`. Dlatego podczas przypisywania klasy obiektu `organizationalPerson` do pozycji automatycznie dziedziczy ona wymagane i dozwolone atrybuty z nadrzędnej klasy obiektu (w tym przypadku klasy obiektu `person`).

Operacje aktualizacji schematu są przed dalszym przetwarzaniem i zatwierdzeniem sprawdzane pod kątem spójności z hierarchią klas schematów.

## Atrybuty

Każda klasa obiektu zawiera pewną ilość atrybutów wymaganych i opcjonalnych. Atrybuty wymagane to atrybuty, które muszą być obecne w pozycjach używających danej klasy obiektu. Atrybuty opcjonalne to atrybuty, które mogą być obecne w pozycjach używających danej klasy obiektu.

## Atrybuty

Każda pozycja katalogu ma zestaw atrybutów powiązanych z nią poprzez jej klasę obiektu.

Klasa obiektu opisuje typ informacji zawartych w pozycji, natomiast rzeczywiste dane znajdują się w atrybucie. Atrybutowi odpowiada jedna lub kilka par nazwa-wartość zawierających konkretny element danych, taki jak nazwisko, adres czy numer telefonu. Serwer Directory Server odzwierciedla dane jako pary nazwa-wartość, atrybut opisowy, taki jak `commonName (cn)` i konkretne informacje, takie jak Jan Kowalski.

Na przykład pozycja Jan Kowalski może zawierać szereg par nazwa-wartość atrybutu.

```
dn: uid=jkowalski, ou=people, ou=mycompany, c=us
objectClass: top
objectClass: person
objectClass: organizationalPerson
cn: Jan Kowalski
sn: Kowalski
givenName: Jan
givenName: Jan
```

Jeśli standardowe atrybuty są już zdefiniowane w schemacie, można tworzyć, edytować, kopiować lub usuwać definicje atrybutów, tak aby odpowiadały potrzebom danej organizacji.

Więcej informacji zawierają następujące tematy:

### Typowe elementy podschematu:

Elementy używane są do definiowania gramatyki wartości atrybutów podschematu.

Poniższe elementy są używane do definiowania gramatyki wartości atrybutów podschematu:

- `alpha = 'a' - 'z', 'A' - 'Z'`
- `number = '0' - '9'`
- `anh = alpha / number / '-' / ','`
- `anhstring = 1 * anh`
- `keystring = alpha [ anhstring ]`
- `numericstring = 1 * number`
- `oid = descr / numericoid`
- `descr = keystring`
- `numericoid = numericstring * ( "." numericstring )`
- `woid = whsp oid whsp ;` zestaw identyfikatorów `oid` w dowolnej formie (numerycznej lub nazwy)
- `oids = woid / ( "(" oidlist ")" )`
- `oidlist = woid * ( "$" woid ) ;` deskryptory obiektów używane jako nazwy elementów schematu
- `qdescrs = qdescr / ( whsp "(" qdescrlist ")" whsp )`



- qdescrlist = [ qdescr \*( qdescr ) ]
- whsp "" descr "" whsp

### Atrybut objectclass:

Atrybut objectclasses zawiera listę klas obiektu obsługiwanych przez serwer.

Każda wartość tego atrybutu przedstawia osobną definicję klasy obiektu. Definicje klas obiektu można dodawać, usuwać lub zmieniać poprzez odpowiednie modyfikacje atrybutu objectclasses pozycji cn=schema. Wartości atrybutu objectclasses mają następującą gramatykę, zdefiniowaną w dokumencie RFC 2252:

```
ObjectClassDescription = "(" whsp
    numericoid whsp ; identyfikator Objectclass
    [ "NAME" qdescrs ]
    [ "DESC" qdstring ]
    [ "OBSOLETE" whsp ]
    [ "SUP" oids ] ; nadrzędne objectclasses
    [ ( "ABSTRACT" / "STRUCTURAL" / "AUXILIARY" ) whsp ] ; domyślną jest strukturalna
    [ "MUST" oids ] ; AttributeTypes
    [ "MAY" oids ] ; AttributeTypes
    whsp ")"
```

Na przykład definicją klasy obiektu person jest:

```
( 2.5.6.6 NAME 'person' DESC 'Definiuje pozycje przedstawiające osoby.' STRUCTURAL SUP top MUST (
cn $ sn ) MAY ( userPassword $ telephoneNumber $ seeAlso $ description ) )
```

- Identyfikatorem OID dla tej klasy jest 2.5.6.6
- Nazwą jest "person"
- Jest to strukturalna klasa obiektu
- Dziedziczy ona z klasy obiektu "top"
- Wymagane są następujące atrybuty: cn, sn
- Następujące atrybuty są opcjonalne: userPassword, telephoneNumber, seeAlso, description

### Pojęcia pokrewne

“Zadania związane ze schematem” na stronie 185

Ten temat zawiera informacje dotyczące zarządzania schematem.

### Atrybut attributetypes:

Atrybut attributetypes zawiera listę atrybutów obsługiwanych przez serwer.

każda wartość tego atrybutu przedstawia oddzielną definicję atrybutu. Definicje atrybutów można dodawać, usuwać lub zmieniać za pomocą odpowiednich zmian atrybutu attributetypes pozycji cn=schema. Wartości atrybutu attributetypes mają następującą gramatykę, zdefiniowaną w dokumencie RFC 2252:

```
AttributeTypeDescription = "(" whsp
    numericoid whsp ; identyfikator AttributeType
    [ "NAME" qdescrs ] ; nazwa używana w AttributeType
    [ "DESC" qdstring ] ; opis
    [ "OBSOLETE" whsp ]
    [ "SUP" woid ] ; określony na podstawie innego AttributeType
    [ "EQUALITY" woid ; nazwa reguły sprawdzania zgodności
    [ "ORDERING" woid ; nazwa reguły sprawdzania zgodności
    [ "SUBSTR" woid ] ; nazwa reguły sprawdzania zgodności
    [ "SYNTAX" whsp noidlen whsp ]
    [ "SINGLE-VALUE" whsp ] ; domyślnie wielowartościowa
    [ "COLLECTIVE" whsp ] ; domyślnie nie jest zbiorcza
    [ "NO-USER-MODIFICATION" whsp ] ; domyślnie modyfikowalny przez użytkownika
    [ "USAGE" whsp AttributeUsage ] ; domyślnie userApplications
    whsp ")"
```

```
AttributeUsage =
    "userApplications" /
    "directoryOperation" /
    "distributedOperation" / ; współużytkowana w DSA
    "dSAOperation" ; specyficzna dla DSA, wartość zależy od serwera
```

Reguły sprawdzania zgodności i wartości składni muszą być jedną z wartości, których definicję zawierają:

- “Reguły sprawdzania zgodności” na stronie 21
- “Składnia atrybutu” na stronie 24

W schemacie można definiować lub zmieniać tylko atrybuty "userApplications". Atrybuty "directoryOperation", "distributedOperation" i "dSAOperation" są definiowane przez serwer i mają konkretne znaczenie dla jego działania.

Na przykład atrybut "description" ma następującą definicję:

```
( 2.5.4.13 NAME 'description' DESC 'Atrybut typowy dla schematu CIM i LDAP określający długi opis pozycji
obiekту katalogu.' EQUALITY caseIgnoreMatch SUBSTR caseIgnoreSubstringsMatch SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 USAGE userApplications )
```

- Jego identyfikatorem OID jest 2.5.4.13
- Jego nazwą jest "description"
- Jego składnią jest 1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

#### Pojęcia pokrewne

“Zadania związane ze schematem” na stronie 185

Ten temat zawiera informacje dotyczące zarządzania schematem.

#### Atrybut IBMAttributeTypes:

Atrybutu IBMAttributeTypes można używać do definiowania danych schematu, które nie są ujęte w standardzie LDAP wersja 3 dla atrybutów.

Wartości IBMAttributeTypes muszą być zgodne z następującą gramatyką:

```
IBMAttributeTypesDescription = "(" whsp
    numericoid whsp
    [ "DBNAME" qdescrs ] ; maksymalnie 2 nazwy (tabela, kolumna)
    [ "ACCESS-CLASS" whsp IBMAccessClass whsp ]
    [ "LENGTH" wlen whsp ] ; maksymalna długość atrybutu
    [ "EQUALITY" [ IBMwlen ] whsp ] ; tworzy indeks dla reguły sprawdzania zgodności
    [ "ORDERING" [ IBMwlen ] whsp ] ; tworzy indeks dla reguły sprawdzania zgodności
    [ "APPROX" [ IBMwlen ] whsp ] ; tworzy indeks dla reguły sprawdzania zgodności
    [ "SUBSTR" [ IBMwlen ] whsp ] ; tworzy indeks dla reguły sprawdzania zgodności
    [ "REVERSE" [ IBMwlen ] whsp ] ; tworzy indeks dla reguły sprawdzania zgodności
    whsp ")"
```

```
IBMAccessClass =
    "NORMAL" / ; wartość domyślna
    "SENSITIVE" /
    "CRITICAL" /
    "RESTRICTED" /
    "SYSTEM" /
    "OBJECT"
```

```
IBMwlen = whsp len
```

#### Numericoid

Używany do korelacji wartości w attributetypes z wartością w IBMAttributeTypes.

#### DBNAME

Można podać maksymalnie 2 nazwy, jeśli w istocie dostępne są dwie nazwy. Pierwsza jest nazwą tabeli używaną dla tego atrybutu. Drugą jest nazwa kolumny używana dla w pełni znormalizowanej wartości

atrybutu w tabeli. Jeśli podano tylko jedną nazwę, służyć ona będzie jako nazwa tabeli i nazwa kolumny. Jeśli nie zostaną wprowadzone żadne nazwy DBNAME, użyta zostanie nazwa oparta na pierwszych 128 znakach nazwy atrybutu, która musi być unikalna. Nazwy tabel w bazie danych są obcinane do 128 znaków. Nazwy kolumn są obcinane do 30 znaków.

#### **ACCESS-CLASS**

Klasyfikacja dostępu dla tego typu atrybutów. Jeśli pominięto ACCESS-CLASS, domyślnym dostępem jest normal.

#### **LENGTH**

Maksymalna długość tego atrybutu. Długość jest wyrażana liczbą bajtów. Serwer Directory Server ma możliwość określania długości atrybutu. W wartości attributetypes łańcuch:

```
( attr-oid ... SYNTAX syntax-oid{len} ... )
```

może służyć do określenia, czy attributetype z oid attr-oid ma maksymalną długość.

#### **EQUALITY, ORDERING, APPROX, SUBSTR, REVERSE**

Jeśli używane są któreś z tych atrybutów, tworzony jest indeks dla odpowiedniej reguły sprawdzania zgodności. Opcjonalna długość określa szerokość indeksowanej kolumny. Pojedynczy indeks służy do zastosowania wielu reguł sprawdzania zgodności. Jeśli użytkownik nie podał długości, serwer Directory Server przypisuje długość 500. W uzasadnionych przypadkach serwer może również używać mniejszej długości niż zażądał użytkownik. Na przykład, gdy długość indeksu przekracza maksymalną wartość atrybutu, jest ona ignorowana.

#### **Reguły sprawdzania zgodności:**

Reguła sprawdzania zgodności stanowi wytyczne do porównywania ciągów znaków podczas wyszukiwania.

Reguły sprawdzania zgodności podzielono na trzy kategorie:

- Równość
- Uporządkowanie
- Podłańcuch

Serwer katalogów obsługuje dopasowanie równości dla wszystkich rodzajów składni poza binarną. W przypadku atrybutów zdefiniowanych za pomocą składni binarnej, serwer obsługuje jedynie wyszukiwanie wystąpienia, na przykład "(jpegphoto=\*)". W przypadku składni łańcucha IA5 oraz Directory String, definicja atrybutu może zostać podana później po dopasowaniu lub zignorowaniu wielkości liter. Na przykład, atrybut cn wykorzystuje regułę zgodności caseIgnoreMatch, co czyni wartości "Jan Kowalski" i "jan kowalski" równymi. W przypadku reguł ignorujących wielkość liter, porównanie odbywa się po dokonaniu konwersji wartości na wielkie litery. Algorytm wielkich liter nie rozpoznaje ustawień narodowych i może nie być poprawny dla wszystkich ustawień narodowych.

Serwer katalogów obsługuje dopasowanie podłańcucha dla atrybutów składni Directory String, IA5 String oraz Distinguished Name. Filtry wyszukiwania dla zgodności podłańcuchów używają znaku "\*", aby dopasować zero lub więcej znaków w łańcuchu. Na przykład, filtr wyszukiwania "(cn=\*smith)" uzgadnia wszystkie wartości cn zakończone łańcuchem "smith".

Serwer katalogów obsługuje dopasowanie podłańcucha dla atrybutów składni Directory String, łańcucha IA5 oraz nazwy wyróżniającej DN. W przypadku składni łańcucha uporządkowanie oparte jest na prostym porządkowaniu bajtów wartości łańcucha UTF-8. Jeśli atrybut został zdefiniowany za pomocą reguły zgodności ignorującej wielkość liter, porządkowanie dokonywane jest przy użyciu wielkich liter dla wartości łańcucha. Jak wspomniano wcześniej, algorytm wielkich liter może nie być poprawny dla wszystkich ustawień narodowych.

Na serwerze IBM Directory Server, zachowanie dopasowania podłańcuchów oraz porządkowania zaimplikowane jest przez regułę zgodności: wszystkie składnie obsługujące zgodność podłańcuchów mają zaimplikowaną regułę zgodności podłańcuchów, a wszystkie składnie obsługujące porządkowanie mają zaimplikowaną regułę porządkowania. W przypadku atrybutów zdefiniowanych za pomocą reguły zgodności ignorującej wielkość liter, zaimplikowane reguły zgodności podłańcuchów i porządkowania również ignorują wielkość liter.

Reguły sprawdzania zgodności oparte na równości		
Reguła sprawdzania zgodności	Identyfikator OID	Składnia
caseExactIA5Match	1.3.6.1.4.1.1466.109.114.1	Składnia Directory String
caseExactMatch	2.5.13.5 IA5	Składnia łańcucha
caseIgnoreIA5Match	1.3.6.1.4.1.1466.109.114.2	Składnia łańcucha IA5
caseIgnoreMatch	2.5.13.2	Składnia Directory String
distinguishedNameMatch	2.5.13.1	DN - nazwa wyróżniająca
generalizedTimeMatch	2.5.13.27	Format ogólny czasu
ibm-entryUuidMatch	1.3.18.0.2.22.2	Składnia Directory String
integerFirstComponentMatch	2.5.13.29	Składnia liczby całkowitej - liczba całkowita
integerMatch	2.5.13.14	Składnia liczby całkowitej - liczba całkowita
objectIdentifierFirstComponentMatch	2.5.13.30	Łańcuch zawierający identyfikatory OID. OID jest łańcuchem zawierającym cyfry (0-9) i kropki (.).
objectIdentifierMatch	2.5.13.0	Łańcuch zawierający identyfikatory OID. OID jest łańcuchem zawierającym cyfry (0-9) i kropki (.).
octetStringMatch	2.5.13.17	Składnia Directory String
telephoneNumberMatch	2.5.13.20	Składnia numeru telefonu
uTCTimeMatch	2.5.13.25	Format uniwersalny czasu

Reguły sprawdzania zgodności oparte na porządkowaniu		
Reguła sprawdzania zgodności	Identyfikator OID	Składnia
caseExactOrderingMatch	2.5.13.6	Składnia Directory String
caseIgnoreOrderingMatch	2.5.13.3	Składnia Directory String
distinguishedNameOrderingMatch	1.3.18.0.2.4.405	DN - nazwa wyróżniająca
generalizedTimeOrderingMatch	2.5.13.28	Format ogólny czasu

Reguły sprawdzania zgodności oparte na podłańcuchu		
Reguła sprawdzania zgodności	Identyfikator OID	Składnia
caseExactSubstringsMatch	2.5.13.7	Składnia Directory String
caseIgnoreSubstringsMatch	2.5.13.4	Składnia Directory String
telephoneNumberSubstringsMatch	2.5.13.21	Składnia numeru telefonu

**Uwaga:** UTC-Time jest formatem łańcucha czasu zdefiniowanym przez standardy ASN.1. Patrz ISO 8601 i X680. Składnia ta służy do przechowywania wartości czasu w formacie uniwersalnym.

#### Odsyłacze pokrewne

“Czas w formacie ogólnym i czas w formacie uniwersalnym” na stronie 33  
 Serwer Directory Server obsługuje format ogólny czasu i format uniwersalny czasu.

#### Reguły indeksowania:

Reguły indeksowania przypisane do atrybutów umożliwiają szybsze pobieranie informacji.

Jeśli podano tylko atrybut, indeksy nie są obsługiwane. Serwer Directory Server udostępnia następujące reguły indeksowania:

- Równość
- Uporządkowanie
- Przybliżenie
- Podłańcuch
- Uporządkowanie odwrotne

*Specyfikacje reguł indeksowania dla atrybutów:*

Zdefiniowanie reguły indeksowania dla atrybutu określa sposób tworzenia i obsługi indeksów specjalnych w wartościach atrybutów. Skraca to znacznie czas odpowiedzi na operacje wyszukiwania z filtrami obejmującymi te atrybuty.

Z operacjami zastosowanymi w filtrze wyszukiwania powiązanych jest pięć możliwych typów reguł indeksowania.

### **Równość**

Stosuje się do następujących operacji wyszukiwania:

- equalityMatch '='

Na przykład:

```
"cn = Jan Kowalski"
```

### **Uporządkowanie**

Stosuje się do następującej operacji wyszukiwania:

- greaterOrEqual '>='
- lessOrEqual '<='

Na przykład:

```
"sn >= Kowalski"
```

### **Przybliżenie**

Stosuje się do następującej operacji wyszukiwania:

- approxMatch '~='

Na przykład:

```
"sn ~= doe"
```

### **Podłańcuch**

Stosuje się do operacji wyszukiwania stosującej składnię podłańcuchów:

- substring '\*'

Na przykład:

```
"sn = McC*"
"cn = J*Doe"
```

### **Uporządkowanie odwrotne**

Stosuje się do następującej operacji wyszukiwania:

- '\*' substring

Na przykład:

```
"sn = *baugh"
```

Zaleca się, aby dla każdego atrybutu, który ma zostać użyty w filtrach wyszukiwania, została określona przynajmniej reguła indeksowania równości.

## Składnia atrybutu:

Składnia atrybutu definiuje jego dozwolone wartości.

Serwer używa definicji składni dla atrybutu w celu sprawdzenia danych i określenia sposobu dopasowania do wartości. Na przykład atrybut boolowski może przyjmować tylko wartości "TRUE" i "FALSE".

Atrybuty można definiować jako jednowartościowe i wielowartościowe. Atrybuty wielowartościowe nie są porządkowane, dlatego działanie aplikacji nie powinno zależeć od zwrócenia zestawu wartości dla danego atrybutu w konkretnej kolejności. Jeśli potrzebny jest uporządkowany zestaw wartości, należy rozważyć możliwość wstawienia listy wartości do pojedynczej wartości atrybutu:

```
preferences: 1-pref 2-pref 3-pref
```

Można też dołączyć do wartości informację o kolejności:

```
preferences: 2 yyy  
preferences: 1 xxx  
preferences: 3 zzz
```

Atrybuty wielowartościowe są przydatne w sytuacji, gdy pozycja ma wiele nazw. Na przykład cn (nazwa zwykła) ma wiele wartości. Pozycję można zdefiniować jako:

```
dn: cn=John Smith,o=My Company,c=US  
objectclass: inetorgperson  
sn: Smith  
cn: John Smith  
cn: Jack Smith  
cn: Johnny Smith
```

Dzięki temu operacje wyszukiwania John Smith i Jack Smith zwracają te same informacje.

Atrybuty binarne, na przykład fotografia w formacie JPEG, zawierają dowolny ciąg bajtów i nie można ich używać do wyszukiwania pozycji.

Atrybuty logiczne zawierają łańcuch TRUE lub FALSE.

Atrybuty nazw wyróżniających zawierają nazwy wyróżniające LDAP. Wartości nie muszą być nazwami wyróżniającymi istniejących pozycji, ale muszą mieć poprawną składnię nazwy wyróżniającej.

Atrybuty Directory String zawierają łańcuch tekstowy składający się ze znaków w kodzie UTF-8. Atrybut może rozpoznawać wielkość liter lub ją ignorować dla wartości używanych w filtrach wyszukiwania (na podstawie reguł zgodności definiowanych dla atrybutu), jednak wartość jest zawsze zwracana w takiej postaci, w jakiej została wprowadzona.

Atrybuty Generalized Time zawierają reprezentację daty i godziny obsługiwanej po roku 2000 przy użyciu czasu GMT z opcjonalnym przesunięciem zgodnie ze strefą czasową.

Atrybuty łańcucha IA5 zawierają łańcuchy tekstowe używane w zestawie znaków IA5 (7-bitowy kod US ASCII). Atrybut może rozpoznawać wielkość liter lub ją ignorować dla wartości używanych w filtrach wyszukiwania (na podstawie reguł zgodności definiowanych dla atrybutu), jednak wartość jest zawsze zwracana w takiej postaci, w jakiej została wprowadzona. Łańcuch IA5 umożliwia również używanie znaków zastępczych w wyszukiwaniu podłańcuchów.

Atrybuty całkowite zawierają wartość w postaci łańcucha tekstowego. Na przykład 0 lub 1000. Wartości atrybutów całkowitych muszą zawierać się w przedziale od 2147483648 do 2147483647.

Atrybuty numeru telefonu zawierają reprezentację tekstową numeru telefonu. Serwer Directory Server nie wymaga żadnej konkretnej składni tych wartości. Poniżej przedstawiono przykłady poprawnych wartości: (555)555-5555, 555.555.5555 i +1 43 555 555 5555.

Atrybuty czasu UTC używają wcześniejszego, nieobsługiwanego po roku 2000, formatu łańcucha do reprezentacji daty i czasu.

W schemacie katalogu, składnia atrybutu określona jest za pomocą identyfikatorów obiektów (OID) przypisanych do każdej składni. Poniższa tabela zawiera listę składni obsługiwanych przez serwer katalogów oraz ich identyfikatory OID.

Składnia	Identyfikator OID
Składnia opisu typu atrybutu	1.3.6.1.4.1.1466.115.121.1.3
Binarny - łańcuch oktetów	1.3.6.1.4.1.1466.115.121.1.5
Boolowski - TRUE/FALSE	1.3.6.1.4.1.1466.115.121.1.7
Składnia Directory String	1.3.6.1.4.1.1466.115.121.1.15
Składnia opisu reguły zawartości DIT	1.3.6.1.4.1.1466.115.121.1.16
Składnia opisu reguły DITStructure	1.3.6.1.4.1.1466.115.121.1.17
DN - nazwa wyróżniająca	1.3.6.1.4.1.1466.115.121.1.12
Format ogólny czasu	1.3.6.1.4.1.1466.115.121.1.24
Składnia łańcucha IA5	1.3.6.1.4.1.1466.115.121.1.26
Opis typu atrybutu IBM	1.3.18.0.2.8.1
Składnia liczby całkowitej - liczba całkowita	1.3.6.1.4.1.1466.115.121.1.27
Składnia opisu składni LDAP	1.3.6.1.4.1.1466.115.121.1.54
Opis reguły sprawdzania zgodności	1.3.6.1.4.1.1466.115.121.1.30
Opis użycia reguły sprawdzania zgodności	1.3.6.1.4.1.1466.115.121.1.31
Opis formularza nazwiska	1.3.6.1.4.1.1466.115.121.1.35
Składnia opisu klasy obiektu	1.3.6.1.4.1.1466.115.121.1.37
Łańcuch zawierający identyfikatory OID. OID jest łańcuchem zawierającym cyfry (0-9) i kropki (.).	1.3.6.1.4.1.1466.115.121.1.38
Składnia numeru telefonu	1.3.6.1.4.1.1466.115.121.1.50
Format uniwersalny czasu. UTC-Time jest formatem łańcucha czasu zdefiniowanym przez standardy ASN.1. Patrz ISO 8601 i X680. Składnia ta służy do przechowywania wartości czasu w formacie uniwersalnym.	1.3.6.1.4.1.1466.115.121.1.53

### Pojęcia pokrewne

“Identyfikator obiektu (OID)”

Identyfikator obiektu (OID) jest łańcuchem liczb dziesiętnych jednoznacznie określającym obiekt. Obiekty te są klasą obiektu lub atrybutem.

### Odsyłacze pokrewne

“Czas w formacie ogólnym i czas w formacie uniwersalnym” na stronie 33

Serwer Directory Server obsługuje format ogólny czasu i format uniwersalny czasu.

## Identyfikator obiektu (OID)

Identyfikator obiektu (OID) jest łańcuchem liczb dziesiętnych jednoznacznie określającym obiekt. Obiekty te są klasą obiektu lub atrybutem.

Jeśli brak identyfikatora OID, można określić klasę obiektu lub dodać nazwę atrybutu z końcówką **-oid**. Na przykład, jeśli tworzony jest atrybut tempID, OID można określić jako **tempID-oid**.

Absolutnie konieczne jest, aby prywatne identyfikatory OID były uzyskiwane od uprawnionych do tego instytucji. Dwie podstawowe strategie uzyskiwania legalnych identyfikatorów OID są następujące:

- Zarejestruj obiekty w uprawnionej instytucji. Ta strategia może być wygodna, jeśli na przykład wymagana jest mała liczba identyfikatorów OID.
- Uzyskaj arc (arc jest indywidualnym poddrzewem drzewa OID) od uprawnionej instytucji i przypisz własne identyfikatory OID. Ta strategia jest korzystniejsza, gdy potrzeba wielu identyfikatorów OID lub przypisania OID nie są stałe.

W Stanach Zjednoczonych uprawnienia dla nazw organizacji może rejestrować ANSI (American National Standards Institute) w ramach globalnych procedur rejestracji określonych przez ISO (International Standards Organization) i ITU (International Telecommunication Union). Więcej informacji na temat rejestrowania nazw organizacji zawiera serwis WWW instytutu ANSI ([www.ansi.org](http://www.ansi.org)). ANSI OID arc dla organizacji to 2.16.840.1. ANSI przypisuje numer (NEWNUM), tworząc nowy OID arc: 2.16.840.1.NEWNUM.

W większości krajów lub regionów rejestrowaniem identyfikatorów OID zajmują się krajowe organizacje określające standardy. Podobnie jak w przypadku ANSI arc, są to identyfikatory arc przypisywane pod OID 2.16. Znalezienie odpowiedniej instytucji uprawnionej do nadawania identyfikatorów OID w konkretnym kraju lub regionie może zająć trochę czasu. Krajowa organizacja określająca standardy w danym kraju lub regionie może być członkiem ISO. Nazwy i informacje kontaktowe członków organizacji ISO można znaleźć w serwisie WWW organizacji ISO ([www.iso.ch](http://www.iso.ch)).

IANA (Internet Assigned Numbers Authority) przypisuje numery przedsiębiorstw prywatnych, które są identyfikatorami OID w arc 1.3.6.1.4.1. IANA przypisze numer (NEWNUM), tak że nowym OID arc będzie 1.3.6.1.4.1.NEWNUM. Numery te można uzyskać z serwisu WWW organizacji IANA ([www.iana.org](http://www.iana.org)).

Po przypisaniu identyfikatora OID organizacja może zdefiniować własne identyfikatory OID, dodając je na końcu identyfikatora OID. Przypuśćmy na przykład, że organizacji przypisano fikcyjny OID 1.1.1. Żadnej innej organizacji nie zostanie przypisany OID zaczynający się od "1.1.1". Można utworzyć zakres dla LDAP, dodając ".1" i tworząc identyfikator 1.1.1.1. Później można go podzielić na zakresy dla klas obiektu (1.1.1.1.1), typów atrybutów (1.1.1.1.2) itd., a OID 1.1.1.1.2.34 przypisać do atrybutu "foo".

#### Informacje pokrewne

 [Serwis WWW ANSI](#)

 [Serwis WWW ISO](#)

 [Serwis WWW IANA](#)

## Pozycje podschematu

Dla każdego serwera istnieje jedna pozycja podschematu. Wszystkie pozycje w katalogu mają w domyśle typ atrybutu subschemaSubentry. Wartością typu atrybutu subschemaSubentry jest nazwa wyróżniająca pozycji podschematu odpowiadająca pozycji. Wszystkie pozycje na tym samym serwerze używają tej samej pozycji podschematu, a ich typ atrybutu subschemaSubentry ma tę samą wartość. Pozycja podschematu ma na stałe wpisaną nawet wyróżniającą 'cn=schema'.

Pozycja podschematu należy do klas obiektu 'top', 'subschemata' i 'IBMsubschemata'. Klasa obiektu 'IBMsubschemata' nie ma typów atrybutów MUST i jeden typ atrybutu MAY ('IBMattributeTypes').

## Klasa obiektu IBMsubschemata

Klasa obiektu IBMsubschemata jest specjalną klasą obiektu, która służy do składowania wszystkich atrybutów i klas obiektu dla danego serwera katalogów.

Klasa obiektu IBMsubschemata jest używana tylko w pozycji subschemata w następujący sposób:

```
( 1.3.18.0.2.6.174
NAME 'ibmSubSchema'
DESC 'Klasa obiektu IBM zawierająca wszystkie atrybuty i klasy obiektu dla danego serwera
katalogów.'
SUP 'subschemata'
STRUCTURAL MAY ( IBMAttributeTypes ) )
```



## Zapytania schematu

Funkcji API `ldap_search()` można używać do odpytywania pozycji podschematu.

Funkcji API `ldap_search()` można używać do odpytywania pozycji podschematu, jak to przedstawiono w poniższym przykładzie:

```
DN          : "cn=schema"
search scope : base
filter      : objectclass=subschema or objectclass=*
```

Ten przykład powoduje wczytanie pełnego schematu. Aby wczytać wszystkie wartości wybranego typu atrybutu, należy użyć parametru `attrs` funkcji `ldap_search`. Nie można wczytać konkretnej wartości wybranego typu atrybutu.

### Pojęcia pokrewne

Funkcje API protokołu LDAP

Temat Funkcje API protokołu LDAP zawiera więcej informacji o funkcjach API serwera katalogów.

## Schemat dynamiczny

Możliwe jest dynamiczne modyfikowanie schematu.

Aby przeprowadzić dynamiczną zmianę schematu, należy użyć funkcji API `ldap_modify` z nazwą wyróżniającą `"cn=schema"`. Można dodawać, usuwać lub zmieniać tylko jedną jednostkę schematu (na przykład typ atrybutu lub klasę obiektu).

Aby usunąć pozycję schematu, należy określić atrybut schematu definiujący pozycję schematu (`objectclasses` lub `attributetypes`), a jako wartość - OID w nawiasach. Na przykład, aby usunąć atrybut z identyfikatorem OID `<OID-atrybutu>`:

```
dn: cn=schema
changetype: modify
delete: attributetypes
attributetypes: ( <OID-atrybutu> )
```

Można również podać pełny opis. W każdym przypadku regułą sprawdzania zgodności, użytą do wyszukania jednostki schematu przeznaczonej do usunięcia, jest `objectIdentifierFirstComponentMatch`.

Aby dodać lub zmienić jednostkę schematu TRZEBA podać definicję LDAP wersja 3 i MOŻNA podać definicję IBM. We wszystkich przypadkach dozwolone jest podanie tylko tych definicji jednostki schematu, które mają ulec zmianie.

Na przykład, aby usunąć typ atrybutu `'cn'` (jego OID to 2.5.4.3), należy użyć funkcji `ldap_modify()` z:

```
LDAPMod attr;
LDAPMod *attrs[] = { &attr, NULL };
char *vals [] = { "( 2.5.4.3 )", NULL };
attr.mod_op = LDAP_MOD_DELETE;
attr.mod_type = "attributeTypes";
attr.mod_values = vals;
ldap_modify_s(ldap_session_handle, "cn=schema", attrs);
```

Aby dodać nowy pasek typu atrybutu z OID 20.20.20, który dziedziczy z atrybutu `"name"` i ma długość 20 znaków:

```
char *vals1[] = { "( 20.20.20 NAME 'bar' SUP name )" NULL };
char *vals2[] = { "( 20.20.20 LENGTH 20 )", NULL };
LDAPMod attr1;
LDAPMod attr2;
LDAPMod *attrs[] = { &attr1, &attr2, NULL };
attr1.mod_op = LDAP_MOD_ADD;
attr1.mod_type = "attributeTypes";
attr1.mod_values = vals1;
attr2.mod_op = LDAP_MOD_ADD;
attr2.mod_type = "IBMattributeTypes";
attr2.mod_values = vals2;
ldap_modify_s(ldap_session_handle, "cn=schema", attrs);
```

Wersją LDIF powyższego może być:

```
dn: cn=schema
changetype: modify
add: attributetypes
attributetypes: ( 20.20.20 NAME 'bar' SUP name )
-
add: ibmattributetypes
ibmattributetypes: (20.20.20 LENGTH 20)
```

## Prawa dostępu

Dynamiczne zmiany schematu może wykonać tylko serwer wysyłający replikacji lub administrator dla nazwy wyróżniającej.

## Replikacja

Po przeprowadzeniu dynamicznej zmiany schemat jest replikowany.

## Niedozwolone zmiany schematu

Nie wszystkie zmiany schematu są dozwolone.

Ograniczenia zmian są następujące:

- Wszystkie zmiany schematu muszą zachować jego spójność.
- Nie można usunąć typu atrybutu, który jest nadtypem innego typu atrybutu. Nie można usuwać typów atrybutów "MAY" ani "MUST" klasy obiektu.
- Nie można usuwać klasy obiektu będącej klasą nadrzędną.
- Nie można dodawać typów atrybutów lub klas obiektu odwołujących się do istniejących encji (na przykład składni lub klas obiektu).
- Nie można zmieniać typów atrybutów ani klas obiektu tak, aby odwoływały się do nieistniejących encji (na przykład składni lub klas obiektu).
- Nowe atrybuty nie mogą wykorzystywać tabel bazy danych w definicji IBMAttributetype.
- Nie można usuwać atrybutów używanych w dowolnych istniejących pozycjach katalogu.
- Nie można zmieniać długości oraz składni atrybutu.
- Nie można zmieniać tabeli bazy danych oraz kolumny przypisanej do atrybutu.
- Nie można usuwać atrybutów używanych w definicjach istniejących klas obiektu.
- Nie można usuwać klas obiektu używanych w dowolnych istniejących pozycjach katalogu.

| Kolumnę można zwiększyć, modyfikując schemat. Umożliwia to zwiększenie maksymalnej długości atrybutów  
| poprzez modyfikację schematu za pomocą narzędzi Web Administration lub ldapmodify.

Zmiany w schemacie mające wpływ na działanie serwera są niedozwolone. Poniższe definicje schematu są wymagane przez serwer katalogów. Nie wolno ich zmieniać.

### Klasy obiektu:

- accessGroup
- accessRole
- alias
- os400-usrprf
- referral
- replicaObject
- top

### Atrybuty:

- aclEntry
- aclPropagate
- aclSource
- aliasedObjectName, aliasedentryName
- businessCategory
- cn, commonName
- createTimestamp
- creatorsName
- description
- dn, distinguishedName
- entryOwner
- hasSubordinates
- ibm-entryChecksum
- ibm-entryChecksumOp
- ibm-entryUuid
- member
- modifiersName
- modifyTimestamp
- name
- o, organizationName, organization
- objectClass
- os400-acgcde
- os400-astlvl
- os400-atnpgm
- os400-audlvl
- os400-aut
- os400-ccsid
- os400-chridctl
- os400-cntryid
- os400-curlib
- os400-dlvry
- os400-docpwd
- os400-dspsgninf
- os400-eimassoc
- os400-gid
- os400-groupmember
- os400-grpaut
- os400-grpauttyp
- os400-grpprf
- os400-homedir
- os400-IaspStorageInformation
- os400-inlmnu
- os400-inlpgm
- os400-invalidSignonCount
- os400-jobd

- os400-kbdbuf
- os400-langid
- os400-lclpwmgt
- os400-lmtcpb
- os400-lmtdevssn
- os400-locale
- os400-maxstg
- os400-msgq
- os400-objaud
- os400-outq
- os400-owner
- os400-password
- os400-passwordExpirationDate
- os400-passwordLastChanged
- os400-previousSignon
- os400-profile
- os400-prtdev
- os400-ptylmt
- os400-pwdexp
- os400-pwdexpitv
- os400-setjobatr
- os400-sev
- os400-spcaut
- os400-spcenv
- os400-srtseq
- os400-status
- os400-storageUsed
- os400-storageUsedOnIasp
- os400-supgrpprf
- os400-sys os400-text
- os400-uid
- os400-usrcls
- os400-usropt
- ou, organizationalUnit, organizationalUnitName
- owner
- ownerPropagate
- ownerSource
- ref
- replicaBindDN
- replicaBindMethod
- replicaCredentials, replicaBindCredentials
- replicaHost
- replicaPort
- replicaUpdateTimeInterval
- replicaUseSSL

- seeAlso

**Składnie:**

Wszystkie

**Reguły sprawdzania zgodności:**

Wszystkie

## Sprawdzanie schematu

Po zainicjowaniu serwera pliki schematu są odczytywane oraz sprawdzana jest ich spójność i poprawność.

Jeśli sprawdzanie zakończy się niepowodzeniem, serwer nie zostanie zainicjowany i wysłany zostanie komunikat o błędzie. Podczas dynamicznej zmiany schematu wynikowy schemat również jest sprawdzany pod względem spójności i poprawności. Jeśli sprawdzanie zakończy się niepowodzeniem, zwracany jest błąd i zmiany nie zostaną wprowadzone. Niektóre sprawdzenia są częścią gramatyki (na przykład typ atrybutu może zawierać tylko jeden typ nadrzędny lub klasa obiektu może zawierać dowolną liczbę klas nadrzędnych).

W poniższych pozycjach sprawdzane są typy atrybutów:

- Dwa różne typy atrybutu nie mogą mieć tej samej nazwy lub identyfikatora OID.
- Hierarchia dziedziczenia typów atrybutów nie zawiera cykli.
- Należy również zdefiniować typ nadrzędny atrybutu, choć jego definicja może być wyświetlona później lub w oddzielnym pliku.
- Jeśli typ atrybutu jest podtypem innego, oba mają taki sam atrybut USAGE.
- Wszystkie typy atrybutów mają składnię definiowaną bezpośrednio lub dziedziczoną.
- Tylko atrybuty operacyjne można oznaczyć jako NO-USER-MODIFICATION.

W poniższych pozycjach sprawdzane są klasy obiektu:

- Dwie różne klasy obiektu nie mogą mieć tej samej nazwy lub identyfikatora OID.
- Hierarchia dziedziczenia klas obiektu nie zawiera cykli.
- Należy również zdefiniować klasy nadrzędne klasy obiektu, choć ich definicja może być wyświetlona później lub w oddzielnym pliku.
- Należy również zdefiniować typy atrybutów "MUST" i "MAY" klasy obiektu, choć ich definicja może być wyświetlona później lub w oddzielnym pliku.
- Każda strukturalna klasa obiektu jest bezpośrednią lub pośrednią podklasą klasy top.
- Jeśli abstrakcyjna klasa obiektu zawiera klasy nadrzędne, również one muszą być abstrakcyjne.

## Sprawdzanie pozycji w schemacie

Po dodaniu lub zmodyfikowaniu pozycji za pomocą operacji LDAP jest ona sprawdzana pod kątem schematu. Domyślnie wykonywane są wszystkie testy wymienione w tej sekcji. Jednakże niektóre operacje sprawdzania schematu można wyłączyć, zmieniając poziom sprawdzania schematu. Robi się to za pomocą programu System i Navigator, zmieniając wartość pola **Sprawdzanie schematu** (Schema checking) na stronie **Bazy danych/przyrostki** (Database/Suffixes) właściwości serwera Directory Server.

Aby pozycja była zgodna ze schematem, sprawdzane są następujące warunki:

**Względem klas obiektu:**

- Musi zawierać przynajmniej jedną wartość typu atrybutu "objectClass".
- Może zawierać dowolną liczbę pomocniczych klas obiektu zawierających, również zero. To nie jest test, tylko wyjaśnienie. Nie można go wyłączyć.
- Może zawierać dowolną liczbę abstrakcyjnych klas obiektu, ale tylko w wyniku dziedziczenia klas. Oznacza to, że każda abstrakcyjna klasa obiektu należąca do pozycji jest również strukturalną lub pomocniczą klasą obiektu dziedziczącą bezpośrednio lub pośrednio z tej abstrakcyjnej klasy obiektu.
- Musi mieć przynajmniej jedną strukturalną klasę obiektu.

- Musi mieć dokładnie jedną bezpośrednią lub podstawową strukturalną klasę obiektu. Innymi słowy, wszystkie strukturalne klasy obiektu dla tej pozycji muszą być klasami nadrzędnymi dokładnie jednej z nich. Bezpośrednio pochodna klasa obiektu jest nazywana "bezpośrednią" lub "podstawową strukturalną" klasą obiektu pozycji lub zwyczajnie "strukturalną" klasą obiektu pozycji.
- Nie można zmieniać bezpośredniej strukturalnej klasy obiektu tej pozycji (w ldap\_modify).
- Dla każdej klasy obiektu dla tej pozycji obliczany jest zestaw wszystkich bezpośrednich i pośrednich klas nadrzędnych. Jeśli jedna z nich nie została określona w pozycji, to jest automatycznie dodawana.
- Jeśli poziom sprawdzania schematu jest ustawiony na **Version 3 (strict)** należy podać wszystkie strukturalne klasy obiektu. Na przykład, aby utworzyć pozycję z klasą obiektu inetorgperson, należy określić następujące klasy obiektu: person, organizationalperson i inetorgperson.

#### **Poprawność typów atrybutów dla pozycji jest określana w następujący sposób:**

- Zestaw typów atrybutu MUST dla pozycji jest obliczony jako unia zestawów typów atrybutu MUST wszystkich jego klas obiektu, włącznie z dziedziczonymi domyślnie klasami obiektu. Jeśli zestaw typów atrybutów MUST dla pozycji nie jest podzestawem zestawu typów atrybutów zawartego w pozycji, pozycja jest odrzucana.
- Zestaw typów atrybutu MAY dla pozycji jest obliczony jako unia zestawów typów atrybutu MAY wszystkich jego klas obiektu, włącznie z dziedziczonymi domyślnie klasami obiektu. Jeśli zestaw typów atrybutów zawartych w pozycji nie jest podzestawem unii zestawów typów atrybutów MUST i MAY dla pozycji, pozycja jest odrzucana.
- Jeśli każdy typ atrybutu zdefiniowany dla pozycji jest zaznaczony jako NO-USER-MODIFICATION, pozycja jest odrzucana.

#### **Poprawność wartości typów atrybutów dla pozycji jest określana w następujący sposób:**

- Dla każdego typu atrybutu w pozycji, jeśli jest on jednowartościowy i pozycja zawiera wiele wartości, pozycja jest odrzucana.
- Dla każdej wartości każdego typu atrybutu w pozycji, jeśli składnia nie odpowiada procedurze kontroli składni tego atrybutu, pozycja jest odrzucana.
- Dla każdej wartości każdego typu atrybutu w pozycji, jeśli długość jest większa niż maksymalna długość przypisana do tego atrybutu, pozycja jest odrzucana.

#### **Poprawność nawy wyróżniającej jest sprawdzana w następujący sposób:**

- Składnia jest sprawdzana pod kątem zgodności z BNF dla DistinguishedNames. Jeśli jej nie odpowiada, pozycja jest odrzucana.
- Sprawdzane jest, czy nazwa RDN składa się tylko z typów atrybutów poprawnych dla tej pozycji.
- Sprawdzane jest, czy wartości typów atrybutów używane w nazwie RDN występują w pozycji.

#### **Pojęcia pokrewne**

"Schemat konfiguracji serwera Directory Server" na stronie 258

W tych informacjach opisano drzewo informacji katalogu (Directory Information Tree - DIT) oraz atrybuty używane do konfigurowania pliku ibmslapd.conf.

## **Zgodność z iPlanet**

Analizator składni używany przez serwer Directory Server pozwala, aby wartości atrybutów typów atrybutów schematu (objectClasses i attributeTypes) były określane za pomocą gramatyki iPlanet.

Na przykład atrybuty descr i numeric-oid można określić cudzysłowach (tak jakby były qdescr). Jednakże informacje schematu są zawsze udostępniane poprzez funkcję ldap\_search. Natychmiast po pojedynczej dynamicznej zmianie (za pomocą funkcji ldap\_modify) przeprowadzonej na wartości atrybutu w pliku cały plik jest zastępowany przez plik, w którym wszystkie wartości atrybutów są zgodne ze specyfikacją serwera Directory Server. Ponieważ analizator składni używany w plikach i żądaniach ldap\_modify jest taki sam, funkcje ldap\_modify używające gramatyki iPlanet dla wartości atrybutów są również obsługiwane poprawnie.

Jeśli utworzono zapytanie o pozycję schematu podrzędnego serwera iPlanet, pozycja wynikowa może zawierać wiele wartości dla jednego identyfikatora OID. Na przykład, jeśli konkretny typ atrybutu ma dwie nazwy (na przykład 'cn' i

'commonName'), opis tego typu atrybutu jest podawany dwa razy. Serwer Directory Server może przeanalizować schemat, w którym opis pojedynczego typu atrybutu lub klasy obiektu występuje kilka razy z tym samym opisem (z wyjątkiem NAME i DESC). Jednakże, gdy serwer Directory Server publikuje schemat, to udostępnia jeden opis takiego typu atrybutu ze wszystkimi wymienionymi nazwami (począwszy od skróconej). Oto przykład sposobu, w jaki iPlanet opisuje atrybuty typowej nazwy:

```
( 2.5.4.3 NAME 'cn'  
  DESC 'Atrybut standardowy'  
  SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )  
  
( 2.5.4.3 NAME 'commonName'  
  DESC 'Atrybut standardowy, alias dla cn'  
  SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )
```

Oto jak opisuje to serwer Directory Server:

```
( 2.5.4.3 NAME ( 'cn' 'commonName' ) SUP name )
```

Serwer Directory Server obsługuje podtypy. Jeśli 'cn' nie ma być podtypem nazwy (różniące się od standardowej), można zadeklarować:

```
( 2.5.4.3 NAME ( 'cn' 'commonName' )  
  DESC 'Atrybut standardowy'  
  SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )
```

Pierwsza nazwa ('cn') jest nazwą preferowaną lub skróconą, a wszystkie pozostałe nazwy po 'cn' są nazwami alternatywnymi. Z tego punktu łańcuchy '2.3.4.3', 'cn' i 'commonName' (jak również ich odpowiedniki bez rozróżniania wielkości liter) mogą być używane zamiennie w schemacie lub w pozycjach dodawanych do katalogu.

## **Czas w formacie ogólnym i czas w formacie uniwersalnym**

Serwer Directory Server obsługuje format ogólny czasu i format uniwersalny czasu.

Istnieją różne sposoby zapisu daty i czasu. Na przykład dzień czwartego lutego 1999 roku można zapisać:

```
2/4/99  
4/2/99  
99/2/4  
4.2.1999  
04-FEB-1999
```

oraz na wiele innych sposobów.

Serwer Directory Server ujednocila reprezentację czasu, wymagając, aby serwery LDAP obsługiwały dwa formaty:

- Format ogólny czasu, który ma postać:

```
RRRRMMDDGGMMSS[. | ,ułamek] [(+|-GGMM) |Z]
```

Są to 4 cyfry oznaczające rok, po 2 oznaczające miesiąc, dzień, godzinę, minutę i sekundę oraz opcjonalny ułamek sekund. Bez żadnych dodatkowych informacji zakłada się, że czas jest lokalny. Aby określić, że jest to czas uniwersalny, należy na końcu dodać wielką literę Z. W przeciwnym razie należy podać różnicę pomiędzy czasem uniwersalnym a lokalnym. Na przykład:

```
"19991106210627.3"
```

w czasie lokalnym oznacza 6 minut, 27,3 sekundy po godzinie 21 dnia 6 listopada 1999.

```
"19991106210627.3Z"
```

określa czas uniwersalny.

```
"19991106210627.3-0500"
```

oznacza czas lokalny w pierwszym przykładzie z różnicą pięciu godzin w porównaniu z czasem uniwersalnym.

Jeśli określono opcjonalny ułamek sekund, kropka lub przecinek są wymagane. W przypadku różnicy czasu lokalnego wartość określającą godzinę i minuty należy poprzedzić znakiem '+' lub '-'.

- Format uniwersalny czasu, który ma postać:

```
RRMMDDGGMM[SS] [(+ | -)GGMM] |Z]
```

Po dwie cyfry oznaczające rok, miesiąc, dzień, godzinę, minuty i opcjonalnie sekundy. Podobnie jak w formacie ogólnym czasu, można określić opcjonalną różnicę czasu. Na przykład, jeśli w czasie lokalnym jest godzina 7 rano dnia 2 stycznia 1999, a w czasie uniwersalnym jest godzina 12:00 w południe dnia 2 stycznia 1999, wartością UTCTime jest:

```
"9901021200Z"
```

lub

```
"9901020700-0500"
```

Jeśli w czasie lokalnym jest godzina 7 rano dnia 2 stycznia 2001, a w czasie uniwersalnym - godzina 12:00 w południe dnia 2 stycznia 2001, wartością UTCTime jest:

```
"0101021200Z"
```

lub

```
"0101020700-0500"
```

Format uniwersalny czasu dopuszcza tylko dwie cyfry określające rok, dlatego jego użycie nie jest zalecane.

Obsługiwane reguły sprawdzania zgodności to `generalizedTimeMatch` dla równości i `generalizedTimeOrderingMatch` dla nierówności. Wyszukiwanie podłańcucha nie jest dozwolone. Na przykład następujące filtry są poprawne:

```
generalized-timestamp-attribute=199910061030  
utc-timestamp-attribute>=991006  
generalized-timestamp-attribute=*
```

Poniższe filtry nie są poprawne:

```
generalized-timestamp-attribute=1999*  
utc-timestamp-attribute>=*1010
```

## Zalecane procedury dla struktury katalogów

Serwer Directory Server jest często używany jako repozytorium dla użytkowników i grup. Poniższa sekcja omawia niektóre z zalecanych procedur konfigurowania struktury zoptymalizowanej dla zarządzania użytkownikami i grupami. Struktura ta i związany z nią model ochrony mogą zostać rozszerzone dla innych użytkowników katalogu.

Użytkownicy są zwykle przechowywani w jednym lub w niewielu miejscach. Może istnieć pojedynczy kontener, `cn=users`, będący macierzystą pozycją dla wszystkich użytkowników lub osobne kontenery dla różnych zestawów użytkowników zarządzanych osobno. Na przykład, pracownicy, dostawcy oraz użytkownicy Internetu zarejestrowani osobiście mogą znajdować się w obiektach nazwanych odpowiednio `cn=pracownicy`, `cn=dostawcy` i `cn=uzytkownicy internetu`. Rozmieszczenie użytkowników według organizacji, do których należą może wydawać się dobrym rozwiązaniem, jednak może to wywołać trudności, jeśli zmienią oni organizację, ponieważ pozycja katalogu musi wówczas zostać również przeniesiona, a grupy lub inne źródła danych (wewnętrzne i zewnętrzne względem katalogu) mogą wymagać aktualizacji, aby odzwierciedlały nową nazwę wyróżniającą. Związek użytkowników ze strukturą organizacyjną można przechwycić w obrębie pozycji użytkownika za pomocą atrybutów katalogu, takich jak "o" (nazwa organizacji), "ou" (nazwa jednostki organizacyjnej) oraz `departmentNumber`, które są częścią standardowego schematu dla `organizationalPerson` i `inetOrgPerson`.

Podobnie grupy zwykle są umieszczane w osobnym kontenerze. Na przykład "cn=groups".

Dzięki zorganizowaniu użytkowników i grup w opisany sposób, istnieje tylko kilka miejsc w których konieczne jest ustawienie list kontroli dostępu (ACL).

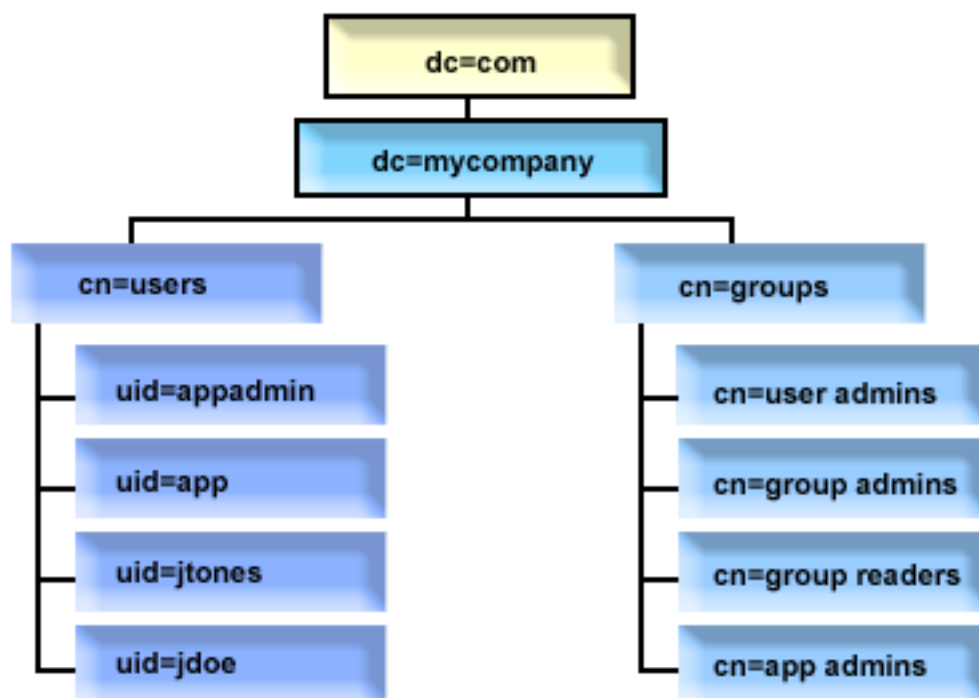
W zależności od sposobu używania serwera katalogów oraz sposobu zarządzania użytkownikami i grupami, można skorzystać z jednego z następujących wzorców kontroli dostępu:

- Jeśli katalog używany jest dla aplikacji, takich jak książka adresowa, można nadać uprawnienia grupowe `cn=anybody` do odczytu i zapisu dla "zwykłych" atrybutów w kontenerze `cn=users` i jego obiektów macierzystych.
- Najczęściej, jedynie nazwy wyróżniające używane przez specyficzne aplikacje i administratorów grup wymagają dostępu do kontenera `cn=groups`. Można utworzyć grupę zawierającą nazwy wyróżniające administratorów grup i uczynić ją właścicielem kontenera `cn=groups` i podporządkowanych mu elementów. Można utworzyć inną grupę zawierającą nazwy wyróżniające używane przez aplikacje do odczytania informacji o grupach i nadać jej uprawnienia do odczytu i wyszukiwania dla `cn=groups`.



- Jeśli obiekty użytkowników aktualizowane są bezpośrednio przez użytkowników, może zaistnieć potrzeba nadania specjalnemu identyfikatorowi dostępowemu `cn=this` odpowiednich uprawnień do odczytu, zapisu i wyszukiwania.
- Jeśli użytkownicy są aktualizowani za pośrednictwem aplikacji, aplikacje te często działają pod własną tożsamością i tylko te aplikacje wymagają uprawnień do aktualizacji obiektów użytkowników. Ponownie, wygodnie jest dodać te nazwy wyróżniające do grupy, na przykład `cn=user administrators` i nadać jej niezbędne uprawnienia do kontenera `cn=users`.

Po zastosowaniu tego typu struktury o kontroli dostępu, katalog początkowy może mieć następująca formę:



Rysunek 2. Przykładowa struktura katalogu

- `c=moje_przedsiębiorstwo, dc=com` należy do administratora katalogu lub innego użytkownika lub grupy z uprawnieniami do zarządzania najwyższym poziomem katalogu. Dodatkowe pozycje listy ACL nadają dostęp do odczytu zwykłych atrybutów dla `cn=anybody` lub `cn=authenticated`, lub ewentualnie innej grupy jeśli wymagana jest bardziej zamknięta lista ACL.
- `cn=users` zawiera pozycje listy ACL inne niż te opisane poniżej, aby umożliwić odpowiedni dostęp do użytkowników. Listy ACL mogą obejmować:
  - dostęp do odczytu i wyszukiwania zwykłych atrybutów dla `cn=anybody` lub `cn=authenticated`
  - dostęp do odczytu i wyszukiwania zwykłych i wrażliwych atrybutów dla menedżerów
  - inne pozycje listy ACL według potrzeb. Na przykład, zezwalające jednostkom na zapis do ich własnych pozycji.

#### Uwagi:

- W celu poprawy odczytu, używane są nazwy RDN pozycji, a nie pełne nazwy wyróżniające. Na przykład, grupa "administratorzy użytkowników" miałyby pełną nazwę wyróżniającą `uid=app,cn=użytkownicy,dc=moje_przedsiębiorstwo,dc=com` jako element, a nie skróconą `uid=app`.
- Niektórzy użytkownicy i grupy mogą być połączeni. Na przykład, jeśli administrator aplikacji miałby posiadać uprawnienia do zarządzania użytkownikami, aplikacja mogłaby działać pod nazwą wyróżniająca administratora aplikacji. Może to jednak ograniczyć możliwość, na przykład, zmiany hasła administratora aplikacji bez konieczności jednoczesnej zmiany konfiguracji hasła w aplikacji.

- O ile powyżej opisano sprawdzone procedury dla katalogów używanych przez tylko jedną aplikację, korzystnie może okazać się wykonanie wszystkich aktualizacji, dokonując uwierzytelnienia jako administrator katalogu. Procedura ta nie jest zalecana z powodów omawianych wcześniej.

## Publikowanie

Serwer Directory Server umożliwia publikowanie przez system określonych rodzajów informacji w katalogu LDAP. Innymi słowy, system utworzy i zaktualizuje pozycje LDAP reprezentujące różne typy danych.

W systemie i5/OS wbudowana jest obsługa publikowania na serwerze LDAP następujących informacji:

### Użytkownicy

Po skonfigurowaniu systemu operacyjnego do publikowania informacji typu Użytkownicy na serwerze Directory Server, system automatycznie eksportuje pozycje z katalogu dystrybucyjnego na serwer Directory Server. Używa wówczas funkcji API QGLDSSDD. Zapewnia w ten sposób synchronizację katalogu LDAP ze zmianami wprowadzonymi w katalogu dystrybucyjnym systemu.

Publikowanie użytkowników zapewnia dostęp poprzez przeszukiwanie LDAP do informacji z katalogu dystrybucyjnego systemu (na przykład, aby zapewnić dostęp do książki adresowej LDAP klientom pocztowym opartym na protokole POP3, takim jak Netscape Communicator lub Microsoft Outlook Express).

Opublikowani użytkownicy również służą do obsługi uwierzytelniania LDAP z niektórymi użytkownikami opublikowanymi z katalogu dystrybucyjnego systemu, a innymi dodanymi do katalogu w inny sposób. Opublikowany użytkownik ma atrybut uid określający nazwę profilu użytkownika i nie ma atrybutu userPassword. Po odebraniu żądania łączenia dla tego typu pozycji serwer wywołuje ochronę systemu operacyjnego w celu sprawdzenia, czy UID i hasło są poprawne dla tego profilu. Ta funkcja może okazać się pomocna, jeśli użytkownik chce używać uwierzytelniania LDAP i uwierzytelniać istniejących użytkowników systemu operacyjnego za pomocą ich haseł w systemie i5/OS, a innych dodawać do katalogu ręcznie.

Innym sposobem publikowania użytkowników jest pobranie pozycji z istniejącej listy sprawdzania HTTP i utworzenie odpowiednich pozycji LDAP na serwerze katalogów. Można to wykonać za pomocą funkcji API QGLDPUBL. Ta funkcja API tworzy pozycje katalogu inetOrgPerson z hasłami powiązаныmi z oryginalną pozycją listy sprawdzania. Funkcja API może zostać uruchomiona raz lub zaplanowana do uruchomienia okresowo w celu sprawdzania nowych pozycji do dodania do serwera katalogów.

**Uwaga:** Jedynie pozycje listy sprawdzania utworzone do użytku z serwerem HTTP Server (oparty na Apache) obsługiwane są przez tę funkcję API. Pozycje istniejące na serwerze katalogów nie zostaną zaktualizowane. Użytkownicy usunięci z listy sprawdzania nie zostaną wykryci.

Po dodaniu użytkowników do katalogu, mogą oni dokonać uwierzytelnienia w aplikacjach, które używają sprawdzania oraz do aplikacji obsługujących uwierzytelnianie LDAP.

### Informacje o systemie

Po skonfigurowaniu systemu operacyjnego do publikowania informacji typu System na serwerze Directory Server publikowane są następujące typy informacji:

- Podstawowe informacje o tej maszynie i o wersji systemu operacyjnego.
- Opcjonalnie można wybrać jedną lub wiele drukarek do publikowania, wtedy system automatycznie dokonuje synchronizacji katalogu LDAP ze zmianami wprowadzonymi dla tych drukarek w systemie.

Informacje o drukarce, które można publikować, obejmują:

- Położenie
- Szybkość w stronach na minutę
- Obsługę duplexu i koloru
- Typ i model
- Opis

Informacje te są pobierane z opisu urządzenia w publikowanym systemie. W środowisku sieciowym użytkownicy mogą skorzystać z tych informacji podczas wyboru drukarki. Informacje są publikowane

pierwszy raz po wybraniu drukarki do publikowania i są aktualizowane, gdy program piszący drukarki jest zatrzymywany lub uruchamiany lub zmieniony został opis drukarki.

### **Współużytkowane zasoby drukarkowe**

Po skonfigurowaniu systemu operacyjnego do publikowania współużytkowanych zasobów drukarki, informacje o wybranych współużytkowanych zasobach drukarkowych iSeries NetServer są publikowane w skonfigurowanym serwerze Active Directory. Publikowanie współużytkowanych zasobów drukarkowych w katalogu Active Directory umożliwia użytkownikom dodawanie drukarek platformy System i do komputerów z systemem Windows 2000 za pomocą kreatora dodawania drukarki systemu Windows 2000. Aby wykonać te czynności za pomocą kreatora dodawania drukarki, należy wybrać odnajdywanie drukarki w katalogu Windows 2000 Active Directory. Współużytkowane zasoby drukarkowe muszą być publikowane do serwera katalogów, który obsługuje schemat Active Directory firmy Microsoft.

### **Jakość usługi TCP/IP**

Serwer QoS TCP/IP można skonfigurować, aby korzystał ze współużytkowanej strategii QoS zdefiniowanej w katalogu LDAP za pomocą schematu określonego przez IBM. Agent publikowania TCP/IP QoS jest używany przez serwer QoS do odczytywania informacji o strategii. Definiuje on serwer, informacje o uwierzytelnianiu oraz miejsce przechowywania informacji o strategii w katalogu.

Można również utworzyć aplikację do publikowania lub wyszukiwania innego rodzaju informacji w katalogu LDAP za pomocą tej struktury poprzez zdefiniowanie dodatkowych agentów publikowania i zastosowanie funkcji API publikowania katalogu.

#### **Pojęcia pokrewne**

Funkcje API protokołu LDAP

Temat Funkcje API protokołu LDAP zawiera więcej informacji o funkcjach API serwera katalogów.

#### **Zadania pokrewne**

“Publikowanie informacji na serwerze Directory Server” na stronie 129

W tym temacie opisano publikowanie informacji na serwerze Directory Server.

## **Replikacja**

Replikacja to technika używana przez serwery katalogów do zwiększania wydajności i niezawodności. Proces replikacji synchronizuje dane w wielu katalogach.

Więcej informacji na temat replikacji znajduje się w następujących sekcjach:

#### **Pojęcia pokrewne**

“Zadania związane z replikacją” na stronie 146

Ten temat zawiera informacje dotyczące zarządzania replikacją.

“Migrowanie sieci serwerów replikacji” na stronie 97

Ten temat zawiera informacje potrzebne do obsługi sieci serwerów replikacji.

## **Replikacja - przegląd**

Poprzez replikację zmiany wprowadzone w jednym katalogu są rozsyłane do jednego lub wielu dodatkowych katalogów. Dzięki temu zmiana w jednym katalogu jest widoczna w wielu różnych katalogach.

Replikacja ma dwie podstawowe zalety:

- Nadmiarowość informacji - repliki zawierają kopię zapasową serwerów źródłowych.
- Szybsze wyszukiwanie - żądania wyszukiwania mogą być wykonywane na wielu serwerach, które mają taką samą zawartość, zamiast na jednym. Skracza to czas odpowiedzi.

Konkretne pozycje w katalogu są określane jako katalogi główne replikowanych poddrzew poprzez dodanie do nich klasy obiektu `ibm-replicationContext`. Każde poddrzewo jest replikowane niezależnie. Poddrzewo przechodzi w dół struktury DIT (directory information tree - drzewa informacji katalogowych) do momentu osiągnięcia pozycji liścia lub innych replikowanych poddrzew. Pozycje są dodawane pod katalogiem głównym replikowanego poddrzewa, tak aby zawierały informacje o topologii replikacji. Pozycje te są jedną lub wieloma pozycjami grup replik, w których

tworzone są pozycje podrzędne replik. Umowy replikacji powiązane z każdą pozycją podrzędną repliki określają serwery obsługiwane przez każdy serwer (na które dane są replikowane) a także definiują referencje i informacje harmonogramu.

Katalog IBM Directory obsługuje rozszerzony model replikacji między serwerem głównym a podrzędnym. Topologie replikacji zostały rozszerzone o:

- replikację poddrzew DIT (Directory Information Tree) do konkretnych serwerów,
- wielowarstwową topologię nazywaną replikacją kaskadową,
- przypisanie roli serwera (główny lub replika) przez poddrzewo,
- obsługę wiele serwerów głównych (tzw. replikacja między serwerami równorzędnymi),
- replikację bramy między sieciami.

Zaletą replikacji poprzez poddrzewa jest to, że replika nie wymaga replikowania całego katalogu. Może to być replika części lub poddrzewa katalogu.

Rozszerzony model zmienia sens serwera głównego i repliki. Terminy te nie będą już dotyczyły serwerów, ale ról, jakie pełnią te serwery w odniesieniu do replikowanego poddrzewa. Serwer może działać jako serwer główny dla niektórych poddrzew i jako replika dla innych. Termin serwer główny oznacza serwer przyjmujący aktualizacje od klientów dla replikowanego poddrzewa. Termin replika oznacza serwer akceptujący aktualizacje tylko z innych serwerów wyznaczonych na wysyłające dla replikowanego poddrzewa.

Typy serwerów według zdefiniowanej funkcji to *nadrzędny/równorzędny*, *kaskadowy*, *brama* i *replika*.

Tabela 1. Rola serwera

Katalog	Opis
Główny/równorzędny	<p>Serwer główny/równorzędny zawiera informacje katalogu serwera głównego z którego aktualizacje są rozsyłane do replik. Wszystkie zmiany są wprowadzane na serwerze głównym, który jest odpowiedzialny za ich rozsyłanie do replik.</p> <p>Jako serwery główne dla informacji katalogu może działać wiele serwerów, z których każdy jest odpowiedzialny za aktualizację innych serwerów głównych i serwerów replik. Nazywa się to replikacją między serwerami równorzędnymi. Replikacja między serwerami równorzędnymi może zwiększyć wydajność i niezawodność. Większa wydajność wynika z tego, że serwer lokalny obsługuje aktualizacje w rozległej sieci rozproszonej. Niezawodność wzrasta dzięki dostępności zapasowego serwera głównego gotowego do natychmiastowej pracy, jeśli podstawowy serwer główny ulegnie awarii.</p> <p><b>Uwagi:</b></p> <ol style="list-style-type: none"> <li>1. Serwery główne replikują wszystkie aktualizacje klientów, ale nie replikują aktualizacji odebranych z innych serwerów głównych.</li> <li>2. Aktualizacje tej samej pozycji wprowadzone na kilku serwerach przez wiele serwerów mogą spowodować niespójność danych katalogu, ponieważ nie ma jednoznacznego rozwiązania konfliktu.</li> </ol>
Kaskadowy (przekazujący)	Serwer kaskadowy jest serwerem replik replikującym wszystkie wysyłane do niego zmiany. Różni się on od serwera głównego/równorzędnego tym, że serwer główny/równorzędny replikuje tylko zmiany wprowadzone przez klientów połączonych z serwerem. Serwer kaskadowy może przejmować obciążenie z serwerów głównych w sieci, która zawiera wiele rozproszonych replik.
Brama	Replikacja bramy wykorzystuje serwery-bramy do wydajnego zbierania i rozprowadzania informacji o replikacji w sieci replikacji. Podstawową zaletą replikacji bramy jest zmniejszenie ruchu w sieci.
Replika (tylko do odczytu)	Replika to dodatkowy serwer zawierający kopię informacji katalogu. Repliki są kopiami obiektu nadrzędnego (lub poddrzewa, którego są replikami). Replika stanowi kopię zapasową replikowanego poddrzewa.

Jeśli replikacja zakończy się niepowodzeniem, zostanie powtórzona nawet wtedy, gdy serwer główny zostanie zrestartowany. Okno Zarządzanie kolejkami w programie Web Administration może być używane do sprawdzania replikacji zakończonych niepowodzeniem.

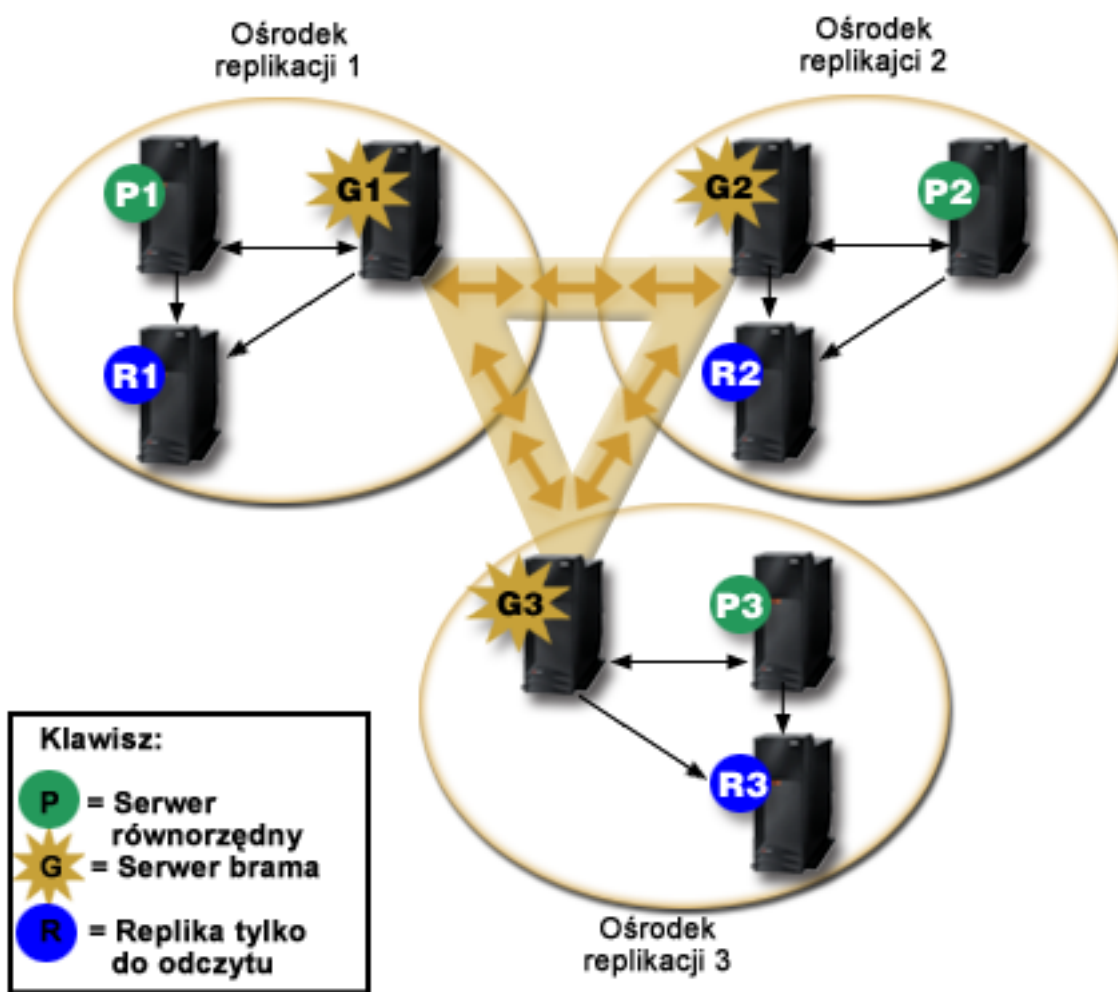
Można zażądać aktualizacji na serwerze replik, ale jest ona przekazywana do serwera głównego poprzez zwrócenie odwołania do klienta. Jeśli aktualizacja zakończy się powodzeniem, serwer główny prześle aktualizację do replik. Do momentu ukończenia replikacji aktualizacji przez serwer główny zmiana nie jest odzwierciedlana na serwerze replik, z którego pochodzi pierwotne żądanie. Zmiany są replikowane w kolejności ich wprowadzania na serwerze głównym.

Jeśli replika nie jest już potrzebna, należy usunąć umowę replikacji z serwera wysyłającego. Pozostawienie definicji powoduje, że serwer tworzy kolejkę wszystkich aktualizacji i niepotrzebnie zajmuje miejsce w katalogu katalogu. Poza tym serwer wysyłający nadal próbuje skontaktować się z brakującym serwerem odbierającym, aby ponowić wysyłanie danych.

## Replikacja bramy

Replikacja bramy wykorzystuje serwery-bramy do wydajnego zbierania i rozprowadzania informacji o replikacji w sieci replikacji. Podstawową zaletą replikacji bramy jest zmniejszenie ruchu w sieci. Serwery-bramy muszą być serwerami nadrzędnymi (z możliwością zapisu).

Poniższy rysunek ilustruje sposób działania replikacji bramy:



Rysunek 3. Sieć replikacji z serwerami-bramami

Sieć replikacji w poprzednim rysunku zawiera trzy ośrodki replikacji, z których każdy zawiera serwer-bramę. Serwer-brama zbiera aktualizacje replikacji z serwerów równorzędnych/replik w ośrodku replikacji, w którym rezyduje

i wysyła aktualizacje do wszystkich pozostałych serwerów-bram w sieci replikacji. Zbiera również aktualizacje replikacji z innych serwerów-bram w sieci replikacji i wysyła je do serwerów równorzędnych/nadrzędnych oraz replik w ośrodku replikacji, w którym rezyduje.

Serwery-bramy używają ID serwerów oraz ID serwerów odbierających w celu określenia, które aktualizacje są wysyłane do innych serwerów-bram w sieci replikacji oraz które aktualizacje są wysyłane do lokalnych serwerów w obrębie ośrodka replikacji.

Aby skonfigurować replikację bramy, należy utworzyć przynajmniej dwa serwery-bramy. Utworzenie serwera-bramy ustanawia ośrodek replikacji. Następnie należy utworzyć umowy replikacji pomiędzy serwerami-bramami, serwerami nadrzędnymi/równorzędnymi i serwerami replik, które mają zostać włączone do ośrodka replikacji bramy.

Serwery-bramy muszą być serwerami nadrzędnymi (z możliwością zapisu). Jeśli użytkownik dokona próby dodania klasy obiektu bramy `ibm-replicaGateway` do podpozycji, która nie jest nadrzędna, zwrócony zostanie komunikat o błędzie.

Istnieją dwie metody tworzenia serwera-bramy. Można wykonać następujące czynności:

- Utworzyć nowy serwer-bramę
- Przekształcić istniejący serwer równorzędny w serwer-bramę

**Uwaga:** Bardzo istotne jest, aby przypisać tylko jeden serwer-bramę dla jednego ośrodka replikacji.

## | Rozstrzygnięcie konfliktów replikacji

| W sieci z wieloma serwerami głównymi można wprowadzić do pozycji powodujące konflikt zmiany. Może to spowodować, że serwery będą miały dla danej pozycji różniące się dane po przeprowadzeniu replikacji zmian. Konflikt między zmianami jest mało prawdopodobny, ponieważ zmiany musiałyby być dokonywane w krótkich odstępach czasu na różnych serwerach głównych. Niektóre przykłady zmian powodujących konflikt:

- dodanie tej samej pozycji o różnych atrybutach na dwóch serwerach,
- zmiana hasła pozycji na różniące się wartości na dwóch serwerach,
- zmiana nazwy pozycji na jednym serwerze podczas modyfikowania pozycji na innym.

| Serwer IBM Tivoli Directory Server ma możliwość automatycznego wykrywania i rozstrzygnięcia konfliktów zmian, aby katalogi na wszystkich serwerach pozostawały spójne. Po wykryciu konfliktów replikacji zmiana powodująca konflikt jest zgłaszana w protokole serwera oraz rejestrowana w pliku protokołu niedokończonych operacji, aby administrator mógł odtworzyć utracone dane.

| Rozstrzygnięcie konfliktów operacji dodawania i modyfikowania w replikacji między serwerami równorzędnymi opiera się na datownikach pozycji i zmian. W środowisku replikacji z wieloma serwerami głównymi pierwszeństwo ma aktualizacja z najnowszym datownikiem na dowolnym serwerze. Po wykryciu konfliktu replikacji zastępowana pozycja jest archiwizowana w protokole niedokończonych operacji w celu późniejszego odtworzenia.

| Replikowane żądania usunięcia i zmiany nazwy są akceptowane w kolejności odbierania bez rozstrzygnięcia konfliktów. W przypadku konfliktów replikacji związanych z operacją `delete` lub `modifyDN` (usunięcie lub zmiana nazwy wyróżniającej) mogą powstać błędy wymagające interwencji administratora. Na przykład w przypadku zmiany nazwy wpisu na jednym serwerze w momencie, gdy jest on modyfikowany na innym, operacja zmiany nazwy `modifyDN` może dotrzeć do repliki przed operacją modyfikowania. W takiej sytuacji operacja modyfikowania nie powiedzie się, kiedy dotrze do repliki. Administrator musi wtedy naprawić błąd, modyfikując pozycję przy użyciu nowej nazwy wyróżniającej. Wszystkie informacje niezbędne do powtórzenia modyfikacji z poprawną nazwą są zapisywane w protokołach replikacji i błędów. Takie błędy replikacji występują rzadko w poprawnie skonfigurowanej topologii replikacji, ale nie można zakładać, że nigdy nie wystąpią.

| Aktualizacje tej samej pozycji wprowadzone przez wiele serwerów mogą spowodować niespójność danych katalogu, ponieważ rozstrzygnięcie konfliktu zależy od datownika pozycji. Pierwszeństwo ma najnowszy datownik modyfikacji.

l Jeśli dane na serwerach staną się niespójne, należy zapoznać się z opisem narzędzia ldapdiff (odsylacz zamieszczono poniżej), aby uzyskać informacje na temat ponownego synchronizowania serwerów.

l Rozstrzygnięcie konfliktu replikacji wymaga, aby serwer wysyłający udostępnił datownik pozycji sprzed jej aktualizacji na serwerze wysyłającym. Serwer IBM Tivoli Directory Server for i5/OS w wersji V5R4 i wcześniejszych nie ma możliwości dostarczania tego rodzaju informacji. Dlatego rozstrzygnięcie konfliktu replikacji nie jest możliwe, gdy serwerem wysyłającym jest nieaktualna wersja serwera. W wersji V6R1 serwer odbierający IBM Tivoli Directory Server for i5/OS uzyskuje w takim przypadku replikowany datownik i aktualizuje oraz stosuje go bez sprawdzania pod kątem występowania konfliktów.

l **Uwaga:** Wcześniejsze wersje serwera IBM Tivoli Directory Server for i5/OS nie obsługują rozstrzygania konfliktów na podstawie datownika. Jeśli w topologii znajdują się wcześniejsze wersje serwera IBM Tivoli Directory Server for i5/OS, nie można zapewnić spójności danych w sieci.

l Konfliktów zmian można uniknąć, używając systemu równoważenia obciążenia, przejęcia wirtualnego adresu IP lub innych metod, które zapewniają, że zmiany w katalogu będą wprowadzane na jednym serwerze, umożliwiając jednocześnie automatyczne przełączenie awaryjne na inne serwery, gdy preferowany serwer jest niedostępny.

l System równoważenia obciążenia, na przykład IBM WebSphere Edge Server, ma wirtualną nazwę hosta, której używają aplikacje podczas wysyłania aktualizacji do katalogu. System równoważenia obciążenia jest skonfigurowany w taki sposób, że wysyła te aktualizacje tylko do jednego serwera. Jeśli ten serwer jest wyłączony lub niedostępny z powodu awarii sieci, system równoważenia obciążenia wysyła te aktualizacje do następnego dostępnego serwera równorzędnego, dopóki pierwszy serwer nie będzie z powrotem dostępny. Informacje dotyczące instalowania i konfigurowania systemu równoważenia obciążenia znajdują się w dokumentacji tego produktu.

#### **Zadania pokrewne**

“Modyfikowanie ustawień protokołu niedokończonych operacji” na stronie 165

W protokole niedokończonych operacji (domyślnie zapisywanym w pliku LostAndFound.log) rejestrowane są błędy, które wystąpiły w wyniku konfliktów replikacji. Dostępne są ustawienia umożliwiające sterowanie obsługą protokołu niedokończonych operacji, w tym określenie położenia i maksymalnej wielkości pliku protokołu oraz zasad archiwizowania starych plików protokołu.

“Tworzenie prostej topologii z replikacją między serwerami równorzędnymi” na stronie 154

Replikacja między serwerami równorzędnymi to topologia replikacji, w której występuje wiele serwerów głównych. Replikacji między serwerami równorzędnymi można używać tylko w środowiskach, w których kierunki aktualizowania są dobrze znane.

#### **Odsyłacze pokrewne**

“ldapdiff” na stronie 247

Program narzędziowy wiersza komend do synchronizowania replik LDAP.

## **Terminologia dotycząca replikacji**

Definicje niektórych terminów używanych w opisach replikacji.

### **Replikacja kaskadowa**

Topologia replikacji składająca się z wielu warstw serwerów. Serwer główny/równorzędny replikuje do zestawu serwerów tylko do odczytu (przekazujących), które z kolei replikują do innych serwerów. Taka topologia odciąża zadania replikacji z serwerów głównych.

### **Serwer odbierający**

Serwer, który odbiera zmiany poprzez replikację z innego serwera (serwera wysyłającego).

### **Referencje**

Określa metodę i wymagane informacje używane przez serwer wysyłający podczas łączenia z klientem. W przypadku prostych operacji łączenia jest to nazwa wyróżniająca i hasło. Referencje są przechowywane w pozycji nazwy wyróżniającej określonej w umowie replikacji.

### **Serwer przekazujący**

Serwer tylko do odczytu replikujący wszystkie zmiany wysłane do niego przez serwer główny lub równorzędny. Żądania aktualizacji z klientów są wysyłane do serwera nadrzędnego lub równorzędnego.

### **Serwer-brama**

Serwer przekazujący cały ruch replikacji z lokalnego ośrodka replikacji, w którym rezyduje do innych serwerów-bram w sieci replikacji. Serwer-brama odbiera ruch replikacji z innych serwerów-bram w sieci replikacji, który przekazuje do wszystkich serwerów w swoim lokalnym ośrodku replikacji. Serwery-bramy muszą być serwerami nadrzędnymi (z możliwością zapisu).

### **Serwer główny**

Serwer, na którym można zapisywać (można go aktualizować) w ramach danego poddrzewa.

### **Poddrzewo zagnieżdżone**

Poddrzewo w replikowanym poddrzewie katalogu.

### **Serwer równorzędny**

Termin oznaczający serwer główny w przypadku, gdy dla danego poddrzewa istnieje wiele serwerów głównych.

### **Grupa replik**

Pierwsza pozycja utworzona w kontekście replikacji ma klasę obiektu `ibm-replicaGroup` i reprezentuje kolekcję serwerów biorących udział w replikacji. Jest to wygodne miejsce do ustawienia list ACL zabezpieczających informacje o topologii replikacji. Narzędzia administrowania obsługują obecnie jedną grupę replik w każdym kontekście replikacji, która nosi nazwę **`ibm-replicagroup=default`**.

### **Pozycja podrzędna replik**

Poniżej pozycji grupy replik można utworzyć jedną lub wiele pozycji z klasą obiektu `ibm-replicaSubentry`. Dla każdego serwera biorącego udział w replikacji jako serwer wysyłający powinna być utworzona jedna pozycja. Pozycja podrzędna repliki określa rolę serwera w replikacji: główny lub tylko do odczytu. Serwer tylko do odczytu może z kolei zawierać umowy replikacji do obsługi replikacji kaskadowej.

### **Replikowane poddrzewo**

Część drzewa DIT, które jest replikowane z jednego serwera na inny. W tej strukturze dane poddrzewo można replikować na niektóre serwery, a na inne nie. Na danym serwerze takie poddrzewo może być zapisywane, a inne poddrzewa mogą być tylko do odczytu.

### **Sieć replikacji**

Sieć zawierająca połączone ośrodki replikacji.

### **Umowa replikacji**

Informacje zawarte w katalogu, które definiują 'połączenie' lub 'ścieżkę replikacji' między dwoma serwerami. Jeden serwer nazywany jest wysyłającym, a drugi odbierającym. Umowa zawiera wszystkie informacje potrzebne do nawiązania połączenia z serwera wysyłającego do odbierającego i zaplanowania replikacji.

### **Kontekst replikacji**

Określa katalog główny replikowanego poddrzewa. Do pozycji można dodać pomocniczą klasę obiektu `ibm-replicationContext` w celu zaznaczenia, że jest to katalog główny replikowanego obszaru. Informacje dotyczące topologii replikacji są obsługiwane w zestawie pozycji utworzonym w kontekście replikacji.

### **Ośrodek replikacji**

Serwer-brama i wszystkie serwery nadrzędne, równorzędne i serwery replik skonfigurowane do wzajemnej replikacji.

### **Harmonogram**

Przeprowadzenie replikacji można zaplanować w określonych godzinach; wtedy zmiany skumulowane na serwerze wysyłającym zostaną wysłane w zadaniu wsadowym. Umowa repliki zawiera nazwę wyróżniającą dla pozycji dostarczającej harmonogram.

### **Serwer wysyłający**

Serwer wysyłający zmiany do innego serwera (odbierającego).

## | **Replikacja wielowątkowa**

| Wykorzystanie replikacji wielowątkowej (asynchronicznej) pozwala administratorom przeprowadzać replikację z wykorzystaniem wielu wątków, co przekłada się na zwiększenie ogólnej przepustowości procesu replikacji.



| Gdy używana jest replikacja jednowątkowa (synchroniczna), może się zdarzyć, że klienci będą modyfikować dane w tempie przekraczającym możliwości replikowania danych na inne serwery. Wynika to stąd, że w standardowym modelu replikacji używany jest tylko jeden wątek, który replikuje kolejne zmiany w kolejności ich otrzymywania.

| Co więcej, działanie standardowego modelu replikacji jest blokowane w przypadku wystąpienia określonych błędów. Może to na przykład mieć miejsce, gdy replikowane żądanie modyfikacji zakończy się niepowodzeniem, gdyż pozycja docelowa nie istnieje na serwerze odbierającym. Zachowanie takie zwraca wprawdzie uwagę administratora na istnienie rozbieżności między serwerami i konieczność ich poprawienia, jednak może również prowadzić do narastania listy oczekujących zmian. W niektórych zastosowaniach takie nagromadzenie niereplikowanych zmian może być niepożądane.

| Aby zapobiec tego typu problemom, mechanizm replikacji wielowątkowej umożliwia zapisywanie w protokole błędów informacji o zakończonych niepowodzeniem próbach wprowadzenia zmian, a następnie kontynuowanie przetwarzania kolejnych zmian. Protokół zawiera informacje pozwalające ustalić, z którymi pozycjami i zmianami wiązały się nieudane operacje, a dostępne narzędzia umożliwiają ponowienie prób wprowadzenia zmian po usunięciu błędów. Aby zapobiec pomijaniu dużej liczby zmian z powodu wystąpienia poważnych rozbieżności, wprowadzono konfigurowalną wartość progową błędów, której osiągnięcie spowoduje zablokowanie procesu replikacji do czasu usunięcia błędów i usunięcia zawartości protokołu błędów replikacji.

| • Administrowanie replikacją wielowątkową (asynchroniczną) może być utrudnione, jeśli używane serwery lub sieci działają zawodnie, przez co wiele replikowanych zmian jest pomijanych.

| Wszelkie błędy są rejestrowane w protokołach i mogą zostać odtworzone przez administratora, jednak konieczne jest bieżące monitorowanie protokołów błędów. Oto komenda wyszukiwania pozwalająca wyświetlić listę niereplikowanych zmian związanych z umowami dostarczonymi przez określony serwer:

```
| ldapsearch -h host_wysyłający -D cn=admin -w ? -s sub  
|   objectclass=ibm-replicationagreement  
|   ibm-replicationpendingchangelcount ibm-replicationstate
```

| Jeśli replikacja znajduje się w stanie aktywnym, a lista oczekujących zmian rośnie, sygnalizuje to istnienie zaległości, których liczba nie zmniejsza się do momentu zmniejszenia tempa napływania zmian lub przełączenia replikacji z trybu synchronicznego w tryb asynchroniczny (wielowątkowy).

| Replikacja zwiększa też obciążenie serwera głównego, na którym zmiany są wprowadzane w pierwszej kolejności. Poza koniecznością zaktualizowania własnej kopii danych katalogu, serwer główny musi przesłać zmiany do wszystkich serwerów replik. Jeśli działanie aplikacji lub użytkowników w danym środowisku nie wymaga natychmiastowej replikacji, możliwe jest zminimalizowanie wpływu procesu replikacji na wydajność pracy serwera głównego poprzez przemyślane zaplanowanie operacji replikacji poza okresami szczytowego obciążenia.

| W przypadku replikacji wielowątkowej błąd replikacji wiąże się z następującymi zdarzeniami:

| • Jeśli parametr `ibm-slapdReplMaxErrors` ma wartość 0, błędy nie będą rejestrowane w protokole błędów replikacji, lecz w protokole serwera, a proces replikacji zostanie wstrzymany do czasu usunięcia wszystkich błędów.

| • Jeśli liczba błędów dotyczących umowy przekroczy zdefiniowany limit, replikacja zostanie zawieszona do czasu usunięcia co najmniej jednego błędu lub zwiększenia limitu liczby błędów na każdą umowę.

| • Status umowy replikacji to:

```
| ibm-replicationStatus: error log full (zapełniony protokół błędów)
```

## | **Tabela błędów replikacji**

| W tabeli błędów replikacji protokołowane są niepowodzenia aktualizacji w celu późniejszego odtwarzania. Po rozpoczęciu replikacji liczona jest liczba zaprotokołowanych niepowodzeń dla każdej umowy replikacji. Gdy aktualizacja zakończy się niepowodzeniem, liczba ta jest zwiększana, a do tabeli dodawana jest nowa pozycja.

| W każdej pozycji w tabeli błędów replikacji znajdują się następujące informacje:

- | • Identyfikator umowy replikacji.
- | • Identyfikator zmiany replikacji.

- Datownik określający moment nieudanej aktualizacji.
- Liczba wykonanych prób (wartość ta domyślnie wynosi 1 i jest zwiększana z każdą próbą).
- Kod wyniku od serwera odbierającego.
- Wszystkie informacje o operacji replikowania mające związek z aktualizowaniem, na przykład nazwa wyróżniająca, faktyczne dane, elementy sterujące, flagi itd.

Jeśli wartość podana w atrybucie `ibm-slapdReplMaxErrors` konfiguracji serwera wynosi 0, replikacja kontynuuje przetwarzanie aktualizacji. Atrybut `ibm-slapdReplMaxErrors` jest atrybutem w pozycji konfiguracji replikacji i można go zmieniać dynamicznie.

Jeśli wartość podana w atrybucie `ibm-slapdReplMaxErrors` jest większa niż 0, to gdy liczba błędów dla danej umowy replikacji przekroczy tę wartość, mechanizm replikacji wykona jedno z następujących działań:

- **Jednowątkowa:** replikacja wejdzie w pętlę, próbując replikować aktualizację, która się nie powiodła.
- **Wielowątkowa:** replikacja zostanie zawieszona.

Jeśli serwer jest skonfigurowany do korzystania z jednego połączenia, mechanizm replikacji będzie próbował wysłać tę samą aktualizację po odczekaniu 60 sekund i będzie powtarzał te próby do momentu, gdy operacja się powiedzie lub gdy administrator pominie tę aktualizację.

W przypadku serwera skonfigurowanego do obsługi wielu połączeń replikacja zostanie zawieszona dla tej umowy. Wątki odbierające będą nadal odpytywały o status wysłanych już aktualizacji, ale żadne aktualizacje nie będą już replikowane. Aby wznowić replikację, administrator katalogu musi usunąć co najmniej jeden błąd dla tej umowy lub zwiększyć limit, modyfikując dynamicznie konfigurację serwera.

Więcej informacji można znaleźć w temacie Zarządzanie kolejkami replikacji, do którego odsyłacz zamieszczono poniżej. Należy się również zapoznać z opisem opcji `-op controlreplerr` w temacie dotyczącym narzędzia `ldapexop`, do którego odsyłacz zamieszczono poniżej.

#### Zadania pokrewne

“Zarządzanie kolejkami replikacji” na stronie 165

Ten temat zawiera informacje dotyczące monitorowania statusu replikacji dla każdej umowy replikacji (kolejki) używanej przez dany serwer.

#### Odsyłacze pokrewne

“`ldapexop`” na stronie 226

Program narzędziowy wiersza komend do operacji rozszerzonych LDAP.

## Umowy replikacji

Umowa replikacji jest pozycją w katalogu z klasą obiektu **ibm-replicationAgreement** utworzoną pod pozycją podrzędną repliki w celu zdefiniowania replikacji z serwera reprezentowanego przez podpozycję do innego serwera.

Obiekty te są podobne do pozycji `replicaObject` używanych we wcześniejszych wersjach serwera Directory Server.

Umowa replikacji zawiera następujące pozycje:

- Nazwa przyjazna użytkownika używana jako atrybut nazwy dla umowy.
- Adres URL LDAP określający serwer, numer portu i czy należy używać protokołu SSL.
- ID serwera odbierającego, jeśli jest znany. Serwery katalogów w wersji wcześniejszej niż V5R3 nie mają ID serwera.
- Nazwa wyróżniająca obiektu zawierającego referencje używane przez serwer wysyłający do łączenia się z klientem.
- Opcjonalny wskaźnik nazwy wyróżniającej do obiektu zawierającego informacje o harmonogramie dla replikacji. Jeśli brak atrybutu, zmiany są replikowane natychmiast.

Nazwa przyjazna użytkownika może być nazwą serwera odbierającego lub innym opisującym go łańcuchem znaków.

Identyfikator serwera odbierającego jest używany przez administracyjny graficzny interfejs użytkownika do poruszania się po topologii. Mając dany identyfikator serwera odbierającego interfejs GUI może znaleźć odpowiednią pozycję

podrzedną i jej umowy. Gdy serwer wysyłający łączy się z odbierającym, pobiera ID serwera z rdzenia nazwy pozycji DSE i porównuje go z wartością w umowie, co pomaga w zapewnieniu dokładności danych. Jeśli identyfikatory serwera są różne, protokołowane jest ostrzeżenie.

Ponieważ umowę replikacji można replikować, używana jest w tym celu nazwa wyróżniająca obiektu referencji. Umożliwia to przechowywanie referencji w niereplikowanym obszarze katalogu. Replikacja obiektów referencji (która musi zawierać referencje w postaci tekstowej) stanowi potencjalne zagrożenie dla ochrony. Przyrostek `cn=localhost` jest odpowiednią domyślną lokalizacją do tworzenia obiektów referencji.

Klasy obiektu są definiowane dla każdej obsługiwanej metody uwierzytelniania:

- Wiązanie proste
- SASL
- Mechanizm EXTERNAL z SSL
- Uwierzytelnianie Kerberos

Można określić, aby ta część replikowanego poddrzewa nie była replikowana poprzez dodanie pomocniczej klasy obiektu `ibm-replicationContext` do katalogu głównego poddrzewa bez definiowania pozycji podrzędnych repliki.

**Uwaga:** Narzędzie Web Administration nazywa także umowy 'kolejkami', gdy mowa jest o zestawie zmian oczekujących na replikację na podstawie danej umowy.

| W przypadku umowy korzystającej z jednowątkowej metody replikacji liczba połączeń serwera odbierającego zawsze  
| wynosi jeden, a wartość atrybutu jest ignorowana. W przypadku umowy korzystającej z wielowątkowej metody  
| replikacji liczbę połączeń można skonfigurować, aby wynosiła od 1 do 32. Jeśli dla umowy nie zostanie określona  
| żadna wartość, liczba połączeń serwera odbierającego jest ustawiana na jedno.

| **Uwaga:** W przypadku poddrzewa `cn=ibmpolicies` wszystkie umowy replikacji będą określały jednowątkową metodę  
| replikacji i jedno połączenie serwera odbierającego, ignorując wartości atrybutu.

## Sposób przechowywania danych replikacji na serwerze

Dane replikacji są przechowywane w katalogu w wielu miejscach.

- W konfiguracji serwera, która zawiera informacje o tym, jak inne serwery mogą uwierzytelnić się w tym serwerze w celu wykonania replikacji (na przykład komu ten serwer pozwala na działanie jako serwer wysyłający).
- W katalogu na szczycie replikowanego poddrzewa. Jeśli pozycja `o=my company` jest szczytem replikowanego poddrzewa, obiekt o nazwie `ibm-replicagroup=default` zostanie utworzony bezpośrednio pod nim (`ibm-replicagroup=default,o=my company`). Pod obiektem `ibm-replicagroup=default` będą znajdować się dodatkowe obiekty opisujące serwery zawierające repliki poddrzewa i umowy między serwerami.
- Obiekt o nazwie `cn=replication,cn=localhost` służy do gromadzenia informacji o replikacji używanych tylko przez jeden serwer. Na przykład obiekt zawierający referencje używane przez serwer wysyłający jest potrzebny tylko serwerowi wysyłającemu. Referencje można umieścić w `cn=replication,cn=localhost` udostępniając je tylko temu serwerowi.
- Obiekt o nazwie `cn=replication, cn=IBMpolicies` służy do gromadzenia informacji o replikacji replikowanych do innych serwerów.

## Uwagi dotyczące bezpieczeństwa informacji o replikacji

Przegląd uwag dotyczących bezpieczeństwa wybranych obiektów.

- `ibm-replicagroup=default`: prawa dostępu do tego obiektu określają, kto może przeglądać lub zmieniać przechowywane tutaj informacje o replikacji. Domyślnie obiekt ten dziedziczy prawa dostępu z obiektu nadrzędnego. Należy rozważyć możliwość ustawienia praw dostępu do tego obiektu w celu ograniczenia dostępu do informacji o replikacji. Można na przykład zdefiniować grupę zawierającą użytkowników, którzy będą zarządzali replikacją. Ta grupa może zostać właścicielem obiektu `ibm-replicagroup=default` i innych użytkowników nie mających dostępu do obiektu.
- `cn=replication,cn=localhost`: w przypadku tego obiektu należy rozważyć dwie kwestie dotyczące bezpieczeństwa:

- Prawa dostępu do tego obiektu określają, kto może przeglądać lub aktualizować obiekty zapisane w tym miejscu. Domyślne prawa dostępu umożliwiają anonimowym użytkownikom odczyt większości informacji z wyjątkiem haseł i wymagają uprawnień administratora w celu dodawania, modyfikowania lub usuwania obiektów.
- Obiekty przechowywane w pozycji "cn=localhost" nie są nigdy replikowane do innych serwerów. Referencje replikacji można umieścić w tym kontenerze na serwerze używającym referencji, a inne serwery nie będą miały do nich dostępu. Ewentualnie można umieścić referencje w obiekcie "ibm-replicagroup=default", aby wiele serwerów współużytkowało te same referencje.
- cn=IBMpolicies: Referencje replikacji można umieścić w tym kontenerze, ale dane w nim zawarte są replikowane na wszystkich serwerach odbierających danego serwera. Umieszczanie referencji w pozycji cn=replication,cn=localhost jest uważane za bardziej bezpieczne.

## Replikacja w środowisku o wysokiej dostępności

Serwer Directory Server jest często wykorzystywany dla rozwiązań pojedynczego wpisania się, co może powodować pojedynczy punkt awarii.

Serwer Directory Server można uczynić wysoce dostępnym, używając replikacji na dwa sposoby: za pomocą programu IBM Load Balancer lub przejęcia adresu IP. Więcej informacji na ten temat zawiera rozdział 13.2 dokumentacji technicznej IBM (Redbooks) *IBM WebSphere V5.1 Performance, Scalability, and High Availability*.

### Informacje pokrewne



IBM WebSphere V5.1 Performance, Scalability, and High Availability

## Dziedziny i szablony użytkowników

Dzięki obiektom dziedziny i szablону użytkowników znajdującym się w narzędziu Web Administration użytkownik nie musi w pełni znać niektórych niskopoziomowych zagadnień związanych z protokołem LDAP.

Dziedzina określa kolekcję użytkowników i grup. Zawiera informacje, w postaci zwykłej struktury katalogu, o położeniu użytkowników i grup. Dziedzina definiuje położenie użytkowników (na przykład "cn=users,o=acme,c=us") i tworzy użytkowników jako bezpośrednie obiekty podrzędne względem tej pozycji (na przykład Jan Kowalski jest tworzony jako "cn=Jan Kowalski,cn=users,o=acme,c=us"). Można zdefiniować wiele dziedziny i nadać im znane nazwy (na przykład Użytkownicy Internetu). Znana nazwa może być używana przez osoby tworzące i obsługujące użytkowników.

Szablon opisuje wygląd użytkownika. Określa klasy obiektu używane podczas tworzenia użytkowników (zarówno strukturalna klasa obiektu, jak i wszystkie klasy pomocnicze). Szablon określa również układ paneli używanych do tworzenia lub edycji użytkowników (na przykład nazwy zakładek, wartości domyślne i atrybuty, które mają być wyświetlane w każdej zakładce).

Podczas dodawania nowej dziedziny w katalogu tworzony jest nowy obiekt `ibm-realm`. Obiekt `ibm-realm` śledzi właściwości dziedziny, takie jak miejsce definiowania użytkowników i grup oraz elementy używane przez szablon. Obiekt `ibm-realm` może wskazywać na istniejącą pozycję katalogu, która jest nadrzędna dla użytkowników, lub na siebie (domyślnie) tworząc kontener dla nowych użytkowników. Można na przykład mieć istniejący kontener `cn=users,o=acme,c=us` i utworzyć dziedziny o nazwie `users` w dowolnym miejscu w katalogu (może to być obiekt kontenera o nazwie `cn=realms,cn=admin stuff,o=acme,c=us`), który jako położenie użytkowników i grup określa wartości `cn=users,o=acme,c=us`. Powoduje to utworzenie obiektu `ibm-realm`:

```
dn: cn=users,cn=realms,cn=admin stuff,o=acme,c=us
objectclass: top
objectclass: ibm-realm
objectclass: ibm-staticGroup
ibm-realmUserTemplate: cn=users template,cn=realms,cn=admin stuff,o=acme,c=us
ibm-realmUserContainer: cn=users,o=acme,c=us
ibm-realmGroupContainer: cn=users,o=acme,c=us
ibm-realmAdminGroup: cn=users,cn=realms,cn=admin stuff,o=acme,c=us
ibm-realmUserSearchFilter:
cn: users
```

Jeśli obiekt `cn=users,o=acme,c=us` nie istniał, można było utworzyć dziedzinę użytkowników w `o=acme,c=us` i sprawić, aby wskazywała sama na siebie.

Administrator katalogu jest odpowiedzialny za zarządzanie szablonami użytkowników, dziedzinami i grupami administratorów dziedzin. Po utworzeniu dziedziny za zarządzanie użytkownikami i grupami do niej należącymi odpowiedzialni są członkowie grupy jej administratorów.

#### Pojęcia pokrewne

“Zadania związane z dziedzinami i szablonami użytkowników” na stronie 206

Ten temat zawiera informacje dotyczące zarządzania dziedzinami i szablonami użytkowników.

#### Zadania pokrewne

“Tworzenie dziedziny” na stronie 206

Ten temat zawiera informacje dotyczące tworzenia dziedziny.

## Parametry wyszukiwania

Aby ograniczyć ilość zasobów używanych przez serwer, administrator może ustawić parametry wyszukiwania tak, aby ograniczyć możliwości wyszukiwania przez użytkowników. Możliwości wyszukiwania mogą także zostać rozszerzone dla specjalnych użytkowników.

Wyszukiwania dokonywane przez użytkowników można ograniczyć lub rozszerzyć za pomocą następujących metod:

### Ograniczenie wyszukiwania

- Wyszukiwanie ze stronicowaniem
- Wyszukiwanie z sortowaniem
- Wyłączenie wyłuskiwania aliasów

### Rozszerzenie wyszukiwania

- Grupy ograniczonego wyszukiwania

### Wyszukiwanie ze stronicowaniem

Wyniki podzielone na strony pozwalają klientowi zarządzać dużą ilością danych zwracanych przez żądanie wyszukiwania. Zamiast jednorazowego odbierania wszystkich rezultatów klient może zażądać podzbioru pozycji (strony). Kolejne żądania wyszukiwania zwracają następną stronę wyników do momentu anulowania działania lub zwrócenia ostatniego wyniku. Administrator może ograniczyć użycie tego wyszukiwania zezwalając na jego używanie jedynie administratorom.

### Wyszukiwanie z sortowaniem

Wyszukiwanie z sortowaniem umożliwia klientowi uzyskanie wyników wyszukiwania posortowanych na podstawie listy kryteriów, gdzie każde kryterium stanowi klucz sortowania. Przenosi to odpowiedzialność za sortowanie z aplikacji klienckiej na serwer. Administrator może ograniczyć użycie tego wyszukiwania zezwalając na jego używanie jedynie administratorom.

### Wyłączenie wyłuskiwania aliasów

Pozycja katalogu o klasie obiektu `alias` lub `aliasObject` zawiera atrybut `aliasedObjectName`, używany dla odniesienia do innej pozycji w katalogu. Jedynie żądania wyszukiwania mogą określać czy aliasy są wyłuskwane. *Wyłuskiwanie* oznacza śledzenie aliasu do oryginalnej pozycji. Czas odpowiedzi serwera IBM Directory Server w przypadku wyszukiwań z opcją wyłuskiwania aliasów **zawsze** lub **wyszukiwanie**, może być znacznie dłuższy niż w przypadku wyszukiwań z opcją wyłuskiwania **nigdy**, nawet jeśli w katalogu nie istnieją żadne pozycje aliasów. Dwa ustawienia określają zachowanie wyłuskiwania aliasów serwera: opcja wyłuskiwania określona przez żądania wyszukiwania serwera oraz opcja wyłuskiwania skonfigurowana na serwerze przez administratora. W przypadku takiej konfiguracji, serwer może automatycznie pominąć wyłuskiwanie aliasów, jeśli w katalogu nie istnieją żadne obiekty aliasów, a także

przesłonić opcję wyłuskiwania określoną w żądaniu wyszukiwania klienta. Poniższa tabela przedstawia sposób mieszania wyłuskiwania aliasów pomiędzy klientem i serwerem.

Tabela 2. Bieżące wyłuskiwanie aliasów w oparciu o ustawienia klienta i serwera

Serwer	Klient	Bieżące
nigdy	dowolne ustawienie	nigdy
zawsze	dowolne ustawienie	ustawienie klienta
dowolne ustawienie	zawsze	ustawienie serwera
wyszukiwanie	odnalezienie	nigdy
odnalezienie	wyszukiwanie	nigdy

## Grupy ograniczonego wyszukiwania

Administrator może utworzyć grupy ograniczonego wyszukiwania posiadające bardziej elastyczne ograniczenia wyszukiwania niż zwykli użytkownicy. Pojedynczy członkowie lub grupy zawarte w grupie ograniczonego wyszukiwania mają nadane mniej ścisłe ograniczenia wyszukiwania, niż te nałożone na zwykłych użytkowników.

Kiedy użytkownik inicjuje wyszukiwanie, najpierw sprawdzane są ograniczenia żądania wyszukiwania. Jeśli użytkownik jest członkiem grupy ograniczonego wyszukiwania, ograniczenia są porównywane. Jeśli ograniczenia grupy ograniczonego wyszukiwania są większe niż ograniczenia żądania wyszukiwania, użyte zostaną ograniczenia żądania wyszukiwania. Jeśli ograniczenia żądania wyszukiwania są większe niż ograniczenia grupy ograniczonego wyszukiwania, użyte zostaną ograniczenia grupy ograniczonego wyszukiwania. Jeśli nie zostaną odnalezione żadne pozycje grupy ograniczonego wyszukiwania, takie samo porównanie dokonywane jest dla ograniczeń wyszukiwania serwera. Jeśli nie zostały ustawione żadne ograniczenia wyszukiwania serwera, porównanie dokonywane jest dla domyślnego ustawienia serwera. Używane są zawsze ograniczenia o najniższych ustawieniach porównaniu.

Jeśli użytkownik należy do wielu grup ograniczonego wyszukiwania, udzielane są mu uprawnienia do najwyższego poziomu możliwości wyszukiwania. Na przykład, użytkownik należy do grupy wyszukiwania 1, która nadaje ograniczenia wyszukiwania o wielkości równej 2000 pozycji i czasie wyszukiwania równym 4000 sekund oraz do grupy wyszukiwania 2, która nadaje ograniczenia czasu wyszukiwania równe 3000 sekund i nieograniczonej liczby pozycji. Użytkownik posiada ograniczenia wyszukiwania o nieograniczonej wielkości wyszukiwania i czasie wyszukiwania równym 4000 sekund.

Grupy ograniczonego wyszukiwania mogą być przechowywane w pozycji localhost lub IBMpolicies. Grupy ograniczonego wyszukiwania znajdujące się w pozycji IBMpolicies są replikowane; te znajdujące się w localhost, nie. Ta sama grupa ograniczonego wyszukiwania może być przechowywana w obu pozycjach: localhost i IBMpolicies. Jeśli grupa ograniczonego wyszukiwania nie jest przechowywana pod jedną z tych nazw DN, serwer ignoruje część grupy dotyczącą ograniczeń wyszukiwania i traktuje ją jak zwykłą grupę.

Kiedy użytkownik inicjuje wyszukiwanie, najpierw sprawdzane są pozycje grupy ograniczonego wyszukiwania zawarte w localhost. Jeśli dla użytkownika nie zostaną odnalezione żadne pozycje, przeszukiwane są pozycje grupy ograniczonego wyszukiwania w IBMpolicies. Jeśli w localhost zostaną odnalezione pozycje, pozycje grupy ograniczonego wyszukiwania w IBMpolicies nie są sprawdzane. Pozycje grupy ograniczonego wyszukiwania w localhost posiadają wyższy priorytet niż pozycje w IBMpolicies.

### Pojęcia pokrewne

“Zadania związane z grupami ograniczonego wyszukiwania” na stronie 135

Ten temat zawiera informacje dotyczące zarządzania grupami ograniczonego wyszukiwania.

### Zadania pokrewne

“Dopasowywanie ustawień wyszukiwania” na stronie 127

Ten temat zawiera informacje dotyczące określania możliwości użytkowników w zakresie wyszukiwania.

“Wyszukiwanie pozycji w katalogu” na stronie 200

Ten temat zawiera informacje dotyczące wyszukiwania pozycji w katalogu.

## Uwagi dotyczące obsługi języków narodowych

Uwagi dotyczące obsługi języków narodowych (national language support - NLS) dotyczą między innymi formatów danych, znaków, metod odwzorowywania i wielkości znaków.

Należy mieć na uwadze następujące zagadnienia dotyczące NLS:

- Dane są przesyłane pomiędzy serwerami LDAP a klientami w formacie UTF-8. Dozwolone są wszystkie znaki ISO 10646.
- Serwer Directory Server w celu wprowadzenia danych do bazy danych korzysta z metody odwzorowania UTF-16.
- Serwer i klient porównują ciągi znaków, nie rozróżniając wielkich i małych liter. Algorytmy wykorzystujące wielkie litery nie działają poprawnie dla wszystkich języków (ustawień narodowych).

### Informacje pokrewne

Globalizacja systemu i5/OS

Więcej informacji dotyczących obsługi języków narodowych zawiera temat Globalizacja systemu i5/OS.

## Znaczniki języka

Termin *znaczniki języka* oznacza mechanizm, dzięki któremu serwer Directory Server może przypisać kody języka naturalnego wartościom przechowywanym w katalogu. Pozwalają one wprowadzać klientom zapytania o wartości w katalogu spełniające określone wymagania języka naturalnego.

Znacznik języka jest komponentem opisu atrybutu. Znacznik języka to łańcuch o przedrostku lang-, podstawowym podznaczniku złożonym ze znaków alfabetycznych i opcjonalnie, z następujących po nich podznaczników połączonych łącznikiem (-). Kolejne podznaczniki mogą być dowolną kombinacją znaków alfanumerycznych. Tylko podstawowy podznacznik musi być złożony ze znaków alfabetycznych. Podznaczniki mogą mieć dowolną długość. Jedynym ograniczeniem jest całkowita długość znacznika, która nie może przekraczać 240 znaków. Znaczniki języka nie rozróżniają wielkości liter; wartości en-us, en-US i EN-US są identyczne. Znaczniki języka nie są dozwolone w komponentach nazw wyróżniających (DN) lub RDN. Dozwolony jest tylko jeden znacznik języka w opisie atrybutu.

**Uwaga:** W zależności od atrybutu, atrybuty unikalne i znaczniki języka wykluczają się wzajemnie. Jeśli pewien atrybut został określony jako unikalny, znaczniki języka nie mogą zostać do niego przypisane.

Jeśli znaczniki języka zostaną włączone podczas dodawania danych do katalogu, mogą być używane w działaniach wyszukiwania do selektywnego pobierania wartości atrybutów w specyficznych językach. Jeśli znacznik języka dostarczany jest przez opis atrybutu w obrębie żądanej w wyszukiwaniu listy atrybutów, zwrócone zostaną tylko te wartości atrybutów w pozycji katalogu, które posiadają ten sam znacznik języka, jak znacznik dostarczony. Dlatego dla wyszukiwania typu:

```
ldapsearch -b "o=ibm,c=us" (objectclass=organization) description;lang=en
```

serwer zwraca wartości atrybutu "description;lang-en", ale nie zwraca wartości atrybutu "description" lub "description;lang-fr".

Jeśli wprowadzone zostanie żądanie określające atrybut bez podania znacznika języka, zwrócone zostaną wszystkie wartości atrybutów niezależnie od ich znaczników języka.

Typ atrybutu i znacznik języka oddzielone są znakiem średnika (;).

**Uwaga:** Znak średnika dozwolony jest w AttributeType w części "NAME". Jednakże, ponieważ znak ten jest używany do oddzielenia AttributeType od znacznika języka, użycie go w AttributeType w części "NAME" nie jest dozwolone.

Na przykład, jeśli klient żąda atrybutu "description", a zgodna pozycja zawiera:

```
objectclass: top
objectclass: organization
o: Software GmbH
description: software
```

```
description;lang-en: software products
description;lang-de: Softwareprodukte
postalAddress: Berlin 8001 Germany
postalAddress;lang-de: Berlin 8001 Deutschland
```

serwer zwraca:

```
description: software
description;lang-en: software products
description;lang-de: Softwareprodukte
```

Jeśli wyszukiwanie żąda atrybutu "description;lang-de", serwer zwraca:

```
description;lang-de: Softwareprodukte
```

Użycie znaczników języka umożliwia istnienie wielojęzycznych danych w katalogach obsługujących klientów działających w różnych językach. Wykorzystując znaczniki języka, można napisać aplikację, aby klient niemiecki widział tylko dane wprowadzone dla atrybutu lang-de, a klient francuski widział tylko dane wprowadzone dla atrybutu lang-fr.

Aby określić, czy funkcja znaczników języka została włączona, należy wprowadzić wyszukiwanie DSE w katalogu głównym określając atrybut "ibm-enabledCapabilities".

```
ldapsearch -b "" -s base objectclass=* ibm-enabledCapabilities
```

Jeśli zwrócono zostanie OID "1.3.6.1.4.1.4203.1.5.4", funkcja jest włączona.

Jeśli obsługa znaczników języka nie jest włączona, każde działanie LDAP przypisujące znacznik języka do atrybutu jest odrzucane i wysyłany jest komunikat o błędzie.

Pewne atrybuty mogą posiadać przypisane im znaczniki języka, inne nie. Aby określić, czy atrybut zezwala na znaczniki języka, należy użyć komendy ldapexop:

- W przypadku atrybutów, które zezwalają na znaczniki języka: ldapexop -op getattributes-attrType language\_tag -matches true
- W przypadku atrybutów, które nie zezwalają na znaczniki języka: ldapexop -op getattributes -attrType language\_tag -matches false

#### **Zadania pokrewne**

“Dodawanie pozycji zawierającej atrybuty ze znacznikami języka” na stronie 197

Ten temat zawiera informacje dotyczące tworzenia pozycji zawierającej atrybuty ze znacznikami języka.

## **Odwołania do katalogu LDAP**

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

Serwer Directory Server pozwala używać dwóch typów odwołań. Można określić domyślne serwery odwołań, w których serwer LDAP będzie odwoływał się do klientów zawsze, gdy nie znajdzie nazwy DN w katalogu. Aby do serwera katalogów dodać pozycje, które mają odwołanie objectClass, można także użyć klienta LDAP. Umożliwia to określanie odwołań zależnych od żądanej przez klienta nazwy DN.

**Uwaga:** W serwerze Directory Server obiekty odwołania muszą zawierać wyłącznie nazwę wyróżniającą (dn), klasę obiektu (objectClass) i atrybut odwołania (ref). Przykład ilustrujący to ograniczenie zawiera temat dotyczący komendy ldapsearch.

Serwery odwołań są ściśle powiązane z serwerami replik. Ponieważ klienci nie mogą zmieniać danych na serwerach replik, to przekazują one wszystkie żądania zmiany danych katalogu do serwera głównego.

#### **Zadania pokrewne**



“Określanie serwera odwołań do katalogu” na stronie 123  
Ten temat zawiera informacje dotyczące określania serwera odwołań.

#### **Odsyłacze pokrewne**

“ldapsearch” na stronie 236  
Program narzędziowy wiersza komend do wyszukiwania w katalogu LDAP.

## **Transakcje**

Serwer Directory Server można tak skonfigurować, aby programy typu klient mogły korzystać z transakcji. Transakcja to grupa działań na katalogu LDAP traktowanych jak jedna jednostka.

Żadne z pojedynczych działań LDAP stanowiących część transakcji nie zostanie wprowadzone na stałe, dopóki wszystkie działania w transakcji nie zakończą się pomyślnie, a transakcja nie zostanie zatwierdzona. Jeśli którakolwiek czynność się nie powiedzie lub transakcja zostanie anulowana, pozostałe działania zostaną wycofane. Umożliwia to utrzymanie porządku w działaniach LDAP. Użytkownik może na przykład skonfigurować w swoim kliencie transakcję, która będzie usuwała kilka pozycji katalogu. Jeśli w trakcie transakcji klient utraci połączenie z serwerem, żadna z pozycji nie zostanie usunięta. Można wtedy uruchomić transakcję ponownie, bez sprawdzania, które pozycje zostały pomyślnie usunięte.

Następujące działania LDAP mogą stanowić część transakcji:

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

**Uwaga:** W transakcjach nie należy umieszczać 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 z serwerem katalogów.

#### **Zadania pokrewne**

“Określanie ustawień transakcji” na stronie 122  
Ten temat zawiera informacje dotyczące konfigurowania ustawień transakcji serwera Directory Server.

## **Bezpieczeństwo serwera Directory Server**

Informacje o funkcjach służących do zabezpieczania serwera Directory Server.

W następujących tematach znajduje się więcej informacji o bezpieczeństwie serwera Directory Server:

#### **Pojęcia pokrewne**

“Katalogi” na stronie 4

Serwer Directory Server umożliwia dostęp do bazy danych specjalnego typu, w której informacje są zapisywane w strukturze hierarchicznej podobnej do organizacji zintegrowanego systemu plików systemu i5/OS.

“Nazwy wyróżniające (DN)” na stronie 9

Każda pozycja w katalogu ma nazwę wyróżniającą (DN). Nazwa DN jednoznacznie identyfikuje pozycję w katalogu. Pierwszy komponent nazwy DN jest nazywany względną nazwą wyróżniającą (RDN).

“Zadania związane z właściwościami bezpieczeństwa” na stronie 176

Ten temat zawiera informacje dotyczące zarządzania zadaniami związanymi z właściwościami bezpieczeństwa.

#### **Zadania pokrewne**

“Włączanie kontrolowania obiektów na serwerze Directory Server” na stronie 127

Ten temat zawiera informacje dotyczące włączania kontrolowania obiektów na serwerze Directory Server.

## **Kontrola**

Kontrola umożliwia śledzenie szczegółów określonych transakcji serwera Directory Server.

Serwer Directory Server obsługuje funkcje kontroli bezpieczeństwa systemu i5/OS. Kontroli podlegają:

- łączenie się z serwerem katalogów i odłączanie od niego;
- zmiany w uprawnieniach do obiektów katalogu LDAP;
- zmiany praw własności obiektów katalogu LDAP;
- tworzenie, usuwanie, wyszukiwanie i modyfikowanie obiektów katalogu LDAP;
- zmiany hasła administratora i aktualizowanie nazw wyróżniających;
- zmiany haseł użytkowników;
- import i eksport plików.

Aby kontrola pozycji katalogu działała, konieczne może się okazać wprowadzenie kilku zmian do ustawień kontroli. Jeśli w wartości systemowej QAUDCTL podano parametr \*OBJAUD, to można włączyć kontrolowanie obiektów za pomocą programu System i Navigator.

Do kontroli można wskazać nazwy grup. Autoryzowani klienci mogą zażądać, aby operacja była wykonywana z uprawnieniem grup podanych przez klienta, a nie grup, jakie serwer powiązał z tożsamością klienta. To ustawienie określa, czy kontrola tych żądań tylko wskazuje na to, że klient określił grupy, jakie mają być używane, czy też dołącza listę podanych grup. Kontrola listy grup tworzy dodatkowe pozycje kontroli z listą grup dla każdego żądania.

Aby określić, czy nazwy grup mają być kontrolowane, należy wykonać następujące czynności:

1. W programie System i Navigator rozwiń pozycję **Sieć**.
2. Rozwiń pozycję **Serwery**.
3. Kliknij **TCP/IP**.
4. Prawym przyciskiem myszy kliknij **IBM Directory Server** i wybierz **Właściwości**.
5. Na karcie **Kontrola** (Auditing) zaznacz pole wyboru **Uwzględnij nazwy grup podczas kontroli użycia grup określonych przez program wywołujący** (Include group names when auditing use of caller-specified groups).

#### Pojęcia pokrewne

“Katalogi rozproszone” na stronie 7

Katalog rozproszony to środowisko, w którym dane są rozdzielone na wiele serwerów katalogów. Aby katalog rozproszony wyglądał dla aplikacji klienckich jak pojedynczy katalog, wykorzystuje się jeden lub wiele serwerów proxy, które mają informacje o wszystkich serwerach i znajdujących się na nich danych.

#### Zadania pokrewne

“Włączanie kontrolowania obiektów na serwerze Directory Server” na stronie 127

Ten temat zawiera informacje dotyczące włączania kontrolowania obiektów na serwerze Directory Server.

#### Informacje pokrewne

Dokumentacja dotycząca bezpieczeństwa

Kontrolowanie bezpieczeństwa

Więcej informacji dotyczących kontroli zawiera temat Kontrolowanie bezpieczeństwa.

## Protokoły SSL (Secure Sockets Layer) i TLS (Transport Layer Security) na serwerze Directory Server

Aby komunikacja z serwerem Directory Server była bezpieczniejsza, serwer może używać protokołów SSL (Secure Sockets Layer) i TLS (Transport Layer Security).

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

Aby używać protokołu SSL, w systemie musi być zainstalowany program Digital Certificate Manager (opcja 34 systemu i5/OS). Program DCM udostępnia interfejs umożliwiający tworzenie certyfikatów cyfrowych i baz certyfikatów oraz zarządzanie nimi.

Protokół TLS został zaprojektowany jako następca protokołu SSL i wykorzystuje te same metody szyfrowania, ale obsługuje więcej algorytmów szyfrowania. Protokół TLS umożliwia serwerowi odbierać bezpieczne i niezabezpieczone połączenia komunikacyjne od klienta, za pośrednictwem domyślnego portu 389. Dla bezpiecznej komunikacji, klient musi używać rozszerzonej operacji StartTLS.

Aby klient mógł używać protokołu TLS:

1. Serwer Directory Server musi być skonfigurowany do używania protokołu TLS lub SSL/TLS.
2. Opcja -Y musi być określona w narzędziach wiersza komend klienta.

**Uwaga:** Protokoły TLS i SSL nie są współdziałające. Wprowadzenie żądania uruchomienia TLS (opcja -Y) poprzez port SSL spowoduje błąd działania.

Klient może połączyć się z bezpiecznym portem (636) za pomocą TLS lub SSL. Opcja StartTLS jest opcją LDAP pozwalającą uruchomić bezpieczne połączenia komunikacyjne za pośrednictwem istniejącego niezabezpieczonego połączenia (tzn. portu 389). Jako takiej, opcji StartTLS (lub opcji -Y narzędzia wiersza komend) można użyć tylko dla standardowego portu niezabezpieczonego (389); opcji StartTLS nie można używać z bezpiecznym połączeniem.

#### **Zadania pokrewne**

“Włączanie SSL i TLS na serwerze Directory Server” na stronie 182

W tym temacie opisano włączanie zabezpieczeń SSL i TLS na serwerze Directory Server.

“Włączanie SSL i TLS na serwerze Directory Server” na stronie 182

W tym temacie opisano włączanie zabezpieczeń SSL i TLS na serwerze Directory Server.

“Używanie protokołu SSL z programami narzędziowymi LDAP wiersza komend” na stronie 250

Ten temat zawiera informacje o używaniu protokołu SSL podczas pracy z programami narzędziowymi LDAP wiersza komend.

#### **Informacje pokrewne**

Program Digital Certificate Manager

Protokół SSL

Obsługiwane protokoły SSL i TLS

## **Uwierzytelnianie Kerberos w serwerze Directory Server**

Serwer Directory Server umożliwia korzystanie z uwierzytelniania Kerberos. Kerberos to sieciowy protokół uwierzytelniania używający szyfrowania kluczem tajnym, który udostępnia usługi silnego uwierzytelniania aplikacjom klienckim i serwerowym.

Aby włączyć uwierzytelnianie protokołem Kerberos, konieczne jest skonfigurowanie usługi uwierzytelniania sieciowego.

Obsługa protokołu Kerberos w serwerze Directory Server obejmuje mechanizm SASL GSSAPI. Umożliwia to zarówno serwerowi Directory Server, jak i klientom LDAP w systemie Windows 2000 korzystanie z uwierzytelniania Kerberos w serwerze Directory Server.

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

`nazwa-usługi/nazwa-hosta@dziedzina`

`nazwa-usługi` to `ldap` (`ldap` musi być pisane małymi literami), `nazwa-hosta` to pełna nazwa systemu w sieci TCP/IP, zaś `dziedzina` jest domyślną dziedziną podawaną w konfiguracji protokołu Kerberos w systemie.

Na przykład, w przypadku systemu o nazwie `mój-as400` w domenie TCP/IP `acme.com`, z domyślną dziedziną Kerberos `ACME.COM`, nazwa użytkownika Kerberos serwera LDAP powinna brzmieć `ldap/mój-as400.acme.com@ACME.COM`. Domyślna dziedzina protokołu Kerberos jest podana w jego pliku konfiguracyjnym (domyślnie jest to `/QIBM/UserData/OS400/NetworkAuthentication/krb5.conf`) z dyrektywą `default_realm` (`default_realm = ACME.COM`). 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 Directory Server przypisuje nazwę wyróżniającą (DN) do połączeniem, określając w ten sposób dostęp do danych katalogu. Nazwę wyróżniającą serwera można przypisać za pomocą jednej z przedstawionych metod:

- Serwer może utworzyć nazwę wyróżniającą w oparciu o identyfikator protokołu Kerberos. Po wybraniu tej opcji tożsamość Kerberos w postaci nazwa\_użytkownika@dzielnicza generuje nazwę wyróżniającą w postaci ibm-nk=nazwa\_użytkownika@dzielnicza. Nazwa ibm-kn= jest równoznaczna z ibm-kerberosName=.
- Serwer wyszukuje w katalogu nazwy wyróżniającej (DN), która zawiera pozycję dla nazwy użytkownika i dziedziny protokołu Kerberos. Po wybraniu tej opcji serwer przeszukuje katalog, aby znaleźć pozycję określającą protokół Kerberos.

Niezbędny jest plik tabeli kluczy (keytab) zawierający klucz dla nazwy użytkownika usługi LDAP.

### **Informacje pokrewne**

Usługa uwierzytelniania sieciowego

Więcej informacji dotyczących protokołu Kerberos zawiera temat Usługa uwierzytelniania sieciowego.

Konfigurowanie usługi uwierzytelniania sieciowego

Instrukcje dodawania informacji do plików tabeli kluczy (keytab) zawiera temat Konfigurowanie usługi uwierzytelniania sieciowego.

## **| Szyfrowanie haseł**

| Serwer IBM Tivoli Directory Server umożliwia zapobieganie nieuprawnionemu dostępowi do haseł użytkowników.

| Administrator może skonfigurować serwer, aby szyfrował wartości atrybutu userPassword w formacie szyfrowania jednokierunkowego lub dwukierunkowego. Zasyfrowane hasła są oznaczane nazwą algorytmu szyfrującego, dlatego w katalogu mogą istnieć jednocześnie hasła zasyfrowane w różnych formatach. Po zmianie konfiguracji szyfrowania istniejące zasyfrowane hasła pozostaną niezmienione i nadal będą działać.

| W przypadku formatów szyfrowania jednokierunkowego hasła użytkowników mogą być szyfrowane i składowane w katalogu, co zapobiega dostępowi do zapisanych jawnym tekstem haseł ze strony jakichkolwiek użytkowników, w tym administratorów systemu. W przypadku szyfrowania dwukierunkowego hasła są szyfrowane podczas składowania w bazie danych, a następnie deszyfrowane podczas udostępniania autoryzowanym klientom. Zastosowanie szyfrowania dwukierunkowego zabezpiecza hasło składowane w bazie danych, umożliwiając jednocześnie użycie takich metod uwierzytelniania, jak DIGEST-MD5, które wymagają dostępu serwera do hasła zapisanego jawnym tekstem, oraz korzystanie z aplikacji, które mogą wymagać hasła w postaci jawnego tekstu.

| Hasła zasyfrowane jednokierunkowo umożliwiają sprawdzenie zgodności hasła, ale nie można ich deszyfrować. Podczas logowania użytkownika podane hasło jest szyfrowane i porównywane z przechowywaną wersją w celu sprawdzenia zgodności.

| Nawet jeśli serwer jest skonfigurowany do przechowywania nowych haseł w określonym formacie, będzie on akceptował hasła poprzednio zasyfrowane inną metodą. Na przykład serwer może być skonfigurowany do szyfrowania hasła algorytmem AES256, ale nadal będzie umożliwiał administratorowi ładowanie danych z innego serwera, który zawiera hasła zasyfrowane algorytmem SHA-1. Oba zestawy haseł mogą służyć do uwierzytelniania w serwerze za pomocą prostego uwierzytelniania hasłem, ale hasła SHA-1 będą zwracane jako zasyfrowane łańcuchy i nie będzie można ich używać do uwierzytelniania metodą DIGEST-MD5.

| Formaty szyfrowania jednokierunkowego to:

- | • SHA-1
- | • MD5
- | • crypt

| Po skonfigurowaniu serwera wszelkie nowe hasła (nowych użytkowników) lub zmodyfikowane hasła (istniejących użytkowników) są szyfrowane przed zapisaniem w bazie danych katalogu. Następujące później wyszukiwania LDAP będą zwracały oznaczoną i zasyfrowaną wartość.

W przypadku aplikacji wymagających pobrania haseł zapisanych jawnym tekstem, na przykład agentów uwierzytelniania warstwy pośredniej, administrator katalogu musi skonfigurować serwer, aby szyfrował hasła użytkowników algorytmem dwukierunkowym. W takim przypadku hasła zwracane przez serwer w postaci jawnego tekstu są zabezpieczone przez mechanizm list kontroli dostępu katalogu.

Formaty szyfrowania dwukierunkowego to:

- Brak
- AES

Opcja szyfrowania dwukierunkowego - algorytm AES - umożliwia szyfrowanie wartości atrybutu userPassword w katalogu i pobieranie jej jako części pozycji w pierwotnej postaci jawnego tekstu. Można ją skonfigurować tak, aby używany był klucz o długości 128, 192 i 256 bitów. Niektóre aplikacje, na przykład serwery uwierzytelniające warstwy pośredniej, wymagają pobierania haseł w postaci jawnego tekstu. Jednakże obowiązująca w firmie strategia bezpieczeństwa może zabraniać przechowywania haseł zapisanych jawnym tekstem w dodatkowej pamięci trwałej. Opcja ta spełnia oba te wymagania.

Ponadto w przypadku użycia szyfrowania haseł algorytmem AES w sieci replikowanej, jeśli wszystkie serwery są skonfigurowane za pomocą tego samego hasła AES i klucza dodatkowego, dane hasła będą replikowane w postaci zaszyfrowanej, co zapewnia lepsze zabezpieczenie hasła. Jeśli serwer nie obsługuje algorytmu AES lub jest skonfigurowany z innymi danymi AES, hasła będą deszyfrowane i replikowane w postaci jawnego tekstu.

**Uwaga:**

1. Algorytm AES nie jest obsługiwany na serwerach LDAP w wersji wcześniejszej niż V6R1. Mówiąc dokładniej, replikacja danych zaszyfrowanych algorytmem AES nie jest obsługiwana na serwerach LDAP w wersji wcześniejszej niż V6R1.
2. Na innych platformach po wybraniu opcji 'Brak' hasła są zapisywane w bazie danych w postaci jawnego tekstu. Jeśli taki serwer jest częścią sieci, w której znajduje się serwer IBM Tivoli Directory Server działający na innych platformach, zaleca się użycie jednej z opcji szyfrowania AES.

Proste łączenie powiedzie się, jeśli hasło podane w żądaniu łączenia jest zgodne z jedną z wielu wartości atrybutu userPassword.

Po skonfigurowaniu serwera za pomocą narzędzia Web Administration można wybrać jedną z następujących opcji szyfrowania:

**Brak** Hasła są zapisywane na liście sprawdzania w postaci zaszyfrowanej dwukierunkowo i wczytywane jako część pozycji w pierwotnej postaci jawnego tekstu. Aby możliwe było używanie tego ustawienia, wartość systemowa QRETSVRSEC musi wynosić 1.

**crypt** Hasła są szyfrowane za pomocą algorytmu szyfrowania crypt systemu UNIX zanim zostaną wprowadzone do katalogu. W przypadku zastosowania tej metody używane będzie tylko pierwszych 8 znaków hasła. Hasła dłuższe niż 8 znaków będą obcinane.

**MD5** Hasła są szyfrowane za pomocą algorytmu MD5 zanim zostaną wprowadzone do katalogu.

**SHA-1** Hasła są szyfrowane za pomocą algorytmu SHA-1 zanim zostaną wprowadzone do katalogu.

**AES128**

Hasła są szyfrowane za pomocą algorytmu AES128 zanim zostaną wprowadzone do katalogu i są wczytywane jako część pozycji w pierwotnej postaci jawnego tekstu.

**AES192**

Hasła są szyfrowane za pomocą algorytmu AES192 zanim zostaną wprowadzone do katalogu i są wczytywane jako część pozycji w pierwotnej postaci jawnego tekstu.

**AES256**

Hasła są szyfrowane za pomocą algorytmu AES256 zanim zostaną wprowadzone do katalogu i są wczytywane jako część pozycji w pierwotnej postaci jawnego tekstu.

| **Uwaga:** Format imask dostępny w poprzednich wersjach nie jest już dostępny w celu szyfrowania. Jednak istniejące  
| wartości zaszyfrowane metodą imask nadal działają.

| Domyślną opcją serwera Tivoli Directory Server for i5/OS jest algorytm SHA-1, który jest kompatybilny z  
| wcześniejszymi wydaniem i nie wymaga ustawiania hasła i klucza dodatkowego AES.

| Oprócz atrybutu `userPassword` w katalogu algorytmem AES256 zawsze szyfrowane są wartości atrybutu `secretKey`.  
| W przeciwieństwie do atrybutu `userPassword`, szyfrowanie wartości atrybutu `secretKey` jest wymuszane. Nie jest  
| dostępna żadna inna opcja. Atrybut `secretKey` to schemat zdefiniowany przez IBM. Aplikacje mogą używać tego  
| atrybutu do przechowywania poufnych danych, które należy w katalogu zawsze szyfrować, oraz do wczytywania tych  
| danych w postaci jawnego tekstu za pomocą mechanizmu kontroli dostępu w katalogu.

| Aby zmienić typ szyfrowania za pomocą wiersza komend, na przykład na format **crypt**, należy uruchomić następującą  
| komendę:

| `ldapmodify -D <nazwa_dn_administratora> -w <hasło_administratora> -i <plik>`

| gdzie <plik> zawiera:

```
| dn: cn=configuration  
| changetype: modify  
| replace: ibm-slappwEncryption  
| ibm-slappwEncryption: crypt
```

| Aby zaktualizowane ustawienia odniosły skutek dynamicznie, należy uruchomić następującą komendę `ldapexop`:

```
| ldapexop -D <nazwa_dn_administratora> -w <hasło_administratora> -op readconfig -scope single  
| "cn=configuration" ibm-slappwEncryption
```

| **Uwaga:** Aby zmienić konfigurację, należy uwierzytelnić się za pomocą nazwy wyróżniającej użytkownika  
| rzutowanego i hasła dla profilu użytkownika i5/OS mającego uprawnienia specjalne `*ALLOBJ` i  
| `*IOSYSCFG`. Są to te same uprawnienia, które są wymagane do zmiany konfiguracji serwera za pomocą  
| innych interfejsów.

### Zadania pokrewne

“Ustawianie właściwości strategii haseł” na stronie 176

Ten temat zawiera informacje dotyczące ustawiania właściwości strategii haseł.

## Grupy i role

Wykorzystanie grup i ról pozwala organizować i kontrolować uprawnienia dostępu poszczególnych członków grup.

Grupa jest listą, czyli kolekcją nazw. Grupa może być podawana w atrybutach **aclentry**, **ibm-filterAclEntry** i **entryowner** w celu kontrolowania dostępu lub w konkretnych zastosowaniach aplikacyjnych, takich jak listy adresowe. Grupy można definiować jako statyczne, dynamiczne lub zagnieżdżone.

Role są podobne do grup, ponieważ w katalogu są reprezentowane przez obiekt. Ponadto role zawierają grupę nazw wyróżniających.

Więcej informacji na ten temat zawierają poniższe sekcje:

### Pojęcia pokrewne

“Listy kontroli dostępu” na stronie 64

Listy kontroli dostępu (ACL) stanowią ochronę informacji zapisanych w katalogu LDAP. Za pomocą list ACL administratorzy ograniczają dostęp do różnych części katalogu lub konkretnych jego pozycji.

“Zadania związane z użytkownikami i grupami” na stronie 203

Ten temat zawiera informacje dotyczące zarządzania użytkownikami i grupami.

### Zadania pokrewne

“Dodawanie grup” na stronie 204

Ten temat zawiera informacje dotyczące dodawania grup.

“Tworzenie grup” na stronie 209

Ten temat zawiera informacje dotyczące tworzenia grup.

### Grupy statyczne:

W grupach statycznych elementy są definiowane przez wyliczenie.

Grupa statyczna definiuje każdy element indywidualnie za pomocą strukturalnej klasy obiektu **groupOfNames**, **groupOfUniqueNames**, **accessGroup** lub **accessRole**, bądź pomocniczej klasy obiektu **ibm-staticgroup**. Statyczna grupa używająca strukturalnej klasy obiektu **groupOfNames** lub **groupOfUniqueNames** musi zawierać przynajmniej jeden element. Grupa używająca strukturalnej klasy obiektu **accessGroup** lub **accessRole** może być pusta. Statyczną grupę można również zdefiniować za pomocą pomocniczej klasy obiektu **ibm-staticGroup**, która nie wymaga atrybutu **member** i dlatego może być pusta.

Typową pozycją grupy jest:

```
DN: cn=Dev.Staff,ou=Austin,c=US
   objectclass: accessGroup
   cn: Dev.Staff
   member: cn=Jan Kowalski,o=IBM,c=US
   member: cn=Janina Nowak,o=IBM,c=US
   member: cn=Tomasz Nowak,o=IBM,c=US
```

Każdy obiekt grupy zawiera wielowartościowy atrybut składający się z nazw wyróżniających elementów.

Po usunięciu grupy dostępu jest ona również kasowana na wszystkich listach ACL, na których się znajdowała.

### Grupy dynamiczne:

Grupa dynamiczna definiuje swoje elementy przy użyciu wyszukiwania LDAP.

Do definiowania wyszukiwania za pomocą uproszczonej składni adresu URL LDAP grupa dynamiczna używa strukturalnej klasy obiektu **groupOfURLs** (lub pomocniczej klasy obiektu **ibm-dynamicGroup**) oraz atrybutu **memberURL**.

```
ldap:///<podstawowa nazwa wyróżniająca wyszukiwania> ? ? <zasięg wyszukiwania> ? <filtr wyszukiwania>
```

**Uwaga:** W powyższym przykładzie nie wolno używać nazwy hosta. Pozostałe parametry należą do normalnej składni adresu URL ldap. Każde pole parametru należy oddzielić znakiem ?, nawet jeśli nie podano żadnego parametru. Zazwyczaj lista atrybutów do zwrócenia znajduje się pomiędzy nazwą wyróżniającą a zakresem wyszukiwania. Podczas określania dynamicznego członkostwa serwer również nie używa tego parametru, zatem można go pominąć, jednak separator ? musi być obecny.

gdzie:

#### podstawowa nazwa DN wyszukiwania

Jest punktem, w którym rozpoczyna się wyszukiwanie katalogu. Może to być przyrostek lub rdzeń nazwy katalogu, na przykład **ou=Austin**. Jest to parametr wymagany.

#### zakres wyszukiwania

Określa obszar wyszukiwania. Domyślnie jest to zakres podstawowy (base).

- base** Zwraca informacje tylko o podstawowej nazwie wyróżniającej określonej w adresie URL
- one** Zwraca informacje o pozycjach znajdujących się jeden poziom poniżej podstawowej nazwy wyróżniającej określonej w adresie URL. Nie zawiera pozycji podstawowej (base).
- sub** Zwraca informacje o pozycjach znajdujących się na wszystkich poziomach poniżej i obejmuje podstawową nazwę wyróżniającą.

## filtr wyszukiwania

Filtr, który ma zostać zastosowany w odniesieniu do pozycji w zakresie wyszukiwania. W temacie Opcja filtru ldapsearch znajdują się informacje o składni filtru wyszukiwania. Wartością domyślną jest `objectclass=*`

Wyszukiwanie dynamicznych elementów zawsze odbywa się w serwerze, dlatego w przeciwieństwie do pełnego adresu URL ldap nigdy nie określa się nazwy hosta ani numeru portu, a protokołem zawsze jest **ldap** (nigdy **ldaps**). Atrybut **memberURL** może zawierać dowolny adres URL, ale w celu określenia dynamicznego przypisania do grupy serwer używa tylko atrybutów **memberURL** zaczynających się od **ldap:///**.

## Przykłady

Pojedyncza pozycja, w której domyślnym zakresem jest base, a domyślnym filtrem `objectclass=*`:

```
ldap:///cn=Jan Kowalski, cn=Employees, o=Acme, c=US
```

Wszystkie pozycje znajdujące się jeden poziom poniżej `cn=Employees` z filtrem domyślnym `objectclass=*`:

```
ldap:///cn=Employees, o=Acme, c=US??one
```

Wszystkie pozycje podrzędne dla `o=Acme` z `objectclass=person`:

```
ldap:///o=Acme, c=US??sub?objectclass=person
```

W zależności od klas obiektu użytych do zdefiniowania pozycji użytkownika, pozycje te mogą nie zawierać atrybutów odpowiednich do określenia członkostwa w grupie. Można użyć pomocniczej klasy obiektu, **ibm-dynamicMember** w celu rozszerzenia pozycji użytkowników tak, aby zawierały atrybut **ibm-group**. Umożliwia on dodawanie dowolnych wartości do pozycji użytkowników, aby były obiektami docelowymi dla filtrów grup dynamicznych. Na przykład:

Do tej grupy dynamicznej należą pozycje znajdujące się bezpośrednio pod pozycją `cn=users,ou=Austin`, które mają atrybut `ibm-group GROUP1`:

```
dn: cn=GROUP1,ou=Austin
objectclass: groupOfURLs
cn: GROUP1
memberURL: ldap:///cn=users,ou=Austin??one?(ibm-group=GROUP1)
```

Oto przykład elementu grupy `cn=GROUP1,ou=Austin`:

```
dn: cn=Group 1 member, cn=users, ou=austin
objectclass: person
objectclass: ibm-dynamicMember
sn: member
userpassword: memberpassword
ibm-group: GROUP1
```

## Grupy zagnieżdżone:

Dzięki zagnieżdżaniu grup można tworzyć hierarchiczne relacje, które mogą służyć do definiowania dziedzicznego członkostwa w grupie.

Grupa zagnieżdżona jest to potomna pozycja grupy, w przypadku której atrybut zawarty w nadrzędnej pozycji grupy odwołuje się do jej nazwy wyróżniającej. Grupę nadrzędną tworzy się poprzez rozszerzenie jednej ze strukturalnych klas obiektu grupy (**groupOfNames**, **groupOfUniqueNames**, **accessGroup**, **accessRole** lub **groupOfURLs**) i dodanie pomocniczej klasy obiektu **ibm-nestedGroup**. Po rozszerzeniu grupy zagnieżdżonej można (ale nie trzeba) dodać dowolną liczbę atrybutów **ibm-memberGroup** o wartościach określających nazwy wyróżniające zagnieżdżonych grup potomnych. Na przykład:

```
dn: cn=Group 2, cn=Groups, o=IBM, c=US
objectclass: groupOfNames
objectclass: ibm-nestedGroup
objectclass: top
cn: Group 2
description: Grupa złożona z elementów statycznych i zagnieżdżonych.
```



```
member: cn=Person 2.1, cn=Dept 2, cn=Employees, o=IBM, c=US
member: cn=Person 2.2, cn=Dept 2, cn=Employees, o=IBM, c=US
ibm-memberGroup: cn=Group 8, cn=Nested Static, cn=Groups, o=IBM, c=US
```

Wprowadzanie cykli do hierarchii grup zagnieżdżonych nie jest dozwolone. Jeśli okaże się, że działanie grupy zagnieżdżonej powoduje cykliczne odwołania, bezpośrednie lub poprzez dziedziczenie, zostanie to uznane za naruszenie ograniczenia i aktualizacja pozycji zakończy się niepowodzeniem.

### Grupy hybrydowe:

Przynależność do grupy hybrydowej opisywana jest przez kombinację statycznych, dynamicznych i zagnieżdżonych typów elementów.

Na przykład:

```
dn: cn=Group 10, cn=Groups, o=IBM, c=US
objectclass: groupOfURLs
objectclass: ibm-nestedGroup
objectclass: ibm-staticGroup
objectclass: top
cn: Group 10
description: Grupa złożona z elementów statycznych, dynamicznych i zagnieżdżonych.
memberURL: ldap:///cn=Austin, cn=Employees, o=IBM, c=US??one?objectClass=person
ibm-memberGroup: cn=Group 9, cn=Nested Dynamic, cn=Groups, o=IBM, c=US
member: cn=Person 10.1, cn=Dept 2, cn=Employees, o=IBM, c=US
member: cn=Person 10.2, cn=Dept 2, cn=Employees, o=IBM, c=US
```

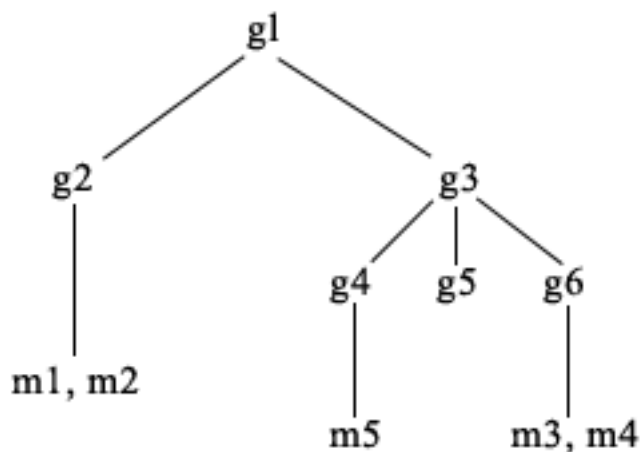
### Określanie członkostwa w grupie:

W celu odpytania agregowanego członkostwa w grupie można użyć dwóch atrybutów operacyjnych.

W przypadku danej pozycji grupy atrybut opcjonalny **ibm-allMembers** określa zagregowany zestaw członkostwa w grupie razem ze statycznymi, dynamicznymi i zagnieżdżonymi elementami w sposób opisany w hierarchii grup zagnieżdżonych. W przypadku danej pozycji użytkownika atrybut operacyjny **ibm-allGroups** określa zestaw agregacji grup, włącznie z grupami nadrzędnymi, których ten użytkownik jest członkiem.

Żądający może odebrać tylko podzestaw żądanych danych w zależności od sposobu ustawienia list ACL dla danych. Każdy może zażądać atrybutów operacyjnych **ibm-allMembers** i **ibm-allGroups**, ale zwrócony zestaw danych zawiera tylko dane dla tych pozycji i atrybutów LDAP, do których użytkownik wysyłający żądanie ma uprawnienia. Aby wyświetlić elementy statyczne, użytkownik żądający atrybutu **ibm-allMembers** lub **ibm-allGroups** musi mieć uprawnienia do wartości atrybutu **member** lub **uniquemember** dla grupy i grup zagnieżdżonych; w celu wyświetlenia dynamicznych członków musi mieć możliwość wykonywania operacji wyszukiwania określonych w wartościach atrybutu **memberURL**.

## Przykłady hierarchii



W tym przykładzie **m1** i **m2** są w atrybucie elementu **g2**. Lista ACL dla pozycji **g2** umożliwia użytkownikowi **user1** odczyt atrybutu elementu, ale użytkownik **user2** nie ma do niego dostępu. Format LDIF pozycji **g2** jest następujący:

```
dn: cn=g2,cn=groups,o=ibm,c=us
objectclass: accessGroup
cn: g2
member: cn=m1,cn=users,o=ibm,c=us
member: cn=m2,cn=users,o=ibm,c=us
aclentry: access-id:cn=user1,cn=users,o=ibm,c=us:normal:rsc
aclentry: access-id:cn=user2,cn=users,o=ibm,c=us:normal:rsc:at.member:deny:rsc
```

Pozycja **g4** ma domyślny atrybut `aclentry`, który umożliwia obu użytkownikom, **user1** i **user2**, odczyt atrybutu elementu. Format LDIF dla pozycji **g4** jest następujący:

```
dn: cn=g4, cn=groups,o=ibm,c=us
objectclass: accessGroup
cn: g4
member: cn=m5, cn=users,o=ibm,c=us
```

Pozycja **g5** jest grupą dynamiczną pobierającą dwa elementy z atrybutu `memberURL`. Format LDIF dla pozycji **g5** jest następujący:

```
dn: cn=g5, cn=groups,o=ibm,c=us
objectclass: container
objectclass: ibm-dynamicGroup
cn: g5
memberURL: ldap:///cn=users,o=ibm,c=us??sub?(|(cn=m3)(cn=m4))
```

Pozycje **m3** and **m4** są elementami grupy **g5**, ponieważ są zgodne z `memberURL`. Lista ACL dla pozycji **m3** umożliwia obu użytkownikom, **user1** i **user2**, jej wyszukiwanie. Lista ACL dla pozycji **m4** nie zezwala użytkownikowi **user2** na jej wyszukiwanie. Format LDIF dla pozycji **m4** jest następujący:

```
dn: cn=m4, cn=users,o=ibm,c=us
objectclass: person
cn: m4
sn: four
aclentry: access-id:cn=user1,cn=users,o=ibm,c=us:normal:rsc
aclentry: access-id:cn=user2,cn=users,o=ibm,c=us
```

### Przykład 1:

Użytkownik 1 przeprowadza wyszukiwanie w celu uzyskania wszystkich elementów grupy **g1**. Ma on dostęp do wszystkich elementów, zatem wszystkie zostaną zwrócone.

```
ldapsearch -D cn=user1,cn=users,o=ibm,c=us -w user1pwd -s base -b cn=g1,  
cn=groups,o=ibm,c=us objectclass=* ibm-allmembers
```

```
cn=g1,cn=groups,o=ibm,c=us  
ibm-allmembers: CN=M1,CN=USERS,O=IBM,C=US  
ibm-allmembers: CN=M2,CN=USERS,O=IBM,C=US  
ibm-allmembers: CN=M3,CN=USERS,O=IBM,C=US  
ibm-allmembers: CN=M4,CN=USERS,O=IBM,C=US  
ibm-allmembers: CN=M5,CN=USERS,O=IBM,C=US
```

### Przykład 2:

Użytkownik 2 przeprowadza wyszukiwanie w celu uzyskania wszystkich elementów grupy **g1**. Nie ma on dostępu do elementów **m1** i **m2**, ponieważ nie mają one dostępu do atrybutu elementu dla grupy **g2**.

Użytkownik 2 ma dostęp do atrybutu elementu dla grupy **g4** i dlatego ma dostęp do elementu **m5**. Może on wykonywać wyszukiwać pozycję **m3** w grupie **g5** atrybutu memberURL, zatem element ten znajduje się na liście, ale nie może przeprowadzać operacji wyszukiwania dla elementu **m4**.

```
ldapsearch -D cn=user2,cn=users,o=ibm,c=us -w user2pwd -s base -b cn=g1,  
cn=groups,o=ibm,c=us objectclass=* ibm-allmembers
```

```
cn=g1,cn=groups,o=ibm,c=us  
ibm-allmembers: CN=M3,CN=USERS,O=IBM,C=US  
ibm-allmembers: CN=M5,CN=USERS,O=IBM,C=US
```

### Przykład 3:

Użytkownik 2 przeprowadza wyszukiwanie, aby sprawdzić, czy **m3** należy do grupy **g1**. Użytkownik 2 ma dostęp do tego wyszukiwania, dlatego w rezultacie tego wyszukiwania wiadomo, że **m3** należy do grupy **g1**.

```
ldapsearch -D cn=user2,cn=users,o=ibm,c=us -w user2pwd -s base -b cn=m3,  
cn=users,o=ibm,c=us objectclass=* ibm-allgroups
```

```
cn=m3,cn=users,o=ibm,c=us  
ibm-allgroups: CN=G1,CN=GROUPS,O=IBM,C=US
```

### Przykład 4:

Użytkownik 2 przeprowadza wyszukiwanie, aby sprawdzić, czy **m1** należy do grupy **g1**. Użytkownik 2 nie ma dostępu do atrybutu elementu, więc wyszukiwanie nie wykaże, że **m1** należy do grupy **g1**.

```
ldapsearch -D cn=user2,cn=users,o=ibm,c=us -w user2pwd -s base -b  
cn=m1,cn=users,o=ibm,c=us objectclass=* ibm-allgroups
```

```
cn=m1,cn=users,o=ibm,c=us
```

## Klasy obiektu dla grup zagnieżdżonych i dynamicznych:

Ten temat zawiera wykaz klas obiektu grup dla grup zagnieżdżonych i dynamicznych.

### ibm-dynamicGroup

Ta klasa pomocnicza dopuszcza opcjonalny atrybut **memberURL**. Używa się jej z klasą strukturalną, na przykład **groupOfNames**, w celu utworzenia grupy hybrydowej z elementami dynamicznymi i statycznymi.

### ibm-dynamicMember

Ta klasa pomocnicza dopuszcza opcjonalny atrybut **ibm-group**. Należy go używać jako atrybutu filtrowania dla grup dynamicznych.

### ibm-nestedGroup

Ta klasa pomocnicza dopuszcza opcjonalny atrybut **ibm-memberGroup**. Używa się jej z klasą strukturalną, na przykład **groupOfNames**, aby możliwe było zagnieżdżanie podgrup w grupie nadrzędnej.

### ibm-staticGroup

Ta klasa pomocnicza dopuszcza opcjonalny atrybut **member**. Używa się jej z klasą strukturalną, na przykład **groupOfURLs**, w celu utworzenia grupy hybrydowej z elementami dynamicznymi i statycznymi.

**Uwaga:** Klasa **ibm-staticGroup** jest jedyną klasą, dla której atrybut **member** jest *opcjonalny*; wszystkie pozostałe klasy korzystające z atrybutu **member** wymagają określenia przynajmniej jednego członka grupy.

### Typy atrybutów grupy:

Ten temat zawiera wykaz typów atrybutów grupy.

#### **ibm-allGroups**

Pokazuje wszystkie grupy, do których należy pozycja. Pozycja może należeć do grupy bezpośrednio poprzez atrybuty **member**, **uniqueMember** lub **memberURL** albo pośrednio przez atrybut **ibm-memberGroup**. Ten atrybut operacyjny **tylko do odczytu** nie jest dozwolony w filtrze wyszukiwania. Atrybutu **ibm-allGroups** można użyć w żądaniu porównania w celu określenia, czy pozycja należy do danej grupy. Na przykład, aby określić, czy "cn=john smith,cn=users,o=my company" należy do grupy "cn=system administrators, o=my company":

```
rc = ldap_compare_s(ld, "cn=john smith,cn=users,o=my company, "ibm-allgroups",  
"cn=system administrators,o=my company");
```

#### **ibm-allMembers**

Pokazuje wszystkich członków grupy. Pozycja może należeć do grupy bezpośrednio poprzez atrybuty **member**, **uniqueMember** lub **memberURL** albo pośrednio przez atrybut **ibm-memberGroup**. Ten atrybut operacyjny **tylko do odczytu** nie jest dozwolony w filtrze wyszukiwania. Atrybutu **ibm-allMembers** można użyć w żądaniu porównania w celu określenia, czy nazwa wyróżniająca należy do danej grupy. Na przykład, aby określić, czy "cn=john smith,cn=users,o=my company" należy do grupy "cn=system administrators, o=my company":

```
rc = ldap_compare_s(ld, "cn=system administrators,o=my company, "ibm-allmembers",  
"cn=john smith,cn=users,o=my company");
```

#### **ibm-group**

Atrybut pobierany przez pomocniczą klasę **ibm-dynamicMember**. Służy do definiowania dowolnych wartości sterujących członkostwem pozycji w grupach dynamicznych. Można na przykład dodać wartość "Drużyna kręglarska", aby uwzględnić pozycję w dowolnym **memberURL** mającym filtr "ibm-group=Drużyna kręglarska".

#### **ibm-memberGroup**

Atrybut pobierany przez pomocniczą klasę **ibm-nestedGroup**. Określa podgrupy pozycji grupy nadrzędnej. Podczas przetwarzania list ACL lub atrybutów operacyjnych **ibm-allMembers** i **ibm-allGroups** elementy wszystkich takich podgrup uznaje się za elementy należące do grupy nadrzędnej. Pozycje podgrupy same *nie* są elementami. Przynależność do grup zagnieżdżonych jest rekurencyjna.

#### **member**

Określa nazwy wyróżniające dla każdego elementu grupy. Na przykład: member: cn=John Smith, dc=ibm, dc=com.

#### **memberURL**

Określa adres URL powiązany z każdym elementem grupy. Można użyć dowolnego typu oznaczonego adresu URL. Na przykład: memberURL: ldap:///cn=jsmith,dc=ibm,dc=com.

#### **uniquemember**

Określa grupę nazw powiązanych z pozycją, przy czym każda nazwa ma przypisany uniqueIdentifier w celu zapewnienia unikalności. Wartością atrybutu uniqueMember jest nazwa wyróżniająca, po której następuje uniqueIdentifier. Na przykład: uniqueMember: cn=John Smith, dc=ibm, dc=com 17.

#### **Role:**

Autoryzacja oparta na rolach to dopełnienie autoryzacji opartej na grupach.

Należąc do roli, użytkownik ma uprawnienia do wykonywania wszystkich operacji, których wymaga praca na jego stanowisku. W przeciwieństwie do grup, zestaw uprawnień przypisany do ról jest niejawni. Nie ma domniemanego założenia dotyczącego rodzaju uprawnień uzyskiwanych (lub traconych) poprzez członkostwo grupy.

Role są podobne do grup, ponieważ w katalogu są reprezentowane przez obiekt. Ponadto role zawierają grupę nazw wyróżniających. Role, które mają służyć do określania praw dostępu, muszą mieć klasę obiektu 'AccessRole'. Klasa obiektu 'Accessrole' jest podklasą klasy obiektu 'GroupOfNames'.

Na przykład jeśli istnieje kolekcja nazw wyróżniających, takich jak 'sys admin', pierwszą reakcją może być traktowanie ich jako 'grupy sys admin' (ponieważ grupy i użytkownicy są najbardziej rozpowszechnionymi typami atrybutów uprawnień). Jednakże, ponieważ istnieje zestaw uprawnień, których użytkownik oczekuje jako członek grupy 'sys admin', nazwy wyróżniające mogą być dokładniej definiowane jako 'rola sys admin'.

## Dostęp administracyjny

Dostęp administracyjny służy do kontrolowania praw dostępu do konkretnych zadań administracyjnych.

Serwer IBM Directory Server zezwala na następujące typy dostępu administracyjnego:

- **Rzutowany administrator systemu i5/OS:** klient uwierzytelniony jako użytkownik rzutowany (wpis LDAP odpowiadający profilowi użytkownika systemu operacyjnego) z uprawnieniami specjalnymi \*ALLOBJ i \*IOSYSCFG jest uprawniony do zmiany konfiguracji katalogu za pomocą interfejsów LDAP (poddzwawa cn=configuration lub zadania "Server administration" w narzędziu Web Administration). Ma także uprawnienia do działania jako administrator LDAP dla innych pozycji w katalogu (zapisanych w jednym z przyrostków DB2 lub w schemacie). Tylko rzutowani administratorzy systemu i5/OS mogą zmieniać konfigurację serwera.
- **Administrator LDAP:** serwer Directory Server zezwala, aby pojedynczy identyfikator użytkownika (określony nazwą wyróżniającą) był głównym administratorem serwera LDAP. Serwer Directory Server zezwala także, aby rzutowane profile użytkowników systemu operacyjnego były administratorami LDAP. Administratorzy serwera LDAP mogą wykonywać wiele czynności administracyjnych, takich jak zarządzanie replikacją, schematem i pozycjami katalogu.
- **Grupa użytkowników administracyjnych:** rzutowany administrator systemu i5/OS może wyznaczyć kilku użytkowników, którzy będą należeć do grupy administracyjnej. Członkowie tej grupy mogą wykonywać wiele zadań, ponieważ posiadają ten sam dostęp administracyjny, jak administrator serwera LDAP.

**Uwaga:** Podczas korzystania z zadań narzędzia Web Administration, zadania które nie zostały nadane członkom grupy administracyjnej są nieaktywne.

Administrator serwera LDAP lub członek grupy administracyjnej mogą wykonywać następujące zadania administrowania serwerem:

- Zmieniać własne hasła.
- Kończyć połączenia.
- Aktywować i zmieniać strategię haseł z wyjątkiem szyfrowania haseł, które może zmienić tylko rzutowany administrator systemu i5/OS.
- Zarządzać atrybutami unikalnymi.
- Zarządzać schematem serwera.
- Zarządzać replikacją, z wyjątkiem zadania dotyczącego właściwości replikacji (obejmującego nazwę wyróżniającą łączenia i hasło serwera głównego oraz domyślne odwołanie), które może wykonać tylko rzutowany administrator systemu i5/OS.

### Pojęcia pokrewne

"Zadania grupy administracyjnej" na stronie 134

Ten temat zawiera informacje dotyczące zarządzania grupami administracyjnymi.

"Nazwy wyróżniające łączenia administratora i repliki" na stronie 89

Jako skonfigurowaną nazwę wyróżniającą łączącą administratora lub replikę można podać profil użytkownika rzutowanego. Użyte zostanie wtedy hasło profilu użytkownika.

### Zadania pokrewne

"Nadawanie dostępu administratora użytkownikom rzutowanym" na stronie 125

Ten temat zawiera informacje dotyczące nadawania dostępu administratora profilom użytkowników.

## Autoryzacja proxy

Autoryzacja proxy jest specjalną formą uwierzytelniania. Dzięki zastosowaniu mechanizmu autoryzacji proxy, aplikacja kliencka może zostać połączona z katalogiem za pomocą własnej tożsamości, ale może wykonywać działania w imieniu innego użytkownika w celu uzyskania dostępu do katalogu docelowego. Zestaw zaufanych aplikacji lub użytkowników może uzyskać dostęp do serwera Directory Server w imieniu wielu użytkowników.

Członkowie grupy autoryzacji proxy mogą przyjmować dowolne uwierzytelnione tożsamości poza tożsamością administratora lub członków grupy administracyjnej.

Grupa autoryzacji proxy może być przechowywana w pozycji localhost lub IBMpolicies. W pozycji IBMpolicies grupa autoryzacji proxy jest replikowana, w pozycji localhost, nie. Grupa autoryzacji proxy może być przechowywana w obu pozycjach: localhost i IBMpolicies. Jeśli grupa autoryzacji proxy nie jest przechowywana pod jedną z tych nazw wyróżniających (DN), serwer ignoruje część grupy dotyczącą autoryzacji proxy i traktuje ją jak zwykłą grupę.

Na przykład, aplikacja kliencka client1 może zostać połączona z serwerem Directory Server z wysokim poziomem zezwoleń dostępu. Użytkownik UserA z ograniczonymi zezwoleniami wysyła żądanie do aplikacji klienckiej. Jeśli klient jest członkiem grupy autoryzacji proxy, zamiast przekazania żądania do serwera Directory Server jako klient client1, może ona przekazać żądanie jako użytkownik UserA wykorzystując bardziej ograniczony poziom zezwoleń. Oznacza to, że zamiast wykonywania żądania jako klient client1, serwer aplikacji może uzyskać dostęp tylko do tych informacji lub wykonać jedynie te działania, do których uprawniony jest użytkownik UserA. Żądanie wykonywane jest w imieniu lub jako proxy dla użytkownika UserA.

**Uwaga:** Element atrybutu musi posiadać wartość w postaci nazwy wyróżniającej (DN). W innym przypadku zwrócony zostanie komunikat Niepoprawna składnia DN. Nazwa wyróżniająca (DN) grupy nie może być elementem grupy autoryzacji proxy.

Administratorzy oraz członkowie grupy administracyjnej nie mogą być członkami grupy autoryzacji proxy. Protokół kontroli zapisuje nazwę wyróżniającą łączenia oraz nazwę wyróżniającą proxy dla działania wyszukiwania wykonywanego za pomocą autoryzacji proxy.

### Pojęcia pokrewne

“Zadania związane z grupami autoryzacji proxy” na stronie 138

Ten temat zawiera informacje dotyczące zarządzania grupami autoryzacji proxy.

## Listy kontroli dostępu

Listy kontroli dostępu (ACL) stanowią ochronę informacji zapisanych w katalogu LDAP. Za pomocą list ACL administratorzy ograniczają dostęp do różnych części katalogu lub konkretnych jego pozycji.

Zmianami każdej pozycji i atrybutu w katalogu można sterować za pomocą list ACL. Lista ACL dla danej pozycji lub atrybutu może być dziedziczona z pozycji nadrzędnej lub zdefiniowana wprost.

Najlepszym rozwiązaniem jest określenie strategii praw dostępu poprzez utworzenie grup użytkowników, które będą używane podczas konfigurowania dostępu dla obiektów i atrybutów. Należy ustawić prawa własności i dostęp na najwyższym poziomie w drzewie i pozwolić elementom sterującym na dziedziczenie w dół drzewa.

Atrybuty operacyjne powiązane z prawami dostępu, takie jak entryOwner, ownerSource, ownerPropagate, aclEntry, aclSource i aclPropagate, są nietypowe, ponieważ są logicznie przypisywane do poszczególnych obiektów, ale mogą mieć wartości zależące od innych obiektów znajdujących się wyżej w drzewie. W zależności od sposobu ich określania, wartości tych atrybutów mogą być jawne dla obiektu lub dziedziczone z elementu nadrzędnego.

Model praw dostępu definiuje dwa zestawy atrybutów: Access Control Information (ACI) i entryOwner. ACI definiuje prawa dostępu określonego użytkownika do operacji, jakie może on wykonywać na obiektach, których prawa te dotyczą. Atrybuty aclEntry i aclPropagate dotyczą definicji ACI. Informacje entryOwner definiują, kto może definiować listy ACI dla powiązanego obiektu pozycji. Atrybuty entryOwner i ownerPropagate dotyczą definicji entryOwner.

Istnieją dwa rodzaje list kontroli dostępu: listy ACL oparte na filtrze i niefiltrowane listy ACL. Niefiltrowane listy ACL jawnie dotyczą pozycji katalogu, która je zawiera, ale mogą zostać przekazane do wszystkich pozycji podrzędnych lub do żadnej z nich. Filtrowane listy ACL cechują się tym, że korzystają z porównywania opartego na filtrze, używając określonego filtru obiektów, w celu uzgadniania obiektów z efektywnymi prawami dostępu, które ich dotyczą.

Za pomocą list ACL administratorzy mogą ograniczać dostęp do różnych części katalogu, określonych pozycji katalogu oraz, w oparciu o nazwę atrybutu lub jego klasę dostępu, do atrybutów zawartych w pozycjach. Każda pozycja w katalogu LDAP zawiera zestaw powiązanych atrybutów ACI. Zgodnie z modelem LDAP informacje ACI i entryOwner są reprezentowane w postaci par atrybut-wartość. Co więcej, do administrowania tymi wartościami używana jest składnia LDIF. Atrybutami są:

- aclEntry
- aclPropagate
- ibm-filterAclEntry
- ibm-filterAclInherit
- entryOwner
- ownerPropagate

Dodatkowe informacje zawierają następujące tematy:

#### **Pojęcia pokrewne**

“Grupy i role” na stronie 56

Wykorzystanie grup i ról pozwala organizować i kontrolować uprawnienia dostępu poszczególnych członków grup.

“Zadania związane z listami kontroli dostępu” na stronie 214

Ten temat zawiera informacje dotyczące zarządzania listami kontroli dostępu.

“Atrybuty operacyjne” na stronie 91

Istnieje szereg atrybutów o specjalnym znaczeniu dla serwera katalogów znanych jako atrybuty operacyjne. Są to atrybuty obsługiwane przez serwer i odzwierciedlające zarządzane przez serwer informacje o pozycji lub wywierające wpływ na działanie serwera.

“Edytowanie list kontroli dostępu” na stronie 198

Ten temat zawiera informacje dotyczące zarządzania listami kontroli dostępu.

“Edytowanie list ACL w dziedzynie” na stronie 211

Ten temat zawiera informacje dotyczące edytowania list ACL w dziedzynie.

#### **Zadania pokrewne**

“Edytowanie list ACL w szablonie” na stronie 214

Ten temat zawiera informacje dotyczące edytowania list ACL w szablonie.

### **Filtrowane listy kontroli dostępu:**

Filtrowane listy kontroli dostępu (ACL) korzystają z porównywania opartego na filtrze. Używają one podanego filtru obiektów w celu określania efektywnych praw dostępu do obiektów docelowych.

Są one propagowane z dziedziczeniem do wszystkich zgodnych obiektów w powiązonym poddrzewie. Z tego powodu atrybut aclPropagate, który służy do zatrzymywania propagacji niefiltrowanych list ACL, nie dotyczy nowych filtrowanych list ACL.

Domyślnie listy ACL oparte na filtrach kumulują się, poczynając od najniższej pozycji zawierającej taką listę, w górę łańcucha pozycji nadrzędnych do najwyższej pozycji w drzewie DIT zawierającej taką listę. Efektywne prawa dostępu są obliczane jako iloczyn mnogościowy praw dostępu nadanych lub odebranych pozycjom nadrzędnym. Istnieje wyjątek od tej reguły. W celu zapewnienia zgodności z funkcją replikacji poddrzewa oraz zwiększenia kontroli administracyjnej wprowadzono atrybut ceiling służący do zatrzymania kumulacji na pozycji, w której znajduje się ten atrybut.

Nowy zestaw atrybutów kontroli dostępu służy specjalnie do obsługi filtrowanych list ACL, natomiast nie jest używany do scalania filtrowanych charakterystyk z istniejącymi niefiltrowanymi opartymi na listach ACL. Atrybutami są:

- ibm-filterAclEntry
- ibm-filterAclInherit

Atrybut `ibm-filterAclEntry` ma ten sam format, co `aclEntry`, i dodatkowo zawiera komponent filtru obiektu. Powiązany atrybutem `ceiling` jest `ibm-filterAclInherit`. Domyślnie ma on wartość `true` (prawda). Jeśli ustawiono wartość `false` (fałsz), kumulowanie jest przerywane.

### Pojęcia pokrewne

“Propagacja” na stronie 69

Kiedy dla pozycji nie są zdefiniowane jawnie klasy `aclEntry` i `entryOwner`, są one dziedziczone z przodka lub propagowane w dół drzewa.

### Składnia atrybutu kontroli dostępu:

Atrybutami listy kontroli dostępu można zarządzać przy użyciu notacji LDIF (LDAP Data Interchange Format). Składnią nowych atrybutów listy ACL opartej na filtrach są zmienione wersje bieżących atrybutów listy ACL, która nie jest oparta na filtrach.

Poniżej zdefiniowana jest składnia atrybutów informacji o kontroli dostępu (access control information - ACI) oraz atrybutu `entryOwner` za pomocą notacji BNF.

```

<aclEntry> ::= <podmiot> [ ":" <uprawnienia> ]

<aclPropagate> ::= "true" | "false"
<ibm-filterAclEntry> ::= <podmiot> ":" <filtr obiektu> [ ":" <uprawnienia> ]

<ibm-filterAclInherit> ::= "true" | "false"
<entryOwner> ::= <podmiot>

<ownerPropagate> ::= "true" | "false"

<podmiot> ::= <typ_nazwy_DN_podmiotu> ':' <nazwa_DN_podmiotu> |
             <pseudo_nazwa_DN>

<typ_nazwy_DN_podmiotu> ::= "role" | "group" | "access-id"

<nazwa_DN_podmiotu> ::= <nazwa_DN>

<nazwa_DN> ::= nazwa wyróżniająca, zgodnie z definicją w dokumencie RFC 2251 (sekcja 4.1.3.)

<pseudo_nazwa_DN> ::= "group:cn=anybody" | "group:cn=authenticated" |
                    "access-id:cn=this"

<filtr obiektu> ::= filtr wyszukiwania łańcucha, zgodnie z definicją w dokumencie RFC 2254 (sekcja 4)
                  (dopasowanie rozszerzone nie jest obsługiwane).

<uprawnienia> ::= <lista_kontroli_dostępu> [ ":" <uprawnienia> ]

<lista_kontroli_dostępu> ::= <dostęp_do_obiektu> | <dostęp_do_atrybutu> |
                           <dostęp_do_klasy_atrybutu>

<dostęp_do_obiektu> ::= "obiekt:" [<działanie> ":"] <uprawnienia_do_obiektu>

<działanie> ::= "grant" | "deny"

<uprawnienia_do_obiektu> ::= <uprawnienie_do_obiektu> [ <uprawnienia_do_obiektu> ]

<uprawnienie_do_obiektu> ::= "a" | "d" | ""

<dostęp_do_atrybutu> ::= "at." <nazwa_atrybutu> ":" [<działanie> ":"]
                       <uprawnienia_do_atrybutu>

<nazwa_atrybutu> ::= nazwa typu atrybutu, zgodnie z definicją w dokumencie RFC 2251 (sekcja 4.1.4.)
                   (OID lub łańcuch alfanumeryczny z możliwością użycia
                    liter oraz znaków "-" i ";" na początku)

```



```

<uprawnienia_do_atrybutu> ::= <uprawnienie_do_atrybutu>
                               [<uprawnienia_do_atrybutu>]

<uprawnienie_do_atrybutu> ::= "r" | "w" | "s" | "c" | ""

<dostęp_do_klasy_atrybutów> ::= <klasa> ":" [<działanie> ":"]
                               <uprawnienia_do_atrybutu>

<klasa> ::= "normal" | "sensitive" | "critical" | "system" | "restricted"

```

## Podmiot

Podmiot (jednostka żądająca dostępu do operacji na obiekcie) składa się z kombinacji typu nazwy wyróżniającej i samej nazwy wyróżniającej. Poprawne typy nazwy wyróżniającej to: ID dostępu, grupa i rola.

Nazwa wyróżniająca określa konkretny ID dostępu, rolę lub grupę. Na przykład podmiotem może być ID dostępu: cn=personA, o=IBM lub grupa: cn=deptXYZ, o=IBM.

Ponieważ ogranicznikiem pola jest dwukropek ( : ), nazwa wyróżniająca zawierająca dwukropki musi być ujęta w podwójny cudzysłów ( “ ” ). Jeśli nazwa wyróżniająca zawiera znaki z podwójnym cudzysłowem, muszą one być poprzedzone ukośnikami odwrotnymi ( \ ).

Do określania praw dostępu można używać wszystkich grup katalogów.

**Uwaga:** Każda grupa strukturalnych klas obiektu **AccessGroup**, **GroupOfNames**, **GroupofUniqueNames** lub **groupOfURLs**, bądź pomocniczych klas obiektu **ibm-dynamicGroup** i **ibm-staticGroup**, może służyć do określania praw dostępu.

Innym typem nazwy wyróżniającej używanej w modelu praw dostępu jest rola. Choć grupy i role są podobne w implementacji, ich koncepcje są różne. Jeśli użytkownik ma przypisaną rolę, to zakłada się, że zdefiniowano już wymagane uprawnienia do wykonywania zadania powiązanego z tą rolą. W przypadku przypisania do grupy nie ma założenia dotyczącego uprawnień nadawanych (lub odbieranych) poprzez przynależność do danej grupy.

Role są podobne do grup, ponieważ w katalogu są reprezentowane przez obiekt. Ponadto role zawierają grupę nazw wyróżniających. Role określające prawa dostępu muszą mieć klasę obiektu **AccessRole**.

## Pseudo nazwa wyróżniająca

Katalog LDAP zawiera szereg pseudo nazw wyróżniających. Są one używane do odwoływania się do dużej liczby nazw wyróżniających, które podczas łączenia używają wspólnych typowych charakterystyk w odniesieniu do wykonywanej operacji lub obiektu docelowego, na którym operacja jest wykonywana.

Obecnie zdefiniowane są trzy pseudo nazwy nazwy wyróżniające:

### **group:cn=anybody**

Odwołuje się do wszystkich obiektów, włącznie z tymi, które nie zostały uwierzytelnione. Wszyscy użytkownicy automatycznie należą do tej grupy.

### **group:cn=authenticated**

Odwołuje się do dowolnej nazwy wyróżniającej, która została uwierzytelniona w katalogu. Metoda uwierzytelniania nie jest brana pod uwagę.

### **access-id:cn=this**

Odwołuje się do nazwy wyróżniającej łączenia zgodnej z nazwą wyróżniająca obiektu docelowego, na którym wykonywana jest operacja.

## Filtr obiektu

Ten parametr dotyczy tylko filtrowanych list ACL. Filtr wyszukiwania łańcucha zdefiniowany w dokumencie RFC 2254 służy jako format filtru obiektu. Ponieważ obiekt docelowy jest już znany, łańcuch nie jest używany do faktycznego wykonania operacji wyszukiwania. Zamiast tego wykonywane jest porównanie na podstawie filtru w danym obiekcie docelowym w celu określenia, czy dany zestaw wartości `ibm-filterAclEntry` ma do niego zastosowanie.

## Uprawnienia

Prawa dostępu mogą dotyczyć całego obiektu lub jego atrybutów. Prawa dostępu LDAP są dyskretne. Z danego prawa nie wynika żadne inne. Prawa można łączyć w celu zapewnienia żądanej listy praw zgodnej z zestawem reguł opisanym w dalszej części. Prawa mogą mieć wartość nieokreśloną, wskazującą, że podmiotowi nie zostały nadane żadne prawa dostępu w obiekcie docelowym. Uprawnienia składają się z trzech części:

### Działanie:

Definiowane wartości są **nadawane** lub **odbierane**. Jeśli tego pola nie ma, wartością domyślną jest **grant** (nadawane).

### Uprawnienie:

Na obiekcie katalogu można wykonać sześć podstawowych operacji. Z tych operacji uzyskiwany jest podstawowy zestaw uprawnień ACL. Są nimi: dodawanie pozycji, usuwanie pozycji, odczytywanie wartości atrybutu, zapisywanie wartości atrybutu, wyszukiwanie atrybutu i porównywanie wartości atrybutu.

Możliwymi uprawnieniami atrybutu są: odczyt ( `r` ), zapis ( `w` ), wyszukiwanie ( `s` ) i porównanie ( `c` ). Ponadto uprawnienia do obiektu dotyczą pozycji jako całości. Uprawnienia te są następujące: dodanie pozycji potomnej ( `a` ) i usunięcie tej pozycji ( `d` ).

Poniższa tabela zawiera podsumowanie uprawnień potrzebnych do wykonywania poszczególnych operacji LDAP.

Operacja	Wymagane uprawnienie
ldappadd	dodawania (dla obiektu nadrzędnego)
ldapdelete	usuwania (dla obiektu)
ldapmodify	zapisu (do modyfikowanych atrybutów)
ldapsearch	<ul style="list-style-type: none"><li>wyszukiwania, odczytu (do atrybutów w RDN)</li><li>Wyszukiwania (do atrybutów określonych w filtrze wyszukiwania)</li><li>wyszukiwania (do atrybutów zwracanych z samymi nazwami)</li><li>wyszukiwania, odczytu (do atrybutów zwracanych z wartościami)</li></ul>
ldapmodrdn	zapisu (do atrybutów RDN)
ldapcompare	porównania (do porównywanych atrybutów)

**Uwaga:** W przypadku operacji wyszukiwania wymagany jest dostęp do wyszukiwania we wszystkich atrybutach w filtrze wyszukiwania; w przeciwnym razie nie zostaną zwrócone żadne pozycje. W przypadku pozycji zwracanych z wyszukiwania podmiot musi mieć prawa dostępu wyszukiwania i odczytu do wszystkich atrybutów w nazwie RDN zwracanych pozycji lub pozycje te nie zostaną zwrócone.

### Obiekt docelowy dostępu:

Uprawnienia można zastosować do całego obiektu (dodawanie pozycji potomnej, usuwanie pozycji), do pojedynczego atrybutu w pozycji lub do grup atrybutów (klasy dostępu do atrybutów) w sposób opisany poniżej.

Atrybuty wymagające podobnych uprawnień dostępu są grupowane w klasy. Atrybuty są przypisywane do swoich klas w pliku schematu katalogu. Klasy te są dyskretne; uzyskanie dostępu do jednej klasy nie ma

wpływu na pozostałe klasy. Uprawnienia są ustawiane w odniesieniu do całej klasy dostępu do atrybutów. Zestaw uprawnień do konkretnej klasy atrybutów dotyczy wszystkich atrybutów w klasie dostępu, chyba że określono prawa dostępu do poszczególnych atrybutów.

Firma IBM definiuje trzy klasy atrybutów używane w celu określania dostępu do atrybutów użytkownika: **normalna**, **wrażliwa** i **newralgiczna**. Na przykład atrybut **commonName** należy do klasy normalnej, a atrybut **userpassword** - do newralgicznej. Atrybuty zdefiniowane przez użytkownika należą do normalnej klasy dostępu, chyba że określono inaczej.

Zdefiniowano również dwie inne klasy dostępu: systemowa i zastrzeżona. Atrybutami klasy systemu są:

- **creatorsName**
- **modifiersName**
- **createTimestamp**
- **modifyTimestamp**
- **ownerSource**
- **aclSource**

Są to atrybuty obsługiwane przez serwer LDAP dostępne dla użytkowników katalogu w trybie tylko do odczytu. Atrybuty **OwnerSource** i **aclSource** są opisane w temacie Propagacja.

Ograniczona klasa atrybutów definiujących kontrolę dostępu:

- **aclEntry**
- **aclPropagate**
- **entryOwner**
- **ownerPropagate**
- **ibm-filterAclEntry**
- **ibm-filterAclInherit**
- **ibm-effectiveAcl**

Wszyscy użytkownicy mają prawa odczytu do ograniczonych atrybutów, ale tylko klasa **entryOwners** może tworzyć, zmieniać i usuwać te atrybuty.

**Uwaga:** Atrybut **ibm-effectiveAcl** jest tylko do odczytu.

#### Pojęcia pokrewne

“Propagacja”

Kiedy dla pozycji nie są zdefiniowane jawnie klasy **aclEntry** i **entryOwner**, są one dziedziczone z przodka lub propagowane w dół drzewa.

#### EntryOwner:

Właściciele pozycji mają pełne uprawnienia do wykonywania wszystkich operacji na nich bez względu na atrybut **aclEntry**.

Poza tym tylko właściciele pozycji mają uprawnienia do administrowania klasami **aclEntry** dla tego obiektu. **EntryOwner** jest podmiotem kontroli dostępu i można go definiować jako pojedyncze osoby, grupy lub role.

**Uwaga:** Administrator katalogu domyślnie jest jednym z właścicieli pozycji w odniesieniu do wszystkich obiektów w katalogu, a prawa własności do pozycji administratora katalogu nie można usunąć z żadnego obiektu.

#### Propagacja:

Kiedy dla pozycji nie są zdefiniowane jawnie klasy **aclEntry** i **entryOwner**, są one dziedziczone z przodka lub propagowane w dół drzewa.

Pozycje, które mają **aclEntry**, są traktowane jako jawne pozycje **aclEntry**. Podobnie, jeśli klasę **entryOwner** ustawiono dla konkretnej pozycji, to pozycja ta ma jawnego właściciela. Pozycja z jawnym właścicielem może, ale nie musi mieć jawnej pozycji **aclEntry**, a pozycja z jawną **aclEntry** może mieć jawnego właściciela. Jeśli jedna z tych wartości nie znajduje się w pozycji w jawnej postaci, brakująca wartość jest dziedziczona z węzła nadrzędnego w drzewie katalogu.

Każda jawna klasa **aclEntry** lub **entryOwner** dotyczy pozycji, dla której została ustawiona. Poza tym wartość może dotyczyć wszystkich pozycji potomnych, które nie mają jawnie ustawionej wartości. Wartości te są uznawane za propagowane; są one rozsyłane po całym drzewie katalogu. Propagacja konkretnej wartości jest kontynuowana do momentu osiągnięcia innej rozsyłanej wartości.

**Uwaga:** Listy ACL oparte na filtrze nie realizują propagacji w ten sam sposób, co listy ACL nieoparte na filtrze. Są one propagowane do wszystkich obiektów zgodnych podczas porównania w powiązonym poddrzewie.

Klasy **AclEntry** i **entryOwner** można ustawić tak, aby dotyczyły tylko konkretnej pozycji z wartością propagacji "false" lub pozycji i jej poddrzewa z wartością propagacji "true". Mimo iż można propagować obie klasy: **aclEntry** i **entryOwner**, to ich propagacja nie jest w żaden sposób powiązana.

Atrybuty **aclEntry** i **entryOwner** umożliwiają korzystanie z wielu wartości, jednakże atrybuty propagacji (**aclPropagate** i **ownerPropagate**) mogą mieć tylko pojedyncze wartości dla wszystkich wartości atrybutu **aclEntry** lub **entryOwner** w tej samej pozycji.

Atrybuty systemowe **aclSource** i **ownerSource** zawierają nazwę wyróżniającą efektywnego węzła, z którego określane są odpowiednio wartości **aclEntry** i **entryOwner**. Jeśli taki węzeł nie istnieje, przypisywana jest wartość **default** (domyślna).

Definicje sterowania dostępem w odniesieniu do obiektu można określać na podstawie następującego schematu:

- Jeśli w obiekcie istnieje zestaw jawnych atrybutów kontroli dostępu, wtedy jest to definicja kontroli dostępu do obiektu.
- Jeśli nie ma wprost zdefiniowanych atrybutów kontroli dostępu, należy przejść w górę drzewa katalogu do momentu osiągnięcia węzła nadrzędnego z zestawem propagowanych atrybutów kontroli dostępu.
- Jeśli nie znaleziono węzła nadrzędnego, podmiotowi nadawane są domyślne prawa dostępu opisane poniżej.

Administrator katalogu jest właścicielem pozycji. Pseudo grupa **cn=anybody** (wszyscy użytkownicy) ma prawa dostępu do odczytu, wyszukiwania i porównywania w odniesieniu do atrybutów w normalnej klasie dostępu.

#### Pojęcia pokrewne

"Filtrowane listy kontroli dostępu" na stronie 65

Filtrowane listy kontroli dostępu (ACL) korzystają z porównywania opartego na filtrze. Używają one podanego filtru obiektów w celu określania efektywnych praw dostępu do obiektów docelowych.

#### Określanie dostępu:

Dostęp dla konkretnej operacji jest nadawany lub odbierany na podstawie nazwy wyróżniającej łączenia podmiotu dla tej operacji w obiekcie docelowym. Przetwarzanie kończy się w momencie określenia praw dostępu.

Sprawdzanie praw dostępu odbywa się najpierw poprzez znalezienie efektywnej definicji **entryOwnership** i **ACI**, sprawdzenie praw własności do pozycji, a następnie określenie wartości ACI obiektu.

Listy ACL oparte na filtrach kumulują się, poczynając od najniższej pozycji zawierającej taką listę, w górę łańcucha pozycji nadrzędnych do najwyższej pozycji w drzewie DIT zawierającej taką listę. Efektywne prawa dostępu są obliczane jako iloczyn mnogościowy praw dostępu nadanych lub odebranych pozycjom nadrzędnym. Istniejący zestaw specyfikacji i reguł łączenia jest używany do określania efektywnego dostępu dla list ACL opartych na filtrze.

Atrybuty oparte na filtrze i nieoparte na filtrze wzajemnie wykluczają się w ramach pojedynczej pozycji katalogu. Umieszczanie obu typów atrybutów w tej samej pozycji nie jest dozwolone i jest naruszeniem ograniczenia. Operacje powiązane z tworzeniem lub aktualizacją pozycji katalogu nie powiodą się, jeśli warunek taki zostanie wykryty.

Podczas określania efektywnego dostępu pierwszy typ listy ACL wykryty w łańcuchu nadrzędnym docelowej pozycji obiektu ustawia tryb obliczania. W trybie opartym na filtrze listy ACL, które nie są oparte na filtrze, są ignorowane podczas określania dostępu. Podobnie w trybie, który nie jest oparty na filtrze, listy ACL oparte na filtrze są ignorowane podczas określania dostępu.

Aby ograniczyć akumulację list ACL opartych na filtrze podczas obliczania efektywnego dostępu, atrybut **ibm-filterAclInherit** o wartości "false" można umieścić w dowolnej pozycji pomiędzy najwyższym i najniższym wystąpieniem atrybutu **ibm-filterAclEntry** w danym poddrzewie. Powoduje to zignorowanie podzbioru atrybutów **ibm-filterAclEntry** powyżej niego w docelowym nadrzędnym łańcuchu obiektu.

W trybie filtrowanej listy ACL, jeśli nie ma zastosowania żadna filtrowana lista ACL, zastosowania, użyta zostanie domyślna lista ACL (cn=anybody ma uprawnienia do odczytu, wyszukiwania i porównywania atrybutów w klasie dostępu normal). Ta sytuacja może mieć miejsce wtedy, gdy prawa dostępu do pozycji nie są zgodne z filtrem określonym w wartościach **ibm-filterAclEntry**. Aby nie były stosowane domyślne prawa dostępu, można określić domyślny filtr ACL, tak jak poniżej:

```
ibm-filterAclEntry: group:cn=anybody:(objectclass=*):
```

W tym przykładzie nie są przyznawane żadne prawa dostępu. Aby zapewnić żądane prawa dostępu, należy go zmienić.

Domyślnie administrator katalogu i serwer główny lub równorzędny (dla replikacji) mają pełne prawa dostępu do wszystkich obiektów w katalogu z wyjątkiem prawa zapisu do atrybutów systemowych. Inni właściciele pozycji (**entryOwner**) uzyskują pełne prawa dostępu do obiektów, których są właścicielami, z wyjątkiem praw zapisu do atrybutów systemowych. Wszyscy użytkownicy mają uprawnienia do odczytu atrybutów systemowych i zastrzeżonych. Predefiniowanych uprawnień nie można zmieniać. Jeśli podmiot żądający dostępu ma uprawnienie **entryOwnership**, dostęp określany jest na podstawie powyższych ustawień domyślnych i przetwarzanie dostępu dobiega końca.

Jeśli żądany podmiot nie jest właścicielem pozycji (entryOwner), sprawdzane są wartości ACI dla pozycji obiektu. Prawa dostępu zdefiniowane w ACI dla obiektu docelowego są określone na podstawie reguł specyficzności i kombinatorycznych.

### Reguły specyficzności

Najbardziej specyficzne definicje aclEntry są używane w obliczeniach uprawnień nadawanych/odbieranych użytkownikowi. Poziomami specyficzności są:

- Access-id jest bardziej specyficzny niż grupa czy rola. Grupy i role są na tym samym poziomie.
- Na tym samym poziomie **dnType** uprawnienia na pojedynczym poziomie atrybutu są bardziej specyficzne niż uprawnienia na poziomie klasy atrybutów.
- Na tym samym poziomie atrybutu lub klasy atrybutów **deny** jest bardziej specyficzny niż **grant**.

### Reguła kombinatoryczna

Uprawnienia nadane obiektom o równej specyficzności są łączone. Jeśli nie można określić dostępu na tym samym poziomie specyficzności, używane są definicje dostępu o niższym poziomie specyficzności. Jeśli po zastosowaniu wszystkich ACI dostęp nie jest określony, nastąpi jego odmowa.

**Uwaga:** Po odnalezieniu pasującej pozycji **aclEntry** na poziomie ID dostępu pozycje **aclEntry** na poziomie grupy nie są podczas określania dostępu brane pod uwagę. Wyjątkiem jest sytuacja, gdy pasujące pozycje **aclEntry** na poziomie identyfikatora dostępu są zdefiniowane w cn=this, wtedy wszystkie pozycje **aclEntry** na poziomie zgodności grupy są również uwzględniane podczas obliczeń.

Innymi słowy, jeśli w ramach pozycji obiektu zdefiniowana pozycja ACI zawiera nazwę wyróżniającą podmiotu identyfikatora dostępu zgodną z nazwą wyróżniającą łączenia, uprawnienia są najpierw określone na podstawie tej pozycji **aclEntry**. W ramach nazwy wyróżniającej tego samego podmiotu, jeśli zdefiniowano pasujące uprawnienia na

poziomie atrybutu, zastępują one wszystkie uprawnienia zdefiniowane w klasach atrybutów. Jeśli w ramach tej samej definicji na poziomie atrybutu lub klasy atrybutów istnieją uprawnienia powodujące konflikt, odrzucone uprawnienia przesłaniają nadane.

**Uwaga:** Zdefiniowane uprawnienia o wartości null uniemożliwiają dołączenie mniej specyficznych definicji uprawnień.

Jeśli dostępu nadal nie można określić i wszystkie pasujące pozycje `aclEntry` są zdefiniowane w `"cn=this"`, określane będzie przypisanie do grupy. Jeśli użytkownik należy do wielu grup, to ma połączone uprawnienia do tych grup. Ponadto użytkownik automatycznie należy do grupy `cn=Anybody` i prawdopodobnie do grupy `cn=Authenticated`, jeśli wykonał uwierzytelnioną operację łączenia. Jeśli dla tych grup zdefiniowano uprawnienia, są one nadawane użytkownikowi.

**Uwaga:** Przypisanie do grupy lub roli jest określane podczas łączenia i trwa do momentu przeprowadzenia następnej operacji łączenia lub do odebrania żądania odłączenia. Zagnieżdżone grupy i role będące członkiem innej grupy lub roli nie są rozstrzygane podczas określania członkostwa czy określania dostępu.

Przyjmijmy na przykład, że `attribute1` jest wrażliwą klasą atrybutów, a użytkownik `cn=Osoba A, o=IBM` należy do obu grup: `grupa1` i `grupa2`, z następującymi zdefiniowanymi pozycjami `aclEntry`:

1. `aclEntry: access-id: cn=Osoba A, o=IBM: at.attribute1:grant:rsc:sensitive:deny:rsc`
2. `aclEntry: group: cn=grupa1,o=IBM:critical:deny:rwc`
3. `aclEntry: group: cn=grupa2,o=IBM:critical:grant:r:normal:grant:rsc`

Ten użytkownik uzyskuje:

- Dostęp `'rsc'` do `attribute1`, (definicja 1. poziomu atrybutu zastępuje definicję poziomu klasy atrybutów).
- Brak dostępu do innych atrybutów klas wrażliwych w obiekcie docelowym (z 1).
- Nie są nadawane inne uprawnienia (2 i 3 NIE są uwzględniane podczas określania dostępu).

Inny przykład z następującymi pozycjami `aclEntry`:

1. `aclEntry: access-id: cn=this: sensitive`
2. `aclEntry: group: cn=grupa1,o=IBM:sensitive:grant:rsc:normal:grant:rsc`

Użytkownik:

- Nie otrzymuje dostępu do wrażliwych atrybutów klas, (z 1. Wartość `null` zdefiniowana w identyfikatorze dostępu uniemożliwia uwzględnienie uprawnień do wrażliwych atrybutów klasy z grupy1).
- Dostęp `'rsc'` do normalnych atrybutów klasy (z 2).

### **Uwagi dotyczące replikacji poddrzewa:**

Aby podczas replikacji poddrzewa uwzględniany był dostęp oparty na filtrze, wszystkie atrybuty `ibm-filterAclEntry` muszą się znajdować w powiązanej pozycji `ibm-replicationContext` lub poniżej niej.

Ponieważ efektywny dostęp nie może być kumulowany z pozycji nadrzędnej względem replikowanego drzewa, atrybut `ibm-filterAclInherit` musi przyjąć wartość `false` i znaleźć się w powiązanej pozycji `ibm-replicationContext`.

### **Przykład definiowania ACI i właścicieli pozycji:**

W następujących dwóch przykładach przedstawiono zakładanie poddomeny administracyjnej za pomocą programów narzędziowych wiersza komend.

W pierwszym przykładzie pojedynczy użytkownik jest przypisywany jako `entryOwner` dla całej domeny. W drugim przykładzie przedstawiono przypisywanie grupy jako `entryOwner`.

```
entryOwner: access-id:cn=Person A,o=IBM
ownerPropagate: true
```

```
entryOwner: group:cn=System Owners, o=IBM
ownerPropagate: true
```

Następny przykład przedstawia sposób nadawania identyfikatorowi dostępu "cn=Person 1, o=IBM" uprawnień do czytania, wyszukiwania i porównywania attribute1. Uprawnienia dotyczą każdego węzła w całym poddrzewie, w lub poniżej węzła zawierającego ten ACI, zgodny z filtrem porównania "(objectclass=groupOfNames)". Akumulacja zgodnych atrybutów ibm-filteraclentry w dowolnym węzle nadrzędnym została przerwana w tej pozycji przez nadanie atrybutowi ibm-filterAclInherit wartości "false".

```
ibm-filterAclEntry: access-id:cn=Person 1,o=IBM:(objectclass=groupOfNames):
    at.attribute1:grant:rsc
```

```
ibm-filterAclInherit: false
```

Następny przykład przedstawia sposób nadawania identyfikatorowi dostępu "cn=Dept XYZ, o=IBM" uprawnień do czytania, wyszukiwania i porównywania attribute1. Uprawnienie dotyczy całego poddrzewa poniżej węzła zawierającego to ACI.

```
aclEntry: group:cn=Dept XYZ,o=IBM:at.attribute1:grant:rsc
aclPropagate: true
```

Następny przykład przedstawia sposób nadawania roli "cn=System Admins,o=IBM" uprawnień do dodawania obiektów pod tym węzłem, a także odczytywania, wyszukiwania i porównywania attribute2 i klasy atrybutów newralgicznych. Uprawnienie dotyczy tylko węzła zawierającego to ACI.

```
aclEntry: role:cn=System Admins,o=IBM:object:grant:a:at.
    attribute2:grant:rsc:critical:grant:rsc
aclPropagate: false
```

### **Przykład zmiany ACI i właściciela pozycji:**

Ten temat zawiera kilka przykładów zmiany ACI i właściciela pozycji za pomocą programów narzędziowych wiersza komend.

#### **Modify-replace**

Modify-replace działa tak samo, jak wszystkie inne atrybuty. Jeśli wartość atrybutu nie istnieje, należy ją utworzyć. Jeśli wartość atrybutu istnieje, należy ją zastąpić.

Mając następujące ACI dla pozycji:

```
aclEntry: group:cn=Dept ABC,o=IBM:normal:grant:rsc
aclPropagate: true
```

dokonaj następującej zmiany:

```
dn: cn=dowolna pozycja
changetype: modify
replace: aclEntry
aclEntry: group:cn=Dept XYZ,o=IBM:normal:grant:rsc
```

Wynikowym ACI jest:

```
aclEntry: group:cn=Dept XYZ,o=IBM:normal:grant:rsc
aclPropagate: true
```

Po zastąpieniu wartości ACI dla Dept ABC ulegają utracie.

Mając następujące ACI dla pozycji:

```
ibm-filterAclEntry: group:cn=Dept ABC,o=IBM:(cn=Manager ABC):normal
    :grant:rsc
ibm-filterAclInherit: true
```

dokonaj następujących zmian:

```
dn: cn=dowolna pozycja
changetype: modify
replace: ibm-filterAclEntry
ibm-filterAclEntry: group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):normal
                  :grant:rsc
```

```
dn: cn=dowolna pozycja
changetype: modify
replace: ibm-filterAclInherit
ibm-filterAclInherit: false
```

Wynikowym ACI jest:

```
ibm-filterAclEntry: group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):normal
                  :grant:rsc
ibm-filterAclInherit: false
```

Po zastąpieniu wartości ACI dla Dept ABC ulegają utracie.

### Modify-add

Jeśli podczas wykonywania operacji ldapmodify-add atrybut ACI lub entryOwner nie istnieje, tworzony jest ACI lub entryOwner z konkretnymi wartościami. Jeśli ACI lub entryOwner istnieje, określone wartości należy dodać do danego ACI lub entryOwner. Mając następujące ACI:

```
aclEntry: group:cn=Dept XYZ,o=IBM:normal:grant:rsc
```

z modyfikacją:

```
dn: cn=dowolna pozycja
changetype: modify
add: aclEntry
aclEntry: group:cn=Dept ABC,o=IBM:at.attribute1:grant:rsc
```

wyłączy wielowartościową pozycję aclEntry:

```
aclEntry: group:cn=Dept XYZ,o=IBM:normal:grant:rsc
aclEntry: group:cn=Dept ABC,o=IBM:at.attribute1:grant:rsc
```

Mając następujące ACI:

```
Ibm-filterAclEntry: group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):normal
                  :grant:rsc
```

z modyfikacją:

```
dn: cn=dowolna pozycja
changetype: modify
add: ibm-filterAclEntry
ibm-filterAclEntry: group:cn=Dept ABC,o=IBM:(cn=Manager ABC)
                  :at.attribute1:grant:rsc
```

wyłączy wielowartościową pozycję aclEntry:

```
Ibm-filterAclEntry: group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):normal
                  :grant:rsc
ibm-filterAclEntry: group:cn=Dept ABC,o=IBM:(cn=Manager ABC):at.attribute1
                  :grant:rsc
```

Uprawnienia w tym samym atrybucie lub klasie atrybutów stanowią elementy podstawowe, a operacje są traktowane jako kwalifikatory. Jeśli ta sama wartość uprawnień zostanie dodana kilka razy, zapisana zostanie tylko jedna wartość. Jeśli ta sama wartość uprawnień zostanie dodana kilka razy z różnymi wartościami czynności, użyta zostanie ostatnia wartość. Jeśli wynikowe pole uprawnienia jest puste (""), uprawnienie przyjmuje wartość null, a czynność przyjmuje wartość **grant**.

Mając na przykład następujące ACI:



```
aclEntry: group:cn=Dept XYZ,o=IBM:normal:grant:rsc
```

z modyfikacją:

```
dn: cn=dowolna pozycja
changetype: modify
add: aclEntry
aclEntry: group:cn=Dept XYZ,o=IBM:normal:deny:r:critical:deny::sensitive
:grant:r
```

wyłącza pozycję aclEntry:

```
aclEntry: group:cn=Dept XYZ,o=IBM:normal:grant:sc:normal:deny:r:critical
:grant::sensitive:grant:r
```

Mając na przykład następujące ACI:

```
Ibm-filterAclEntry: group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):normal
:grant:rsc
```

z modyfikacją:

```
dn: cn=dowolna pozycja
changetype: modify
add: ibm-filterAclEntry
ibm-filterAclEntry: group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):normal
:deny:r:critical:deny::sensitive:grant:r
```

wyłącza pozycję aclEntry:

```
ibm-filterAclEntry: group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):normal
:grant:sc:normal:deny:r:critical:grant::sensitive
:grant:r
```

## Modify-delete

Aby usunąć konkretną wartość ACI, należy użyć zwykłej składni ldapmodify-delete.

Mając następujące ACI:

```
aclEntry: group:cn=Dept XYZ,o=IBM:object:grant:ad
aclEntry: group:cn=Dept XYZ,o=IBM:normal:grant:rwc
```

```
dn: cn=dowolna pozycja
changetype: modify
delete: aclEntry
aclEntry: group:cn=Dept XYZ,o=IBM:object:grant:ad
```

daje w rezultacie następujące pozostałe ACI na serwerze:

```
aclEntry: group:cn=Dept XYZ,o=IBM:normal:grant:rwc
```

Mając następujące ACI:

```
ibm-filterAclEntry: group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):object
:grant:ad
ibm-filterAclEntry: group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):normal
:grant:rwc
```

```
dn: cn=dowolna pozycja
changetype: modify
delete: ibm-filterAclEntry
ibm-filterAclEntry: group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):object
:grant:ad
```

daje w rezultacie następujące pozostałe ACI na serwerze:

```
ibm-filterAclEntry: group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):normal
:grant:rwc
```

Usunięcie nieistniejącej wartości ACI lub entryOwner pozostawia niezmienione wartości ACI lub entryOwner i daje kod powrotu określający, że wartość atrybutu nie istnieje.

### **Przykład usuwania ACI i wartości właściciela pozycji:**

Przykład usuwania ACI i wartości właściciela pozycji za pomocą programów narzędziowych wiersza komend.

W przypadku operacji ldapmodify-delete wartość entryOwner można usunąć, podając

```
dn: cn=dowolna pozycja
changetype: modify
delete: entryOwner
```

W tym przypadku pozycja nie będzie zawierać jawnej wartości entryOwner. Atrybut ownerPropagate jest również automatycznie usuwany. Ta pozycja powinna dziedziczyć wartość entryOwner z węzła nadrzędnego w drzewie katalogu zgodnie z regułą propagacji.

To samo można zrobić w celu całkowitego usunięcia pozycji aclEntry:

```
dn: cn=dowolna pozycja
changetype: modify
delete: aclEntry
```

Usunięcie ostatniej wartości ACI lub entryOwner z pozycji różni się od usunięcia atrybutów ACI lub entryOwner. Pozycja może zawierać ACI lub entryOwner bez wartości. W tym przypadku podczas wyszukiwania ACI lub entryOwner do klienta nie jest zwracana żadna wartość, a ustawienie jest przekazywane do węzłów podrzędnych aż do jego nadpisania. Aby uniknąć zawieszonych pozycji, do których nikt nie ma dostępu, administrator katalogu zawsze ma pełny dostęp do każdej pozycji, nawet jeśli ma ona pustą wartość ACI lub entryOwner.

### **Przykład wczytywania ACI i wartości właścicieli pozycji:**

Przykład wczytywania ACI i wartości właścicieli pozycji za pomocą programów narzędziowych wiersza komend.

Efektywne wartości ACI lub entryOwner można wczytywać, podając podczas wyszukiwania żądane atrybuty listy ACL lub entryOwner. Na przykład:

```
ldapsearch -b "cn=object A, o=ibm" -s base "objectclass=*"
aclentry aclpropagate aclsource entryowner ownerpropagate ownersource
ibm-filterAclEntry ibm-filterAclInherit ibm-effectiveAcl
```

zwraca wszystkie informacje ACL lub entryOwner używane do określania dostępu dla obiektu A. Należy zauważyć, że zwrócone wartości mogą nie być takie same, jak podczas ich pierwszego zdefiniowania. Wartości są odpowiednikami pierwotnej formy.

Wyszukiwanie atrybutu ibm-filterAclEntry zwraca tylko konkretne wartości dla danej pozycji zawierającej atrybut.

Atrybut operacyjny tylko do odczytu, ibm-effectiveAcl, służy do przedstawiania skumulowanego efektywnego dostępu. Żądanie wyszukiwania dla ibm-effectiveAcl zwraca efektywny dostęp dotyczący docelowego obiektu na podstawie: list ACL bez filtru lub list ACL z filtrem w zależności od sposobu ich dystrybucji w drzewie DIT.

Ponieważ listy ACL oparte na filtrze mogą pochodzić z szeregu źródeł nadrzędnych, wyszukiwanie atrybutu aclSource generuje listę przypisanych zasobów.

## **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.

Aby przypisać prawo własności, można wykonać jedną z następujących czynności:

- nadać w sposób jawny prawo własności do konkretnego obiektu,
- określić, że obiekty dziedziczą prawa własności od obiektów znajdujących się wyżej w hierarchii katalogów LDAP.

Serwer Directory Server umożliwia określenie wielu właścicieli tego samego obiektu. Można także określić, że obiekt jest właścicielem samego siebie. W tym celu do listy właścicieli obiektu należy dołączyć wartość specjalną DN `cn=this`. Przyjmijmy na przykład, że właścicielem obiektu `cn=A` jest `cn=this`. Każdy użytkownik będzie miał dostęp do obiektu `cn=A` na prawach właściciela, jeśli połączy się z serwerem jako `cn=A`.

### Pojęcia pokrewne

“Zadania związane z pozycjami katalogu” na stronie 195

Ten temat zawiera informacje dotyczące zarządzania pozycjami katalogu.

## Strategia haseł

Jeśli serwery LDAP służą do uwierzytelniania, to ważne jest, aby obsługiwały strategię dotyczące wygaśnięcia hasła, zakończonych niepowodzeniem prób zalogowania się i reguł dotyczących haseł. Serwer Directory Server udostępnia konfigurowalną obsługę wszystkich trzech rodzajów strategii.

Strategia haseł jest stosowana wobec wszystkich pozycji katalogu z atrybutem `userPassword`. Nie można definiować jednej strategii dla danego zestawu użytkowników, a innych strategii dla pozostałych zestawów użytkowników. Serwer Directory Server udostępnia również mechanizm informowania klientów o sytuacjach związanych ze strategią haseł (hasło wygasa za trzy dni) oraz zestaw atrybutów operacyjnych, których administrator może użyć między innymi do wyszukiwania użytkowników z hasłami, które straciły ważność, lub zablokowanych kont.

## Konfiguracja

Można skonfigurować sposób obsługi haseł przez serwer w następujących obszarach:

- Globalny przełącznik do włączania lub wyłączania strategii haseł.
- Reguły zmiany haseł obejmujące:
  - Użytkownicy mogą zmieniać swoje hasła. Należy zauważyć, że ta strategia stanowi dodatek do praw dostępu. Innymi słowy, aby użytkownik mógł zmienić hasło, musi mieć uprawnienie do zmiany atrybutu `userPassword`, a strategia haseł musi umożliwiać użytkownikom zmianę ich haseł. Jeśli ta strategia jest wyłączona, użytkownicy nie mogą zmieniać swoich haseł. Hasło dla pozycji może zmieniać tylko administrator lub inny użytkownik mający uprawnienia do zmiany atrybutu `userPassword`.
  - Hasło należy zmienić po jego zresetowaniu. Jeśli ta strategia jest włączona, hasło zmienione przez osobę inną niż ten użytkownik jest oznaczane jako zresetowane i użytkownik musi je zmienić przed wykonaniem innych operacji na katalogu. Żądanie łączenia ze zresetowanym hasłem powiedzie się. Aby otrzymać powiadomienie o tym, że hasło należy zresetować, aplikacja musi korzystać ze strategii haseł.
  - Podczas zmiany hasła użytkownik musi wysłać stare hasło. Jeśli ta strategia jest włączona, hasło można zmienić tylko poprzez żądanie zmiany obejmujące usunięcie atrybutu `userPassword` (ze starą wartością) i dodanie nowej wartości `userPassword`. Dzięki temu hasło może zmienić tylko użytkownik, który je zna. Administrator lub inny użytkownik uprawniony do zmiany atrybutu `userPassword` może ustawiać hasło niezależnie od tego ustawienia.
- Reguły wygaśnięcia haseł obejmujące:
  - Hasło nigdy nie wygasa lub wygasa po określonym czasie od ostatniej zmiany.
  - Nie ostrzegaj użytkowników o wygaśnięciu hasła lub ostrzegaj użytkowników na określony czas przed wygaśnięciem hasła. Aby otrzymać ostrzeżenie o zbliżającym się wygaśnięciu hasła, aplikacja musi używać strategii hasła.
  - Zezwól na konfigurowalną liczbę operacji zalogowania się po wygaśnięciu hasła. Aplikacja korzystająca ze strategii haseł zostanie powiadomiona o liczbie pozostałych operacji logowania. Jeśli dodatkowe operacje logowania nie są dozwolone, użytkownik nie może być uwierzytelniany ani nie może zmienić własnego hasła po jego wygaśnięciu.
- Reguły weryfikacji hasła obejmujące:
  - Konfigurowalną wielkość historii haseł, która instruuje serwer, aby zachował historię ostatnich N haseł i odrzucał wcześniej używane hasła.

- Sprawdzanie składni hasła, włącznie z ustawieniem reakcji serwera na hasła zakodowane. To ustawienie określa, czy serwer ma ignorować strategię pod jednym z następujących warunków:
  - Serwer przechowuje hasła zakodowane.
  - Klient wysyła do serwera hasło zakodowane (ta sytuacja może mieć miejsce podczas przesyłania danych między serwerami za pomocą pliku LDIF, jeśli serwer źródłowy przechowuje hasła zakodowane).

W każdym z tych przypadków serwer może nie być w stanie zastosować wszystkich reguł dotyczących składni. Obsługiwane są następujące reguły składni: minimalna długość, minimalna liczba liter, minimalna liczba cyfr lub znaków specjalnych, liczba powtórzeń znaków oraz liczba znaków, o jaką nowe hasło musi się różnić od poprzedniego.

- Reguły dla operacji logowania zakończonych niepowodzeniem obejmujące:
  - Minimalny czas między zmianami hasła, który zapobiega zbyt częstemu zmienianiu haseł z danego zestawu i zbyt szybkiemu powroćeniu do hasła początkowego.
  - Maksymalna liczba operacji logowania zakończonych niepowodzeniem przed zablokowaniem konta.
  - Konfigurowalny czas trwania blokady hasła. Po tym czasie można używać wcześniej zablokowanego konta. Może to ułatwić zablokowanie podejmowanych przez hakera prób mających na celu złamanie hasła, pomagając jednocześnie użytkownikowi, który go zapomniał.
  - Konfigurowalny czas, przez który serwer śledzi próby logowania zakończone niepowodzeniem. Jeśli w tym czasie wystąpi maksymalna liczba nieudanych prób podania hasła, konto zostaje zablokowane. Po upływie tego czasu serwer usuwa informacje o poprzednich próbach logowania zakończonych niepowodzeniem dla tego konta.

Ustawienia strategii haseł dla serwera katalogów są przechowywane w obiekcie "cn=pwdpolicy", który wygląda następująco:

```
cn=pwdpolicy
objectclass=container
objectclass=pwdPolicy
objectclass=ibm-pwdPolicyExt
objectclass=top
cn=pwdPolicy
pwdExpireWarning=0
pwdGraceLoginLimit=0
passwordMaxRepeatedChars=0
pwdSafeModify=false
pwdattribute=userpassword
pwdinhistory=0
pwdchecksyntax=0
passwordminotherchars=0
passwordminalphachars=0
pwdminlength=0
passwordmindiffchars=0
pwdminage=0
pwdmaxage=0
pwdallowuserchange=true
pwdlockoutduration=0
ibm-pwdpolicy=true
pwdlockout=true
pwdmaxfailure=2
pwdfailurecountinterval=0
pwdmustchange=false
```

## Aplikacje używające strategii haseł

Obsługa strategii haseł na serwerze Directory Server obejmuje zestaw elementów sterujących LDAP, których mogą używać aplikacje obsługujące strategię haseł w celu odbierania powiadomień o dodatkowych warunkach związanych z tą strategią.

Aplikacja może być powiadamiana o następujących warunkach ostrzeżenia:

- czas pozostały do wygaśnięcia hasła,

- liczba operacji logowania pozostających po wygaśnięciu hasła.

Aplikacja może być również powiadamiana o następujących warunkach błędu:

- hasło utraciło ważność,
- konto jest zablokowane,
- hasło zostało zresetowane i należy je zmienić,
- użytkownik nie ma prawa do zmiany swojego hasła,
- podczas zmiany hasła należy podać stare hasło,
- nowe hasło nie jest zgodne z regułami składni,
- nowe hasło jest zbyt krótkie,
- hasło niedawno zmieniano,
- nowe hasło jest już w historii.

Używane są dwa elementy sterujące. Żądanie sterowania strategią haseł służy do informowania serwera o tym, że aplikacja ma być informowana o sytuacji związanej ze strategią haseł. Ten element sterujący aplikacja musi określać we wszystkich operacjach, które chce wykonać, zwykle w żądaniach początkowego łączenia i wszystkich żądaniach zmiany hasła. Jeśli istnieje element sterujący żądania strategii haseł, element sterujący odpowiedzi strategii haseł jest zwracany przez serwer, gdy wystąpi jeden z powyższych błędów.

Funkcje API klienta Directory Server obejmują zestaw funkcji API, których mogą używać aplikacje w języku C do pracy z tymi elementami sterującymi. Tymi funkcjami API są:

- ldap\_parse\_pwdpolicy\_response
- ldap\_pwdpolicy\_err2string

W przypadku aplikacji, które nie używają tych funkcji API, elementy sterujące są zdefiniowane poniżej. Zastosowanie możliwości udostępnianych przez funkcje API klienta LDAP używanych do przetwarzania elementów sterujących jest konieczne. Na przykład interfejs JNDI (Java Naming and Directory Interface) ma wbudowaną obsługę niektórych najpopularniejszych elementów sterujących, a także udostępnia środowisko do obsługi elementów sterujących, których nie rozpoznaje.

### Sterowane żądaniami strategii haseł

Control name: 1.3.6.1.4.1.42.2.27.8.5.1  
Control criticality: FALSE  
Control value: None

### Sterowanie odpowiedziami strategii haseł

Control name: 1.3.6.1.4.1.42.2.27.8.5.1 (taka sama jak element sterujący żądania)  
Control criticality: FALSE  
Control value: Wartość zakodowana za pomocą BER zdefiniowana w ASN.1:

```

PasswordPolicyResponseValue ::= SEQUENCE {
  warning [0] CHOICE OPTIONAL {
    timeBeforeExpiration [0] INTEGER (0 .. MaxInt),
    graceLoginsRemaining [1] INTEGER (0 .. maxInt) }
  error [1] ENUMERATED OPTIONAL {
    passwordExpired (0),
    accountLocked (1),
    changeAfterReset (2),
    passwordModNotAllowed (3),
    mustSupplyOldPassword (4),
    invalidPasswordSyntax (5),
    passwordTooShort (6),
    passwordTooYoung (7),
    passwordInHistory (8) } }

```

Podobnie jak inne elementy protokołu LDAP, kodowanie BER używa niejawnych znaczników.

## Atrybuty operacyjne strategii haseł

Serwer Directory Server obsługuje zestaw atrybutów operacyjnych dla każdej pozycji z atrybutem userPassword. Atrybutów tych mogą wyszukiwać uprawnieni użytkownicy; są stosowane w filtrach wyszukiwania lub zwracane przez żądanie wyszukiwania. Tymi atrybutami są:

- pwdChangedTime - atrybut GeneralizedTime zawierający czas ostatniej zmiany i hasła.
- pwdAccountLockedTime - atrybut GeneralizedTime zawierający czas zablokowania konta. Jeśli konto nie jest zablokowane, ten atrybut jest niedostępny.
- pwdExpirationWarned - atrybut GeneralizedTime zawierający czas pierwszego wysłania ostrzeżenia o wygaśnięciu hasła do klienta.
- pwdFailureTime - wielowartościowy atrybut GeneralizedTime zawierający czasy poprzednich operacji logowania, które zakończyły się niepowodzeniem. Jeśli ostatnie logowanie było pomyślne, ten atrybut jest niedostępny.
- pwdGraceUseTime - wielowartościowy atrybut GeneralizedTime zawierający czasy poprzednich operacji logowania po zablokowaniu konta.
- pwdReset - atrybut Boolean zawierający wartość TRUE, jeśli hasło zostało zresetowane i wymaga zmiany przez użytkownika.
- ibm-pwdAccountLocked - Atrybut boolowski wskazujący, że konto zostało zablokowane z poziomu administracyjnego.

## Replikacja strategii haseł

Informacje o strategii haseł są replikowane przez serwery wysyłające na serwery odbierające. Zmiany w pozycji cn=pwdpolicy są replikowane jako zmiany globalne, podobnie jak zmiany schematu. Informacje o stanie strategii haseł dla pojedynczych pozycji również są replikowane, więc na przykład jeśli pozycja jest zablokowana na serwerze wysyłającym, operacja ta będzie replikowana na wszystkich serwerach odbierających. Zmiany stanu strategii haseł w replice tylko do odczytu nie są replikowane do żadnego serwera.

### Pojęcia pokrewne

“Zadania związane z hasłami” na stronie 176

Ten temat zawiera informacje dotyczące zadań związanych z hasłami.

“Atrybuty operacyjne” na stronie 91

Istnieje szereg atrybutów o specjalnym znaczeniu dla serwera katalogów znanych jako atrybuty operacyjne. Są to atrybuty obsługiwane przez serwer i odzwierciedlające zarządzane przez serwer informacje o pozycji lub wywierające wpływ na działanie serwera.

## Wskazówki dotyczące strategii haseł

Strategia haseł nie zawsze działa zgodnie z oczekiwaniami.

Istnieją dwa obszary, w których implementacja strategii haseł może zachowywać się niezgodnie z oczekiwaniami:

1. Jeśli dla pozycji określony został atrybut pwdReset, klient może łączyć się bezterminowo używając nazwy wyróżniającej pozycji i wyzerowanego hasła. Jeśli występuje kontrola żądań strategii haseł, powoduje to pomyślne połączenie z ostrzeżeniem w kontroli odpowiedzi. Jeśli jednak klient nie określi kontroli odpowiedzi, klient nie znający strategii haseł widzi pomyślne połączenie bez wskazania potrzeby zmiany hasła. Kolejne działania wykonywane pod tą nazwą wyróżniającą nie powiodą się i wywołają błąd "nie można wykonać", chociaż początkowy wynik połączenia może być mylący. Może to stanowić problem, jeśli połączenie zostało nawiązane jedynie dla uwierzytelnienia, jak w przypadku aplikacji sieciowej używającej katalogu do uwierzytelniania.
2. Strategie pwdSafeModify i pwdMustChange nie działają zgodnie z oczekiwaniami w przypadku aplikacji, która zmienia hasła z poziomu tożsamości innej niż nazwa wyróżniająca pozycji, dla której hasło jest zmieniane. W takim przypadku, bezpieczna zmiana hasła dokonana, na przykład z poziomu tożsamości administracyjnej, spowoduje ustawienie atrybutu pwdReset. Aplikacja zmieniająca hasło może korzystać z konta administratora i usunąć atrybut pwdReset, jak opisano to wcześniej.

## Uwierzytelnianie

Uwierzytelnianie umożliwia kontrolę dostępu w ramach serwera Directory Server.

Kontrola dostępu na serwerze Directory Server opiera się na nazwie wyróżniającej powiązanej z danym połączeniem. Nazwa ta jest określana jako wynik łączenia z serwerem Directory Server (zalogowania w nim).

Po pierwszym skonfigurowaniu serwera Directory Server można używać poniższych identyfikatorów w celu uwierzytelniania na serwerze:

- Anonimowy
- Administrator katalogu (domyślnie cn=adminstrator)
- Rzutowany profil użytkownika systemu i5/OS

Dobrym pomysłem jest utworzenie dodatkowych użytkowników, którym można nadać uprawnienia do zarządzania różnymi częściami katalogu bez konieczności współużytkowania tożsamości administratora katalogu.

Z perspektywy protokołu LDAP istnieją następujące struktury uwierzytelniania w LDAP:

- Proste łączenie, w którym aplikacja udostępnia nazwę wyróżniającą i hasło dla tej nazwy wyróżniającej w postaci tekstowej.
- Uwierzytelnianie SASL (Simple Authentication and Security Layer), które zapewnia szereg dodatkowych metod uwierzytelniania, włącznie z CRAM-MD5, DIGEST-MD5, EXTERNAL, GSSAPI oraz OS400-PRFTKN.

## Proste łączenie DIGEST-MD5 i CRAM-MD5

Aby używać prostego łączenia, klient musi podać nazwę wyróżniającą istniejącej pozycji LDAP oraz hasło, które jest zgodne z atrybutem userPassword dla tej pozycji. Na przykład pozycję dla Johna Smitha można utworzyć w następujący sposób:

```
sample.ldif:
dn: cn=John Smith,cn=users,o=acme,c=us
objectclass: inetorgperson
cn: John Smith
sn: smith
userPassword: mypassword
```

```
ldapadd -D cn=adminstrator -w secret -f sample.ldif
```

W kontroli dostępu można użyć nazwy wyróżniającej "cn=John Smith,cn=users,o=acme,c=us" lub przypisać ją do grupy używanej w kontroli dostępu.

Szereg predefiniowanych klas obiektu umożliwia określenie atrybutu userPassword; niektóre z nich to: person, organizationalperson, inetorgperson, organization, organizationalunit itd.

W hasłach serwera Directory Server rozróżniana jest wielkość liter. Jeśli tworzona jest pozycja z wartością userPassword **sekret**, łączenie określające hasło **SEKRET** zakończy się niepowodzeniem.

Podczas prostego łączenia klient wysyła na serwer hasło w postaci jawnego tekstu jako część żądania łączenia. Stwarza to ryzyko przechwycenia hasła za pomocą nasłuchu na poziomie protokołu. Do zabezpieczenia hasła można użyć połączenia SSL (wszystkie informacje wysyłane przez połączenie SSL są szyfrowane). Można użyć metody DIGEST-MD5 lub CRAM-MD5 SASL.

Metoda CRAM-MD5 wymaga, aby serwer miał dostęp do hasła w postaci tekstowej (zabezpieczenie hasłem ma ustawioną wartość none, co w rzeczywistości oznacza, że hasło jest przechowywane postaci, którą łatwo odszyfrować i które podczas wyszukiwania jest zwracane w postaci zwykłego tekstu) i aby wartość systemowa Zachowanie danych ochrony serwera (Retain server security data - QRETSVRSEC ) wynosiła 1 (Zachowanie danych). Klient wysyła nazwę wyróżniającą do serwera. Serwer wczytuje wartość userPassword dla pozycji i generuje losowy łańcuch. Łańcuch ten jest wysyłany do klienta. Zarówno klient, jak i serwer szyfrują go, używając hasła jako klucza, a klient wysyła wynik do serwera. Jeśli dwa zakodowane łańcuchy są zgodne, żądanie łączenia zakończy się powodzeniem, a hasło nie zostanie wysłane do serwera.

Metoda DIGEST-MD5 jest zbliżona do metody CRAM-MD5. Wymaga, aby serwer miał dostęp do hasła w postaci jawnego tekstu (zabezpieczenie hasła ustawione na wartość none (brak)) oraz aby wartość systemowa QRETSVRSEC była ustawiona na 1. Zamiast wysłać nazwę wyróżniającą do serwera, metoda DIGEST-MD5 wymaga, aby klient wysłał do niego nazwę użytkownika. Aby zwykły użytkownik (nie administrator) mógł używać metody DIGEST-MD5, wymagane jest, aby żadna inna pozycja w katalogu nie miała tej samej wartości atrybutu username. Inne różnice dotyczące metody DIGEST-MD5 obejmują więcej opcji konfiguracyjnych: dziedzinę serwera, atrybut username oraz hasło administratora. Serwer Directory Server zezwala użytkownikom na łączenie jako użytkownicy rzutowani lub publikowani i sprawdza podane hasło względem hasła w profilu użytkownika w systemie. Ponieważ hasło dla profili użytkowników w postaci zwykłego tekstu nie jest dostępne dla serwera, metoda DIGEST-MD5 nie może być używana w przypadku użytkowników rzutowanych lub publikowanych.

## Łączenie jako użytkownik opublikowany

Serwer Directory Server udostępnia pozycję LDAP, której hasło jest takie, jak hasło profilu użytkownika systemu operacyjnego w tym samym systemie. W tym celu pozycja musi:

- Posiadać atrybut UID, którego wartość jest nazwą profilu użytkownika systemu operacyjnego
- Nie posiadać atrybutu userPassword

Gdy serwer odbiera żądanie łączenia, które ma wartość UID, ale nie ma userPassword, serwer wywołuje ochronę systemu operacyjnego w celu sprawdzenia, czy ten UID jest poprawną nazwą profilu użytkownika i czy podane hasło jest poprawne dla tego profilu. Taka pozycja jest nazywana użytkownikiem opublikowanym w kontekście publikowania katalogu SDD (system distribution directory) do LDAP, co powoduje tworzenie takich pozycji.

## Łączenie jako użytkownik rzutowany

Pozycja LDAP przedstawiająca profil użytkownika systemu operacyjnego zwana jest użytkownikiem rzutowanym. Nazwy wyróżniającej użytkownika rzutowanego wraz z poprawnym hasłem dla profilu użytkownika można użyć w prostym łączeniu. Na przykład nazwą wyróżniającą dla użytkownika JSMITH w systemie moj-system.acme.com powinna być:

```
os400-profile=JSMITH,cn=accounts,os400-sys=moj-system.acme.com
```

## Łączenie SASL EXTERNAL

Jeśli połączenie SSL lub TLS jest używane razem z uwierzytelnianiem klienta (na przykład klient ma prywatny certyfikat), można użyć metody SASL EXTERNAL. Ta metoda informuje serwer, aby uzyskał tożsamość klienta z zewnętrznego źródła, w tym przypadku z połączenia SSL. Serwer pobiera publiczną część certyfikatu klienta (wysłaną na serwer w ramach ustanawiania połączenia SSL) i wyodrębnia nazwę wyróżniającą tego podmiotu. Ta nazwa wyróżniająca jest przypisywana do połączenia przez serwer LDAP.

Jeśli na przykład certyfikat jest przypisany do:

```
common name: John Smith
organization unit: Engineering
organization: ACME
locality: Minneapolis
state: MN
country: US
```

Nazwą wyróżniającą podmiotu może być:

```
cn=John Smith,ou=Engineering,o=acme,l=Minneapolis,st=MN,c=US
```

Należy zauważyć, że elementy cn, ou, o, l, st i c są używane w przedstawionej kolejności w celu wygenerowania nazwy wyróżniającej podmiotu.



## Łączenie SASL GSSAPI

Mechanizm łączenia SASL GSSAPI służy do uwierzytelniania serwera przy użyciu biletu Kerberos. Jest to przydatne, gdy klient wykonał uwierzytelnianie KINIT lub inną formę uwierzytelniania Kerberos (na przykład logowanie do domeny Windows 2000). W tym przypadku serwer sprawdza bilet klienta, a następnie pobiera nazwę użytkownika i dziedziny Kerberos; na przykład nazwa użytkownika jsmith w dziedzinie acme.com, określana jako jsmith@acme.com. Serwer można zdefiniować tak, aby odwzorował tę tożsamość na nazwę wyróżniającą w jeden z dwóch sposobów:

- Wygenerowanie pseudo nazwy wyróżniającej w postaci `ibm-kn=jankowski@firma.pl`.
- Wyszukanie pozycji mającej pomocniczą klasę `ibm-securityidentities` i wartość `altsecurityidentities` w formie `KERBEROS:<nazwa_użytkownika>@<dziedzina>`.

Pozycja, której można użyć dla `jsmith@acme.com`, może wyglądać następująco:

```
dn: cn=John Smith,cn=users,o=acme,c=us
objectclass: inetorgperson
objectclass: ibm-securityidentities
cn: John Smith
sn: Smith
altsecurityidentities: kerberos:jsmith@acme.com
```

## Łączenie OS400-PRFTKN

Mechanizm łączenia SASL OS400-PRFTKN służy do uwierzytelniania na serwerze za pomocą leksemu profilu (patrz funkcja API Generate Profile Token). Jeśli używany jest ten mechanizm, serwer sprawdza leksem profilu i przypisuje nazwę wyróżniającą profilu użytkownika rzutowanego do połączenia (na przykład `os400-profile=JSMITH,cn=accounts,os400-system=my-as400.mojafirma.com`). Jeśli aplikacja ma już leksem profilu, ten mechanizm pozwala uniknąć potrzeby pobierania nazwy profilu użytkownika i hasła użytkownika do wykonania prostego łączenia. Aby skorzystać z tego mechanizmu, użyj funkcji API `ldap_sasl_bind_s`, podając pustą nazwę wyróżniającą, `OS400-PRFTKN`, jako mechanizm i wartość `berval` (dane binarne zakodowane przy użyciu uproszczonych podstawowych reguł kodowania) zawierającą 32-bajtowy token profilu dla referencji. Korzystając z funkcji API LDAP w systemie i5/OS lub komend QSH (na przykład `ldapsearch`) w celu uzyskania dostępu do lokalnego serwera katalogów, można pominąć hasło, a funkcje API klienta dokonają uwierzytelniania na serwerze jako bieżący profil użytkownika dla zadania. Na przykład:

```
> ldapsearch -m OS400-PRFTKN -b "o=ibm,c=us" "(uid=jankowski)"
```

funkcja wykona wyszukiwanie z uprawnieniami bieżącego profilu użytkownika, tak jakby użyta została funkcja:

```
> ldapsearch -D os400-profile=profil,cn=accounts,os400-sys=system -w hasło -b
"o=ibm,c=us" "(uid=jankowski)"
```

## LDAP jako usługa uwierzytelniania

LDAP jest zwykle używany jako usługa uwierzytelniania. Serwer WWW można skonfigurować tak, aby uwierzytelniał LDAP. Konfigurując wiele serwerów WWW (lub innych aplikacji) do uwierzytelniania w LDAP, można ustanowić pojedynczy rejestr użytkowników dla tych aplikacji zamiast definiowania użytkowników dla każdej aplikacji lub instancji serwera WWW.

Jak to działa? W skrócie serwer WWW prosi użytkownika o podanie nazwy i hasła. Serwer WWW pobiera te informacje i w katalogu LDAP szuka pozycji z tą nazwą użytkownika (na przykład można skonfigurować serwer WWW, tak aby przypisał nazwę użytkownika do atrybutów 'uid' lub 'mail' protokołu LDAP). Jeśli znajdzie dokładnie jedną pozycję, wysyła żądanie łączenia do serwera, używając nazwy wyróżniającej odnalezionej pozycji i hasła podanego przez użytkownika. Jeśli operacja łączenia zakończy się powodzeniem, użytkownik został uwierzytelniony. Połączeń SSL można używać do ochrony hasła przed nasłuchiowaniem na poziomie protokołu.

Serwer WWW może również śledzić używane nazwy wyróżniające, aby dana aplikacja mogła ich używać, być może poprzez przechowywanie danych dostosowania w tej pozycji, innej pozycji z nią powiązanej lub w oddzielnej bazie danych używającej nazwy wyróżniającej jako klucza do wyszukiwania informacji.

Często używaną alternatywą dla żądania łączenia jest operacja porównania LDAP. Na przykład `ldap_compare(ldap_session, dn, "userPassword", enteredPassword)`. Umożliwia to aplikacji korzystanie z pojedynczej sesji LDAP zamiast sesji uruchamiania i kończenia dla każdego żądania uwierzytelniania.

### **Pojęcia pokrewne**

“Mechanizm rzutowania systemu operacyjnego”

Systemowy mechanizm rzutowania ma możliwość odwzorowywania obiektów systemu i5/OS jako pozycji wewnątrz drzewa katalogów dostępnego z LDAP. Rzutowane obiekty są reprezentacjami LDAP obiektów systemu operacyjnego, zastępującymi rzeczywiste pozycje przechowywane w bazie danych serwera LDAP.

“Zadania związane z użytkownikami” na stronie 203

Ten temat zawiera informacje dotyczące zarządzania użytkownikami.

Funkcje API protokołu LDAP

Temat Funkcje API protokołu LDAP zawiera więcej informacji o funkcjach API serwera katalogów.

### **Zadania pokrewne**

“Konfigurowanie uwierzytelniania DIGEST-MD5 na serwerze Directory Server” na stronie 184

Ten temat zawiera informacje dotyczące konfigurowania uwierzytelniania DIGEST-MD5 na serwerze Directory Server.

“Włączanie uwierzytelniania Kerberos na serwerze Directory Server” na stronie 184

Ten temat zawiera informacje dotyczące włączania uwierzytelniania Kerberos na serwerze Directory Server.

## **Odmowa usługi**

Opisana w tym temacie opcja konfiguracyjna zapewnia ochronę przed atakami polegającymi na spowodowaniu odmowy usługi.

Serwer katalogów zabezpiecza przed następującymi formami odmowy usługi:

- Klienci wolno wysyłający dane, wysyłający częściowe dane lub nie wysyłający danych
- Klienci nie odczytujący rezultatów danych lub odczytujący rezultaty wolno
- Klienci, którzy nie kończą łączenia
- Klienci wprowadzający żądania, które tworzą długotrwałe żądania bazy danych
- Klienci tworzący powiązanie anonimowo
- Obciążenia serwera uniemożliwiające administratorowi zarządzanie serwerem

Serwer katalogów udostępnia administratorowi kilka metod zapobiegania odmowie usługi. Administrator zawsze posiada dostęp do serwera poprzez wykorzystanie wątku ratunkowego, nawet jeśli serwer jest zajęty długotrwałymi działaniami. Ponadto, administrator steruje dostępem do serwera i ma możliwość odłączenia klientów z określoną nazwą wyróżniającą łączenia lub adresem IP i skonfigurowania serwera, aby nie zezwalał na anonimowy dostęp. Aby umożliwić serwerowi aktywne zapobieganie odmowie dostępu, można aktywować inne opcje konfiguracyjne.

### **Zadania pokrewne**

“Zarządzanie połączeniami serwera” na stronie 118

Ten temat zawiera informacje o wyświetleniu połączeń z serwerem oraz o działaniach wykonywanych przy użyciu tych połączeń.

“Zarządzanie właściwościami połączenia” na stronie 119

Ten temat zawiera informacje o ustawianiu właściwości połączenia, w tym właściwości zapobiegających blokowaniu serwera przez klientów.

## **Mechanizm rzutowania systemu operacyjnego**

Systemowy mechanizm rzutowania ma możliwość odwzorowywania obiektów systemu i5/OS jako pozycji wewnątrz drzewa katalogów dostępnego z LDAP. Rzutowane obiekty są reprezentacjami LDAP obiektów systemu operacyjnego, zastępującymi rzeczywiste pozycje przechowywane w bazie danych serwera LDAP.

Profile użytkowników są jedynymi obiektami odwzorowywanymi lub rzutowanymi jako pozycje wewnątrz drzewa katalogowego. Odwzorowywanie obiektów profilu użytkownika nosi nazwę mechanizmu rzutowania użytkowników systemu operacyjnego.

Operacje LDAP są odwzorowywane na odpowiadające im obiekty systemu operacyjnego 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 powiązanego z połączeniem klienta.

Więcej informacji na temat systemowego mechanizmu rzutowania znajduje się w następujących sekcjach:

#### Zadania pokrewne

“Nadawanie dostępu administratora użytkownikom rzutowanym” na stronie 125

Ten temat zawiera informacje dotyczące nadawania dostępu administratora profilom użytkowników.

#### Odsyłacze pokrewne

“Uwierzytelnianie” na stronie 80

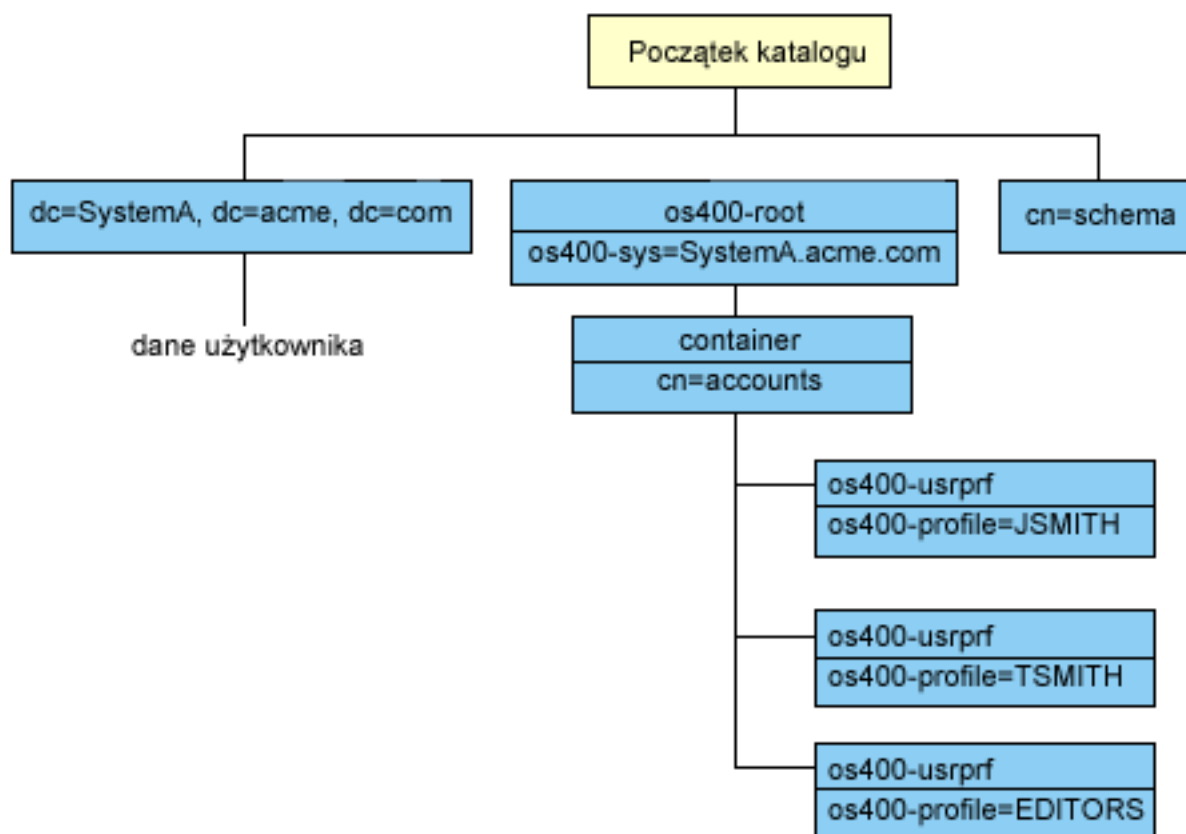
Uwierzytelnianie umożliwia kontrolę dostępu w ramach serwera Directory Server.

## Drzewo informacji katalogu dla mechanizmu rzutowania użytkowników

Ten temat zawiera informacje o sposobie reprezentacji przyrostków i profili użytkowników w drzewie informacji katalogu dla mechanizmu rzutowania użytkowników.

Poniższy rysunek przedstawia przykładowe drzewo informacji katalogu (DIT) dla mechanizmu rzutowania użytkowników. 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 ma na celu pokazanie odniesienia. Ten przyrostek przedstawia bieżący postprocesor bazy danych zarządzający innymi pozycjami LDAP. Przyrostek cn=schema jest używanym obecnie schematem serwera rozległego.



Początek drzewa jest przyrostkiem, którego wartością domyślną jest os400-sys=SystemA.acme.com, gdzie SystemA.acme.com jest nazwą systemu. Klasą obiektu (objectclass) jest os400-root. Mimo iż nie da się

zmodyfikować ani usunąć drzewa DIT, można przekonfigurować przyrostek obiektów systemowych. W tym celu należy się upewnić, czy bieżący przyrostek nie jest używany na listach ACL lub gdzie indziej w systemie. Jeśli tak, należy zmodyfikować wszystkie pozycje, w których zmieniany jest przyrostek.

Na poprzednim rysunku pojemnik `cn=accounts` został umieszczony poniżej początku hierarchii. Tego obiektu nie można modyfikować. Pojemnik umieszczono na tym poziomie, przewidując innego rodzaju informacje lub obiekty, 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 te noszą nazwę profili użytkowników rzutowanych i są znane protokołowi LDAP w postaci `os400-profile=JSMITH,cn=accounts,os400-sys=SystemA.acme.com`.

## Operacje LDAP

W tym temacie opisano operacje LDAP, które mogą być wykonywane w mechanizmie rzutowania.

Poniżej przedstawione są operacje LDAP, które można wykonywać 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) rzutowanego profilu użytkownika jako nazwy wyróżniającej połączenia i poprawnego hasła profilu użytkownika w celu uwierzytelnienia. Przykładem użycia nazwy wyróżniającej w żądaniu połączenia jest: `os400-profile=jsmith,cn=accounts,os400-sys=systemA.acme.com`.

Aby mieć dostęp do informacji w mechanizmie rzutowania użytkowników, klient musi połączyć się jako użytkownik rzutowany.

Dostępne są dwa dodatkowe mechanizmy umożliwiające uwierzytelnienie na serwerze katalogów jako użytkownik rzutowany:

- Łączenie SASL GSSAPI. Jeśli system operacyjny został skonfigurowany, aby używał odwzorowania EIM (Enterprise Identity Mapping), serwer katalogów odpytuje EIM w celu określenia, czy istnieje powiązanie początkowej tożsamości Kerberos z lokalnym profilem użytkownika. Jeśli istnieje takie powiązanie, serwer przypisze profil użytkownika do połączenia i będzie go można używać do uzyskania dostępu do systemowego mechanizmu rzutowania.
- Łączenie SASL OS400-PRFTKN. Leksemu profilu można używać do uwierzytelniania na serwerze katalogów. Serwer przypisuje profil użytkownika leksemu profilu do połączenia.

Serwer wykonuje wszystkie te operacje, korzystając z uprawnień tego profilu użytkownika. Nazwa wyróżniająca profilu użytkownika rzutowanego może być również wykorzystana w listach ACL LDAP, tak jak inne nazwy wyróżniające pozycji LDAP. Prosta metoda łączenia jest jedyną dozwoloną metodą łączenia, kiedy w żądaniu określono użytkownika rzutowanego.

### Wyszukiwanie

Systemowy mechanizm rzutowania obsługuje kilka podstawowych filtrów wyszukiwania. Można w nich określić atrybuty klasy obiektu `os400-profile` oraz `os400-gid`. Atrybut `os400-profile` obsługuje znaki zastępcze. Atrybut `os400-gid` jest ograniczony do określania pojedynczego profilu użytkownika (`os400-gid=0`) lub grupy profili (`!(os400-gid=0)`). Użytkownik może odtworzyć wszystkie atrybuty profilu z wyjątkiem hasła i podobnych atrybutów.

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.

| Administratorzy LDAP mają możliwość blokowania dostępu do wszelkich operacji wyszukiwania kierowanych do  
| mechanizmu rzutowania użytkowników. Więcej informacji można znaleźć w temacie Dostęp do odczytu profili  
| użytkowników rzutowanych, do którego odsyłacz zamieszczono poniżej.

Poniższa tabela opisuje zachowanie systemowego mechanizmu rzutowania w przypadku operacji wyszukiwania.

**Tabela 3. Zachowanie systemowego mechanizmu rzutowania dla operacji wyszukiwania**

Żądanie wyszukiwania	Podstawa wyszukiwania	Zasięg wyszukiwania	Filtr wyszukiwania	Komentarze
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 podany zasięg oraz filtr. Zwracane są określone na stałe atrybuty oraz ich wartości dla przyrostka obiektów systemowych 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 użytkowników rzutowanych zwracane są jedynie wartości nazwy wyróżniającej (DN), klasy obiektu oraz atrybutu os400-profile. Jeśli zostanie podany dowolny inny filtr, zwracana jest wartość LDAP_UNWILLING_TO_PERFORM.
Zwróć wszystkie profile grup.	cn=accounts, os400-sys=SystemA.acme.com	jednopoziomowy lub w poddrzewie	(!(os400-gid=0))	Dla profili użytkowników rzutowanych zwracane są jedynie wartości nazwy wyróżniającej (DN), klasy obiektu oraz atrybutu os400-profile. Jeśli zostanie podany dowolny inny filtr, zwracana jest wartość 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 użytkowników rzutowanych zwracane są jedynie wartości nazwy wyróżniającej (DN), klasy obiektu oraz atrybutu os400-profile. Jeśli zostanie podany dowolny inny filtr, zwracana jest wartość LDAP_UNWILLING_TO_PERFORM.
Zwróć informacje dla profilu określonego użytkownika lub grupy, na przykład JSMITH.	cn=accounts, os400-sys=SystemA.acme.com	jednopoziomowy lub w poddrzewie	os400-profile=JSMITH	Można określić, że mają być zwracane inne atrybuty.
Zwróć informacje dla profilu określonego użytkownika lub grupy, na przykład 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. Mimo iż 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 użytkowników rzutowanych zwracane są jedynie wartości nazwy wyróżniającej (DN), klasy obiektu oraz atrybutu os400-profile. Jeśli zostanie podany dowolny inny filtr, zwracana jest wartość LDAP_UNWILLING_TO_PERFORM.
Zwróć wszystkie profile grupowe zaczynające się na G.	cn=accounts, os400-sys=SystemA.acme.com	jednopoziomowy lub w poddrzewie	(&(!(os400-gid=0)) (os400-profile=G*))	Dla profili użytkowników rzutowanych zwracane są jedynie wartości nazwy wyróżniającej (DN), klasy obiektu oraz atrybutu os400-profile. Jeśli zostanie podany dowolny inny filtr, zwracana jest wartość 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 użytkowników rzutowanych zwracane są jedynie wartości nazwy wyróżniającej (DN), klasy obiektu oraz atrybutu os400-profile. Jeśli zostanie podany dowolny inny filtr, zwracana jest wartość LDAP_UNWILLING_TO_PERFORM.

## Porównywanie

Operacja porównywania LDAP może zostać użyta do porównania wartości atrybutu profilu użytkownika rzutowanego. Atrybutów os400-aut oraz os400-docpwd nie można porównywać.

- | Administratorzy LDAP mają możliwość blokowania dostępu do wszelkich operacji porównywania kierowanych do mechanizmu rzutowania użytkowników. Więcej informacji można znaleźć w temacie Dostęp do odczytu profili użytkowników rzutowanych, do którego odsyłacz zamieszczono poniżej.

## 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. Dostępne są teraz dwa elementy kontrolne serwera LDAP umożliwiające określenie zachowania parametrów DLTUSRPRF OWNBJOPT i PGPOPT. Można je podać w operacji usuwania LDAP. Więcej informacji na temat zachowania tych parametrów znajduje się w pomocy komendy Usunięcie profilu użytkownika (Delete User Profile - DLTUSRPRF).

Poniżej przedstawiono elementy kontrolne i ich identyfikatory obiektu (OID), które można określić podczas operacji klienckiej usuwania.

- **os400-dltusrprf-ownobjopt** 1.3.18.0.2.10.8

Wartość elementu sterującego jest łańcuchem o następującej postaci:

- `controlValue ::= ownObjOpt [ newOwner]`
- `ownObjOpt ::= *NODLT / *DLT / *CHGOWN`

Wartość sterująca `ownObjOpt` określa rodzaj działania w przypadku, gdy do profilu użytkownika należą jakieś obiekty. Wartość `*NODLT` oznacza, że profil użytkownika nie ma być usuwany, 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. Jest ona wymagana, jeśli `ownObjOpt` ma wartość `*CHGOWN`.

Przykłady wartości sterujących są następujące:

- `*NODLT`: określa, że profil nie może być usunięty, jeśli należy do niego jakikolwiek obiekt.
- `*CHGOWN SMITH`: określa, że prawa własności jakichkolwiek obiektów mają zostać przeniesione na profil 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 definiowana jako łańcuch w następującej formie:

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

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

Przykłady wartości sterujących są następujące:

- `*NOCHG`: określa, że profil nie może być usunięty, jeśli jest grupą podstawową dla jakichkolwiek obiektów
- `*CHGPGP *NONE`: określa, że należy usunąć grupę podstawową obiektów
- `*CHGPGP SMITH *USE`: określa, że należy zmienić grupę podstawową na profil użytkownika SMITH i przydzielić uprawnienia `*USE` grupie podstawowej.

Jeśli podczas usuwania żaden z tych elementów kontrolnych nie zostanie określony, użyte zostaną bieżące wartości domyślne dla komendy `QSYS/DLTUSRPRF`.

## ModRDN

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

## Funkcje API importu i eksportu

Funkcje API QgldImportLdif i QgldExportLdif nie obsługują opcji importowania lub eksportowania danych wewnątrz systemowego mechanizmu rzutowania.

### Pojęcia pokrewne

Odwzorowywanie tożsamości dla przedsiębiorstwa (Enterprise Identity Mapping - EIM)

“Dostęp do odczytu profili użytkowników rzutowanych”

Domyślnie systemowy mechanizm rzutowania umożliwia autoryzowanym użytkownikom dostęp do odczytu informacji o profilach użytkowników przez operacje wyszukiwania i porównywania LDAP. Dostęp do odczytu informacji o profilach użytkowników rzutowanych można włączać i wyłączać za pomocą programu System i Navigator lub ustawienia konfiguracyjnego w pliku /QIBM/UserData/OS400/DirSrv/idsslapd-instance/etc/ibmslapd.conf (/QIBM/UserData/OS400/DirSrv/idsslapd-QUSRDIR/etc/ibmslapd.conf w przypadku domyślnej instancji serwera).

## Nazwy wyróżniające łączenia administratora i repliki

Jako skonfigurowaną nazwę wyróżniającą łączącą administratora lub replikę można podać profil użytkownika rzutowanego. Użyte zostanie wtedy hasło profilu użytkownika.

Profile użytkowników rzutowanych mogą także być administratorami LDAP, jeśli mają uprawnienia do identyfikatora funkcji Directory Server Administrator (QIBM\_DIRSRV\_ADMIN). Dostęp administratora można nadać wielu profilom użytkowników.

### Pojęcia pokrewne

“Dostęp administracyjny” na stronie 63

Dostęp administracyjny służy do kontrolowania praw dostępu do konkretnych zadań administracyjnych.

## Schemat użytkowników rzutowanych

Klasy obiektu oraz atrybuty z mechanizmu rzutowania można znaleźć w schemacie obejmującym cały serwer.

Nazwy atrybutów LDAP mają format `os400-nnn`, gdzie *nnn* jest zazwyczaj słowem kluczowym atrybutu w komendach profilu użytkownika. Na przykład atrybut `os400-usrcls` odpowiada parametrowi `USRCLS` komendy `CRTUSRPRF`. Wartości atrybutów odpowiadają wartościom parametrów akceptowanych przez komendy `CRTUSRPRF` i `CHGUSRPRF` lub wartościom wyświetlanym podczas wyświetlania profilu użytkownika. Aby przejrzeć definicje klasy obiektu `os400-usrprf` i powiązanych atrybutów `os400-xxx`, należy użyć narzędzia Web Administration lub innej aplikacji.

## Dostęp do odczytu profili użytkowników rzutowanych

| Domyślnie systemowy mechanizm rzutowania umożliwia autoryzowanym użytkownikom dostęp do odczytu  
| informacji o profilach użytkowników przez operacje wyszukiwania i porównywania LDAP. Dostęp do odczytu  
| informacji o profilach użytkowników rzutowanych można włączać i wyłączać za pomocą programu System i Navigator  
| lub ustawienia konfiguracyjnego w pliku /QIBM/UserData/OS400/DirSrv/idsslapd-instance/etc/ibmslapd.conf  
| (/QIBM/UserData/OS400/DirSrv/idsslapd-QUSRDIR/etc/ibmslapd.conf w przypadku domyślnej instancji serwera).

| Aby wyłączyć dostęp do odczytu informacji o profilach użytkowników, należy wykonać następujące czynności:

- | 1. W programie System i Navigator rozwiń pozycję **Sieć**.
- | 2. Rozwiń gałąź **Serwery>TCP/IP** (Servers > TCP/IP).
- | 3. Prawym przyciskiem myszy kliknij element **IBM Tivoli Directory Server** i wybierz opcję **Właściwości** (Properties).
- | 4. Wybierz zakładkę **Baza danych/przyrostki** (Database/Suffixes).
- | 5. Usuń zaznaczenie z pola wyboru **Zezwól na dostęp do odczytu informacji o użytkowniku** (Allow read access to user information).

| W sekcji `cn=Front End, cn=Configuration` pliku konfiguracyjnego można zmienić następujący wiersz, aby wyłączyć  
| operacje wyszukiwania i porównywania w mechanizmie rzutowania użytkowników:

| ibm-slapdOs400UsrprjRead: TRUE

| Aby wyłączyć dostęp do odczytu, należy zmienić wartość z TRUE na FALSE. Jeśli wartość to TRUE lub w pliku konfiguracyjnym nie ma tego ustawienia, dostęp do odczytu profili użytkowników rzutowanych jest włączony.

#### **Zadania pokrewne**

“Włączanie i wyłączanie dostępu do odczytu profili użytkowników rzutowanych” na stronie 129

Aby uniemożliwić operacje wyszukiwania i porównywania w mechanizmie rzutowania użytkowników, należy skorzystać z poniższych informacji.

#### **Odsyłacze pokrewne**

“Operacje LDAP” na stronie 86

W tym temacie opisano operacje LDAP, które mogą być wykonywane w mechanizmie rzutowania.

## **Obsługa funkcji kronikowania systemu i5/OS w serwerze Directory Server**

Zapisywanie danych katalogowych przez produkt Directory Server odbywa się z wykorzystaniem oferowanych przez system i5/OS funkcji obsługi baz danych. Podczas zapisu pozycji katalogów w bazie danych przez serwer Directory Server używana jest kontrola transakcji. Wymaga to obsługi mechanizmów kronikowania w systemie i5/OS.

Po pierwszym uruchomieniu serwera lub narzędzia LDIF do importu tworzone są następujące elementy:

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

Kronika QSQRN jest wbudowana w skonfigurowaną bibliotekę bazy danych. Dziennik QSQRN0001 jest na wstępie 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 użytymi wielkościami progowymi. Jeśli jest to konieczne, można zmienić parametry komendy kronikowania. Kronikowanie LDAP jest domyślnie skonfigurowane do usuwania poprzednich dzienników. Jeśli skonfigurowano protokół zmian i użytkownik chce zachować poprzednie dzienniki, powinien uruchomić następującą komendę z poziomu wiersza komend:

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

Jeśli skonfigurowano protokół zmian, za pomocą następującej komendy można usunąć jego stare dzienniki:

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

#### **Informacje pokrewne**

Zmiana kroniki (Change Journal - CHGJRN)

## **Atrybuty unikalne**

Funkcja atrybutów unikalnych zapewnia, że w obrębie katalogu określone atrybuty posiadają zawsze wartości unikalne.

Atrybuty te można określić jedynie w dwóch pozycjach: `cn=uniqueattribute,cn=localhost` i `cn=uniqueattribute,cn=IBMpolicies`. Wyniki wyszukiwania dla atrybutów unikalnych są unikalne jedynie dla bazy danych tego serwera. Wyniki wyszukiwania obejmujące wyniki z odwołań mogą nie być unikalne.

**Uwaga:** Atrybuty binarne, atrybuty wykonawcze, atrybuty konfiguracyjne oraz atrybut `objectclass` nie mogą zostać oznaczone jako unikalne.

Nie wszystkie atrybuty można określić jako unikalne. Aby ustalić, czy atrybut można określić jako unikalny, należy użyć komendy `ldapexop`:

- W przypadku atrybutów, które mogą być unikalne: `ldapexop -op getattributes -attrType unique -ma wartość true`



- W przypadku atrybutów, które nie mogą być unikalne: `ldapexop -op getattributes -attrType unique -ma wartość false`

### Pojęcia pokrewne

“Zadania związane z atrybutami unikalnymi” na stronie 141

Ten temat zawiera informacje dotyczące zarządzania atrybutami unikalnymi.

## Atrybuty operacyjne

Istnieje szereg atrybutów o specjalnym znaczeniu dla serwera katalogów znanych jako atrybuty operacyjne. Są to atrybuty obsługiwane przez serwer i odzwierciedlające zarządzane przez serwer informacje o pozycji lub wywierające wpływ na działanie serwera.

Atrybuty te mają specjalne charakterystyki:

- Nie są zwracane przez operację wyszukiwania, chyba że zostały wyszczególnione (według nazwy) w żądaniu wyszukiwania.
- Nie należą do żadnej klasy obiektu. Serwer określa, które pozycje mają atrybuty.

Serwer katalogów obsługuje między innymi następujące zestawy atrybutów operacyjnych:

- `creatorsName`, `createTimestamp`, `modifiersName`, `modifyTimestamp` występują w każdej pozycji. Atrybuty te przedstawiają nazwę wyróżniającą łączenia oraz czas pierwszego utworzenia lub ostatniej modyfikacji pozycji. Atrybutów tych można używać w filtrach wyszukiwania, na przykład w celu wyszukania wszystkich pozycji zmodyfikowanych po określonym czasie. Użytkownik nie może zmieniać tych atrybutów. Atrybuty te są replikowane do serwerów odbierających oraz importowane i eksportowane w plikach LDIF.
- `ibm-entryuuid`. Obecny w każdej pozycji utworzonej w wersji V5R3 lub nowszej serwera. Atrybut ten jest unikalnym identyfikatorem łańcucha przypisanym przez serwer do każdej pozycji podczas jej tworzenia. Jest użyteczny dla aplikacji wymagających rozróżnienia między pozycjami o identycznych nazwach na różnych serwerach. Atrybut używa algorytmu DCE UUID do generowania ID unikalnego we wszystkich pozycjach na wszystkich serwerach używających datownika, adresu adaptera i innych informacji.
- `entryowner`, `ownersource`, `ownerpropagate`, `aclentry`, `aclsource`, `aclpropagate`, `ibm-filteracl`, `ibm-filteraclinherit`, `ibm-effectiveAcl`.
- `hasSubordinates`. Obecny w każdej pozycji i ma wartość TRUE, jeśli pozycja jest podrzędna.
- `numSubordinates`. Obecny w każdej pozycji i zawiera liczbę pozycji podrzędnych dla tej pozycji.
- `pwdChangedTime`, `pwdAccountLockedTime`, `pwdExpirationWarned`, `pwdFailureTime`, `pwdGraceUseTime`, `pwdReset`, `pwdHistory`.
- `subschemasubentry` - Obecny w każdej pozycji; określa położenie schematu dla tej części drzewa. Jest użyteczny dla serwerów z wieloma schematami, jeśli użytkownik chce odnaleźć schemat używany w tej części drzewa.

Aby wyświetlić pełną listę atrybutów wykonawczych, należy użyć następującej operacji rozszerzonej: `ldapexop -op getattributes -attrType operational -matches true`.

### Pojęcia pokrewne

“Katalogi” na stronie 4

Serwer Directory Server umożliwia dostęp do bazy danych specjalnego typu, w której informacje są zapisywane w strukturze hierarchicznej podobnej do organizacji zintegrowanego systemu plików systemu i5/OS.

“Listy kontroli dostępu” na stronie 64

Listy kontroli dostępu (ACL) stanowią ochronę informacji zapisanych w katalogu LDAP. Za pomocą list ACL administratorzy ograniczają dostęp do różnych części katalogu lub konkretnych jego pozycji.

“Strategia haseł” na stronie 77

Jeśli serwery LDAP służą do uwierzytelniania, to ważne jest, aby obsługiwały strategię dotyczące wygaśnięcia hasła, zakończonych niepowodzeniem prób zalogowania się i reguł dotyczących haseł. Serwer Directory Server udostępnia konfigurowalną obsługę wszystkich trzech rodzajów strategii.

## Pamięci podręczne serwera

Pamięci podręczne LDAP to buforory szybkiej pamięci używane do przechowywania informacji LDAP, takich jak zapytania, odpowiedzi oraz uwierzytelnienie użytkownika do późniejszego wykorzystania. Strojenie pamięci podręcznych LDAP jest kluczowe dla poprawy wydajności.

Wyszukiwanie w katalogu LDAP korzystające z pamięci podręcznej LDAP może być szybsze od wyszukiwania wymagającego połączenia z bazą danych DB2, nawet jeśli informacje są w tej bazie buforowane. Z tego powodu strojenie pamięci podręcznych LDAP może poprawić wydajność dzięki uniknięciu wywołań do bazy danych. Pamięci podręczne LDAP są szczególnie użyteczne w przypadku aplikacji często pobierających powtarzające się informacje buforowane.

Poniższe sekcje omawiają wszystkie pamięci podręczne LDAP i demonstrują sposób określania i ustawiania najkorzystniejszych ustawień pamięci podręcznej dla systemu.

### Pojęcia pokrewne

“Zadania związane z wydajnością” na stronie 143

Ten temat zawiera informacje dotyczące dopasowywania ustawień wydajności.

## Pamięć podręczna atrybutu

Pamięć podręczna atrybutu ma tę zaletę, że pozwala rozstrzygać wyszukiwanie filtru w pamięci zamiast wstępnie rozstrzygać w bazie danych i przechowywać w pamięci podręcznej. Jest także aktualizowana za każdym razem, kiedy wykonywane jest działanie dodawania, usuwania, modyfikacji LDAP lub działanie modrdn.

Podczas podejmowania decyzji, które atrybuty mają być przechowywane w pamięci, należy rozważyć:

- Ilość pamięci dostępnej dla serwera
- Wielkość katalogu
- Typy filtrów wyszukiwania, których aplikacja zwykle używa

**Uwaga:** Menedżer pamięci podręcznej atrybutu może rozstrzygać następujące typy prostych filtrów: filtry dokładnego dopasowania i filtry obecności. Może on rozstrzygać złożone filtry dotyczące spójności lub niespójności, a podfiltry muszą dotyczyć dokładnego dopasowania, obecności, spójności lub niespójności.

Nie wszystkie atrybuty można dodawać do pamięci podręcznej atrybutu. Aby określić, czy atrybut może zostać dodany do pamięci podręcznej, należy użyć komendy `ldapexop`:

- W przypadku atrybutów, które można dodawać: `ldapexop -op getattributes -attrType attribute_cache -ma wartość true`
- W przypadku atrybutów, których nie można dodawać: `ldapexop -op getattributes -attrType attribute_cache -ma wartość false`

Buforowanie atrybutów można skonfigurować na dwa sposoby: ręcznie lub automatycznie. Aby skonfigurować buforowanie atrybutów ręcznie, administrator powinien wykonać wyszukiwania `cn=monitor`, aby sprawdzić w jaki sposób uczynić buforowanie atrybutów najbardziej wydajnym. Wyszukiwania te zwracają bieżące informacje o atrybutach, które są buforowane, ilości pamięci wykorzystanej przez każdy z atrybutów, całkowitej ilości pamięci wykorzystanej dla buforowania atrybutów oraz listę atrybutów najczęściej wykorzystywanych w filtrach wyszukiwania. Wykorzystując te informacje administrator może zmienić ilość pamięci dozwolonej do użycia przez buforowanie atrybutów oraz określić w oparciu o wyszukiwania `cn=monitor`, które atrybuty powinny być buforowane, kiedy jest to konieczne.

Alternatywnie, administrator może skonfigurować automatyczne buforowanie atrybutów. Kiedy włączona jest opcja automatycznego buforowania atrybutów, serwer Directory Server śledzi kombinację atrybutów, które są najbardziej potrzebne do buforowania w obrębie ograniczeń pamięci zdefiniowanych przez administratora. Następnie aktualizuje buforowanie atrybutów z częstotliwością skonfigurowaną przez administratora.

## Pamięć podręczna filtru

Kiedy klient wprowadza zapytanie o dane, a zapytanie nie może zostać rozstrzygnięte przez menedżera pamięci podręcznej atrybutu w pamięci, zapytanie przechodzi do pamięci podręcznej filtru. Ta pamięć podręczna zawiera buforowane identyfikatory pozycji.

Kiedy zapytanie wprowadzane jest do pamięci podręcznej filtru, możliwe są dwa zdarzenia:

- **Identyfikatory zgodne z ustawieniami filtru użytymi w zapytaniu są umieszczane w pamięci podręcznej filtru.** W takim przypadku, lista identyfikatorów zgodnych pozycji wysyłana jest do pamięci podręcznej pozycji.
- **Identyfikatory zgodnych pozycji nie są buforowane w pamięci podręcznej filtru.** W takim przypadku, zapytanie musi mieć dostęp do bazy DB2 w celu wyszukania wymaganych danych.

Aby określić jaką wielkość powinna mieć pamięć podręczna filtru, należy uruchomić obciążenie z różnymi wartościami pamięci podręcznej filtru i zmierzyć różnice w liczbie działań wykonywanych na sekundę.

Zmienna konfiguracyjna limitu obejścia pamięci podręcznej filtru ogranicza liczbę pozycji, które można dodać do pamięci podręcznej filtru. Na przykład, jeśli zmienna konfiguracyjna limitu obejścia ma ustawioną wartość 1,000, filtry wyszukiwania zgodne z więcej niż 1,000 pozycji nie są dodawane do pamięci podręcznej filtru. Zapobiega to nadpisaniu użytecznych pozycji pamięci podręcznej przez obszerne nietypowe wyszukiwania. Aby określić najkorzystniejszy limit obejścia pamięci podręcznej filtru dla danego obciążenia, należy kilkakrotnie uruchomić obciążenie i zmierzyć przepustowość.

## Pamięć podręczna pozycji

Pamięć podręczna pozycji zawiera dane buforowanych pozycji. Identyfikatory pozycji wysyłane są do pamięci podręcznej pozycji.

Jeśli pozycje zgodne z identyfikatorami pozycji znajdują się w pamięci podręcznej pozycji, wyniki zwracane są do klienta. Jeśli pamięć podręczna nie zawiera pozycji odpowiadających identyfikatorom pozycji, zapytanie przechodzi do bazy DB2, aby wyszukać zgodne pozycje.

Aby określić jaką wielkość powinna mieć pamięć podręczna pozycji, należy uruchomić obciążenie z różnymi wartościami pamięci podręcznej pozycji i zmierzyć różnice w liczbie działań wykonywanych na sekundę.

## Pamięć podręczna listy ACL

Pamięć podręczna listy ACL zawiera informacje o kontroli dostępu, takie jak właściciel pozycji i uprawnienia do pozycji dla ostatnio używanych pozycji. Ta pamięć podręczna używana jest do poprawy wydajności oceny uprawnień do dodawania, usuwania, modyfikowania lub wyszukiwania dla pozycji.

Jeśli pozycja nie znajduje się w pamięci podręcznej listy ACL, informacje o kontroli dostępu pobierane są z bazy danych. Aby określić odpowiednią wielkość pamięci podręcznej listy ACL, należy zmierzyć wydajność serwera używając typowego obciążenia i różnych wielkości pamięci podręcznej listy ACL.

## Elementy sterujące i rozszerzone operacje

Elementy sterujące i rozszerzone operacje umożliwiają zwiększanie możliwości protokołu LDAP bez jego modyfikowania.

### Elementy sterujące

Elementy sterujące udostępniają dodatkowe informacje, aby serwer sterował interpretacją danego żądania. Na przykład element sterujący `delete subtree` można określić w żądaniu usunięcia LDAP, wskazując, że oprócz określonej pozycji serwer powinien usunąć wszystkie jej pozycje podrzędne. Element sterujący składa się z trzech części:

- Typ elementu sterującego, którym jest OID identyfikujący element sterujący.
- Wskaźnik newralgiczności określający zachowanie serwera, jeśli nie obsługuje elementu sterującego. Jest to wartość boolowska. `FALSE` oznacza, że element sterujący nie jest newralgiczny, a serwer powinien go zignorować, jeśli go

nie obsługuje. TRUE oznacza, że element sterujący jest newralgiczny i jeśli serwer go nie obsługuje, całe żądanie powinno zakończyć się niepowodzeniem (z nieobsługiwanym krytycznym błędem rozszerzenia).

- Opcjonalna wartość elementu sterującego, która zawiera inne informacje specyficzne dla niego. Zawartość wartości elementu sterującego jest określona w postaci ASN.1. Sama wartość jest w kodzie BER danych elementu sterującego.

## Rozszerzone operacje

Rozszerzone operacje służą do uruchamiania operacji stanowiących dodatek do podstawowych operacji LDAP. Na przykład zdefiniowano rozszerzone operacje w celu grupowania zestawu operacji w ramach pojedynczej transakcji. Rozszerzona operacja składa się z następujących elementów:

- Nazwa żądania, OID określający konkretną operację.
- Opcjonalna wartość żądania, która zawiera inne informacje specyficzne dla niego. Zawartość wartości żądania jest określona w postaci ASN.1. Sama wartość jest w kodzie BER danych żądania.

Rozszerzone operacje zwykle mają rozszerzoną odpowiedź. Odpowiedź składa się z następujących elementów:

- Komponenty standardowego wyniku LDAP (kod błędu, pasująca nazwa wyróżniająca i komunikat o błędzie).
- Nazwa odpowiedzi, OID określający typ odpowiedzi.
- Opcjonalna wartość, która zawiera inne informacje specyficzne dla odpowiedzi. Zawartość wartości odpowiedzi jest określona w postaci ASN.1. Sama wartość jest w kodzie BER danych odpowiedzi.

### Pojęcia pokrewne

“Nazwy wyróżniające (DN)” na stronie 9

Każda pozycja w katalogu ma nazwę wyróżniającą (DN). Nazwa DN jednoznacznie identyfikuje pozycję w katalogu. Pierwszy komponent nazwy DN jest nazywany względną nazwą wyróżniającą (RDN).

### Odsyłacze pokrewne

“Identyfikatory obiektów (OID)” na stronie 298

Informacje w tym temacie zawierają identyfikatory obiektów (object identifier - OID) używane w serwerze Directory Server.

## Uwagi na temat składowania i odtwarzania

Serwer Directory Server przechowuje dane i informacje konfiguracyjne w kilku miejscach.

Serwer Directory Server przechowuje informacje w następujących miejscach:

- w bibliotece bazy danych (domyślnie QUSRDIRDB), która przechowuje zawartość serwera katalogów;

**Uwaga:** Używaną bibliotekę bazy danych można wyświetlić na karcie **Baza danych/przyrostki**

(Database/Suffixes) na panelu właściwości serwera IBM Directory Server w programie System i Navigator.

- 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, w bibliotece baz danych o nazwie QUSRDIRCL, której używa protokół zmian.

Jeśli zawartość katalogu zmienia się regularnie, bibliotekę baz danych i jej obiekty należy także składować 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 pokrewne

Składowanie i odtwarzanie

---

## Pierwsze kroki z serwerem Directory Server

Ten temat zawiera informacje o serwerze Directory Server obejmujące instalowanie, migrowanie, planowanie, dostosowywanie i administrowanie.

Serwer Directory Server jest instalowany automatycznie podczas instalowania systemu operacyjnego i5/OS. Na początku używana jest domyślna konfiguracja. Aby rozpocząć pracę z serwerem Directory Server, należy zapoznać się z następującymi tematami.

### Uwagi dotyczące migracji

Jeśli instalowany jest system w wersji V5R4, a serwer Directory Server był używany w poprzedniej wersji, należy zapoznać się z uwagami dotyczącymi migracji.

Serwer Directory Server jest instalowany automatycznie podczas instalowania systemu operacyjnego i5/OS. Podczas pierwszego uruchomienia serwer automatycznie migruje istniejącą konfigurację i dane. Może to spowodować długie opóźnienie przed pierwszym uruchomieniem serwera.

**Uwaga:** Migracja konfiguracji i plików schematu dokonywana jest podczas instalacji i pierwszego uruchomienia serwera. Po zakończeniu pierwszego uruchomienia serwera, jeśli konfiguracja i pliki schematu w /qibm/userdata/os400/dirsrv są odtwarzane z kopii zapasowej poprzedniego wydania, schemat i konfiguracja dla nowego wydania zostaną nadpisane przez pliki poprzedniego wydania, które nie będą migrowane ponownie. Przywracanie schematu i konfiguracji poprzedniego wydania po migracji może spowodować, że serwer nie zostanie uruchomiony. Mogą także wystąpić inne nieprzewidziane błędy. Jeśli kopie zapasowe konfiguracji oraz schematu serwera są wymagane, dane te powinny być składowane po pomyślnym uruchomieniu serwera.

### Migrowanie do wersji V6R1 z wersji V5R4 lub V5R3

| Ten temat zawiera informacje przydatne dla użytkowników serwera Directory Server w wersji systemu V5R4 lub V5R3.

| System operacyjny i5/OS w wersji V6R1 dostarcza nowe funkcje i możliwości serwera Directory Server. Zmiany te dotyczą zarówno serwera katalogów LDAP, jak i interfejsu GUI programu System i Navigator. Aby skorzystać z nowych opcji interfejsu GUI, należy zainstalować program System i Navigator na komputerze PC, który może komunikować się z serwerem iSeries za pośrednictwem protokołu TCP/IP. Program System i Navigator jest komponentem aplikacji System i Access for Windows. Jeśli na komputerze jest zainstalowana wcześniejsza wersja programu System i Navigator, należy ją zaktualizować do wersji V6R1.

| System operacyjny i5/OS w wersji V6R1 umożliwia bezpośrednie aktualizowanie z wersji V5R4 i V5R3. Serwer Directory Server zostanie zaktualizowany do wersji V6R1 przy pierwszym uruchomieniu serwera. Dane katalogu LDAP i pliki schematu katalogu zostaną poddane automatycznej migracji w celu zapewnienia ich zgodności z formatami wersji V6R1.

| Podczas aktualizowania systemu i5/OS do wersji V6R1 należy mieć na uwadze kilka kwestii związanych z migracją:

- Po zaktualizowaniu do wersji V6R1 i uruchomieniu serwera katalogów produkt Directory Server automatycznie migruje istniejące pliki schematów do wersji V6R1 i usuwa stare pliki schematów. Jeśli jednak pliki schematów zostały usunięte lub zmieniono ich nazwy, serwer Directory Server nie będzie w stanie dokonać ich migracji. Może wtedy wystąpić błąd lub serwer Directory Server może przyjąć, że migracja plików została już przeprowadzona.
- Po uaktualnieniu do wersji V6R1, ale przed zaimportowaniem nowych danych, należy jednorazowo uruchomić serwer i przeprowadzić migrację istniejących danych. Próba zaimportowania danych przed uruchomieniem serwera może się nie powieść, jeśli użytkownik nie posiada wystarczających uprawnień. Serwer Directory Server przeprowadzi migrację danych katalogu do formatu V6R1 podczas pierwszego uruchomienia serwera lub importowania pliku LDIF. Należy zarezerwować czas niezbędny na wykonanie migracji.
- Wersja V6R1 wprowadza możliwość uruchamiania w systemie i5/OS wielu instancji serwera katalogów. Jeśli serwer katalogów był używany przed aktualizowaniem do wersji V6R1, zostanie przeprowadzona migracja istniejącego

- | serwera katalogów do instancji. Wiąże się to między innymi z przeniesieniem plików konfiguracji i plików
- | schematów z katalogu /QIBM/UserData/OS400/DirSrv do katalogu /QIBM/UserData/OS400/DirSrv/idsslapd-
- | QUSRDIR. Jest to tak zwana domyślna instancja serwera katalogów i nosi nazwę QUSRDIR. Dodatkowo dwa
- | obiekty z biblioteki QUSRSYS przenoszone są do nowej biblioteki QUSRDIRCF. Migracja ta ma miejsce podczas
- | pierwszego uruchomienia serwera katalogów po zaktualizowaniu do wersji V6R1.
- | • Po migracji serwer katalogów LDAP będzie uruchamiany automatycznie w momencie uruchomienia protokołu
- | TCP/IP. Jeśli serwer katalogów nie ma uruchamiać się automatycznie, należy zmienić to ustawienie za pomocą
- | programu System i Navigator.

## **Migrowanie danych z wersji V4R4 ,V4R5, V5R1 lub V5R2 do wersji V6R1**

Ten temat zawiera informacje przydatne dla użytkowników serwera Directory Server w wersji systemu V4R4, V4R5 lub V5R1.

System operacyjny i5/OS w wersji V5R4 nie umożliwia bezpośredniego aktualizowania z wersji V4R4, V4R5 ani V5R1.

**Uwaga:** Podczas aktualizacji z wersji V4R4 do dowolnej późniejszej wersji należy uwzględnić następujące uwagi:

- Wersja V4R4 i wcześniejsze wersje serwera Directory Server nie uwzględniały stref czasowych podczas tworzenia pozycji datownika. Począwszy od wersji V4R5, strefa czasowa jest uwzględniana podczas wszystkich czynności dodawania pozycji i modyfikowania katalogu. Dlatego podczas aktualizowania z wersji V4R4 lub wcześniejszej serwer Directory Server dopasowuje istniejące atrybuty `createtimestamp` i `modifytimestamp`, aby odpowiadały one właściwej strefie czasowej. Odbywa się to poprzez odjęcie strefy czasowej aktualnie zdefiniowanej w systemie od datowników przechowywanych 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.
- Podczas aktualizacji do wersji V5R2 z wersji V4R4 lub wcześniejszych należy zwrócić uwagę na fakt, iż dane katalogowe będą wymagać około dwa razy więcej przestrzeni pamięci niż poprzednio. Wynika to stąd, że w wersji V4R4 i wcześniejszych serwer Directory Server obsługiwał tylko zestaw znaków IA5 i przechowywał dane w formacie CCSID=37 (jednobajtowym). Obecnie serwer Directory Server obsługuje pełen zestaw znaków ISO 10646. Po uaktualnieniu, a przed zaimportowaniem nowych danych, należy uruchomić serwer i przeprowadzić migrację istniejących danych. Próba zaimportowania danych przed uruchomieniem serwera może się nie powieść, jeśli użytkownik nie posiada wystarczających uprawnień.

Aby migrować te wersje do wersji V5R4, można wykonać jedną z następujących procedur.

### **Aktualizowanie z wersji V4R4, V4R5 lub V5R1 do wersji przejściowej:**

- | Serwer Directory Server można migrować w celu zaktualizowania go do wersji przejściowej (V5R2 lub V5R3), a
- | następnie do wersji V6R1.
- | Chociaż aktualizacje z wersji V4R4, V4R5, V5R1 i V5R2 do wersji V6R1 nie są obsługiwane, obsługiwane są
- | następujące aktualizacje:
- wersja V4R4 i V4R5 aktualizowane do wersji V5R1
- wersja V4R5 i V5R1 aktualizowane do wersji V5R2
- wersja V5R1 i V5R2 aktualizowane do wersji V5R3
- wersja V5R2 i V5R3 aktualizowane do wersji V5R4
- | • wersja V5R3 i V5R4 aktualizowane do wersji V6R1

Szczegółowe informacje dotyczące procedur instalowania systemu i5/OS zawiera temat Instalowanie, aktualizowanie lub usuwanie systemu i5/OS i oprogramowania pokrewnego. Aby dokonać migracji, należy wykonać następujące czynności. Zmiany w schemacie powinny być migrowane automatycznie. Po każdej instalacji należy sprawdzić, czy zmiany w schemacie są nadal obecne.

1. W przypadku wersji V4R4, przeprowadź instalację wersji V5R1. Następnie przeprowadź instalację wersji V5R3.

2. W przypadku wersji V4R5, przeprowadź instalację wersji V5R1 lub V5R2. W przypadku instalowania wersji V5R1 należy następnie zainstalować wersję V5R3. W przypadku instalowania wersji V5R2 należy następnie zainstalować wersję V5R3 lub V5R4.
3. W przypadku wersji V5R1 zainstaluj wersję V5R3.
4. W przypadku wersji V5R2 zainstaluj wersję V5R3 lub V5R4.
5. Po zainstalowaniu wersji V5R3 lub V5R4 zainstaluj wersję V6R1.
6. Uruchom serwer Directory Server, jeśli nie jest jeszcze uruchomiony.

### **Składowanie biblioteki bazy danych i instalowanie wersji V6R1:**

Serwer Directory Server można migrować, składując używaną przez niego bibliotekę bazy danych w wersji V4R4 lub V4R5, a następnie odtwarzając ją po zainstalowaniu wersji V6R1.

Metoda ta pozwala uniknąć instalowania wersji pośredniej. Jednak ustawienia serwera nie podlegają migracji i konieczne jest jego ponowne skonfigurowanie. Szczegółowe informacje dotyczące procedur instalowania systemu i5/OS zawiera temat Instalowanie, aktualizowanie lub usuwanie systemu i5/OS i oprogramowania pokrewnego. 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 aby zachować zmiany, należy je wprowadzić ponownie ręcznie. Jeśli aktualizacje schematu zostały dokonane przy użyciu plików LDIF w połączeniu z programem narzędziowym ldapmodify, należy odszukać te pliki, aby można było ich użyć po uruchomieniu serwera w nowej wersji. Aby wyświetlić pojedyncze definicje typów atrybutów i klas obiektu, można użyć narzędzia Directory Management lub Web Administration (działającego w innym systemie w wersji V6R1). Jeśli zmiany obejmują jedynie dodanie nowych typów atrybutów i klas obiektu, należy utworzyć kopię pliku /qibm/userdata/os400/dirsrv/v3.modifiedschema. Plik ten można wykorzystać do utworzenia pliku LDIF zawierającego aktualizacje schematu. Więcej informacji zawiera sekcja "Schemat" na stronie 14.
2. Zanotuj ustawienia konfiguracji we właściwościach serwera Directory Server, w tym nazwę biblioteki bazy danych.
3. Zeskładuj bibliotekę bazy danych określoną w konfiguracji serwera Directory Server. Jeśli skonfigurowano protokół zmian, należy również zeszkładować bibliotekę QUSRDIRCL.
4. Zanotuj konfigurację publikowania. Konfigurację publikowania, z wyjątkiem informacji o hasłach, można wyświetlać za pomocą programu System i Navigator, wybierając opcję **Właściwości** (Properties) dla systemu i klikając zakładkę **Usługi katalogowe** (Directory Services).
5. Zainstaluj system i5/OS w wersji V6R1.
6. Użyj kreatora w programie System i Navigator, aby skonfigurować serwer Directory Server.
7. Odtwórz bibliotekę bazy danych zeszkładowaną w punkcie 3. Jeśli bibliotekę QUSRDIRCL zeszkładowano w punkcie 3, należy ją teraz odtworzyć.
8. Skorzystaj z narzędzia System i Navigator, aby ponownie skonfigurować serwer Directory Server. Określ bibliotekę bazy danych, która była wcześniej skonfigurowana oraz czy została ona zeszkładowana w poprzednich punktach.
9. Skorzystaj z narzędzia System i Navigator, aby ponownie skonfigurować publikowanie.
10. Zrestartuj serwer Directory Server.
11. Skorzystaj z narzędzia Web Administration, aby wprowadzić zmiany w plikach schematów dla wszystkich zmian użytkowników zanotowanych w punkcie 1.

### **Migrowanie sieci serwerów replikacji**

Ten temat zawiera informacje potrzebne do obsługi sieci serwerów replikacji.

Przy pierwszym uruchomieniu serwera głównego migrowane są informacje znajdujące się w katalogu sterującym replikacją. Pozyce z klasą obiektu replicaObject przypisane do nazwy cn=localhost są zastępowane pozycjami używanymi przez nowy model replikacji. Serwer główny jest skonfigurowany do replikowania wszystkich przyrostków

w katalogu. Pozycje umowy są tworzone z atrybutem `ibm-replicationOnHold` o wartości `true`. Umożliwia to kumulowanie aktualizacji na serwerze głównym do momentu, gdy replika będzie gotowa.

Pozycje te są nazywane topologią replikacji. Nowy serwer główny może być używany z replikami działającymi we wcześniejszych wersjach; dane powiązane z nowymi funkcjami nie będą replikowane do serwerów we wcześniejszych wersjach. Konieczne jest wyeksportowanie pozycji topologii replikacji z serwera głównego i dodanie ich do każdej repliki po migrowaniu serwera replik. Aby wyeksportować pozycje, należy użyć narzędzia wiersza komend Qshell "ldapsearch" na stronie 236 i zapisać dane wyjściowe w pliku. Komenda wyszukiwania jest podobna do następującej:

```
ldapsearch -h nazwa_hosta_serwera_głównego -p port_serwera_głównego \
-D nazwa_DN_administratora_serwera_głównego -w hasło_administratora_serwera_głównego \
-b ibm-replicagroup=default,nazwa_DN_pozycji_przyrostka \
-L "(|(objectclass=ibm-replicaSubEntry)(objectclass=ibm-replicationAgreement))" \
> replication.topology.ldif
```

Ta komenda tworzy wyjściowy plik LDIF o nazwie `replication.topology.ldif` w bieżącym katalogu roboczym. Plik zawiera tylko nowe pozycje.

**Uwaga:** Nie należy dołączać następujących przyrostków:

- `cn=changelog`
- `cn=localhost`
- `cn=pwdpolicy`
- `cn=schema`
- `cn=configuration`

Należy dołączyć tylko przyrostki utworzone przez użytkownika.

Powtórz komendę dla każdej pozycji przyrostka na serwerze głównym, ale zastąp znak ">" znakami ">>", aby dopisać dane do pliku wyjściowego dla kolejnych wyszukiwań. Po ukończeniu pliku należy skopiować go do serwerów replik.

Plik należy dodać do serwerów replik po ich pomyślnym migrowaniu; nie należy go dodawać do serwerów działających w poprzednich wersjach serwera katalogów. Przed dodaniem pliku serwer należy uruchomić i zatrzymać.

Aby uruchomić serwer, użyj opcji **Uruchom** (Start) w programie System i Navigator.

Aby zatrzymać serwer, użyj opcji **Zatrzymaj** (Stop) w programie System i Navigator.

Dodając plik do serwera replik należy sprawdzić, czy serwer ten nie jest uruchomiony. Aby dodać dane, użyj opcji **Importuj plik** (Import File) w programie System i Navigator.

Po załadowaniu pozycji topologii replikacji należy uruchomić serwer replik i wznowić replikację. Replikację można wznowić na jeden z następujących sposobów:

- Na serwerze głównym należy użyć funkcji **Manage Queues in Replication Management** (Zarządzanie kolejkami w replikacji) w narzędziu Web Administration.
- Służy do tego program narzędziowy wiersza komend **ldapexop**. Na przykład:

```
ldapexop -h nazwa_hosta_serwera_głównego -p port_serwera_głównego \
-D nazwa_DN_administratora_serwera_głównego -w hasło_administratora_serwera_głównego \
-op controlrepl -action resume -ra nazwa_wyróżniająca_umowy_replikowania
```

Ta komenda wznowia replikację dla serwera zdefiniowanego w pozycji z podaną nazwą wyróżniającą.

Aby określić, która nazwa wyróżniająca umowy repliki odpowiada serwerowi replik, należy przeszukać plik `replication.topology.ldif`. Serwer główny zapisze w protokole komunikat o uruchomieniu replikacji dla tej repliki oraz ostrzeżeniu o tym, że identyfikator serwera replik nie zgadza się z identyfikatorem serwera repliki. Aby zaktualizować umowę repliki, tak aby używała odpowiedniego identyfikatora serwera, należy użyć funkcji **Replication Management** (Zarządzanie replikacją) w narzędziu Web Administration lub narzędzia wiersza komend **ldapmodify**. Na przykład:



```
ldapmodify -c -h nazwa_hosta_serwera_głównego -p port_serwera_głównego \  
-D nazwa_DN_administratora_serwera_głównego -w hasło_administratora_serwera_głównego \  
dn: nazwa_DN_umowy_repliki \  
changetype: modify \  
replace: ibm-replicaConsumerID \  
ibm-replicaConsumerID: ID_serwera_replik
```

Komendy te można wprowadzić bezpośrednio w wierszu komend lub zapisać w pliku LDIF i przekazać do komendy za pomocą opcji **-i plik**. Aby zatrzymać komendę, należy użyć funkcji **End Previous Request** (Zakończenie poprzedniego żądania).

Migracja dla tej repliki została zakończona.

Aby nadal korzystać z repliki działającej w poprzedniej wersji, trzeba wznowić replikację za pomocą narzędzia wiersza komend **ldapexop** lub funkcji **Replication Management** (Zarządzanie replikacją) w narzędziu Web Administration dla tej repliki. Jeśli replika działająca w poprzedniej wersji będzie migrowana później, należy użyć narzędzia wiersza komend **ldapdiff**, aby zsynchronizować dane katalogu. Umożliwi to aktualizację w replice pozycji lub atrybutów, które nie były replikowane.

#### Pojęcia pokrewne

“Replikacja” na stronie 37

Replikacja to technika używana przez serwery katalogów do zwiększania wydajności i niezawodności. Proces replikacji synchronizuje dane w wielu katalogach.

#### Zadania pokrewne

“Uruchamianie serwera Directory Server” na stronie 116

Ten temat zawiera informacje dotyczące uruchamiania serwera Directory Server.

## Zmiana nazwy usługi Kerberos

Ten temat zawiera informacje dotyczące korzystania z protokołu Kerberos w wersji wcześniejszej niż V5R3.

Począwszy od wersji V5R3 zmieniono nazwę usługi używaną przez funkcje API serwera katalogów i klienta dla uwierzytelniania GSSAPI (Kerberos). Ta zmiana jest niezgodna z nazwą usługi używaną w wersjach wcześniejszych niż V5R3 (V5R2M0 PTF 5722SS1-SI08487 zawiera tę samą zmianę).

W wersjach wcześniejszych od V5R3 funkcje API serwera Directory Server i klienta używały nazwy usługi w postaci LDAP/nazwa-dns-hosta@diedzina-Kerberos, gdy do uwierzytelniania używany był mechanizm GSSAPI (Kerberos). Ta nazwa nie jest zgodna ze standardami definiującymi uwierzytelnianie GSSAPI, które stanowią, że nazwa jednostki głównej powinna zaczynać się od "ldap". W wyniku tego zarówno funkcje API serwera Directory Server jak i klienta mogą nie współdziałać z produktami innych dostawców. Dzieje się tak szczególnie wtedy, gdy centrum dystrybucji kluczy Kerberos (KDC) zawiera nazwy użytkowników z rozróżnieniem wielkości liter. Dostawca usług LDAP dla JNDI, używanego powszechnie interfejsu API języka Java dla protokołu LDAP, jest przykładem klienta dołączonego do systemu operacyjnego używającego poprawnej nazwy usługi.

W wersji V5R3M0 zmieniono nazwę usługi na zgodną ze standardami. Powoduje to jednak problemy ze zgodnością.

- Serwer katalogów skonfigurowany tak, aby używał uwierzytelniania GSSAPI, nie rozpocznie instalowania tej wersji. Jest to spowodowane tym, że plik keytab używany przez serwer ma referencje używające starej nazwy usługi (LDAP/mojssystem.ibm.com@IBM.COM), a serwer szuka referencji, używając nowej nazwy (ldap/mojssystem.ibm.com@IBM.COM).
- Serwer katalogów lub aplikacja LDAP używające funkcji API LDAP w wersji V5R3M0 mogą nie być w stanie przeprowadzić uwierzytelniania na starszych serwerach lub klientach systemu OS/400. Aby to naprawić, należy wykonać następujące czynności:
  1. Jeśli KDC używa nazw użytkowników z rozpoznawaniem wielkości liter, utwórz konto używając odpowiedniej nazwy usługi (ldap/mojssystem.ibm.com@IBM.COM).
  2. Zaktualizuj plik keytab używany przez serwer Directory Server do przechowywania referencji dla nowej nazwy usługi. Być może zechcesz również usunąć stare referencje. Możesz użyć narzędzia Qshell keytab do aktualizacji pliku keytab. Domyślnie serwer katalogów używa pliku /QIBM/UserData/OS/400/

NetworkAuthentication/keytab/krb5.keytab. Kreator usługi uwierzytelniania sieciowego (Kerberos) wersji V5R3M0 w programie System i Navigator również tworzy pozycje keytab, używając nowej nazwy usługi.

3. Zaktualizuj systemy OS/400 w wersji V5R2M0, w których używane jest uwierzytelnianie GSSAPI, poprzez zastosowanie poprawki PTF 5722SS1-SI08487.

Alternatywnie można wybrać, aby funkcje API serwera katalogów i klienta nadal używały starej nazwy usługi. Może to być przydatne, gdy używane jest uwierzytelnianie Kerberos w mieszanej sieci systemów działających z poprawkami PTF i bez nich. W tym celu należy ustawić zmienną środowiskową LDAP\_KRB\_SERVICE\_NAME. Można ją ustawić dla całego systemu (wymagana do ustawienia nazwy usługi dla serwera) za pomocą następującej komendy:

```
ADDENVVAR ENVVAR(LDAP_KRB_SERVICE_NAME)
```

lub w QSH (aby dotyczyła też narzędzi LDAP uruchamianych z tej sesji QSH):

```
export LDAP_KRB_SERVICE_NAME=1
```

## Planowanie serwera Directory Server

Przed rozpoczęciem konfigurowania serwera Directory Server i utworzeniem struktury katalogu LDAP należy poświęcić kilka minut na przygotowanie planu.

Przed rozpoczęciem konfigurowania serwera katalogów i utworzeniem struktury katalogu LDAP należy rozważyć następujące kwestie:

- **Zorganizowanie katalogu.** Należy zaplanować strukturę katalogu i określić przyrostki oraz atrybuty wymagane przez serwer. Więcej informacji na ten temat zawierają tematy Zalecane procedury dotyczące struktury katalogu, Katalogi, Przyrostek i Atrybuty.
- **Określenie wielkości katalogu.** Pozwala to 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 wykorzystujący domyślny schemat serwera Directory Server wymaga około 10 MB 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 metod ochrony.**

Serwer katalogów umożliwia zastosowanie strategii haseł w celu zapewnienia, że użytkownicy zmieniają swoje hasła cyklicznie i że hasła są zgodne z wymaganiami dotyczącymi haseł w danej organizacji.

Serwer Directory Server obsługuje protokół SSL (Secure Sockets Layer), certyfikaty cyfrowe, a także protokół TLS (Transport Layer Security) zabezpieczające komunikację. Uwierzytelnianie Kerberos również jest obsługiwane.

Serwer Directory Server umożliwia kontrolę dostępu do obiektów katalogu za pomocą list kontroli dostępu. Do zabezpieczenia katalogu można również użyć kontroli ochrony systemu operacyjnego.

Dodatkowo można określić strategię haseł, która zostanie zastosowana.

- **Wybranie nazwy wyróżniającej i hasła administratora.** Domyślną nazwą wyróżniającą administratora jest `cn=admin`. Jest to jedyny identyfikator mający uprawnienia do tworzenia lub zmiany pozycji katalogu po początkowym konfigurowaniu serwera. Można użyć nazwy wyróżniającej administratora lub wybrać inną nazwę wyróżniającą. Należy również utworzyć hasło dla nazwy wyróżniającej administratora.
- **Zainstaluj wymagane oprogramowanie dla narzędzia Directory Server Web Administration.** Aby korzystać z narzędzia Web Administration serwera Directory Server, muszą być zainstalowane następujące produkty:
  - IBM HTTP Server for i5/OS (5761-DG1)
  - IBM WebSphere Application Server 6.0 (5733-W60 opcja Base lub Express)
- **Planowanie strategii składowania i odtwarzania.** Zaplanowanie sposobu składowania danych i informacji konfiguracyjnych.

### Pojęcia pokrewne

“Zalecane procedury dla struktury katalogów” na stronie 34

Serwer Directory Server jest często używany jako repozytorium dla użytkowników i grup. Poniższa sekcja omawia niektóre z zalecanych procedur konfigurowania struktury zoptymalizowanej dla zarządzania użytkownikami i grupami. Struktura ta i związany z nią model ochrony mogą zostać rozszerzone dla innych użytkowników katalogu.

“Katalogi” na stronie 4

Serwer Directory Server umożliwia dostęp do bazy danych specjalnego typu, w której informacje są zapisywane w strukturze hierarchicznej podobnej do organizacji zintegrowanego systemu plików systemu i5/OS.

“Przyrostek (kontekst nazwy)” na stronie 12

Przyrostek (znany również jako kontekst nazwy) to nazwa DN identyfikująca najwyższą pozycję w lokalnej hierarchii katalogu.

“Atrybuty” na stronie 18

Każda pozycja katalogu ma zestaw atrybutów powiązanych z nią poprzez jej klasę obiektu.

“Uwagi na temat składowania i odtwarzania” na stronie 94

Serwer Directory Server przechowuje dane i informacje konfiguracyjne w kilku miejscach.

### Informacje pokrewne

IBM HTTP Server

Więcej informacji o serwerach IBM HTTP Server i IBM WebSphere Application Server zawiera temat IBM HTTP Server.

## Konfigurowanie serwera Directory Server

Ustawienia serwera Directory Server można dostosować za pomocą Kreatora konfiguracji serwera katalogów.

1. Jeśli system nie został skonfigurowany do rozpowszechnienia informacji na inny serwer LDAP i w serwerze DNS sieci TCP/IP nie ma skonfigurowanych innych serwerów LDAP, to serwer Directory Server zostanie automatycznie zainstalowany w ograniczonej konfiguracji domyślnej. Serwer Directory Server udostępnia kreatora ułatwiającego przystosowywanie serwera do określonych potrzeb. Kreator można uruchomić później przy użyciu programu System i Navigator. Należy go użyć podczas początkowego konfigurowania serwera katalogów. Można go także użyć do zmiany konfiguracji serwera katalogów.

**Uwaga:** Użycie kreatora do ponownego skonfigurowania 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 bezpieczeństwa, konieczne jest posiadanie uprawnień specjalnych \*AUDIT.

2. Aby uruchomić Kreatora konfiguracji serwera katalogów (Directory Server Configuration Wizard), należy wykonać następujące czynności:
  - a. W programie System i Navigator rozwiń pozycję **Sieć**.
  - b. Rozwiń pozycję **Serwery**.
  - c. Kliknij **TCP/IP**.
  - d. Prawym przyciskiem myszy kliknij **IBM Directory Server** i wybierz **Konfiguruj**.

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

3. Wykonując instrukcje kreatora konfiguracji serwera Directory skonfiguruj serwer Directory Server.

**Uwaga:** Bibliotekę przechowującą dane katalogowe można umieścić w puli pamięci dyskowej (ASP) użytkownika, a nie w systemowej ASP. Biblioteka ta nie może być jednak przechowywana w niezależnej

ASP, ponieważ każda próba skonfigurowania, zmiany konfiguracji lub uruchomienia serwera z biblioteką, która znajduje się w niezależnej ASP, nie powiedzie się.

4. Po zakończeniu pracy kreatora serwer Directory Server ma konfigurację podstawową. Jeśli w systemie używany jest serwer Lotus Domino, port 389 (domyślny port dla serwera LDAP) może być już używany przez funkcję LDAP. Należy wykonać wtedy jedną z następujących czynności:
  - Zmień port używany przez serwer Lotus Domino. Więcej informacji zawiera sekcja Wykorzystanie Domino LDAP oraz Directory Server w tym samym systemie w temacie Poczta elektroniczna.
  - Zmień port używany przez serwer Directory Server. Więcej informacji zawiera temat “Zmiana portu lub adresu IP” na stronie 123.
  - Użyj konkretnych adresów IP. Więcej informacji zawiera temat “Zmiana portu lub adresu IP” na stronie 123.
5. Utwórz pozycje odpowiadające skonfigurowanym przyrostkom. Więcej informacji znajduje się w sekcji “Dodawanie i usuwanie przyrostków serwera Directory Server” na stronie 124.
6. Przed kontynuacją można wykonać niektóre lub wszystkie z poniższych operacji:
  - Włącz ochronę SSL (Secure Sockets Layer), patrz sekcja “Włączanie SSL i TLS na serwerze Directory Server” na stronie 182.
  - Włącz uwierzytelnianie Kerberos, patrz sekcja “Włączanie uwierzytelniania Kerberos na serwerze Directory Server” na stronie 184.
  - Skonfiguruj odwołanie, patrz sekcja “Określanie serwera odwołań do katalogu” na stronie 123.
7. Uruchom serwer Directory Server. Więcej informacji znajduje się w sekcji “Uruchamianie serwera Directory Server” na stronie 116.
8. Istniejąca instancja serwera katalogów nosi nazwę instancji QUSRDIR. Jej pliki schematu i plik konfiguracyjny znajdują się w katalogu /QIBM/UserData/OS400/DirSrv/idsslapd-QUSRDIR. W przypadku próby uruchomienia instancji domyślnej, instancja serwera może zostać utworzona automatycznie. Żadna inna instancja nie zostanie utworzona automatycznie.

#### Pojęcia pokrewne

“Konfiguracja domyślna serwera Directory Server” na stronie 308

Serwer Directory Server jest instalowany automatycznie podczas instalowania systemu operacyjnego i5/OS. Instalacja ta obejmuje konfigurację domyślną.

## Zapełnianie katalogu

W tym temacie opisano zapełnianie katalogu danymi.

Istnieje wiele sposobów zapełnienia katalogu danymi:

- opublikowanie informacji na serwerze Directory Server,
- zaimportowanie danych z pliku LDIF,
- skopiowanie użytkowników z listy sprawdzania serwera HTTP do serwera Directory Server.

#### Zadania pokrewne

“Publikowanie informacji na serwerze Directory Server” na stronie 129

W tym temacie opisano publikowanie informacji na serwerze Directory Server.

“Importowanie pliku LDIF” na stronie 131

W tym temacie opisano importowanie pliku w formacie LDIF (LDAP Data Interchange Format).

“Kopiowanie użytkowników z listy sprawdzania serwera HTTP do serwera Directory Server” na stronie 132

Ten temat zawiera informacje dotyczące kopiowania użytkowników z listy sprawdzania serwera HTTP do serwera Directory Server.

## Administrowanie przez sieć WWW

Konfigurowanie konsoli Web Administration i używanie jej do administrowania serwerami Directory Server.

Jednym lub kilkoma serwerami Directory Servers można administrować za pomocą konsoli administrowania przez sieć WWW. Konsola ta umożliwia:

- Dodawanie lub zmianę listy serwerów Directory Server, którymi można administrować.
- Administrowanie serwerem Directory Server za pomocą narzędzia Web Administration.
- Zmianę atrybutów konsoli administrowania przez sieć WWW.

Aby korzystać z konsoli administrowania przez sieć WWW, wykonaj poniższe czynności:

1. Używając po raz pierwszy narzędzia Directory Server Web Administration, najpierw należy je skonfigurować (patrz sekcja “Konfigurowanie narzędzia Web Administration po raz pierwszy”), a następnie przejść do następnego punktu.
2. Zaloguj się w narzędziu Directory Server Web Administration, wykonując jedną z poniższych czynności:
  - W programie System i Navigator zaznacz serwer i kliknij opcje **Sieć** → **Serwery** → **TCP/IP** (Network > Servers > TCP/IP), kliknij prawym przyciskiem myszy serwer **IBM Directory Server**, a następnie kliknij opcję **Administrowanie serwerem** (Server Administration).
  - Na stronie zadań produktu iSeries ([http://nazwa\\_serwera:2001](http://nazwa_serwera:2001)) kliknij pozycję **IBM Directory Server**.
3. Jeśli chcesz administrować serwerem Directory Server, wykonaj następujące czynności:
  - a. W polu **LDAP Hostname** (Nazwa hosta LDAP) wybierz serwer Directory Server, którym chcesz administrować.
  - b. Wprowadź nazwę wyróżniającą logowania administratora używaną do łączenia z serwerem katalogów.
  - c. Wpisz hasło administratora.
  - d. Kliknij przycisk **Login** (Zaloguj). Wyświetlona zostanie strona IBM Directory Server Web Administration. Więcej informacji na temat strony IBM Directory Server Web Administration zawiera sekcja “Narzędzie Web Administration” na stronie 105.
4. Jeśli chcesz dodać lub zmienić listę serwerów, którymi można administrować, lub zmienić atrybuty konsoli administrowania przez sieć WWW, wykonaj następujące czynności:
  - a. W polu **LDAP Hostname** (Nazwa hosta LDAP) kliknij opcję **Console Admin** (Administrator konsoli).
  - b. Wprowadź identyfikator administratora konsoli.
  - c. Wprowadź hasło administratora konsoli.
  - d. Kliknij przycisk **Login** (Zaloguj). Wyświetlona zostanie strona IBM Directory Server Web Administration. Więcej informacji na temat strony IBM Directory Server Web Administration zawiera sekcja “Narzędzie Web Administration” na stronie 105.
  - e. Kliknij opcję **Console administration** (Administrowanie konsolą), a następnie wybierz jedną z poniższych opcji:
    - **Change console administrator login** (Zmień identyfikator administratora konsoli), aby zmienić identyfikator administratora konsoli.
    - **Change console administrator password** (Zmień hasła administratora konsoli), aby zmienić hasło administratora konsoli.
    - **Manage console servers** (Zarządzaj serwerami konsoli), aby zmienić serwery Directory Server, którymi można administrować za pomocą konsoli administrowania przez sieć WWW.
    - **Manage console properties** (Zarządzaj właściwościami konsoli), aby zmienić właściwości konsoli administrowania przez sieć WWW.

## Konfigurowanie narzędzia Web Administration po raz pierwszy

W tym temacie podano instrukcje konfigurowania narzędzia Web Administration po raz pierwszy.

1. Zainstaluj serwer IBM WebSphere Application Server 6.0 (5733-W60, opcje Base lub Express) i wstępnie wymagane oprogramowanie, jeśli jeszcze tego nie zrobiono.
2. Włącz systemową instancję serwera aplikacji na serwerze HTTP ADMIN. Więcej informacji znajduje się w temacie IBM HTTP Server.
  - a. Uruchom instancję serwera HTTP ADMIN, wykonując jedną z poniższych czynności:
    - W programie System i Navigator wybierz kolejno opcje **Sieć** → **Serwery** → **TCP/IP** (Network > Servers > TCP/IP) i kliknij prawym przyciskiem myszy element **Administrowanie HTTP** (HTTP Administration). Następnie kliknij przycisk **Uruchom**.

- W wierszu komend wpisz STRTCPSVR SERVER(\*HTTP) HTTPSVR(\*ADMIN).
- b. Zaloguj się do narzędzia IBM Web Administration for iSeries. Użyj profilu użytkownika systemu operacyjnego i hasła w celu zalogowania się na stronie Tasks (Zadania) iSeries ([http://nazwa\\_serwera:2001](http://nazwa_serwera:2001)), a następnie kliknij opcję **IBM Web Administration for iSeries**.
- c. Na stronie HTTP Server Administration *nazwa\_serwera* (Administrowanie serwerem HTTP *nazwa\_serwera*) kliknij zakładkę **Manage** (Zarządzanie), a następnie zakładkę **HTTP Servers** (Serwery HTTP). Sprawdź, czy na liście rozwijanej **Server** (Serwer) zaznaczona jest opcja **ADMIN**  $\Delta$ ?**Apache** i czy na liście rozwijanej **Server Area** (Obszar serwera) wybrana jest opcja **Include /QIBM/UserData/HTTPA/admin/conf/admin-cust.conf**.
- d. Z opcji w lewym panelu strony wybierz **General Server Configuration** (Ogólna konfiguracja serwera).

**Uwaga:** Może być konieczne rozwinięcie sekcji **Server Properties** (Właściwości serwera), aby została wyświetlona opcja **General Server Configuration** (Ogólna konfiguracja serwera).

- e. Dla opcji **Start the system application server instance when the 'Admin' server is started** (Uruchom instancję serwera aplikacji systemu gdy uruchamiany jest serwer 'Admin') wybierz wartość **Tak**.
- f. Kliknij przycisk **OK**.
- g. Restartuj instancję serwera HTTP ADMIN poprzez kliknięcie przycisku restartowania (jest to drugi przycisk w zakładce **HTTP Servers** - Serwery HTTP). Instancję serwera HTTP ADMIN można także zatrzymać i uruchomić za pomocą programu System i Navigator lub wiersza komend.

Instancję serwera HTTP ADMIN można zatrzymać, wykonując jedną z poniższych czynności.

- W programie System i Navigator wybierz kolejno opcje **Sieć**  $\rightarrow$  **Serwery**  $\rightarrow$  **TCP/IP** (Network > Servers > TCP/IP) i kliknij prawym przyciskiem myszy element **Administrowanie HTTP** (HTTP Administration). Następnie kliknij przycisk **Stop** (Zatrzymaj).

- W wierszu komend wpisz ENDTCPSVR SERVER(\*HTTP) HTTPSVR(\*ADMIN).

Instancję serwera HTTP ADMIN można uruchomić, wykonując jedną z poniższych czynności.

- W programie System i Navigator wybierz kolejno opcje **Sieć**  $\rightarrow$  **Serwery**  $\rightarrow$  **TCP/IP** (Network > Servers > TCP/IP) i kliknij prawym przyciskiem myszy element **Administrowanie HTTP** (HTTP Administration). Następnie kliknij przycisk **Uruchom**.

- W wierszu komend wpisz STRTCPSVR SERVER(\*HTTP) HTTPSVR(\*ADMIN).

Więcej informacji znajduje się w temacie IBM HTTP Server.

3. Zaloguj się do narzędzia Web Administration serwera Directory Server.
  - a. Wywołaj **ekran logowania się**, wykonując jedną z poniższych czynności:
    - W programie System i Navigator wybierz serwer i kliknij opcje **Sieć**  $\rightarrow$  **Serwery**  $\rightarrow$  **TCP/IP** (Network > Servers > TCP/IP), kliknij prawym przyciskiem myszy serwer **IBM Directory Server**, a następnie kliknij opcję **Administrowanie serwerem** (Server Administration).
    - Na stronie iSeries Tasks ([http://nazwa\\_serwera:2001](http://nazwa_serwera:2001)) kliknij pozycję **IBM Directory Server for iSeries**.
  - b. Wybierz **Console Admin** (Administrator konsoli) w polu **LDAP Hostname** (Nazwa hosta LDAP).
  - c. Wpisz superadmin w polu **Username** (Nazwa użytkownika).
  - d. W polu **Password** (Hasło) wpisz tajne\_hasło.
  - e. Kliknij przycisk **Login** (Zaloguj). Wyświetlona zostanie strona IBM Directory Server Web Administration Tool.
4. Zmień identyfikator administratora konsoli.
  - a. Kliknij opcję **Console administration** (Administrowanie konsolą) w lewym panelu, aby rozwinąć sekcję, a następnie kliknij opcję **Change console administrator login** (Zmiana identyfikatora administratora konsoli).
  - b. W polu **Console administrator login** (Identyfikator administratora konsoli) wpisz nową nazwę administratora konsoli.
  - c. W polu **Current password** (Bieżące hasło) wpisz bieżące hasło (secret).
  - d. Kliknij przycisk **OK**.

5. Zmień hasło administratora konsoli. Kliknij opcję **Change console administrator password** (Zmień hasło administratora konsoli).
6. Dodaj serwer Directory Server, którym chcesz administrować. Kliknij opcję **Manage console servers** (Zarządzaj serwerami konsoli).

**Uwaga:** Podczas dodawania serwera Directory Server, **port administrowania** nie jest używany i będzie pomijany.

7. Jeśli zachodzi potrzeba zmian właściwości konsoli, kliknij opcję **Manage console properties** (Zarządzanie właściwościami konsoli) w lewym panelu.
8. Kliknij przycisk **Logout** (Wyloguj). Po wyświetleniu komunikatu o pomyślnym wylogowaniu kliknij **tutaj**, aby wrócić do strony logowania narzędzia Web Administration.

Po pierwszym skonfigurowaniu konsoli można powrócić do niej w dowolnej chwili w celu:

- zmiany identyfikatora i hasła administratora konsoli,
- zmiany serwerów Directory Server, którymi można administrować za pomocą narzędzia Web Administration,
- zmiany właściwości konsoli.

## Narzędzie Web Administration

Po zalogowaniu się do narzędzia Web Administration zostanie wyświetlone okno aplikacji składające się z pięciu części.

### Obszar baneru

Obszar baneru znajduje się na górze panelu i zawiera nazwę aplikacji i logo IBM.

### Obszar nawigacyjny

Obszar nawigacyjny, znajdujący się po lewej stronie panelu, wyświetla rozwijane kategorie dla różnych zadań serwera, takich jak:

#### Właściwości użytkownika

Umożliwia zmianę bieżącego hasła użytkownika.

#### Zarządzanie schematami

Umożliwia pracę z klasami obiektu, atrybutami, regułami sprawdzania zgodności i składniami.

#### Zarządzanie katalogiem

Umożliwia pracę z pozycjami katalogu.

#### Zarządzanie replikacją

Umożliwia pracę z referencjami, topologią, harmonogramami i kolejkami.

#### Dziedziny i szablony

Umożliwia pracę z szablonami użytkowników i dziedzinaми.

#### Użytkownicy i grupy

Umożliwia pracę z użytkownikami i grupami w zdefiniowanych dziedzinaх. Na przykład, jeśli chcesz utworzyć nowego użytkownika WWW, zadanie **Użytkownicy i grupy** działa z pojedynczą klasą obiektu grupy groupOfNames. Nie można dostosować obsługi grupy.

#### Server administration

Zadania te umożliwiają zmianę konfiguracji serwera i ustawień ochrony.

### Obszar roboczy

Obszar roboczy wyświetla zadania powiązane z wybranym zadaniem w obszarze nawigacyjnym. Na przykład, jeśli w obszarze nawigacyjnym wybrano kategorię Managing server security (Zarządzanie ochroną serwera), obszar roboczy wyświetla stronę Ochrona serwera i zakładki zawierające zadania powiązane z konfigurowaniem ochrony serwera.

### Obszar statusu serwera

Obszar statusu serwera znajduje się u góry obszaru roboczego. Ikona po lewej stronie obszaru statusu serwera określa bieżący status serwera. Obok ikony znajduje się nazwa administrowanego serwera. Ikona po prawej stronie obszaru statusu serwera zawiera odsyłacz do pomocy elektronicznej.

## Obszar statusu zadania

Obszar zadania, znajdujący się pod obszarem roboczym, wyświetla status bieżącego zadania.

---

## Scenariusze związane z serwerem Directory Server

Ten temat zawiera scenariusze z przykładami typowych zadań związanych z serwerem Directory Server.

### Scenariusz: konfigurowanie serwera Directory Server

Przykład konfigurowania katalogu LDAP na serwerze Directory Server.

#### Sytuacja

Administrator systemów komputerowych w firmie zdecydował się umieścić informacje o pracownikach, takie jak numer telefonu i adres poczty elektronicznej, w centralnym repozytorium LDAP.

#### Cele

W tym scenariuszu firma MyCo, Inc. chce skonfigurować serwer Directory Server i utworzyć bazę danych katalogu zawierającą informacje o pracownikach, takie jak nazwisko, adres poczty elektronicznej oraz numer telefonu.

Cele tego scenariusza są następujące:

- Udostępnić informacje kadrowe we wszystkich miejscach w sieci przedsiębiorstwa pracownikom używającym klienta poczty Lotus Notes lub Microsoft Outlook Express.
- Umożliwić menedżerom zmianę danych pracownika w bazie danych katalogu i uniemożliwić ją innym osobom.
- Umożliwić systemowi publikowanie danych o pracownikach w bazie danych katalogu.

#### Informacje szczegółowe

Serwer Directory Server będzie uruchomiony w systemie o nazwie mySystem.

Poniższy przykład ilustruje informacje, które MyCo, Inc. chce umieścić w bazie danych katalogu dla każdego pracownika.

Nazwa: Jose Alvarez  
Wydział: DEPTA  
Numer telefonu: 999 999 9999  
Adres e-mail: jalvarez@my\_co.com

Struktura katalogu dla tego scenariusza może mieć postać podobną do przedstawionej poniżej:

```
/
|
+- my_co.com
  |
  +- employees
    |
    +- Jose Alvarez
      |
      DEPTA
      999-555-1234
      jalvarez@my_co.com
    |
    +- John Smith
      |
      DEPTA
      999-555-1235
      jsmith@my_co.com
    |
    + Managers group
      Jose Alvarez
```



mySystem.my\_co.com

Wszyscy pracownicy (menedżerowie i inni) znajdują się w drzewie katalogów pracowników. Menedżerowie należą również do grupy menedżerów. Członkowie grupy menedżerów mają uprawnienia do zmiany danych pracownika.

Również system (mySystem) wymaga uprawnień do zmiany danych pracowników. W tym scenariuszu system jest umieszczony w drzewie katalogów pracowników i staje się członkiem grupy menedżerów.

Jeśli konieczne jest oddzielenie pozycji pracowników od pozycji systemu, można utworzyć inne drzewo katalogów (na przykład: komputery) i dodać system do niego. System będzie wymagał takich samych uprawnień, jak menedżerowie.

### Wymagania wstępne i założenia

Narzędzie Web Administration jest poprawnie skonfigurowane i działa. Więcej informacji zawiera temat “Administrowanie przez sieć WWW” na stronie 102.

## Czynności konfiguracji

Wykonaj poniższe zadania:

### Szczegóły scenariusza: konfigurowanie serwera Directory Server

#### Czynność 1: konfigurowanie serwera Directory Server:

**Uwaga:** Do konfigurowania niezbędne są uprawnienia specjalne \*ALLOBJ i \*IOSYSCFG.

1. W programie System i Navigator kliknij kolejno opcje **Sieć** → **Serwery** → **TCP/IP** (Network > Servers > TCP/IP).
2. W oknie **Zadania konfiguracji serwera** (Server Configuration tasks) w prawej dolnej części okna programu System i Navigator kliknij opcję **Konfiguruj system jako serwer katalogów** (Configure system as Directory server).
3. Wyświetlony zostanie **Directory Server Configuration Wizard** (Kreator konfiguracji serwera Directory Server).
4. Kliknij **Configure a local LDAP directory server** (Konfiguruj lokalny serwer katalogów LDAP) w oknie **IBM Directory Server Configuration Wizard - Welcome** (Kreator konfiguracji serwera IBM Directory Server - Witamy).
5. Kliknij przycisk **Next** (Dalej) w oknie **IBM Directory Server Configuration Wizard - Welcome** (Kreator konfiguracji serwera IBM Directory Server - Witamy).
6. Wybierz **No** (Nie) w oknie **IBM Directory Server Configuration Wizard - Specify Settings** (Kreator konfiguracji serwera IBM Directory Server - Określanie ustawień). Umożliwi to skonfigurowanie serwera LDAP bez domyślnych ustawień.
7. Kliknij przycisk **Next** (Dalej) w oknie **IBM Directory Server Configuration Wizard - Specify Settings** (Kreator konfiguracji serwera IBM Directory Server - Określanie ustawień).
8. Usuń zaznaczenie pola **System-generated** (Wygenerowana przez system) w oknie **IBM Directory Server Configuration Wizard - Specify Administrator DN** (Kreator konfiguracji serwera IBM Directory Server - Określanie nazwy wyróżniającej administratora) i wprowadź następujące dane:

Nazwa wyróżniająca administratora	cn=administrator
Hasło	sekret
Potwierdź hasło	sekret

**Uwaga:** Wszystkie hasła określone w tym scenariuszu stanowią tylko przykład. Aby uniknąć złamania ochrony systemu lub sieci, nie powinno się używać tych haseł we własnej konfiguracji.

9. Kliknij przycisk **Next** (Dalej) w oknie **IBM Directory Server Configuration Wizard - Specify Administrator DN** (Kreator konfiguracji serwera IBM Directory Server - Określanie nazwy wyróżniającej administratora).
10. Wpisz `dc=my_co,dc=com` w polu **Suffix** (Przyrostek) w oknie **IBM Directory Server Configuration Wizard - Specify Suffixes** (Kreator konfiguracji serwera IBM Directory Server - Określanie przyrostków).
11. Kliknij przycisk **Add** (Dodaj) w oknie **IBM Directory Server Configuration Wizard - Specify Suffixes** (Kreator konfiguracji serwera IBM Directory Server - Określanie przyrostków).
12. Kliknij przycisk **Next** (Dalej) w oknie **IBM Directory Server Configuration Wizard - Specify Suffixes** (Kreator konfiguracji serwera IBM Directory Server - Określanie przyrostków).
13. Wybierz opcję **Yes, use all IP addresses** (Tak, użyj wszystkich adresów IP) w oknie **IBM Directory Server Configuration Wizard - Select IP Addresses** (Kreator konfiguracji serwera IBM Directory Server - Wybieranie adresów IP).
14. Kliknij przycisk **Next** (Dalej) w oknie **IBM Directory Server Configuration Wizard - Select IP Addresses** (Kreator konfiguracji serwera IBM Directory Server - Wybieranie adresów IP).
15. Wybierz opcję **Yes** (Tak) w oknie **IBM Directory Server Configuration Wizard - Specify TCP/IP Preference** (Kreator konfiguracji serwera IBM Directory Server - Określanie właściwości TCP/IP).
16. Kliknij przycisk **Next** (Dalej) w oknie **IBM Directory Server Configuration Wizard - Specify TCP/IP Preference** (Kreator konfiguracji serwera IBM Directory Server - Określanie właściwości TCP/IP).
17. Kliknij przycisk **Finish** (Zakończ) w oknie **IBM Directory Server Configuration Wizard - Summary** (Kreator konfiguracji serwera IBM Directory Server - Podsumowanie).
18. Prawym przyciskiem myszy kliknij serwer **IBM Directory Server** i kliknij **Uruchom**.

## Czynność 2: konfigurowanie narzędzia Directory Server Web Administration:

1. Otwórz w przeglądarce stronę `http://mySystem.my_co.com:9080/IDSWebApp/IDSjsp/Login.jsp`, gdzie `mySystem.my_co.com` jest używanym systemem.
2. Powinna zostać wyświetlona strona logowania. Kliknij listę **LDAP Hostname** (Nazwa hosta LDAP) i wybierz pozycję **Console Admin** (Administrator konsoli). Jako nazwę użytkownika wpisz `superadmin`, a jako hasło - `secret`. Kliknij przycisk **Logon** (Zaloguj).
3. Skonfiguruj narzędzie Web Administration do łączenia się z serwerem LDAP w systemie. Wybierz opcje **Console administration** → **Manage console servers** (Administrowanie konsolą > Zarządzaj serwerami konsoli) z lewej strony.
4. Kliknij przycisk **Add** (Dodaj).
5. W polu **Add server** (Dodaj serwer) wpisz `mySystem.my_co.com`.
6. Kliknij przycisk **OK**. Nowy serwer pojawi się na liście pod **Manage console servers** (Zarządzaj serwerami konsoli).
7. Kliknij przycisk **Logout** (Wyloguj) w oknie nawigacyjnym po lewej stronie.
8. Na stronie logowania do narzędzia Web Administration kliknij listę **LDAP Hostname** (Nazwa hosta LDAP) i wybierz skonfigurowany właśnie serwer (`mySystem.my_co.com`).
9. W polu **Username** (Nazwa użytkownika) wpisz `cn=administrator`, a w polu **Password** (Hasło) wpisz `tajne_haslo`. Kliknij przycisk **Login** (Zaloguj). Powinna zostać wyświetlona strona główna narzędzia IBM Directory Server Web Administration.

## Szczegóły scenariusza: tworzenie bazy danych katalogu

Przed rozpoczęciem wprowadzania danych należy utworzyć miejsce, w którym będą one przechowywane.

### Czynność 1: tworzenie obiektu podstawowej nazwy wyróżniającej:

1. W narzędziu Web Administration kliknij kolejno opcje **Directory management** → **Manage entries** (Zarządzanie katalogiem > Zarządzanie pozycjami). Wyświetlona zostanie lista obiektów na podstawowym poziomie katalogu. Ponieważ serwer jest nowy, wyświetlone zostaną tylko obiekty strukturalne zawierające informacje o konfiguracji.
2. Nowy obiekt ma zawierać dane firmy MyCo, Inc. Najpierw kliknij przycisk **Add...** (Dodaj...) po prawej stronie okna. W następnym oknie przewiń listę **Object class** (Klasa obiektu), aby wybrać **domenę** i kliknij przycisk **Next** (Dalej).

3. Ponieważ nie dodajesz żadnych pomocniczych klas obiektu, ponownie kliknij przycisk **Next** (Dalej).
4. W oknie **Enter the attributes** (Wprowadź atrybuty) wprowadź dane odpowiadające przyrostkowi utworzonemu wcześniej w kreatorze. Listę rozwijaną **Object class** (Klasa obiektu) pozostaw na pozycji **domain** (domena). W polu **Relative DN** (Względna nazwa wyróżniająca) wpisz **dc=my\_co**. W polu **Parent DN** (Nadrzędna nazwa wyróżniająca) wpisz **dc=com**. W polu **dc** wpisz **my\_co**.
5. Kliknij przycisk **Finish** (Zakończ) na dole okna. Powróć na podstawowy poziom, na którym powinna być widoczna nowa podstawowa nazwa wyróżniająca.

### Czynność 2: tworzenie szablonu użytkownika:

Utworzysz szablon użytkownika stanowiący pomoc w dodawaniu danych pracownika MyCo, Inc.

1. W narzędziu Web Administration kliknij kolejno opcje **Realms and templates** → **Add user template** (Dziedziny i szablony > Dodaj szablon użytkownika).
2. W polu **User template name** (Nazwa szablonu użytkownika) wpisz **Employee** (Pracownik).
3. Kliknij przycisk **Browse...** (Przeglądaj...) obok pola **Parent DN** (Nadrzędna nazwa wyróżniająca). Kliknij utworzoną w poprzedniej sekcji nadrzędną nazwę wyróżniającą, **dc=my\_co,dc=com**, a następnie kliknij przycisk **Select** (Wybierz) po prawej stronie okna.
4. Kliknij przycisk **Next** (Dalej).
5. Z listy rozwijanej **Structural object class** (Strukturalna klasa obiektu) wybierz opcję **inetOrgPerson** i kliknij przycisk **Next** (Dalej).
6. Z listy rozwijanej **Naming attribute** (Atrybut nazewnictwa) wybierz **cn**.
7. Z listy **Tags** (Zakładki) wybierz **Required** (Wymagane) i kliknij przycisk **Edit** (Edycja).
8. W oknie **Edit tab** (Edycja zakładki) wybiera się pola, które mają znaleźć się w szablonie użytkownika. Pozycje **sn** i **cn** są wymagane.
9. Z listy **Attributes** (Atrybuty) wybierz pozycję **departmentNumber** (numer działu) i kliknij przycisk **Add >>>** (Dodaj >>>).
10. Wybierz atrybut **telephoneNumber** i kliknij przycisk **Add>>>** (Dodaj).
11. Wybierz atrybut **mail** (poczta) i kliknij przycisk **Add >>>** (Dodaj >>>).
12. Wybierz atrybut **userPassword** (hasło użytkownika) i kliknij przycisk **Add >>>** (Dodaj >>>).
13. Kliknij przycisk **OK**, a następnie **Finish** (Zakończ), aby utworzyć szablon użytkownika.

### Czynność 3: tworzenie dziedziny:

1. W narzędziu Web Administration kliknij kolejno opcje **Realms and templates** → **Add realm** (Dziedziny i szablony > Dodaj dziedzinę).
2. W polu **Realm name** (Nazwa dziedziny) wpisz **employees** (pracownicy).
3. Kliknij **Browse...** (Przeglądaj...) po prawej stronie pola **Parent DN** (Nadrzędna nazwa wyróżniająca).
4. Wybierz utworzoną nadrzędną nazwę wyróżniającą **dc=my\_co,dc=com** i kliknij przycisk **Select** (Wybierz) po prawej stronie okna.
5. Kliknij przycisk **Next** (Dalej).
6. W następnym oknie wystarczy zmienić listę rozwijaną **User template** (Szablon użytkownika). Wybierz utworzony szablon użytkownika **cn=employees,dc=my\_co,dc=com**.
7. Kliknij przycisk **Finish** (Zakończ).

### Czynność 4: tworzenie grupy menedżerów:

1. Utwórz grupę menedżerów.
  - a. W narzędziu Web Administration kliknij kolejno opcje **Users and groups** → **Add group** (Użytkownicy i grupy > Dodaj grupę).
  - b. W polu **Group name** (Nazwa grupy) wpisz **menedzerowie**.
  - c. Sprawdź, czy na liście rozwijanej **Realm** (Dziedzina) wybrano pozycję **pracownicy**.
  - d. Kliknij przycisk **Finish** (Zakończ).

2. Skonfiguruj administratora grupy menedżerów dla dziedziny **pracownicy**.
  - a. Kliknij kolejno opcje **Realms and templates** → **Manage realms** (Dziedziny i szablony > Zarządzaj dziedzinaми).
  - b. Wybierz utworzoną dziedzinę, **cn=employees,dc=my\_co,dc=com**, a następnie kliknij przycisk **Edit** (Edycja).
  - c. Po prawej stronie pola **Administrator group** (Grupa administratora) kliknij przycisk **Browse...** (Przeglądaj...).
  - d. Wybierz pozycję **dc=my\_co,dc=com** i kliknij przycisk **Expand** (Rozwiń).
  - e. Wybierz pozycję **cn=employees** i kliknij przycisk **Expand** (Rozwiń).
  - f. Wybierz pozycję **cn=managers** i kliknij przycisk **Select** (Wybierz).
  - g. W oknie **Edit realm** (Edycja dziedziny) kliknij przycisk **OK**.
3. Nadaj grupie menedżerów uprawnienia do przyrostka **dc=my\_co,dc=com**.
  - a. Kliknij kolejno opcje **Directory management** → **Manage entries** (Zarządzanie katalogiem > Zarządzanie pozycjami).
  - b. Wybierz pozycję **dc=my\_co,dc=com** i kliknij przycisk **Edit ACL...** (Edycja listy ACL...).
  - c. W oknie **Edit ACL** (Edycja listy ACL) kliknij zakładkę **Owners** (Właściciele).
  - d. Zaznacz pole wyboru **Propagate owner** (Propagacja właściciela). Każdy członek grupy menedżerów zostanie właścicielem drzewa danych **dc=my\_co,dc=com**.
  - e. Z listy rozwijanej **Type** (Typ) wybierz pozycję **Group** (Grupa).
  - f. W polu **DN (Distinguished name)** (Nazwa wyróżniająca) wpisz **cn=managers,cn=employees,dc=my\_co,dc=com**.
  - g. Kliknij przycisk **Add** (Dodaj).
  - h. Kliknij przycisk **OK**.

#### Czynność 5: dodawanie użytkownika jako menedżera:

1. W narzędziu Web Administration kliknij kolejno opcje **Users and groups** → **Add user** (Użytkownicy i grupy > Dodaj użytkownika).
2. Wybierz utworzoną dziedzinę **pracownicy** z listy rozwijanej **Realm** (Dziedzina) i kliknij przycisk **Next** (Dalej).
3. W polu **cn** wpisz Jose Alvarez.
4. W polu **\*sn** (nazwisko) wpisz Alvarez.
5. W polu **\*cn** (imię i nazwisko) wpisz Jose Alvarez. Nazwa cn służy do tworzenia nazwy wyróżniającej pozycji. Nazwa \*cn jest atrybutem obiektu.
6. W polu **telephoneNumber** (numer telefonu) wpisz 999 555 1234.
7. W polu **departmentNumber** (numer działu) wpisz DEPTA.
8. W polu **mail** (poczta) wpisz jalvarez@my\_co.com.
9. w polu **userPassword** (hasło użytkownika) wpisz tajne\_hasło.
10. Kliknij zakładkę **User groups** (Grupy użytkowników).
11. Na liście **Available groups** (Dostępne grupy) wybierz pozycję **menedżerowie** i kliknij przycisk **Add** → (Dodaj →).
12. Na dole okna kliknij **Finish** (Zakończ).
13. Wyloguj się z Web Administration, klikając **Log out** (Wyloguj) z lewej strony obszaru nawigacyjnego.

### Szczegóły scenariusza: publikowanie danych serwera System i5 w bazie danych katalogu

Skonfigurowanie publikowania umożliwi systemowi automatyczne wprowadzanie informacji o użytkownikach do katalogu LDAP. Informacje o użytkowniku z katalogu dystrybucyjnego systemu są publikowane w katalogu LDAP.

**Uwaga:** Użytkownikom utworzonym za pomocą programu System i Navigator nadawany jest zarówno profil użytkownika, jak i wpis w katalogu dystrybucyjnym systemu. Jeśli do tworzenia użytkowników używane są komendy CL, należy utworzyć profil użytkownika (**CRTUSRPRF**) oraz pozycję użytkownika w katalogu

dystrybucyjnym systemu (**WRKDIRE**). Jeśli użytkownicy istnieją tylko jako profile użytkowników i mają być publikowani w katalogu LDAP, należy dla nich utworzyć pozycje użytkowników katalogu dystrybucyjnego systemu.

#### **Czynność 1: ustawianie systemu jako użytkownika serwera Directory Server:**

1. Zaloguj się w narzędziu Web Administration ([http://mySystem.my\\_co.com:9080/IDSWebApp/IDSjsp/Login](http://mySystem.my_co.com:9080/IDSWebApp/IDSjsp/Login)) jako administrator.
  - a. Wybierz **mySystem.my\_co.com** z listy **LDAP Hostname** (Nazwa hosta LDAP).
  - b. Wpisz **cn=admin** w polu **Username** (Nazwa użytkownika).
  - c. Wpisz **tajne\_haslo** w polu **Password** (Hasło).
  - d. Kliknij przycisk **Login** (Zaloguj).
2. Wybierz kolejno opcje **Users and groups** → **Add user** (Użytkownicy i grupy > Dodaj użytkownika).
3. Na liście **Realm** (Dziedzina) wybierz **pracownicy**.
4. Kliknij przycisk **Next** (Dalej).
5. Wpisz **mySystem.my\_co.com** w polu **cn**.
6. Wpisz **mySystem.my\_co.com** w polu **\*sn**.
7. Wpisz **mySystem.my\_co.com** w polu **\*cn**.
8. W polu **userPassword** wpisz **tajne\_haslo**.
9. Kliknij zakładkę **User groups** (Grupy użytkowników).
10. Wybierz grupę **managers**.
11. Kliknij przycisk **Add** → (Dodaj).
12. Kliknij przycisk **Finish** (Zakończ).

#### **Czynność 2: konfigurowanie systemu do publikowania danych:**

1. W programie System i Navigator kliknij prawym przyciskiem myszy serwer iSeries w okienku nawigacji z lewej strony i wybierz opcję **Właściwości** (Properties).
2. W oknie dialogowym **Właściwości** (Properties) wybierz zakładkę **Directory Server**.
3. Wybierz opcję **Użytkownicy** (Users) i kliknij przycisk **Szczegóły** (Details).
4. Zaznacz pole wyboru **Publikuj informacje o użytkowniku** (Publish user information).
5. W sekcji **Miejsce publikowania** (Where to publish) kliknij przycisk **Edycja** (Edit). Wyświetlone zostanie okno.
6. Wpisz **mySystem.my\_co.com**.
7. W polu **Pod nazwą DN** (Under DN) wpisz **cn=employees,dc=my\_co,dc=com**.
8. W sekcji **Połączenie serwera** (Server connection) sprawdź, czy w polu **Port** wprowadzono domyślny numer portu, **389**. Na liście rozwijanej **Metoda uwierzytelniania** (Authentication method) wybierz pozycję **Nazwa wyróżniająca** (Distinguished name) i wpisz **cn=mySystem,cn=employees,dc=my\_co,dc=com** w polu **Nazwa wyróżniająca** (Distinguished name).
9. Kliknij przycisk **Hasło** (Password).
10. W polu **Hasło** (Password) wpisz **tajne\_haslo**.
11. W polu **Potwierdź hasło** (Confirm Password) wpisz **tajne\_haslo**.
12. Kliknij przycisk **OK**.
13. Kliknij przycisk **Sprawdź** (Verify). Ta funkcja sprawdza, czy wszystkie informacje wprowadzono poprawnie i czy system może połączyć się z katalogiem LDAP.
14. Kliknij przycisk **OK**.
15. Kliknij przycisk **OK**.

## Szczegóły scenariusza: wprowadź informacje do bazy danych katalogu

Jako menedżer, Jose Alvarez dodaje teraz i aktualizuje dane dla pojedynczych osób w danym departamencie. Chce dodać trochę informacji o osobie Jane Doe. Jane Doe jest użytkownikiem systemu i informacje o niej są opublikowane. Jose Alvarez również zamierza dodać informacje o użytkowniku John Smith. John Smith nie jest użytkownikiem systemu. Jose Alvarez wykonuje następujące czynności:

### Czynność 1: logowanie się do narzędzia Web Administration:

Zaloguj się w narzędziu Web Administration, ([http://mySystem.my\\_co.com:9080/IDSWebApp/IDSjsp/Login](http://mySystem.my_co.com:9080/IDSWebApp/IDSjsp/Login)), wykonując następujące czynności:

1. Wybierz **mySystem.my\_co.com** z listy **LDAP Hostname** (Nazwa hosta LDAP).
2. W polu Username wpisz `cn=Jose Alvarez,cn=myco employees,dc=my_co,dc=com`.
3. W polu hasła wpisz `secret`.
4. Kliknij przycisk **Logon** (Zaloguj).

### Czynność 2: zmiana danych pracownika:

1. Kliknij opcje **Users and groups** → **Manage users** (Użytkownicy i grupy > Zarządzaj użytkownikami).
2. Na liście **Realm** (Dziedzina) wybierz pozycję **pracownicy** i kliknij **View users** (Wyświetl użytkowników).
3. Z listy użytkowników wybierz **Jane Doe** i kliknij **Edit** (Edycja).
4. W polu **departmentNumber** (numer działu) wpisz `DEPTA`.
5. Kliknij przycisk **OK**.
6. Kliknij przycisk **Close** (Zamknij).

### Czynność 3: dodawanie danych pracownika:

1. Kliknij opcje **Users and groups** → **Add user** (Użytkownicy i grupy > Dodaj użytkownika).
2. W menu rozwijanym **Realm** (Dziedzina) wybierz pozycję **pracownicy** i kliknij **Next** (Dalej).
3. W polu **cn** wpisz `John Smith`.
4. W polu **\*sn** wpisz `Smith`.
5. W polu **\*cn** wpisz `John Smith`.
6. W polu **telephoneNumber** (numer telefonu) wpisz `999 555 1235`.
7. W polu **departmentNumber** (numer działu) wpisz `DEPTA`.
8. W polu **mail** (poczta) wpisz `jsmith@my_co.com`.
9. Kliknij przycisk **Finish** (Zakończ) na dole okna.

## Szczegóły scenariusza: testowanie bazy danych katalogu

Po wprowadzeniu danych pracownika do bazy danych katalogu należy przetestować bazę danych katalogu i serwer Directory Server, wykonując jedną z poniższych operacji:

### Przeszukaj bazę danych katalogu, używając książki adresów poczty elektronicznej:

Informacje w katalogu LDAP można łatwo przeszukiwać za pomocą programów obsługujących protokół LDAP. W wielu klientach poczty elektronicznej przeszukiwanie serwerów katalogów LDAP jest jedną z funkcji książki adresowej. Poniższe przykładowe procedury służą do skonfigurowania programów Lotus Notes 6 i Microsoft Outlook Express 6. Procedura dla większości innych klientów poczty elektronicznej będzie podobna.

#### *Lotus Notes:*

1. Otwórz książkę adresową.
2. Kliknij opcje **Działania** → **Nowe** → **Konto**.
3. Wpisz `mySystem` w polu **Nazwa konta**.
4. Wpisz `mySystem.my_co.com` w polu **Nazwa serwera kont**.
5. W polu **Protokół** wybierz **LDAP**.

6. Kliknij zakładkę **Konfiguracja protokołu**.
7. W polu **Baza wyszukiwania** wpisz `dc=my_co,dc=com`.
8. Kliknij przycisk **Zapisz i zamknij**.
9. Kliknij **Utwórz** → **Poczta** → **Wiadomość**.
10. Kliknij **Adres...**
11. Wybierz `mySystem` w polu **Wybierz książkę adresową**.
12. Wpisz `Alvarez` w polu **Szukaj**.
13. Kliknij **Wyszukaj**. Wyświetlone zostaną dane dotyczące użytkownika `Jose Alvarez`.

*Microsoft Outlook Express:*

1. Kliknij **Narzędzia** → **Konta**.
2. Kliknij **Dodaj** → **Usługa katalogowa**.
3. W polu **Serwer katalogowy (LDAP)** wpisz adres WWW systemu (`mySystem.my_co.com`).
4. Usuń zaznaczenie pola wyboru **Serwer LDAP wymaga logowania**.
5. Kliknij przycisk **Dalej**.
6. Kliknij przycisk **Dalej**.
7. Kliknij przycisk **Zakończ**.
8. Wybierz `mySystem.my_co.com` (skonfigurowaną właśnie usługę katalogową) i kliknij **Właściwości**.
9. Kliknij **Zaawansowane**.
10. W polu **Baza wyszukiwania** wpisz `dc=my_co,dc=com`.
11. Kliknij przycisk **OK**.
12. Kliknij przycisk **Zamknij**.
13. Naciśnij `Ctrl+E`, aby otworzyć okno **Znajdowanie osób**.
14. Wybierz `moj_system.my_co.com` z listy **Szukaj w**.
15. Wpisz `Alvarez` w polu **Nazwa**.
16. Kliknij **Znajdź teraz**. Wyświetlone zostaną dane dotyczące użytkownika `Jose Alvarez`.

**Przeszukaj bazę danych katalogu, używając komendy `ldapsearch` w wierszu komend:**

1. W interfejsie znakowym wprowadź komendę `CL QSH`, aby otworzyć sesję `Qshell`.
2. Wprowadź następujące dane, aby pobrać listę wszystkich pozycji LDAP w bazie danych.

```
ldapsearch -h moj_system.my_co.com -b dc=my_co,dc=com objectclass=*
```

gdzie:

**-h** jest nazwą hosta z serwerem LDAP.

**-b** jest podstawową nazwą wyróżniającą do wyszukiwania.

**objectclass=\***

zwraca wszystkie pozycje w katalogu.

Ta komenda zwraca dane podobne do poniższych:

```
dc=my_co,dc=com
dc=my_co
objectclass=domain
objectclass=top
```

```
cn=MyCo_employee,dc=my_co,dc=com
```

```
.
.
.
```

```
cn=Jose Alvarez,cn=MyCo_Employees,dc=my_co,dc=com
```

```
sn=Alvirez
departmentNumber=DEPTA
mail=jalvirez@my_co.com
telephoneNumber=999 999 9999
objectclass=top
objectclass=inetOrgPerson
objectclass=organizationalPerson
objectclass=person
cn=Jose Alvirez
```

```
.
.
.
```

Pierwszy wiersz każdej pozycji jest nazwą wyróżniającą. Nazwy wyróżniające są podobne do pełnej nazwy pliku każdej pozycji. Niektóre pozycje nie zawierają danych, są tylko pozycjami strukturalnymi. Pozycje z wierszem **objectclass=inetOrgPerson** odpowiadają pozycjom utworzonym przez użytkowników. Nazwa wyróżniająca osoby Jose Alvirez brzmi: **cn=Jose Alvirez,cn=MyCo Employees,dc=my\_co,dc=com**.

## Scenariusz: kopiowanie użytkowników z listy sprawdzania serwera HTTP do serwera Directory Server

Przykład kopiowania użytkowników z listy sprawdzania serwera HTTP do serwera Directory Server.

### Sytuacja i przegląd

Na serwerze HTTP Server (oparty na Apache) uruchomiona jest obecnie aplikacja korzystająca z listy użytkowników Internetu z listy sprawdzania MYLIB/HTTPVLDL. Użytkownik ma zamiar użyć tych samych użytkowników Internetu z serwerem WebSphere Application Server (WAS) i uwierzytelnianiem LDAP. Aby uniknąć duplikowania obsługi informacji o użytkownikach na liście sprawdzania i LDAP, aplikacja serwera HTTP zostanie także skonfigurowana do używania uwierzytelniania LDAP.

W tym celu konieczne jest wykonanie następujących czynności:

1. Kopiowanie istniejących użytkowników z listy sprawdzania do lokalnego serwera katalogów.
2. Konfiguracja serwera WAS do używania uwierzytelniania LDAP.
3. Zmiana konfiguracji serwera HTTP, aby używał uwierzytelniania LDAP zamiast listy sprawdzania.

### Czynność 1: kopiowanie istniejących użytkowników z listy sprawdzania do lokalnego serwera katalogów

Przyjęto założenie, że serwer katalogów został wcześniej skonfigurowany za pomocą przyrostka "o=moje przedsiębiorstwo" i został uruchomiony. Użytkownicy LDAP mają być przechowywani w poddrzewie katalogu "cn=users,o=moje przedsiębiorstwo". Nazwa wyróżniająca administratora serwera katalogów to "cn=administrator", a hasło administratora to "sekret".

Z wiersza komend wywołaj funkcję API w następujący sposób:

```
CALL PGM(QSYS/QGLDCPYVL) PARM('HTTPVLDL MYLIB ' 'cn=administrator'
X'00000000' 'sekret' X'00000000' 'cn=users,o=moje przedsiębiorstwo' X'00000000' '' X'00000000'
X'00000000')
```

Po zakończeniu serwer katalogów będzie zawierał pozycje inetorgperson oparte na pozycjach listy sprawdzania. Na przykład, użytkownikowi z listy sprawdzania:

```
Nazwa użytkownika: jsmith
Opis: John Smith
Hasło: *****
```

będzie odpowiadała następująca pozycja katalogu:



```
dn: uid=jsmith,cn=users,o=moje przedsiebiorstwo
objectclass: top
objectclass: person
objectclass: organizationalperson
objectclass: inetorgperson
uid: jsmith
sn: jsmith
cn: jsmith
opis: John Smith
haslo_uzytkownika: *****
```

Ta pozycja może następnie zostać użyta do uwierzytelniania na serwerze katalogów. Na przykład, wykonanie działania QSH ldapsearch odczyta pozycję DSE katalogu głównego serwera:

```
> ldapsearch -D "uid=jsmith,cn=users,o=my company" -w ***** -s base "(objectclass=*)"
```

Po utworzeniu pozycje katalogu można edytować, aby zawierały dodatkowe informacje. Na przykład, wartości cn i sn można zmienić, aby odzwierciedlały odpowiednio pełną nazwę użytkownika i nazwisko lub dodać numer telefonu i adres poczty elektronicznej.

## Czynność 2: konfigurowanie serwera WAS do używania uwierzytelniania LDAP

Ochrona LDAP serwera WAS wymaga takiej konfiguracji, aby wyszukiwane były pozycje według nazwy wyróżniającej "cn=users,o=moje przedsiebiorstwo", za pomocą filtra wyszukiwania, który przypisuje wprowadzoną nazwę użytkownika pozycjom inetOrgPerson zawierającym tę wartość atrybutu uid. Na przykład, uwierzytelnienie na serwerze WAS za pomocą nazwy użytkownika jsmith spowoduje wyszukiwanie pozycji zgodnych z filtrem wyszukiwania "(uid=jsmith)". Więcej informacji zawiera temat Configure LDAP search filters w Centrum informacyjnym iSeries Websphere Application Server.

## Zmiana konfiguracji serwera HTTP, aby używał uwierzytelniania LDAP zamiast listy sprawdzania.

**Uwaga:** Procedura opisana poniżej ma na celu ułatwienie zilustrowania przykładów zawartych w tym scenariuszu poprzez zaprezentowanie szczegółowego przeglądu konfiguracji serwera HTTP do używania uwierzytelniania LDAP. Mogą być potrzebne bardziej szczegółowe informacje, które znajdują się w dokumentacji technicznej IBM (Redbooks) Implementation and Practical Use of LDAP on the IBM eServer iSeries Server, SG24-6193



(sekcja 6.3.2 - "Setting up LDAP authentication for the powered by Apache server"), a także w temacie Set up password protection on HTTP Server (powered by Apache).

1. Kliknij **Basic Authentication** (Podstawowe uwierzytelnianie) w zakładce **Configuration** (Konfiguracja) dla serwera HTTP w narzędziu HTTP Administration tool.
2. W pozycji **User authentication method** (Metoda uwierzytelniania użytkownika), zmień **Use Internet users in validation lists** (Używaj listy sprawdzania użytkowników Internetu) na **Use user entries in LDAP server** (Używaj pozycji użytkowników serwera LDAP) i kliknij przycisk **OK**.
3. Powróć do zakładki **Configuration** (Konfiguracja) i kliknij **Control Access** (Kontrola praw dostępu). Skonfiguruj kontrolę dostępu w sposób opisany w dokumentacji technicznej IBM (Redbooks), do której odsyłacz znajduje się powyżej, i kliknij przycisk **OK**.
4. Na zakładce **Configuration** (Konfiguracja) kliknij **LDAP Authentication** (Uwierzytelnianie LDAP).
  - a. Wprowadź nazwę i port hosta serwera LDAP. W pozycji **User search base DN** (Podstawowa nazwa wyróżniająca wyszukiwania użytkowników) wpisz cn=users,o=moje przedsiebiorstwo.
  - b. W pozycji **Create a unique LDAP DN for user authentication** (Utwórz unikalna nazwę wyróżniająca LDAP dla uwierzytelniania użytkowników) wprowadź filtr (&objectclass=person)(uid=%v1)).
  - c. Wprowadź informacje o grupie i kliknij przycisk **OK**.
5. Skonfiguruj połączenie z serwerem LDAP w sposób opisany w dokumentacji technicznej IBM (Redbooks), do której odsyłacz znajduje się powyżej.

---

## Administrowanie serwerem Directory Server

Ten temat zawiera informacje dotyczące administrowania serwerem Directory Server.

Aby zarządzać serwerem Directory Server, profil użytkownika musi posiadać następujące uprawnienia:

- Aby skonfigurować serwer lub zmienić jego konfigurację: uprawnienia specjalne do wszystkich obiektów (All Object – \*ALLOBJ) i do konfigurowania we/wy systemu (I/O System Configuration – \*IOSYSCFG).
- Aby uruchomić lub zamknąć serwer: uprawnienie Job Control (\*JOBCTL) i uprawnienia do obiektów dla komend: Zakończenie pracy TCP/IP (End TCP/IP - ENDTCP), Uruchomienie 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 parametry kontroli serwera katalogów: uprawnienie specjalne Audit (\*AUDIT).
- Aby wyświetlić 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 użyciu nazwy wyróżniającej administratora lub innej nazwy wyróżniającej, która ma odpowiednie uprawnienia LDAP. Jeśli wykorzystywana jest integracja uprawnień, administratorem może być także użytkownik rzutowany (zapoznaj się z sekcją “Mechanizm rzutowania systemu operacyjnego” na stronie 84), który ma uprawnienia do identyfikatora funkcji Directory Server Administrator (Administratora Usług katalogowych). Większość zadań administracyjnych może być także wykonywana przez użytkowników z grupy administracyjnej (zapoznaj się z sekcją “Dostęp administracyjny” na stronie 63).

## Ogólne zadania administrowania

Ten temat zawiera informacje dotyczące wykonywania ogólnych zadań administrowania serwerem Directory Server.

### Uruchamianie serwera Directory Server

Ten temat zawiera informacje dotyczące uruchamiania serwera Directory Server.

1. W programie System i Navigator rozwiń pozycję **Sieć**.
2. Rozwiń pozycję **Serwery**.
3. Kliknij **TCP/IP**.
4. Prawym przyciskiem myszy kliknij **IBM Directory Server** i wybierz **Uruchom**.

Uruchomienie serwera katalogów może potrwać kilka minut. Jest to uzależnione od szybkości serwera i ilości dostępnej pamięci. Pierwsze uruchomienie serwera katalogów może trwać nieco dłużej niż zazwyczaj, ponieważ serwer musi utworzyć nowe pliki. Podobnie uruchomienie serwera katalogów po raz pierwszy po jego zaktualizowaniu z wcześniejszej wersji może zająć więcej czasu niż zwykle, ponieważ serwer musi przeprowadzić migrację plików. Istnieje możliwość regularnego sprawdzania statusu serwera (zapoznaj się z tematem “Sprawdzanie statusu serwera Directory Server” na stronie 117) w celu zweryfikowania, czy został już uruchomiony.

Serwer Directory Server można także uruchomić za pomocą interfejsu znakowego, wpisując komendę STRTCPSVR \*DIRSRV. Ponadto, jeśli serwer katalogów został skonfigurowany tak, aby rozpoczynał działanie w momencie uruchamiania protokołu TCP/IP, można go uruchomić, wpisując komendę STRTCP.

Serwer katalogu można uruchomić w trybie samej konfiguracji z interfejsu znakowego poprzez wprowadzenie komendy TRCTCPAPP APP(\*DIRSRV) ARGLIST(SAFEMODE).

Tryb samej konfiguracji uruchamia serwer tylko z aktywnym przyrostkiem cn=configuration i nie zależy od pomyślnego zainicjowania postprocesorów bazy danych.

#### Zadania pokrewne

“Zatrzymywanie serwera Directory Server” na stronie 117

Ten temat zawiera informacje dotyczące zatrzymywania serwera Directory Server.

“Sprawdzanie statusu serwera Directory Server”

Ten temat zawiera informacje dotyczące sprawdzania statusu serwera Directory Server.

## Zatrzymywanie serwera Directory Server

Ten temat zawiera informacje dotyczące zatrzymywania serwera Directory Server.

**Uwaga:** Zatrzymanie serwera Directory Server ma wpływ na wszystkie aplikacje korzystające z niego w momencie 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.

1. W programie System i Navigator rozwiń pozycję **Sieć**.
2. Rozwiń pozycję **Serwery**.
3. Kliknij **TCP/IP**.
4. Prawym przyciskiem myszy kliknij **IBM Directory Server** i wybierz **Zatrzymaj**.

Aby zakończyć pracę, serwer katalogów potrzebuje kilku minut, w zależności od szybkości serwera, jego obciążenia oraz ilości dostępnej pamięci. Istnieje możliwość regularnego sprawdzania statusu serwera (zapoznaj się z tematem “Sprawdzanie statusu serwera Directory Server”) w celu zweryfikowania, czy został już uruchomiony.

Serwer Directory Server można także zatrzymać za pomocą interfejsu znakowego, wpisując komendę `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.

### Zadania pokrewne

“Uruchamianie serwera Directory Server” na stronie 116

Ten temat zawiera informacje dotyczące uruchamiania serwera Directory Server.

## Sprawdzanie statusu serwera Directory Server

Ten temat zawiera informacje dotyczące sprawdzania statusu serwera Directory Server.

Do podstawowych informacji o statusie można dotrzeć za pomocą programu System i Navigator. Bardziej zaawansowane i szczegółowe informacje o statusie można uzyskać za pomocą narzędzia Web Administration.

Program System i Navigator wyświetla status serwera Directory Server w kolumnie **Status** w prawej ramce.

Aby sprawdzić status serwera katalogów w programie System i Navigator, należy wykonać następujące czynności:

1. Rozwiń pozycję **Sieć** (Network).
2. Rozwiń pozycję **Serwery**.
3. Kliknij **TCP/IP**. System i 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 **IBM Directory Server** i wybierz opcję **Status**. Spowoduje to wyświetlenie informacji o liczbie aktywnych połączeń, a także innych informacji, np. o wcześniejszych i bieżących poziomach aktywności.

Poza dostarczaniem dodatkowych informacji, sprawdzanie statusu serwera za pomocą tej opcji może zaoszczędzić czas. Status serwera Directory Server można odświeżyć bez czekania na sprawdzenie statusu innych serwerów TCP/IP.

Aby wyświetlić status serwera katalogów za pomocą narzędzia Web Administration, wykonaj następujące czynności:

1. W obszarze nawigacyjnym rozwiń kategorię **Server administration** (Administrowanie serwerem).

**Uwaga:** Aby zmienić konfigurację serwera za pomocą zadań w kategorii Server administration (Administrowanie serwerem) w narzędziu Web Administration, należy uwierzytelnić się na serwerze jako profil użytkownika systemu i5/OS z uprawnieniami specjalnymi \*ALLOBJ i IOSYSCFG. Można to zrobić, dokonując uwierzytelnienia jako użytkownik rzutowany i używając hasła dla tego profilu. Aby nawiązać

połączenie jako użytkownik rzutowany z poziomu narzędzia Web Administration, należy wprowadzić nazwę użytkownika w postaci `os400-profile=MOJANAZWAUŻYTKOWNIKA,cn=accounts,os400-sys=MÓJSYSTEM.PL`, gdzie łańcuchy znaków `MOJANAZWAUŻYTKOWNIKA` i `MÓJSYSTEM.PL` zastępowane są odpowiednio nazwą profilu użytkownika i skonfigurowanym przyrostkiem rzutowania.

2. Kliknij **View server status** (Wyświetl status serwera).
3. W panelu **View server status** (Widok statusu serwera) wybierz odpowiednie zakładki, aby wyświetlić informacje o statusie.

## Sprawdzanie zadań na serwerze Directory Server

Ten temat zawiera informacje dotyczące monitorowania wybranych zadań na serwerze Directory Server.

Aby sprawdzić zadania na serwerze za pomocą programu System i Navigator, należy wykonać następujące czynności:

1. W programie System i Navigator rozwiń pozycję **Sieć**.
2. Rozwiń pozycję **Serwery**.
3. Kliknij **TCP/IP**.
4. Prawym przyciskiem myszy kliknij element **IBM Directory Server** i wybierz opcję **Zadania serwera** (Server Jobs).

## Zarządzanie połączeniami serwera

Ten temat zawiera informacje o wyświetleniu połączeń z serwerem oraz o działaniach wykonywanych przy użyciu tych połączeń.

Administrator może na podstawie analizy połączeń podejmować decyzje dotyczące kontroli praw dostępu i zapobiegania atakom polegającym na spowodowaniu odmowy usługi. Można to zrobić za pomocą narzędzia Web Administration.

**Uwaga:** Aby zmienić konfigurację serwera za pomocą zadań w kategorii Server administration (Administrowanie serwerem) w narzędziu Web Administration, należy uwierzytelnić się na serwerze jako profil użytkownika systemu i5/OS z uprawnieniami specjalnymi \*ALLOBJ i IOSYSCFG. Można to zrobić, dokonując uwierzytelnienia jako użytkownik rzutowany i używając hasła dla tego profilu. Aby nawiązać połączenie jako użytkownik rzutowany z poziomu narzędzia Web Administration, należy wprowadzić nazwę użytkownika w postaci `os400-profile=MOJANAZWAUŻYTKOWNIKA,cn=accounts,os400-sys=MÓJSYSTEM.PL`, gdzie łańcuchy znaków `MOJANAZWAUŻYTKOWNIKA` i `MÓJSYSTEM.PL` zastępowane są odpowiednio nazwą profilu użytkownika i skonfigurowanym przyrostkiem rzutowania.

1. W obszarze nawigacyjnym rozwiń kategorię **Server administration** (Administrowanie serwerem).
2. Kliknij **Manage server connections** (Zarządzaj połączeniami serwera).

Wyświetlona zostanie tabela zawierająca następujące informacje dla każdego połączenia:

### **DN (Nazwa wyróżniająca)**

Określa nazwy wyróżniające połączenia klienta z serwerem.

### **IP address (Adres IP)**

Określa adres IP klienta połączony z serwerem.

### **Start time (Czas uruchomienia)**

Określa datę i godzinę (według czasu miejscowego serwera), kiedy połączenie zostało nawiązane.

**Status** Określa, czy połączenie jest aktywne czy bezczynne. Połączenie uznawane jest za aktywne, jeśli istnieją działania w toku.

### **Ops initiated (Zainicjowane działania)**

Określa liczbę działań żądanych od momentu ustanowienia połączenia.

### **Ops completed (Zakończone działania)**

Określa liczbę zakończonych działań dla każdego połączenia.

## Type (Typ)

Określa, czy połączenie jest chronione przez SSL lub TLS. W przeciwnym razie pole to jest puste.

**Uwaga:** Tabela wyświetla do 20 połączeń jednocześnie.

Można określić, czy tabela ma być wyświetlana według nazwy wyróżniającej czy adresu IP rozwijając menu rozwijane u góry panelu i dokonując wyboru. Domyślnym ustawieniem jest wyświetlanie według nazwy wyróżniającej. Podobnie, można także określić, czy tabela ma być wyświetlana w porządku rosnącym czy malejącym.

3. Kliknij przycisk **Refresh** (Odśwież), aby zaktualizować informacje o bieżącym połączeniu.
4. Jeśli użytkownik jest zalogowany jako administrator lub członek grupy administracyjnej, w panelu dostępne są dodatkowe opcje umożliwiające rozłączenie połączeń serwera. Możliwość rozłączenia połączeń serwera pozwala powstrzymać odmowę usługi i sterować dostępem do serwera. Połączenie można rozłączyć rozwijając menu rozwijane i wybierając nazwę wyróżniającą, adres IP lub jedno i drugie i klikając **Disconnect** (Rozłącz). Aby rozłączyć wszystkie połączenia serwera poza jednym, za pośrednictwem którego wprowadzane jest to żądanie, należy kliknąć **Disconnect all** (Rozłącz wszystkie). Wyświetlany jest komunikat potwierdzenia. Kliknij przycisk **OK**, aby kontynuować rozłączanie lub **Cancel** (Anuluj), aby zakończyć działanie i powrócić do panelu **Manage server connections** (Zarządzaj połączeniami serwera).

Więcej informacji o zapobieganiu atakom polegającym na spowodowaniu odmowy usługi zawiera temat Zarządzanie właściwościami połączeń.

### Pojęcia pokrewne

“Odmowa usługi” na stronie 84

Opisana w tym temacie opcja konfiguracyjna zapewnia ochronę przed atakami polegającymi na spowodowaniu odmowy usługi.

### Zadania pokrewne

“Zarządzanie właściwościami połączenia”

Ten temat zawiera informacje o ustawianiu właściwości połączenia, w tym właściwości zapobiegających blokowaniu serwera przez klientów.

## Zarządzanie właściwościami połączenia

Ten temat zawiera informacje o ustawianiu właściwości połączenia, w tym właściwości zapobiegających blokowaniu serwera przez klientów.

Możliwość zarządzania właściwościami połączenia pozwala zapobiegać blokowaniu serwera przez klientów. Zapewnia także, że administrator zawsze posiada dostęp do serwera w przypadkach, kiedy postprocesor jest obciążony długotrwałymi zadaniami. Zarządzanie właściwościami połączenia wykonywane jest za pomocą narzędzia Web Administration.

**Uwaga:** Te opcje wyświetlone są jedynie, jeśli użytkownik jest zalogowany na serwerze obsługującym tę funkcję jako administrator lub członek grupy administracyjnej.

Aby ustawić właściwości połączenia, należy wykonać następujące czynności:

1. W obszarze nawigacyjnym rozwiń kategorię **Server administration** (Administrowanie serwerem) i kliknij **Manage connection properties** (Zarządzaj właściwościami połączenia).

**Uwaga:** Aby zmienić konfigurację serwera za pomocą zadań w kategorii Server administration (Administrowanie serwerem) w narzędziu Web Administration, należy uwierzytelnić się na serwerze jako profil użytkownika systemu i5/OS z uprawnieniami specjalnymi \*ALLOBJ i IOSYSCFG. Można to zrobić, dokonując uwierzytelnienia jako użytkownik rzutowany i używając hasła dla tego profilu. Aby nawiązać połączenie jako użytkownik rzutowany z poziomu narzędzia Web Administration, należy wprowadzić nazwę użytkownika w postaci `os400-profile=MOJANAZWAUŻYTKOWNIKA,cn=accounts,os400-sys=MÓJSYSTEM.PL`, gdzie łańcuchy znaków MOJANAZWAUŻYTKOWNIKA i MÓJSYSTEM.PL zastępowane są odpowiednio nazwą profilu użytkownika i skonfigurowanym przyrostkiem rzutowania.

- Wybierz zakładkę **General** (Ogólne).
- Określ ustawienie połączenia anonimowego. Pole wyboru **Allow anonymous connections** (Zezwalaj na anonimowe połączenia) jest już zaznaczone, zatem połączenia anonimowe są dozwolone. Jest to ustawienie domyślne. Można kliknąć pole wyboru, aby usunąć zaznaczenie funkcji **Allow anonymous connections** (Zezwalaj na anonimowe połączenia). Działanie to spowoduje, że serwer rozłączy wszystkie połączenia anonimowe.

**Uwaga:** Niektóre aplikacje mogą przestać działać, jeśli połączenia anonimowe zostaną zabronione.

- W polu **Cleanup threshold for anonymous connections** (Próg czyszczenia dla połączeń anonimowych) określ wartość progu inicjowania rozłączania połączeń anonimowych. Można określić liczbę z przedziału od 0 do 65535.

**Uwaga:** Rzeczywista liczba maksymalna jest ograniczona przez liczbę plików dozwolonych dla jednego procesu. W systemach UNIX można użyć komendy **ulimit -a** w celu określenia limitu. W systemach Windows jest to stała liczba.

Ustawieniem domyślnym jest 0. Jeśli liczba anonimowych połączeń zostanie przekroczona, połączenia są czyszczone w oparciu o limit czasu bezczynności określony w polu **Idle time out** (Limit czasu bezczynności).

- W polu **Cleanup threshold for authenticated connections** (Próg czyszczenia dla połączeń uwierzytnionych) określ wartość progu inicjowania rozłączania połączeń uwierzytnionych. Można określić liczbę z przedziału od 0 do 65535.

**Uwaga:** Rzeczywista liczba maksymalna jest ograniczona przez liczbę plików dozwolonych dla jednego procesu. W systemach UNIX można użyć komendy **ulimit -a** w celu określenia limitu. W systemach Windows jest to stała liczba.

Ustawieniem domyślnym jest 1100. Jeśli liczba uwierzytnionych połączeń zostanie przekroczona, połączenia są czyszczone w oparciu o limit czasu bezczynności określony w polu **Idle time out** (Limit czasu bezczynności).

- W polu **Cleanup threshold for all connections** (Próg czyszczenia dla wszystkich połączeń) określ wartość progu inicjowania rozłączania wszystkich połączeń. Można określić liczbę z przedziału od 0 do 65535.

**Uwaga:** Rzeczywista liczba maksymalna jest ograniczona przez liczbę plików dozwolonych dla jednego procesu. W systemach UNIX można użyć komendy **ulimit -a** w celu określenia limitu. W systemach Windows jest to stała liczba.

Ustawieniem domyślnym jest 1200. Jeśli całkowita liczba połączeń zostanie przekroczona, połączenia są czyszczone w oparciu o limit czasu bezczynności określony w polu **Idle time out** (Limit czasu bezczynności).

- W polu **Idle timeout limit** (Limit czasu bezczynności) określ liczbę sekund, kiedy połączenie może być bezczynne zanim zostanie zamknięte przez procedurę czyszczącą. Można określić liczbę z przedziału od 0 do 65535.

**Uwaga:** Rzeczywista liczba maksymalna jest ograniczona przez liczbę plików dozwolonych dla jednego procesu. W systemach UNIX można użyć komendy **ulimit -a** w celu określenia limitu. W systemach Windows jest to stała liczba.

Ustawieniem domyślnym jest 300. Po zainicjowaniu procedury czyszczącej wszystkie połączenia, które przekroczyły limit zostaną zamknięte.

- W polu **Result timeout limit** (Limit czasu wyniku) określ liczbę sekund dozwolonych pomiędzy próbami zapisu. Można określić liczbę z przedziału od 0 do 65535. Ustawieniem domyślnym jest 120. Wszystkie połączenia, które przekroczą ten limit zostaną zakończone.

**Uwaga:** Dotyczy to tylko systemów Windows. Połączenie, które przekracza 30 sekund zostanie automatycznie zerwane przez system operacyjny. Dlatego ustawienie **Result timeout limit** (Limit czasu wyniku) jest przesłaniane przez system operacyjny po 30 sekundach.

- Kliknij zakładkę **Emergency thread** (Wątek ratunkowy).

10. Określ ustawienie wątku ratunkowego. Pole wyboru **Enable emergency thread** (Włącz wątek ratunkowy) jest już zaznaczone, zatem wątek ratunkowy może być aktywowany. Jest to ustawienie domyślne. Można kliknąć pole wyboru, aby usunąć zaznaczenie funkcji **Enable emergency thread** (Włącz wątek ratunkowy). Działanie to zapobiegnie aktywowaniu wątku ratunkowego.
11. W polu **Pending request threshold** (Próg zadań oczekujących) określ wartość limitu dla żądań pracy, które aktywują wątek ratunkowy. Określ wartość z przedziału od 0 do 65535, aby ustawić limit żądań pracy, które mogą znajdować się w kolejce zanim aktywowany zostanie wątek ratunkowy. Wartością domyślną jest 50. Po przekroczeniu określonego limitu aktywowany jest wątek ratunkowy.
12. W polu **Time threshold** (Próg czasu) określ liczbę minut, które mogą upłynąć od momentu usunięcia z kolejki ostatniej pozycji roboczej. Jeśli w kolejce znajdują się pozycje robocze, a limit czasu zostanie przekroczony, wątek ratunkowy zostanie aktywowany. Można określić liczbę z przedziału od 0 do 240. Ustawieniem domyślnym jest 5.
13. Z menu rozwijanego wybierz kryterium, które ma być używane do aktywowania wątku ratunkowego. Można wybrać:
  - **Size only:** (Tylko wielkość) wątek ratunkowy jest aktywowany jedynie, kiedy kolejka przekroczy określoną ilość oczekujących pozycji roboczych.
  - **Time only:** (Tylko czas) wątek ratunkowy jest aktywowany jedynie, kiedy limit czasu pomiędzy usuniętymi pozycjami roboczymi przekroczy określoną wartość.
  - **Size or time:** (Wielkość lub czas) wątek ratunkowy jest aktywowany, kiedy wielkość kolejki lub próg czasu przekroczą określone wartości.
  - **Size and time:** (Wielkość i czas) wątek ratunkowy jest aktywowany, kiedy wielkość kolejki i próg czasu przekroczą określone wartości.

Domyślnym ustawieniem jest wielkość i czas.

14. Kliknij przycisk **OK**.

#### Pojęcia pokrewne

“Odmowa usługi” na stronie 84

Opisana w tym temacie opcja konfiguracyjna zapewnia ochronę przed atakami polegającymi na spowodowaniu odmowy usługi.

#### Zadania pokrewne

“Zarządzanie połączeniami serwera” na stronie 118

Ten temat zawiera informacje o wyświetleniu połączeń z serwerem oraz o działaniach wykonywanych przy użyciu tych połączeń.

## Włączanie powiadamiania o zdarzeniach

Ten temat zawiera informacje dotyczące włączania powiadamiania o zdarzeniach na serwerze Directory Server.

Powiadamianie o zdarzeniach pozwala klientom rejestrować się na serwerze Directory Server, aby otrzymywać powiadomienia o wystąpieniu określonych zdarzeń, takich jak dodanie informacji do katalogu.

Aby włączyć powiadamianie o zdarzeniach dla serwera, wykonaj następujące czynności:

1. W obszarze nawigacyjnym narzędzia Web Administration rozwiń kategorię **Manage server properties** (Zarządzanie właściwościami serwera) i wybierz zakładkę **Event notification** (Powiadomienie o zdarzeniu).
2. Zaznacz pole wyboru **Enable event notification** (Włącz powiadamianie o zdarzeniach), aby włączyć powiadamianie o zdarzeniach. Jeśli opcja **Enable event notification** (Włącz powiadamianie o zdarzeniach) jest wyłączona, serwer ignoruje pozostałe opcje w tym panelu.
3. Ustaw opcję **Maximum registrations per connection** (Maksymalna liczba rejestracji dla połączenia). Kliknij przełącznik **Registrations** (Rejestracje) lub **Unlimited** (Nieograniczona). Jeśli wybrana zostanie opcja **Registrations** (Rejestracje), należy określić w polu maksymalną liczbę rejestracji dozwolonych dla każdego połączenia. Maksymalna liczba transakcji wynosi 2147483647. Ustawieniem domyślnym jest 100 rejestracji.
4. Ustaw opcję **Maximum registrations total** (Maksymalna całkowita liczba rejestracji). Wybór ten określa liczbę rejestracji, które serwer może obsłużyć jednocześnie. Kliknij przełącznik **Registrations** (Rejestracje) lub **Unlimited** (Nieograniczona). Jeśli wybrana zostanie opcja **Registrations** (Rejestracje), należy określić w polu

maksymalną liczbę rejestracji dozwolonych dla każdego połączenia. Maksymalna liczba transakcji wynosi 2147483647. Domyślnie, liczba rejestracji jest **Unlimited** (Nieograniczona).

5. Po zakończeniu kliknij przycisk **Apply** (Zastosuj), aby zachować zmiany nie wychodząc lub kliknij przycisk **OK**, aby zachować zmiany i wyjść lub kliknij przycisk **Cancel** (Anuluj), aby opuścić panel nie zachowując zmian.
6. Jeśli aktywowano opcję powiadamiania o zdarzeniach, należy ponownie uruchomić serwer, aby zmiany zostały zastosowane. Jeśli modyfikowane były tylko ustawienia, serwer nie wymaga restartowania.

**Uwaga:** Aby wyłączyć opcję powiadamiania o zdarzeniach, usuń zaznaczenie w polu wyboru **Enable event notification** (Włącz Powiadamianie o zdarzeniach) i uruchom serwer ponownie.

- l Dodatkowe informacje na temat powiadamiania o zdarzeniach można znaleźć w sekcji Event notification
- l (Powiadamianie o zdarzeniach) podręcznika IBM Tivoli Directory Server Version 6.0 Programming Reference.

### Informacje pokrewne



Centrum informacyjne oprogramowania IBM Tivoli

Informacje dotyczące serwera IBM Tivoli Directory Server zawiera Centrum informacyjne oprogramowania IBM Tivoli.

## Określanie ustawień transakcji

Ten temat zawiera informacje dotyczące konfigurowania ustawień transakcji serwera Directory Server.

Transakcje serwera Directory Server umożliwiają traktowanie kilku operacji w katalogu LDAP jako jednego działania.

Aby skonfigurować transakcje serwera, wykonaj następujące czynności:

1. W obszarze nawigacyjnym narzędzia Web Administration rozwiń kategorię **Manage server properties** (Zarządzanie właściwościami serwera) i wybierz zakładkę **Transactions** (Transakcje).
2. Zaznacz pole wyboru **Enable transaction processing** (Włącz przetwarzanie transakcji), aby włączyć przetwarzanie transakcji. Jeśli opcja **Enable transaction processing** (Włącz przetwarzanie transakcji) jest wyłączona, pozostałe opcje w tym panelu, takie jak **Maximum number of operations per transaction** (Maksymalna liczba działań dla transakcji) i **Pending time limit** (Limit czasu oczekiwania), są ignorowane przez serwer.
3. Ustaw opcję **Maximum number of transactions** (Maksymalna liczba transakcji). Kliknij przełącznik **Transactions** (Transakcje) lub **Unlimited** (Nieograniczona). Jeśli wybrana zostanie opcja **Transactions** (Transakcje), należy określić w polu maksymalną liczbę transakcji. Maksymalna liczba transakcji wynosi 2147483647. Ustawieniem domyślnym jest 20 transakcji.
4. Ustaw opcję **Maximum number of operations per transaction** (Maksymalna liczba działań na transakcję). Kliknij przełącznik **Operations** (Działania) lub **Unlimited** (Nieograniczona). Jeśli wybrana zostanie opcja **Operations** (Działania), należy określić w polu maksymalną liczbę działań dozwolonych dla każdej transakcji. Maksymalna liczba działań wynosi 2147483647. Im niższa liczba, tym większa wydajność. Ustawieniem domyślnym jest 5 działań.
5. Ustaw opcję **Pending time limit** (Limit czasu oczekiwania). Wybór ten określa w sekundach maksymalną wartość limitu czasu dla oczekującej transakcji. Kliknij przełącznik **Seconds** (Sekundy) lub **Unlimited** (Nieograniczony). Jeśli wybrana zostanie opcja **Seconds** (Sekundy), należy określić w polu maksymalną liczbę sekund dozwoloną dla każdej transakcji. Maksymalna liczba sekund wynosi 2147483647. Transakcje, które nie zostaną zakończone przed upływem tego czasu są anulowane (wycofywane). Wartością domyślną jest 300 sekund.
6. Po zakończeniu kliknij przycisk **Apply** (Zastosuj), aby zachować zmiany nie wychodząc lub kliknij przycisk **OK**, aby zachować zmiany i wyjść lub kliknij przycisk **Cancel** (Anuluj), aby opuścić panel nie zachowując zmian.
7. Jeśli aktywowano obsługę transakcji, należy ponownie uruchomić serwer, aby zmiany zostały zastosowane. Jeśli modyfikowane były tylko ustawienia, serwer nie wymaga restartowania.

**Uwaga:** Aby wyłączyć przetwarzanie transakcji, usuń zaznaczenie w polu wyboru **Enable transaction processing** (Włącz przetwarzanie transakcji) i uruchom serwer ponownie.

### Pojęcia pokrewne



“Transakcje” na stronie 51

Serwer Directory Server można tak skonfigurować, aby programy typu klient mogły korzystać z transakcji. Transakcja to grupa działań na katalogu LDAP traktowanych jak jedna jednostka.

## Zmiana portu lub adresu IP

Procedura ta służy do zmiany portów, z których korzysta serwer Directory Server, lub adresu IP, na którym serwer akceptuje połączenia.

Serwer Directory Server używa następujących portów domyślnych:

- 389 dla połączeń niezabezpieczonych,
- 636 dla połączeń zabezpieczonych (jeśli użyto programu Digital Certificate Manager w celu wyznaczenia serwera Directory Server jako aplikacji, która może korzystać z zabezpieczonego portu).

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

Jeśli porty te są już używane przez inną aplikację, można przypisać inny port do serwera Directory Server lub użyć innych adresów IP dla obu serwerów, pod warunkiem, że aplikacje obsługują łączenie z konkretnym adresem IP.

Aby zmienić porty, z których korzysta serwer Directory Server, lub adres IP, na którym serwer akceptuje połączenia, należy wykonać następujące czynności:

1. W programie System i Navigator rozwiń pozycję **Sieć**.
2. Rozwiń pozycję **Serwery**.
3. Kliknij **TCP/IP**.
4. Prawym przyciskiem myszy kliknij **IBM Directory Server** i wybierz **Właściwości**.
5. Kliknij zakładkę **Sieć**.
6. Aby zmienić numer portu, wpisz odpowiednie numery portów i kliknij przycisk **OK**.
7. Aby zmienić adres IP, kliknij przycisk **Adresy IP...** (IP Addresses...). Następnie przejdź do następnego punktu.
8. Zaznacz **Użyj wybranych adresów IP**, a następnie wybierz adresy IP, których serwer ma używać do akceptowania połączeń.

### Informacje pokrewne

Wykorzystanie Domino LDAP oraz Directory Server w tym samym systemie

## Określanie serwera odwołań do katalogu

Ten temat zawiera informacje dotyczące określania serwera odwołań.

Aby przypisać serwery odwołań dla serwera Directory Server, należy wykonać następujące czynności:

1. W programie System i Navigator rozwiń pozycję **Sieć**.
2. Rozwiń pozycję **Serwery**.
3. Kliknij **TCP/IP**.
4. Prawym przyciskiem myszy kliknij **IBM Directory Server** i wybierz **Właściwości**.
5. Wybierz stronę właściwości **Ogólne**.
6. W polu **Nowe odwołanie** określ adres URL serwera odwołań.
7. W wierszu komend podaj nazwę serwera odwołań w formacie adresu URL. Poniżej znajdują się przykłady akceptowalnych adresów URL protokołu 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 w sposób podany dla portu 400 w drugim przykładzie powyżej.

8. Kliknij przycisk **Dodaj** (Add).
9. Kliknij przycisk **OK**.

#### Pojęcia pokrewne

“Odwołania do katalogu LDAP” na stronie 50

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

## Dodawanie i usuwanie przyrostków serwera Directory Server

W tym temacie opisano dodawanie i usuwanie przyrostków serwera Directory Server.

Dodanie przyrostka do serwera Directory Server 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, należy wykonać następujące czynności:

1. W programie System i Navigator rozwiń pozycję **Sieć**.
2. Rozwiń pozycję **Serwery**.
3. Kliknij **TCP/IP**.
4. Prawym przyciskiem myszy kliknij **IBM Directory Server** i wybierz **Właściwości**.
5. Kliknij zakładkę **Baza danych/Przyrostki**.
6. W polu **Nowy przyrostek** wpisz nazwę nowego przyrostka.
7. Kliknij przycisk **Dodaj** (Add).
8. Kliknij przycisk **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.

Aby usunąć przyrostek z serwera Directory Server, należy wykonać następujące czynności:

1. W programie System i Navigator rozwiń pozycję **Sieć**.
2. Rozwiń pozycję **Serwery**.
3. Kliknij **TCP/IP**.
4. Prawym przyciskiem myszy kliknij element **IBM Directory Server** i wybierz opcję **Właściwości** (Properties).
5. Kliknij zakładkę **Baza danych/Przyrostki**.
6. Zaznacz przyrostek, który ma zostać usunięty, klikając go.
7. Kliknij przycisk **Remove** (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.

#### Pojęcia pokrewne

“Przyrostek (kontekst nazwy)” na stronie 12

Przyrostek (znany również jako kontekst nazwy) to nazwa DN identyfikująca najwyższą pozycję w lokalnej hierarchii katalogu.

### Dodawanie przyrostka do serwera Directory Server:

Aby dodać przyrostek do serwera katalogów, należy wykonać następujące czynności:

1. W programie System i Navigator rozwiń pozycję **Sieć**.

2. Rozwiń pozycję **Serwery**.
3. Kliknij **TCP/IP**.
4. Prawym przyciskiem myszy kliknij **IBM Directory Server** i wybierz **Właściwości**.
5. Kliknij zakładkę **Baza danych/Przyrostki**.
6. W polu **Nowy przyrostek** wpisz nazwę nowego przyrostka.
7. Kliknij przycisk **Dodaj** (Add).
8. Kliknij przycisk **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 przyrostka z serwera Directory Server:**

Aby usunąć przyrostek z serwera Directory Server, należy wykonać następujące czynności:

1. W programie System i Navigator rozwiń pozycję **Sieć**.
2. Rozwiń pozycję **Serwery**.
3. Kliknij **TCP/IP**.
4. Prawym przyciskiem myszy kliknij **IBM Directory Server** i wybierz **Właściwości**.
5. Kliknij zakładkę **Baza danych/Przyrostki**.
6. Zaznacz przyrostek, który ma zostać usunięty, klikając go.
7. Kliknij przycisk **Remove** (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.

## **Nadawanie dostępu administratora użytkownikom rzutowanym**

Ten temat zawiera informacje dotyczące nadawania dostępu administratora profilom użytkowników.

Dostęp administratora można nadawać profilom użytkowników, które mają dostęp do identyfikatora funkcji Directory Server Administrator (QIBM\_DIRSRV\_ADMIN).

Na przykład, jeśli profil użytkownika JOHNSMITH ma dostęp do identyfikatora funkcji Directory Server Administrator oraz w oknie dialogowym Właściwości katalogu wybrano opcję Nadaj dostęp administratora użytkownikom autoryzowanym, profil JOHNSMITH ma wtedy uprawnienia administratora LDAP. Jeśli profil ten używany jest do łączenia z serwerem katalogów za pomocą nazwy wyróżniającej (DN) os400-profile=JOHNSMTH,cn=accounts,os400-sys=systemA.acme.com, użytkownik ma uprawnienia administratora. Przyrostek obiektów systemowych w tym przykładzie wygląda następująco: os400-sys=systemA.acme.com.

Aby wybrać opcję Nadaj dostęp administratora użytkownikom autoryzowanym (Grant administrator access to authorized users) i identyfikator funkcji administratora serwera Directory Server, należy wykonać następujące czynności:

1. W programie System i Navigator rozwiń pozycję **Sieć**.
2. Rozwiń pozycję **Serwery**.
3. Prawym przyciskiem myszy kliknij **Katalog** i wybierz opcję **Właściwości**.
4. Na karcie **Ogólne** (General) w oknie **Informacje administratora** (Administrator information) wybierz opcję **Nadaj dostęp administratora użytkownikom autoryzowanym** (Grant administrator access to authorized users).
5. W programie System i Navigator prawym przyciskiem myszy kliknij nazwę systemu i wybierz **Application administration** (Administrowanie aplikacji).
6. Kliknij zakładkę **Host Applications** (Aplikacje hosta).
7. Rozwiń **Operating System/400** (System OS/400).

8. Kliknij **Directory Server Administrator** (Administrator serwera katalogów), aby wyróżnić opcję.
9. Kliknij przycisk **Customize** (Dostosuj).
10. Rozwiń pozycję **Users** (Użytkownicy), **Groups** (Grupy) lub **Users not in a group** (Użytkownicy spoza grup), w zależności od tego, która jest odpowiednia dla danego użytkownika.
11. Wybierz użytkownika lub grupę, którego lub którą należy dodać do listy **Access allowed** (Dostęp zezwolony).
12. Kliknij przycisk **Add** (Dodaj).
13. Kliknij przycisk **OK**, aby zapisać zmiany.
14. W oknie dialogowym **Application Administration** (Administrowanie aplikacji) kliknij przycisk **OK**.

#### Pojęcia pokrewne

“Dostęp administracyjny” na stronie 63

Dostęp administracyjny służy do kontrolowania praw dostępu do konkretnych zadań administracyjnych.

“Mechanizm rzutowania systemu operacyjnego” na stronie 84

Systemowy mechanizm rzutowania ma możliwość odwzorowywania obiektów systemu i5/OS jako pozycji wewnątrz drzewa katalogów dostępnego z LDAP. Rzutowane obiekty są reprezentacjami LDAP obiektów systemu operacyjnego, zastępującymi rzeczywiste pozycje przechowywane w bazie danych serwera LDAP.

## Włączanie znaczników języka

Ten temat zawiera informacje dotyczące włączania znaczników języka.

Aby aktywować znaczniki języka, wykonaj następujące działania (domyślnie znaczniki są nieaktywne):

1. W kategorii **Server administration** (Administrowanie serwerem) w obszarze nawigacyjnym kliknij przycisk **Manage server properties** (Zarządzaj właściwościami serwera).

**Uwaga:** Aby zmienić konfigurację serwera za pomocą zadań w kategorii Server administration (Administrowanie serwerem) w narzędziu Web Administration, należy uwierzytelnić się na serwerze jako profil użytkownika systemu i5/OS z uprawnieniami specjalnymi \*ALLOBJ i IOSYSCFG. Można to zrobić, dokonując uwierzytelnienia jako użytkownik rzutowany i używając hasła dla tego profilu. Aby nawiązać połączenie jako użytkownik rzutowany z poziomu narzędzia Web Administration, należy wprowadzić nazwę użytkownika w postaci `os400-profile=MOJANAZWAUŻYTKOWNIKA,cn=accounts,os400-sys=MÓJSYSTEM.PL`, gdzie łańcuchy znaków MOJANAZWAUŻYTKOWNIKA i MÓJSYSTEM.PL zastępowane są odpowiednio nazwą profilu użytkownika i skonfigurowanym przyrostkiem rzutowania.

2. Zakładka **General** (Ogólne) jest wybrana domyślnie. Kliknij pole wyboru **Enable language tag support** (Aktywuj obsługę znaczników języka), aby aktywować obsługę.

**Uwaga:** Jeśli opcja ta jest aktywna, przypisanie znaczników języka atrybutom pozycji spowoduje, że serwer będzie zwracał pozycję ze znacznikami języka. Będzie to miało miejsce nawet jeśli opcja znaczników języka zostanie później wyłączona. Ponieważ zachowanie serwera może być niezgodne z oczekiwaniami aplikacji, w celu uniknięcia ewentualnych błędów nie należy wyłączać opcji znaczników języka po jej włączeniu.

## Śledzenie dostępu do katalogu LDAP i wprowadzanych do niego zmian

Ten temat zawiera informacje dotyczące śledzenia dostępu do katalogu LDAP i wprowadzanych do niego zmian.

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 czynności:

1. W programie System i Navigator rozwiń pozycję **Sieć**.
2. Rozwiń pozycję **Serwery**.
3. Kliknij **TCP/IP**.
4. Prawym przyciskiem myszy kliknij **IBM Directory Server** i wybierz **Właściwości**.
5. Kliknij zakładkę **Protokół zmian**.

6. Wybierz **Protokołowanie zmian katalogu**.
7. Opcjonalne: W polu **Maksymalna liczba pozycji** (Maximum entries) określ maksymalną liczbę pozycji, jaka może znajdować się w protokole zmian. W polu **Maksymalny wiek** określ, jak długo przechowywane będą pozycje protokołu zmian.

**Uwaga:** Choć parametry te są opcjonalne, należy wziąć pod uwagę określenie maksymalnej liczby pozycji lub maksymalnego wieku. Jeśli nie zostaną one określone, protokół zmian będzie zawierał wszystkie pozycje i może stać się zbyt duży.

Klasa obiektu `changeLogEntry` reprezentuje zmiany zastosowane w serwerze katalogów. Zestaw zmian jest podany w postaci uporządkowanego zestawu wszystkich pozycji znajdujących się w kontenerze protokołu zmian, zgodnie z definicją w parametrze `changeNumber` (liczba zmian). Informacje w protokole zmian są tylko do odczytu.

Dowolny użytkownik znajdujący się na liście ACL dla przyrostka `cn=changelog` może wyszukiwać pozycje w protokole zmian. Dla przyrostka protokołu zmian `cn=changelog` można przeprowadzać tylko wyszukiwanie. Nie należy próbować dodawać, zmieniać ani usuwać przyrostka protokołu zmian nawet wtedy, gdy posiada się stosowne uprawnienia. Może to wywołać nieprzewidywalne skutki.

### Przykład:

W poniższym przykładzie zastosowano program narzędziowy wiersza komend **ldapsearch** w celu wczytania wszystkich pozycji protokołu zmian zarejestrowanych na serwerze:

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

## Włączanie kontrolowania obiektów na serwerze Directory Server

Ten temat zawiera informacje dotyczące włączania kontrolowania obiektów na serwerze Directory Server.

Serwer Directory Server obsługuje funkcje kontroli bezpieczeństwa systemu i5/OS. Jeśli w wartości systemowej QAUDCTL podano parametr \*OBJAUD, to można włączyć kontrolowanie obiektów za pomocą programu System i Navigator.

Aby włączyć kontrolowanie obiektów na serwerze Directory Server, należy wykonać następujące czynności:

1. W programie System i Navigator rozwiń pozycję **Sieć**.
2. Rozwiń pozycję **Serwery**.
3. Kliknij **TCP/IP**.
4. Prawym przyciskiem myszy kliknij **IBM Directory Server** i wybierz **Właściwości**.
5. Kliknij zakładkę **Kontrola**.
6. Wybierz ustawienia kontroli dla serwera.
7. Kliknij przycisk **OK**.

Zmiany ustawień kontroli odniosą skutek natychmiast po kliknięciu przycisku **OK**, nie trzeba restartować serwera Directory Server.

### Pojęcia pokrewne

“Kontrola” na stronie 51

Kontrola umożliwia śledzenie szczegółów określonych transakcji serwera Directory Server.

“Bezpieczeństwo serwera Directory Server” na stronie 51

Informacje o funkcjach służących do zabezpieczania serwera Directory Server.

## Dopasowywanie ustawień wyszukiwania

Ten temat zawiera informacje dotyczące określania możliwości użytkowników w zakresie wyszukiwania.

Można ustawić parametry wyszukiwania określające możliwości użytkowników w zakresie wyszukiwania, na przykład wyszukiwanie na stronie i wyszukiwanie z sortowaniem, limit czasu i wielkości oraz opcje wyłuskiwania aliasów za pomocą narzędzia Web Administration.

Wyniki podzielone na strony pozwalają klientowi zarządzać dużą ilością danych zwracanych przez żądanie wyszukiwania. Zamiast jednorazowego odbierania wszystkich rezultatów klient może zażądać podzbioru pozycji (strony). Kolejne żądania wyszukiwania wyświetlają następną stronę wyników do momentu anulowania operacji lub zwrócenia ostatniego wyniku.

Wyszukiwanie z sortowaniem umożliwia klientowi uzyskanie wyników wyszukiwania posortowanych na podstawie listy kryteriów, gdzie każde kryterium stanowi klucz sortowania. Przenosi to odpowiedzialność za sortowanie z aplikacji klienckiej na serwer.

Aby dostosować ustawienia wyszukiwania na serwerze katalogów, wykonaj następujące czynności:

1. Rozwiń kategorię **Server administration** (Administrowanie serwerem) w obszarze nawigacyjnym i wybierz **Manage server properties** (Zarządzaj właściwościami serwera).

**Uwaga:** Aby zmienić konfigurację serwera za pomocą zadań w kategorii Server administration (Administrowanie serwerem) w narzędziu Web Administration, należy uwierzytelnić się na serwerze jako profil użytkownika systemu i5/OS z uprawnieniami specjalnymi \*ALLOBJ i IOSYSCFG. Można to zrobić, dokonując uwierzytelnienia jako użytkownik rzutowany i używając hasła dla tego profilu. Aby nawiązać połączenie jako użytkownik rzutowany z poziomu narzędzia Web Administration, należy wprowadzić nazwę użytkownika w postaci `os400-profile=MOJANAZWAUŻYTKOWNIKA,cn=accounts,os400-sys=MÓJSYSTEM.PL`, gdzie łańcuchy znaków MOJANAZWAUŻYTKOWNIKA i MÓJSYSTEM.PL zastępowane są odpowiednio nazwą profilu użytkownika i skonfigurowanym przyrostkiem rzutowania.

2. Wybierz zakładkę **Search settings** (Ustawienia wyszukiwania).
3. Ustaw **Search size limit** (Limit wielkości wyszukiwania). Kliknij przełącznik **Entries** (Pozycje) lub **Unlimited** (Nieograniczona). Zaznaczenie **Entries** (Pozycje) wymaga określenia w danym polu maksymalnej liczby pozycji zwracanych przez wyszukiwanie. Ustawieniem domyślnym jest 500. Jeśli więcej pozycji spełnia kryteria wyszukiwania, nie są one zwracane. Ograniczenie to nie ma zastosowania wobec administratorów i członków grup ograniczonego wyszukiwania, którym nadano większe limity wielkości wyszukiwania.
4. Ustaw **Search time limit** (Limit czasu wyszukiwania). Kliknij przełącznik **Seconds** (Sekundy) lub **Unlimited** (Nieograniczony). Zaznaczenie **Seconds** (Sekundy) wymaga określenia w danym polu maksymalnej ilości czasu, jaką serwer przeznaczyć ma na przetwarzanie żądania. Ustawieniem domyślnym jest 900. Ograniczenie to nie ma zastosowania wobec administratorów i członków grup ograniczonego wyszukiwania, którym nadano większe limity czasu wyszukiwania.
5. Aby zastrzec możliwość sortowania wyszukiwania jedynie dla administratorów, zaznacz pole wyboru **Only allow administrators to sort searches** (Zezwalaj tylko administratorom na sortowanie wyszukiwania).
6. Aby zastrzec możliwość wyszukiwania na stronie jedynie dla administratorów, zaznacz pole wyboru **Only allow administrators to page searches** (Zezwalaj tylko administratorom na wyszukiwanie na stronie).
7. Rozwiń menu **Alias dereferencing** i zaznacz jedną z następujących opcji. Ustawieniem domyślnym jest **Always** (Zawsze).

#### **Never (Nigdy)**

Aliasy nigdy nie są wyłuskiwane.

#### **Find (Odnajdywanie)**

Aliasy wyłuskiwane są po odnalezieniu punktu początkowego wyszukiwania, ale nie podczas wyszukiwania pod tą pozycją początkową.

#### **Wyszukiwanie**

Aliasy wyłuskiwane są podczas wyszukiwania poniżej punktu początkowego wyszukiwania, ale nie podczas odnajdywania pozycji początkowej.

### **Always (Zawsze)**

Aliasy zawsze są wyłuskiwane, zarówno podczas odnajdywania punktu początkowego wyszukiwania, jak i podczas wyszukiwania poniżej pozycji początkowej. Always (Zawsze) jest ustawieniem domyślnym.

### **Zadania pokrewne**

“Wyszukiwanie pozycji w katalogu” na stronie 200

Ten temat zawiera informacje dotyczące wyszukiwania pozycji w katalogu.

### **Odsyłacze pokrewne**

“Parametry wyszukiwania” na stronie 47

Aby ograniczyć ilość zasobów używanych przez serwer, administrator może ustawić parametry wyszukiwania tak, aby ograniczyć możliwości wyszukiwania przez użytkowników. Możliwości wyszukiwania mogą także zostać rozszerzone dla specjalnych użytkowników.

## **Włączanie i wyłączanie dostępu do odczytu profili użytkowników rzutowanych**

Aby uniemożliwić operacje wyszukiwania i porównywania w mechanizmie rzutowania użytkowników, należy skorzystać z poniższych informacji.

Aby uniemożliwić operacje wyszukiwania i porównywania w mechanizmie rzutowania użytkowników, należy wykonać następujące czynności:

1. Zakończ pracę serwera katalogów. Wpisz komendę `ENDTCPSVR *DIRSRV`.
2. Edytuj plik `/QIBM/UserData/OS400/DirSrv/ibmslapd.conf`. Na przykład wpisz `EDTF '/QIBM/UserData/OS400/DirSrv/ibmslapd.conf'`.
3. Wyszukaj tekst `cn=Front End`.
4. Wstaw nowy wiersz zawierający tekst `ibm-slapdSetEnv: IBMSLAPDOS400USRPRJREAD=FALSE` tuż pod wierszem zawierającym tekst `cn=Front End`. W następującym przykładzie wstawiono drugi wiersz:  

```
dn: cn=Front End, cn=Configuration  
ibm-slapdSetEnv: IBMSLAPDOS400USRPRJREAD=FALSE  
cn: Front End
```
5. Zapisz plik i wyjdź z edytora. Na przykład, jeśli używasz edytora EDTF, naciśnij klawisz F2, aby zapisać plik, a następnie klawisz F3, aby wyjść z edytora.
6. Zrestartuj serwer katalogów. Wpisz komendę `STRTCPSVR *DIRSRV`.

### **Pojęcia pokrewne**

“Dostęp do odczytu profili użytkowników rzutowanych” na stronie 89

Domyślnie systemowy mechanizm rzutowania umożliwia autoryzowanym użytkownikom dostęp do odczytu informacji o profilach użytkowników przez operacje wyszukiwania i porównywania LDAP. Dostęp do odczytu informacji o profilach użytkowników rzutowanych można włączać i wyłączać za pomocą programu System i Navigator lub ustawienia konfiguracyjnego w pliku `/QIBM/UserData/OS400/DirSrv/idsslapd-instance/etc/ibmslapd.conf` (`/QIBM/UserData/OS400/DirSrv/idsslapd-QUSRDIR/etc/ibmslapd.conf` w przypadku domyślnej instancji serwera).

## **Publikowanie informacji na serwerze Directory Server**

W tym temacie opisano publikowanie informacji na serwerze Directory Server.

System można skonfigurować tak, aby publikował określone informacje oraz informacje zdefiniowane przez użytkownika na serwerze Directory Server znajdującym się w tym samym lub w innym systemie. System operacyjny automatycznie publikuje informacje na serwerze Directory Server, gdy użytkownik zmieni te informacje w systemie i5/OS za pomocą programu System i Navigator. Można publikować między innymi informacje o systemie (systemy i drukarki), współużytkowanych zasobach drukarkowych, użytkownikach oraz strategiach jakości usługi (QoS) TCP/IP.

Jeśli nadrzędna nazwa wyróżniająca, do której dane są publikowane, nie istnieje, serwer Directory Server utworzy ją automatycznie. Możliwe, że zainstalowano inne aplikacje systemu i5/OS, które publikują informacje w katalogu LDAP. Można także wywoływać funkcje API z własnych programów w celu publikowania w katalogach LDAP innych typów informacji.

**Uwaga:** Można także opublikować informacje systemu i5/OS na serwerze katalogów, który nie działa w systemie i5/OS, pod warunkiem skonfigurowania tego serwera tak, aby korzystał ze schematu IBM.

Aby skonfigurować system do publikowania informacji i5/OS na serwerze katalogów, należy wykonać następujące czynności:

1. W programie System i Navigator kliknij prawym przyciskiem myszy swój system i wybierz opcję **Właściwości**.
2. Kliknij zakładkę **Directory Server**.
3. Wybierz typy informacji, które mają być publikowane. Wybierz typy informacji, które mają być publikowane.

**Wskazówka:** Jeśli zamierzasz publikować do tego samego miejsca więcej niż jeden typ informacji, możesz zaoszczędzić czas, konfigurując jednocześnie wiele rodzajów informacji. iSeries Navigator użyje wówczas wartości wpisanych w trakcie konfigurowania jednego typu informacji jako domyślnych przy konfigurowaniu kolejnych typów.

4. Kliknij **Details** (Szczegóły).
5. Kliknij pole wyboru **Publish system information** (Publikuj informacje o systemie).
6. Określ **Authentication method** (Metodę uwierzytelniania), której serwer ma używać, i odpowiednie informacje uwierzytelniające.
7. Kliknij przycisk **Edit** (Edycja) obok pola **(Active) Directory server** ((Aktywny) Serwer LDAP). W wyświetlonym oknie dialogowym wpisz lub wybierz nazwę serwera katalogów, na którym mają być publikowane informacje i5/OS, a następnie kliknij przycisk **OK**.
8. W polu **Under DN** (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 **Server connection** (Połączenie serwera).

**Uwaga:** Aby opublikować informacje systemu i5/OS na serwerze katalogów przy użyciu protokołu SSL lub Kerberos, należy najpierw skonfigurować serwer katalogów, aby korzystał z odpowiedniego protokołu. Więcej informacji dotyczących protokołów SSL i Kerberos zawiera sekcja “Uwierzytelnianie Kerberos w serwerze Directory Server” na stronie 53.

10. Jeśli serwer katalogów używa portu innego niż domyślny, w polu **Port** należy podać odpowiedni numer portu.
11. Kliknij opcję **Verify** (Sprawdź), aby upewnić się, czy nadrzędna nazwa wyróżniająca istnieje w danym serwerze i czy informacje o połączeniu są poprawne. Jeśli w katalogu nie ma potrzebnej ścieżki, zostanie wyświetlone okno dialogowe, w którym będzie trzeba ją utworzyć.

**Uwaga:** Jeśli nadrzędna nazwa wyróżniająca nie istnieje i nie zostanie utworzona, wówczas publikowanie nie powiedzie się.

12. Kliknij przycisk **OK**.

**Uwaga:** Można także opublikować informacje systemu i5/OS na serwerze katalogów, który działa na innej platformie. Informacje o użytkownikach i systemie należy opublikować na serwerze katalogów, który używa schematu kompatybilnego ze schematem serwera IBM Directory Server. Więcej informacji na temat schematu IBM Directory Schema zawiera sekcja “Schemat serwera Directory Server” na stronie 14.

Można także użyć funkcji API służących do konfigurowania serwera LDAP i publikowania w celu umożliwienia działającym pod kontrolą systemu i5/OS programom publikowania innych rodzajów informacji. Te rodzaje informacji można także wyświetlać na stronie **Directory Server**. Tak jak użytkownicy i systemy, początkowo 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 publikowanych informacji wyświetlanych na stronie **Directory Server** jest nazwą agenta.

Włączenie obsługi publikowania do własnych programów umożliwiają następujące funkcje API:

#### **QgldChgDirSvrA**

Aplikacja używa formatu CSVR0500, aby na początku dodać nazwę agenta zaznaczoną jako pozycja



nieaktywna. Instrukcje dla użytkowników aplikacji powinny informować, że aby skonfigurować agenta publikacji (publishing agent), należy korzystać z programu System i Navigator, w celu przejścia na stronę właściwości serwera Directory Server. Przykładami nazw agentów są nazwy agentów systemów i użytkowników automatycznie dostępne na stronie serwera **Directory Server**.

### **QgldLstDirSvrA**

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

### **QgldPubDirObj**

Ta funkcja API służy do faktycznego publikowania informacji.

#### **Pojęcia pokrewne**

“Publikowanie” na stronie 36

Serwer Directory Server umożliwia publikowanie przez system określonych rodzajów informacji w katalogu LDAP. Innymi słowy, system utworzy i zaktualizuje pozycje LDAP reprezentujące różne typy danych.

Funkcje API serwera Directory Server

## **Importowanie pliku LDIF**

W tym temacie opisano importowanie pliku w formacie LDIF (LDAP Data Interchange Format).

Informacje można przenosić między różnymi serwerami Directory Server za pomocą plików w formacie LDIF (LDAP Data Interchange Format). Do dodawania nowych wpisów do katalogu służy narzędzie importu (i odpowiadająca mu funkcja API QgldImportLdif). Narzędzie importu nie może być używane do modyfikowania ani usuwania pozycji, a rekordy w importowanym pliku LDIF powinny być zapisane w formacie zawartości katalogu, a nie w formacie modyfikowania rekordów. Jeśli plik wejściowy LDIF zawiera dyrektywy changetype używane w formacie modyfikowania rekordów, każdy wiersz zawierający dyrektywę changetype zostanie zinterpretowany jako atrybut, a pozycja nie zostanie dodana do katalogu.

Typowe użycie polega na eksportowaniu całego katalogu lub poddrzewa katalogu z jednego serwera za pomocą narzędzia eksportu (lub funkcji API QgldExportLdif), a następnie importowaniu go do innego serwera.

Narzędzia eksportu i importu nie są równoważne wykorzystaniu narzędzi wiersza komend ldapsearch i ldapadd. Narzędzie eksportu udostępnia kilka atrybutów operacyjnych, które nie są na ogół zwracane przez komendę ldapsearch (w tym informacje o kontroli dostępu i datowniki utworzenia rekordów), a narzędzie importu umożliwia ustawianie atrybutów, które w normalnych warunkach nie mogą być ustawiane przez aplikację kliencką, jaką jest ldapadd. Pliki takie można załadować, uruchamiając narzędzie ldapadd z opcją -k (administrowanie serwerem).

Przed rozpoczęciem tej procedury należy przesłać plik LDIF na używany system jako plik strumieniowy.

Aby zaimportować plik LDIF do serwera Directory Server, wykonaj następujące czynności:

1. Jeśli serwer katalogów jest uruchomiony, zatrzymaj go. Informacje o tym, jak zatrzymać serwer katalogów, zawiera sekcja “Uruchamianie serwera Directory Server” na stronie 116.
2. W programie System i Navigator rozwiń pozycję **Sieć**.
3. Rozwiń pozycję **Serwery**.
4. Kliknij **TCP/IP**.
5. Prawym przyciskiem myszy kliknij element **IBM Directory Server** i wybierz opcję **Narzędzia** (Tools), a następnie opcję **Importuj plik** (Import file).

Opcjonalnie serwer może replikować nowo zaimportowane dane podczas następnego uruchomienia poprzez wybranie opcji **Replikuj importowane dane**. Jest to użyteczne podczas dodawania nowych pozycji do istniejącego drzewa katalogów na serwerze głównym. W przypadku importowania danych do zainicjowania serwera replik (lub równorzędnego) zazwyczaj replikacja danych jest niepożądana, ponieważ mogą już one istnieć na serwerach, dla których ten serwer jest serwerem wysyłającym.

**Uwaga:** Do importowania plików LDIF można również użyć programu narzędziowego ldapadd.

#### **Odsyłacze pokrewne**

“Format wymiany danych LDAP (LDIF)” na stronie 251

Format wymiany danych LDAP (LDAP Data Interchange Format - LDIF) to standardowy format używany do tekstowego zapisu reprezentacji obiektów LDAP i operacji na obiektach LDAP (dodawanie, modyfikowanie, usuwanie, zmiana nazwy wyróżniającej). Pliki zawierające rekordy LDIF mogą być używane do przenoszenia danych między serwerami katalogów lub podawane jako dane wejściowe programów narzędziowych LDAP, takich jak **ldapadd** i **ldapmodify**.

“ldapmodify i ldapadd” na stronie 218

Programy narzędziowe wiersza komend służące do dodawania i modyfikowania pozycji w katalogu LDAP.

## Eksportowanie pliku LDIF

W tym temacie opisano eksportowanie pliku w formacie LDIF (LDAP Data Interchange Format).

Możliwe jest przenoszenie informacji między różnymi plikami LDIF. Do pliku LDIF można eksportować cały katalog LDAP lub jego część.

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

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

**Uwaga:** Jeśli nie zostanie podana pełna ścieżka pliku LDIF do eksportowania danych, plik zostanie utworzony w katalogu osobistym określonym w profilu użytkownika systemu operacyjnego.

5. W zależności od potrzeb zaznacz opcje **Eksportuj cały katalog** lub **Eksportuj zaznaczone poddrzewo** oraz opcję **Eksportuj atrybuty wykonawcze**. Eksportowane są następujące atrybuty wykonawcze: creatorsName, createTimestamp, modifiersName i modifyTimestamp.

### Uwagi:

1. Podczas eksportowania danych do zaimportowania do serwera katalogów w wersji V5R3 lub wersji wcześniejszej, nie należy zaznaczać opcji **Eksportuj atrybuty wykonawcze**. Tych atrybutów wykonawczych nie można zaimportować do serwera katalogów w wersji V5R3 lub wersji wcześniejszej.
2. Można także utworzyć pełny lub częściowy plik LDIF, używając programu narzędziowego ldapsearch. Użyj opcji -L i przekieruj dane wyjściowe do pliku.
3. Upewnij się, że ustawione są odpowiednie uprawnienia do pliku LDIF, co zapobiegnie nieuprawnionemu dostępowi do danych katalogu. Aby to zrobić, kliknij plik prawym przyciskiem myszy w programie System i Navigator, a następnie wybierz opcję **Uprawnienia**.

### Odsyłacze pokrewne

“Format wymiany danych LDAP (LDIF)” na stronie 251

Format wymiany danych LDAP (LDAP Data Interchange Format - LDIF) to standardowy format używany do tekstowego zapisu reprezentacji obiektów LDAP i operacji na obiektach LDAP (dodawanie, modyfikowanie, usuwanie, zmiana nazwy wyróżniającej). Pliki zawierające rekordy LDIF mogą być używane do przenoszenia danych między serwerami katalogów lub podawane jako dane wejściowe programów narzędziowych LDAP, takich jak **ldapadd** i **ldapmodify**.

“ldapsearch” na stronie 236

Program narzędziowy wiersza komend do wyszukiwania w katalogu LDAP.

## Kopiowanie użytkowników z listy sprawdzania serwera HTTP do serwera Directory Server

Ten temat zawiera informacje dotyczące kopiowania użytkowników z listy sprawdzania serwera HTTP do serwera Directory Server.

Jeśli użytkownik korzysta obecnie z serwera HTTP lub używał go w przeszłości, mógł on utworzyć listy sprawdzania przechowujące użytkowników Internetu i ich hasła. Przejście do aplikacji WebSphere Application Server, Portal Server i innych aplikacji obsługujących uwierzytelnianie LDAP może wiązać się z potrzebą dalszego wykorzystania istniejących użytkowników i ich haseł. Można skorzystać z funkcji API "Kopiowanie listy sprawdzania do katalogu" (Copy Validation List to Directory - QGLDCPYVL).

Komenda QGLDCPYVL odczytuje pozycje z listy sprawdzania i tworzy odpowiadające im obiekty LDAP na lokalnym serwerze katalogów. Obiekty są szkieletowymi pozycjami inetOrgPerson z atrybutem userPassword, który zawiera kopię informacji o hasle z pozycji na liście sprawdzania. Użytkownik decyduje kiedy i w jaki sposób funkcja API jest wywoływana. Można użyć jej jako pojedynczego działania dla listy sprawdzania, która nie będzie zmieniana lub jako zaplanowanego zadania aktualizującego serwer katalogów w celu odzwierciedlenia nowych pozycji listy sprawdzania.

Na przykład:

```
CALL PGM(QSYS/QGLDCPYVL) PARM('HTTPVLDL MYLIB ' 'cn=administrator'  
X'00000000' 'sekret' X'00000000' 'cn=users,o=moje przedsiebiorstwo' X'00000000' '' X'00000000'  
X'00000000')
```

#### Pojęcia pokrewne

Funkcje API protokołu LDAP

Temat Funkcje API protokołu LDAP zawiera więcej informacji o funkcjach API serwera katalogów.

#### Zadania pokrewne

“Scenariusz: kopiowanie użytkowników z listy sprawdzania serwera HTTP do serwera Directory Server” na stronie 114

Przykład kopiowania użytkowników z listy sprawdzania serwera HTTP do serwera Directory Server.

## Zarządzanie instancjami

W systemie i5/OS może funkcjonować wiele serwerów katalogów. Każdy serwer jest nazywany instancją. Jeśli korzystano z serwera katalogów we wcześniejszej wersji systemu i5/OS, zostanie on migrowany do instancji o nazwie QUSRDIR. Na potrzeby obsługi aplikacji można tworzyć wiele instancji serwera katalogów.

Unikalność poszczególnych instancji serwera katalogów jest określona przez adres IP i/lub port, na którym zgodnie z konfiguracją nasłuchuje dana instancja. Każda uruchomiona instancja serwera katalogów musi też posiadać unikalną bazę danych, protokół zmian i plik konfiguracyjny. System nie zapobiega tworzeniu i konfigurowaniu instancji serwerów w sposób powodujący konflikty, jednak w razie próby uruchomienia instancji serwera, która jest w konflikcie z inną aktywną instancją, instancja ta nie zostanie uruchomiona i zostanie zwrócony komunikat o błędzie.

Instancja serwera katalogów zawiera wszystkie pliki niezbędne do funkcjonowania serwera katalogów na komputerze.

Do plików instancji serwera katalogów należą:

- ibmslapd.conf (plik konfiguracyjny),
- pliki schematów,
- pliki protokołów,
- tymczasowe pliki statusu.

Pliki instancji serwera katalogów są składowane w katalogu o nazwie *idsslapd-nazwa\_instancji*, gdzie *nazwa\_instancji* jest nazwą instancji serwera katalogów. Katalog *idsslapd-nazwa\_instancji* znajduje się w katalogu */QIBM/UserData/OS400/DirSrv*.

Każda instancja serwera katalogów jest w chwili utworzenia rejestrowana jako nowa aplikacja w programie Digital Certificate Manager (DCM). Nowe instancje serwera katalogów mają nazwy postaci *QIBM\_DIRECTORY\_SERVER\_<nazwa\_instancji>*. Jeśli planowane jest używanie szyfrowania SSL, należy za pomocą programu DCM przypisać certyfikat cyfrowy do instancji serwera katalogów. Każda instancja serwera katalogów w chwili uruchomienia rejestruje się w programie System i Navigator jako serwer, co umożliwia jej śledzenie za pomocą tego programu.

l Nazwa zadania odpowiadającego instancji serwera katalogów jest taka sama, jak nazwa instancji. Na przykład pełna kwalifikowana nazwa zadania dla instancji QUSRDIR będzie miała postać xxxxxx/QDIRSRV/QUSRDIR. Ciąg 'xxxxxx' to numer zadania, który jest określany w chwili uruchomienia zadania. Nazwa zadania jest tworzona w inny sposób niż we wcześniejszej wersji serwera katalogów, w której nazwa zadania miała postać xxxxxx/QDIRSRV/QDIRSRV.

l Aby zarządzać instancjami, należy wykonać następujące czynności:

1. W programie System i Navigator rozwiń pozycję **Sieć**.
2. Rozwiń pozycję **Serwery**.
3. Kliknij **TCP/IP**.
4. Prawym przyciskiem myszy kliknij element **IBM Tivoli Directory Server** i wybierz opcję **Zarządzaj instancjami** (Manage Instances).

l Jeśli planowane jest okresowe składowanie instancji, należy wraz z katalogiem zawierającym bazę danych składać bibliotekę <nazwa\_instancji>CF.

## Zadania grupy administracyjnej

Ten temat zawiera informacje dotyczące zarządzania grupami administracyjnymi.

Grupa administracyjna udostępnia możliwość nadania uprawnień administracyjnych bez konieczności współużytkownika przez administratorów pojedynczego identyfikatora i hasła. Członkowie grupy administracyjnej posiadają własne unikalne identyfikatory i hasła. Nazwy wyróżniające członków grupy administracyjnej nie mogą być zgodne ze sobą i nie mogą być zgodne z nazwą wyróżniającą administratora serwera IBM Directory Server. Podobnie, nazwa wyróżniająca administratora serwera IBM Directory Server nie może być zgodna z nazwą wyróżniającą żadnego z członków grupy administracyjnej.

Ta reguła ma również zastosowanie w przypadku administratora serwera IBM Directory Server i członków grupy administracyjnej w odniesieniu do identyfikatorów Kerberos lub Digest-MD5. Te nazwy wyróżniające nie mogą być zgodne z żadną z nazw wyróżniających serwera wysyłającego replikacji na serwerze IBM Directory Server. Oznacza to również, że nazwa wyróżniająca serwera wysyłającego replikacji na serwerze IBM Directory Server nie może być zgodna z żadną z nazw wyróżniających członków grupy administracyjnej lub z nazwą wyróżniającą administratora serwera IBM Directory Server.

**Uwaga:** Nazwy wyróżniające serwerów wysyłających na serwerze IBM Directory Server mogą być zgodne ze sobą.

### Pojęcia pokrewne

“Dostęp administracyjny” na stronie 63

Dostęp administracyjny służy do kontrolowania praw dostępu do konkretnych zadań administracyjnych.

## Włączanie grupy administracyjnej

Ten temat zawiera informacje dotyczące włączania grupy administracyjnej.

Aby wykonać to działanie, użytkownik musi być administratorem serwera IBM Directory Server.

1. W obszarze nawigacyjnym narzędzia Web Administration rozwiń węzeł **Server administration** (Administrowanie serwerem) i kliknij element **Manage administrative group** (Zarządzaj grupą administracyjną).

**Uwaga:** Aby zmienić konfigurację serwera za pomocą zadań w kategorii Server administration (Administrowanie serwerem) w narzędziu Web Administration, należy uwierzytelnić się na serwerze jako profil użytkownika systemu i5/OS z uprawnieniami specjalnymi \*ALLOBJ i IOSYSCFG. Można to zrobić, dokonując uwierzytelnienia jako użytkownik rzutowany i używając hasła dla tego profilu. Aby nawiązać połączenie jako użytkownik rzutowany z poziomu narzędzia Web Administration, należy wprowadzić nazwę użytkownika w postaci os400-profile=MOJANAZWAUŻYTKOWNIKA,cn=accounts,os400-sys=MÓJSYSTEM.PL, gdzie łańcuchy znaków MOJANAZWAUŻYTKOWNIKA i MÓJSYSTEM.PL zastępowane są odpowiednio nazwą profilu użytkownika i skonfigurowanym przyrostkiem rzutowania.

2. Aby włączyć lub wyłączyć grupę administracyjną, kliknij pole wyboru obok pola **Enable administrative group** (Włącz grupę administracyjną). Jeśli pole wyboru jest zaznaczone, grupa administracyjna jest włączona.
3. Kliknij przycisk **OK**.

**Uwaga:** Jeśli grupa administracyjna zostanie wyłączona, zalogowany członek grupy administracyjnej może kontynuować wykonywanie działań administracyjnych do momentu, kiedy konieczne będzie ponowne połączenie.

## Dodawanie, edytowanie i usuwanie członków grupy administracyjnej

Ten temat zawiera informacje dotyczące dodawania, edytowania i usuwania członków grupy administracyjnej.

**Wymaganie wstępne:** aby wykonać to działanie, użytkownik musi być administratorem serwera IBM Directory Server.

1. W obszarze nawigacyjnym narzędzia Web Administration rozwiń węzeł **Server administration** (Administrowanie serwerem) i kliknij element **Manage administrative group** (Zarządzaj grupą administracyjną).

**Uwaga:** Aby zmienić konfigurację serwera za pomocą zadań w kategorii Server administration (Administrowanie serwerem) w narzędziu Web Administration, należy uwierzytelnić się na serwerze jako profil użytkownika systemu i5/OS z uprawnieniami specjalnymi \*ALLOBJ i IOSYSCFG. Można to zrobić, dokonując uwierzytelnienia jako użytkownik rzutowany i używając hasła dla tego profilu. Aby nawiązać połączenie jako użytkownik rzutowany z poziomu narzędzia Web Administration, należy wprowadzić nazwę użytkownika w postaci `os400-profile=MOJANAZWAUŻYTKOWNIKA,cn=accounts,os400-sys=MÓJSYSTEM.PL`, gdzie łańcuchy znaków MOJANAZWAUŻYTKOWNIKA i MÓJSYSTEM.PL zastępowane są odpowiednio nazwą profilu użytkownika i skonfigurowanym przyrostkiem rzutowania.

2. W panelu **Manage administrative group** (Zarządzanie grupą administracyjną) kliknij przycisk **Add** (Dodaj).
3. W panelu **Add administrative group member** (Dodawanie członka grupy administracyjnej):
  - a. Wprowadź nazwę wyróżniającą administratora dla członka grupy (musi mieć ona poprawną składnię).
  - b. Wprowadź hasło dla członka grupy.
  - c. Wprowadź hasło ponownie w celu potwierdzenia.
  - d. Opcjonalne: Wpisz identyfikator Kerberos członka grupy. Identyfikator Kerberos musi mieć format `ibm-kn` lub `ibm-KerberosName`. Wartości nie uwzględniają rozróżniania wielkości liter. Na przykład, wartość `ibm-kn=root@TEST.ROCHESTER.IBM.COM` jest odpowiednikiem wartości `ibm-kn=ROOT@TEST.ROCHESTER.IBM.COM`.
4. Opcjonalne: Wpisz **nazwę użytkownika Digest-MD5** członka grupy.

**Uwaga:** Nazwa użytkownika Digest-MD5 uwzględnia rozróżnianie wielkości liter.

5. Kliknij przycisk **OK**.
6. Powtórz tę procedurę dla wszystkich członków, którzy mają zostać dodani do grupy administracyjnej.

Nazwa wyróżniająca administratora, nazwa użytkownika Digest-MD5 (jeśli została określona) oraz identyfikator Kerberos (jeśli został określony) wyświetlone są w polu listy członków grupy administracyjnej.

Aby zmienić lub usunąć członków grupy administracyjnej, należy wykonać tę samą procedurę stosując przyciski **Edit** (Edytuj) oraz **Delete** (Usuń) w panelu **Manage administrative group** (Zarządzanie grupą administracyjną).

- | Hasło członka grupy administracyjnej można także zmienić za pomocą komendy Zmiana atrybutów serwera katalogów (Change Directory Server Attributes - CHGDIRSVRA). Aby zmienić hasło członka grupy administracyjnej z nazwą wyróżniającą łączenia `cn=adminuser1` na "nowehasło", należy użyć następującej komendy:
- | `CHGDIRSVRA INSTANCE(QUSRDIR) DN('cn=adminuser1' 'nowehasło')`

## Zadania związane z grupami ograniczonego wyszukiwania

Ten temat zawiera informacje dotyczące zarządzania grupami ograniczonego wyszukiwania.

Aby zapobiec pochłanianiu zbyt dużej ilości zasobów przez żądania wyszukiwania klientów i zmniejszeniu wydajności serwera, można narzucić ograniczenia żądań wyszukiwania dla dowolnego serwera. Administrator ustawia te ograniczenia dla wielkości i czasu trwania działań wyszukiwania podczas konfigurowania serwera.

Jedynie administrator i członkowie grupy administracyjnej są wolni od tych ograniczeń, które mają zastosowanie dla pozostałych użytkowników. Jednak w zależności od potrzeb, administrator może utworzyć grupy ograniczonego wyszukiwania posiadające bardziej elastyczne ograniczenia wyszukiwania niż zwykli użytkownicy. W ten sposób, administrator może nadać specjalne przywileje wyszukiwania grupie użytkowników.

Do zarządzania grupami ograniczonego wyszukiwania używane jest narzędzie Web Administration.

### Odsyłacze pokrewne

“Parametry wyszukiwania” na stronie 47

Aby ograniczyć ilość zasobów używanych przez serwer, administrator może ustawić parametry wyszukiwania tak, aby ograniczyć możliwości wyszukiwania przez użytkowników. Możliwości wyszukiwania mogą także zostać rozszerzone dla specjalnych użytkowników.

## Tworzenie grupy ograniczonego wyszukiwania

Ten temat zawiera informacje dotyczące tworzenia grupy ograniczonego wyszukiwania.

Aby utworzyć grupę ograniczonego wyszukiwania, pozycja grupy musi zostać utworzona za pomocą narzędzia Web Administration.

1. W obszarze nawigacyjnym rozwiń kategorię **Directory management** (Zarządzanie katalogiem) i kliknij opcję **Add an entry** (Dodaj pozycję). Można także kliknąć **Manage entries** (Zarządzaj pozycjami) i wybrać miejsce (cn=IBMpolicies lub cn=localhost), a następnie kliknąć **Add** (Dodaj). Pozycje w cn=IBMpolicies będą replikowane, pozycje w cn=localhost, nie.
2. Wybierz klasy obiektu z menu **Structural object class** (Strukturalna klasa obiektu).
3. Kliknij przycisk **Next** (Dalej).
4. Wybierz pomocniczą klasę obiektu **ibm-searchLimits** z menu **Available** (Dostępne) i kliknij **Add** (Dodaj). Powtórz tę czynność dla każdej dodatkowej pomocniczej klasy obiektu, która powinna zostać dodana. Pomocnicza klasa obiektu może zostać usunięta z menu **Selected** (Wybrane) poprzez zaznaczenie jej i kliknięcie **Remove** (Usuń).
5. Kliknij przycisk **Next** (Dalej).
6. W polu **Relative DN** (Nazwa RDN) wpisz względną nazwę wyróżniającą (RDN) dodawanej grupy. Na przykład, cn=Search Group1.
7. W polu **Parent DN** (Nadrzędna nazwa DN) wpisz nazwę wyróżniającą wybranej pozycji drzewa. Na przykład, cn=localhost. Możesz także kliknąć przycisk **Browse** (Przeglądaj), aby wybrać z nadrzędną nazwą DN z listy. Dokonaj wyboru i kliknij **Select** (Wybierz), aby określić nadrzędną nazwę wyróżniającą. Domyślną nadrzędną nazwą wyróżniającą (**Parent DN**) jest pozycja wybrana w drzewie.

**Uwaga:** Jeśli wykonywanie tego zadania zostało rozpoczęte na panelu **Manage entries** (Zarządzanie pozycjami), pole to jest już wypełnione. Opcja **Parent DN** (Nadrzędna nazwa DN) wybrano przed kliknięciem przycisku **Add** (Dodaj) w celu rozpoczęcia procesu dodawania pozycji.

8. W zakładce **Required attributes** (Atrybuty wymagane) wprowadź wartości atrybutów wymaganych.
  - **cn** to względna nazwa wyróżniająca określona wcześniej.
  - W polu **ibm-searchSizeLimit** określ liczbę pozycji, według której wielkość wyszukiwania ma zostać ograniczona. Liczba ta może przybierać wartości z zakresu od 0 do 2147483647. Ustawienie 0 daje ten sam efekt, co **Unlimited** (Nieograniczone).
  - W polu **ibm-searchTimeLimit** określ liczbę sekund, według której czas trwania wyszukiwania ma zostać ograniczony. Liczba ta może przybierać wartości z zakresu od 0 do 2147483647. Ustawienie 0 daje ten sam efekt, co **Unlimited** (Nieograniczone).
  - W zależności od zaznaczonej klasy obiektu widoczne może być pole **Member** (Członek) lub **uniqueMember** (unikalny\_członek). Są to członkowie tworzonej grupy. Ta pozycja ma postać nazwy wyróżniającej, na przykład cn=Bob Garcia,ou=austin,o=ibm,c=us.

9. Jeśli chcesz wpisać więcej niż jedną wartość określonego atrybutu, kliknij przycisk **Multiple values** (Wartości wielokrotne), a następnie dodaj wszystkie wartości, po jednej w wierszu. Po zakończeniu dodawania wartości wielokrotnych kliknij przycisk **OK**. Wartości są dodawane do rozwijanego menu wyświetlanego dla atrybutu.
10. Jeśli na serwerze włączona jest funkcja znaczników języka, kliknij **Language tag value** (Wartość znacznika języka), aby dodać lub usunąć deskryptory znaczników języka.
11. Kliknij zakładkę **Other attributes** (Inne atrybuty).
12. W zakładce **Other attributes** (Inne atrybuty) wprowadź odpowiednie wartości atrybutów. Więcej informacji zawiera temat “Zmiana atrybutów binarnych” na stronie 202.
13. Kliknij przycisk **Finish** (Zakończ), aby utworzyć pozycję.

## Zmiana grupy ograniczonego wyszukiwania

Ten temat zawiera informacje o modyfikowaniu grupy ograniczonego wyszukiwania.

Atrybuty wielkości i limitu czasu grupy ograniczonego wyszukiwania można zmieniać. Można także dodawać i usuwać członków grupy. Aby dokonać zmian w grupie ograniczonego wyszukiwania, należy użyć narzędzia z Web Administration.

1. Jeśli jeszcze tego nie zrobiono, rozwiń kategorię **Directory management** (Zarządzanie katalogami) w obszarze nawigacyjnym, a następnie kliknij przycisk **Manage entries** (Zarządzanie pozycjami). W celu wybrania pozycji, z którą chce się pracować, można rozwijać różne poddrzewa drzewa katalogu. Kliknij przycisk **Edit attributes** (Edycja atrybutów) znajdujący się na pasku narzędzi umieszczonym po prawej stronie.
2. Na karcie **Required attributes** (Atrybuty wymagane) wpisz wartości atrybutów wymaganych. Sekcja “Zmiana atrybutów binarnych” na stronie 202 zawiera informacje na temat dodawania wartości binarnych. Jeśli chcesz wpisać więcej niż jedną wartość określonego atrybutu, kliknij przycisk **Multiple values** (Wartości wielokrotne), a następnie dodaj wszystkie wartości, po jednej w wierszu.
3. Kliknij zakładkę **Optional attributes** (Atrybuty opcjonalne).
4. Na karcie **Optional attributes** (Atrybuty opcjonalne) wpisz odpowiednie wartości atrybutów opcjonalnych. Jeśli chcesz wpisać więcej niż jedną wartość określonego atrybutu, kliknij przycisk **Multiple values** (Wartości wielokrotne), a następnie dodaj wszystkie wartości, po jednej w wierszu.
5. Kliknij zakładkę **Memberships** (Przynależność do grup).
6. Jeśli utworzono grupy, to na karcie **Memberships** (Przynależność do grup):
  - Wybierz grupę z listy **Available groups** (Dostępne grupy) i kliknij przycisk **Add** (Dodaj), aby przypisać pozycję do wybranej grupy statycznej (**Static group membership**).
  - Wybierz grupę z listy **Static group memberships** (Członkostwo w grupach statycznych) i kliknij przycisk **Remove** (Usuń), aby usunąć pozycję z wybranej grupy.
7. Jeśli jest to pozycja grupowa, dostępna będzie zakładka **Members** (Elementy). Zakładka **Members** (Elementy) zawiera elementy wybranej grupy. Elementy można dodawać do grupy oraz ich z niej usuwać.
  - Aby dodać element do grupy:
    - a. Kliknij opcję **Multiple values** (Wiele wartości) obok zakładki **Members** (Elementy) lub na zakładce **Members** (Elementy) kliknij opcję **Members** (Elementy).
    - b. W polu Member (Element) wprowadź nazwę wyróżniającą pozycji, którą chcesz dodać.
    - c. Kliknij przycisk **Add** (Dodaj).
    - d. Kliknij przycisk **OK**.
  - Aby usunąć element z grupy:
    - a. Kliknij opcję **Multiple values** (Wiele wartości) obok zakładki **Members** (Elementy) lub na zakładce **Members** (Elementy) kliknij opcję **Members** (Elementy).
    - b. Wybierz pozycję do usunięcia.
    - c. Kliknij przycisk **Remove** (Usuń).
    - d. Kliknij przycisk **OK**.
  - Aby odświeżyć listę elementów, kliknij przycisk **Update** (Aktualizuj).
8. Kliknij przycisk **OK**, aby zmodyfikować pozycję.

## Kopiowanie grupy ograniczonego wyszukiwania

Ten temat zawiera informacje dotyczące kopiowania grupy ograniczonego wyszukiwania.

Skopiowanie grupy ograniczonego wyszukiwania może być pomocne, jeśli w obu pozycjach localhost i IBMpolicies ma znajdować się ta sama grupa ograniczonego wyszukiwania. Dotyczy to także sytuacji, kiedy ma zostać utworzona nowa grupa zawierająca podobne informacje jak istniejąca grupa z niewielkimi różnicami.

1. Jeśli jeszcze tego nie zrobiono, rozwiń kategorię **Directory management** (Zarządzanie katalogami) w obszarze nawigacyjnym, a następnie kliknij przycisk **Manage entries** (Zarządzanie pozycjami). Aby wybrać pozycję, z którą chcesz pracować, na przykład Jan Kowalski, możesz rozwijać różne poddrzewa. Kliknij przycisk **Copy** (Kopiuj) znajdujący się na pasku narzędzi umieszczonym po prawej stronie.
2. Zmień pozycję RDN w polu DN (Nazwa wyróżniająca). Na przykład zmień cn=Jan Kowalski na cn=Tomasz Nowak.
3. Na zakładce wymaganych atrybutów zmień pozycję cn na nową nazwę RDN. W tym przykładzie jest to Tomasz Nowak.
4. Zmień odpowiednie inne wymagane atrybuty. W tym przykładzie zmień atrybut z Kowalski na Nowak.
5. Po zakończeniu wprowadzania niezbędnych zmian kliknij przycisk **OK**, aby utworzyć nową pozycję. Nowa pozycja Tomasz Nowak zostanie dodana na końcu listy pozycji.

## Usuwanie grupy ograniczonego wyszukiwania

Ten temat zawiera informacje dotyczące usuwania grupy ograniczonego wyszukiwania.

1. Jeśli jeszcze tego nie zrobiono, rozwiń kategorię **Directory management** (Zarządzanie katalogami) w obszarze nawigacyjnym, a następnie kliknij przycisk **Manage entries** (Zarządzanie pozycjami). W celu wybrania pozycji, przyrostka lub poddrzewa, z którym chce się pracować, można rozwijać różne poddrzewa drzewa katalogu. Kliknij przycisk **Delete** (Usuń) znajdujący się na pasku narzędzi umieszczonym po prawej stronie.
2. Zostanie wyświetlony monit o potwierdzenie kasowania pozycji. Kliknij przycisk **OK**. Pozycja zostanie usunięta z katalogu i ponownie zostanie wyświetlona lista pozycji.

## Zadania związane z grupami autoryzacji proxy

Ten temat zawiera informacje dotyczące zarządzania grupami autoryzacji proxy.

Członkowie grupy autoryzacji proxy mogą uzyskać dostęp do serwera Directory Server i wykonywać wiele zadań w imieniu wielu użytkowników bez potrzeby ponownego łączenia dla każdego użytkownika. Członkowie grupy autoryzacji proxy mogą przyjmować dowolne uwierzytelnione tożsamości poza tożsamością administratora lub członków grupy administracyjnej.

Do zarządzania autoryzacją proxy używane jest narzędzie Web Administration.

### Pojęcia pokrewne

“Autoryzacja proxy” na stronie 64

Autoryzacja proxy jest specjalną formą uwierzytelniania. Dzięki zastosowaniu mechanizmu autoryzacji proxy, aplikacja kliencka może zostać połączona z katalogiem za pomocą własnej tożsamości, ale może wykonywać działania w imieniu innego użytkownika w celu uzyskania dostępu do katalogu docelowego. Zestaw zaufanych aplikacji lub użytkowników może uzyskać dostęp do serwera Directory Server w imieniu wielu użytkowników.

## Tworzenie grupy autoryzacji proxy

Ten temat zawiera informacje dotyczące tworzenia grupy autoryzacji proxy.

1. W obszarze nawigacyjnym rozwiń kategorię **Directory management** (Zarządzanie katalogiem) i kliknij opcję **Add an entry** (Dodaj pozycję). Można także kliknąć **Manage entries** (Zarządzaj pozycjami) i wybrać miejsce (cn=ibmPolicies l ub cn=localhost), a następnie kliknąć **Add** (Dodaj).
2. Wybierz klasę obiektu **groupof Names** (grupa\_nazw) z menu **Structural object class** (Strukturalna klasa obiektu).
3. Kliknij przycisk **Next** (Dalej).



4. Wybierz pomocniczą klasę obiektu **ibm-proxyGroup** z menu **Available** (Dostępne) i kliknij **Add** (Dodaj). Powtórz tę czynność dla każdej dodatkowej pomocniczej klasy obiektu, która powinna zostać dodana.
5. Kliknij przycisk **Next** (Dalej).
6. W polu **Relative DN** (Nazwa RDN) wpisz `cn=proxyGroup`.
7. W polu **Parent DN** (Nadrzędna nazwa DN) wpisz nazwę wyróżniającą wybranej pozycji drzewa, np. `cn=localhost`. Można także kliknąć przycisk **Browse** (Przeglądaj), aby wybrać **Parent DN** (nadrzędna nazwę DN) z listy. Zaznacz opcję i kliknij przycisk **Select** (Wybierz), aby określić żądaną nadrzędna nazwę wyróżniającą. Domyślna nadrzędna nazwą DN jest pozycja wybrana w drzewie.

**Uwaga:** Jeśli wykonywanie tego zadania zostało rozpoczęte na panelu Manage entries (Zarządzanie pozycjami), pole to jest już wypełnione. Opcję Parent DN (Nadrzędna nazwa DN) wybrano przed kliknięciem przycisku Add (Dodaj) w celu rozpoczęcia procesu dodawania pozycji.

8. W zakładce **Required attributes** (Atrybuty wymagane) wprowadź wartości atrybutów wymaganych.
  - **cn** to proxyGroup.
  - **Member** (Członek) ma postać nazwy wyróżniającej, na przykład `cn=Bob Garcia,ou=austin,o=ibm,c=us`. Sekcja “Zmiana atrybutów binarnych” na stronie 202 zawiera informacje na temat dodawania wartości binarnych.
9. Jeśli chcesz wpisać więcej niż jedną wartość określonego atrybutu, kliknij przycisk **Multiple values** (Wartości wielokrotne), a następnie dodaj wszystkie wartości, po jednej w wierszu.

**Uwaga:** Nie należy tworzyć wartości wielokrotnych dla wartości cn. Grupa autoryzacji proxy musi posiadać powszechnie znaną nazwę, proxyGroup.

Po zakończeniu dodawania wartości wielokrotnych kliknij przycisk **OK**. Wartości są dodawane do rozwijanego menu wyświetlanego dla atrybutu.

10. Jeśli na serwerze włączona jest funkcja znaczników języka, kliknij **Language tag value** (Wartość znacznika języka), aby dodać lub usunąć deskryptory znaczników języka.
11. Kliknij zakładkę **Other attributes** (Inne atrybuty).
12. W zakładce **Other attributes** (Inne atrybuty) wprowadź odpowiednie wartości atrybutów. Sekcja “Zmiana atrybutów binarnych” na stronie 202 zawiera informacje na temat dodawania wartości binarnych.
13. Jeśli chcesz wpisać więcej niż jedną wartość określonego atrybutu, kliknij przycisk **Multiple values** (Wartości wielokrotne), a następnie dodaj wszystkie wartości, po jednej w wierszu. Po zakończeniu dodawania wartości wielokrotnych kliknij przycisk **OK**. Wartości są dodawane do rozwijanego menu wyświetlanego dla atrybutu.
14. Jeśli na serwerze włączona jest funkcja znaczników języka, kliknij **Language tag value** (Wartość znacznika języka), aby dodać lub usunąć deskryptory znaczników języka.
15. Kliknij przycisk **Finish** (Zakończ), aby utworzyć pozycję.

## Zmiana grupy autoryzacji proxy

Ten temat zawiera informacje o modyfikowaniu grupy autoryzacji proxy.

Grupę autoryzacji proxy można zmieniać, na przykład dodać lub usunąć członków grupy, za pomocą narzędzia Web Administration.

1. Jeśli jeszcze tego nie zrobiono, rozwiń kategorię **Directory management** (Zarządzanie katalogami) w obszarze nawigacyjnym, a następnie kliknij przycisk **Manage entries** (Zarządzanie pozycjami). W celu wybrania pozycji, z którą chce się pracować, można rozwijać różne poddrzewa drzewa katalogu. Kliknij przycisk **Edit attributes** (Edycja atrybutów) znajdujący się na pasku narzędzi umieszczonym po prawej stronie.
2. Na karcie **Required attributes** (Atrybuty wymagane) wpisz wartości atrybutów wymaganych. Sekcja “Zmiana atrybutów binarnych” na stronie 202 zawiera informacje na temat dodawania wartości binarnych. Jeśli chcesz wpisać więcej niż jedną wartość określonego atrybutu, kliknij przycisk **Multiple values** (Wartości wielokrotne), a następnie dodaj wszystkie wartości, po jednej w wierszu.
3. Kliknij zakładkę **Optional attributes** (Atrybuty opcjonalne).

4. Na karcie **Optional attributes** (Atrybuty opcjonalne) wpisz odpowiednie wartości atrybutów opcjonalnych. Jeśli chcesz wpisać więcej niż jedną wartość określonego atrybutu, kliknij przycisk **Multiple values** (Wartości wielokrotne), a następnie dodaj wszystkie wartości, po jednej w wierszu.
5. Kliknij zakładkę **Memberships** (Przynależność do grup).
6. Jeśli utworzono grupy, to na karcie **Memberships** (Przynależność do grup):
  - Wybierz grupę z listy **Available groups** (Dostępne grupy) i kliknij przycisk **Add** (Dodaj), aby przypisać pozycję do wybranej grupy statycznej (**Static group membership**).
  - Wybierz grupę z listy **Static group memberships** (Członkostwo w grupach statycznych) i kliknij przycisk **Remove** (Usuń), aby usunąć pozycję z wybranej grupy.
7. Jeśli jest to pozycja grupowa, dostępna będzie zakładka **Members** (Elementy). Zakładka **Members** (Elementy) zawiera elementy wybranej grupy. Elementy można dodawać do grupy oraz ich z niej usuwać.
  - Aby dodać element do grupy:
    - a. Kliknij opcję **Multiple values** (Wiele wartości) obok zakładki **Members** (Elementy) lub na zakładce **Members** (Elementy) kliknij opcję **Members** (Elementy).
    - b. W polu Member (Element) wprowadź wprowadź nazwę wyróżniającą pozycji, którą chcesz dodać.
    - c. Kliknij przycisk **Add** (Dodaj).
    - d. Kliknij przycisk **OK**.
  - Aby usunąć element z grupy:
    - a. Kliknij opcję **Multiple values** (Wiele wartości) obok zakładki **Members** (Elementy) lub na zakładce **Members** (Elementy) kliknij opcję **Members** (Elementy).
    - b. Wybierz pozycję do usunięcia.
    - c. Kliknij przycisk **Remove** (Usuń).
    - d. Kliknij przycisk **OK**.
  - Aby odświeżyć listę elementów, kliknij przycisk **Update** (Aktualizuj).
8. Kliknij przycisk **OK**, aby zmodyfikować pozycję.

## Kopiowanie grupy autoryzacji proxy

Ten temat zawiera informacje dotyczące kopiowania grupy autoryzacji proxy.

Skopiowanie grupy autoryzacji proxy może być pomocne, jeśli w obu pozycjach localhost i IBMpolicies na znajdować się ta sama grupa autoryzacji proxy.

1. Jeśli jeszcze tego nie zrobiono, rozwiń kategorię **Directory management** (Zarządzanie katalogami) w obszarze nawigacyjnym, a następnie kliknij przycisk **Manage entries** (Zarządzanie pozycjami). Aby wybrać pozycję, z którą chcesz pracować, na przykład Jan Kowalski, możesz rozwijać różne poddrzewa. Kliknij przycisk **Copy** (Kopiuj) znajdujący się na pasku narzędzi umieszczonym po prawej stronie.
2. Zmień pozycję RDN w polu DN (Nazwa wyróżniająca). Na przykład zmień cn=Jan Kowalski na cn=Tomasz Nowak.
3. Na zakładce wymaganych atrybutów zmień pozycję cn na nową nazwę RDN. W tym przykładzie jest to Tomasz Nowak.
4. Zmień odpowiednie inne wymagane atrybuty. W tym przykładzie zmień atrybut z Kowalski na Nowak.
5. Po zakończeniu wprowadzania niezbędnych zmian kliknij przycisk **OK**, aby utworzyć nową pozycję. Nowa pozycja Tomasz Nowak zostanie dodana na końcu listy pozycji.

## Usuwanie grupy autoryzacji proxy

Ten temat zawiera informacje dotyczące usuwania grupy autoryzacji proxy.

1. Jeśli jeszcze tego nie zrobiono, rozwiń kategorię **Directory management** (Zarządzanie katalogami) w obszarze nawigacyjnym, a następnie kliknij przycisk **Manage entries** (Zarządzanie pozycjami). W celu wybrania pozycji, przyrostka lub poddrzewa, z którym chce się pracować, można rozwijać różne poddrzewa drzewa katalogu. Kliknij przycisk **Delete** (Usuń) znajdujący się na pasku narzędzi umieszczonym po prawej stronie.

2. Zostanie wyświetlony monit o potwierdzenie kasowania pozycji. Kliknij przycisk **OK**. Pozycja zostanie usunięta z katalogu i ponownie zostanie wyświetlona lista pozycji.

## Zadania związane z atrybutami unikalnymi

Ten temat zawiera informacje dotyczące zarządzania atrybutami unikalnymi.

Zarządzanie atrybutami unikalnymi wykonywane jest za pomocą kategorii **Server administration** (Administrowanie serwerem) narzędzia Web Administration.

**Uwaga:** W zależności od atrybutu, atrybuty unikalne i znaczniki języka wykluczają się wzajemnie. Jeśli pewien atrybut został określony jako unikalny, znaczniki języka nie mogą zostać do niego przypisane.

**Uwaga:** Aby zmienić konfigurację serwera za pomocą zadań w kategorii Server administration (Administrowanie serwerem) w narzędziu Web Administration, należy uwierzytelnić się na serwerze jako profil użytkownika systemu i5/OS z uprawnieniami specjalnymi \*ALLOBJ i IOSYSCFG. Można to zrobić, dokonując uwierzytelnienia jako użytkownik rzutowany i używając hasła dla tego profilu. Aby nawiązać połączenie jako użytkownik rzutowany z poziomu narzędzia Web Administration, należy wprowadzić nazwę użytkownika w postaci `os400-profile=MOJANAZWAUŻYTKOWNIKA,cn=accounts,os400-sys=MÓJSYSTEM.PL`, gdzie łańcuchy znaków MOJANAZWAUŻYTKOWNIKA i MÓJSYSTEM.PL zastępowane są odpowiednio nazwą profilu użytkownika i skonfigurowanym przyrostkiem rzutowania.

### Pojęcia pokrewne

“Atrybuty unikalne” na stronie 90

Funkcja atrybutów unikalnych zapewnia, że w obrębie katalogu określone atrybuty posiadają zawsze wartości unikalne.

### Zadania pokrewne

“Tworzenie listy atrybutów unikalnych” na stronie 142

Ten temat zawiera informacje dotyczące tworzenia listy atrybutów unikalnych.

“Usuwanie pozycji z listy atrybutów unikalnych” na stronie 142

Ten temat zawiera informacje dotyczące usuwania pozycji z listy atrybutów unikalnych.

## Ustalanie, czy atrybut można określić jako unikalny

Ten temat zawiera informacje dotyczące ustalania, czy atrybut można określić jako unikalny.

Nie wszystkie atrybuty można określić jako unikalne. Poniżej znajduje się lista atrybutów, które nie mogą zostać wyznaczone jako unikalne:

- Atrybuty binarne, atrybuty wykonawcze, atrybuty konfiguracyjne oraz atrybut `objectclass` nie mogą zostać oznaczone jako unikalne.
- Atrybuty z istniejącymi wartościami będącymi w konflikcie nie mogą być unikalne.
- W zależności od atrybutu, atrybuty unikalne i znaczniki języka wykluczają się wzajemnie. Jeśli pewien atrybut został określony jako unikalny, znaczniki języka nie mogą zostać do niego przypisane.

Zadanie zarządzania atrybutami unikalnymi w narzędziu Web Administration pokazuje tylko te atrybuty, które spełniają pierwszy warunek. Tę samą listę atrybutów można uzyskać, uruchamiając komendę `ldapexop` po podłączeniu się jako administrator. Aby uzyskać listę atrybutów, które mogą być unikalne, należy wpisać:

```
ldapexop -op getattributes -attrType unique -matches true
```

Aby uzyskać listę atrybutów, które nie mogą być unikalne, należy wpisać:

```
ldapexop -op getattributes -attrType unique -matches false
```

Niektóre z atrybutów wyświetlonych jako te, które mogą być unikalne, mogą mieć wartości będące w konflikcie, zatem nie mogą być unikalne. Aby ustalić, czy konkretny atrybut można określić jako unikalny, należy użyć komendy `ldapexop`. Na przykład komenda:

```
ldapexop -op uniqueattr -a uid
```

wskazuje, czy atrybut UID może być unikalny. Wyświetla także wartości atrybutu będące w konflikcie, jeśli takie istnieją.

Jeśli komenda `ldapexop` wykaże, że istnieją wartości będące w konflikcie, za pomocą komendy `ldapsearch` można znaleźć pozycje, które mają takie wartości. Na przykład następująca komenda wyświetla wszystkie wpisy z identyfikatorem `uid=jkowalski`:

```
ldapsearch -b "" -s sub "(uid=jkowalski)"
```

## Tworzenie listy atrybutów unikalnych

Ten temat zawiera informacje dotyczące tworzenia listy atrybutów unikalnych.

1. W obszarze nawigacyjnym rozwiń kategorię **Server administration** (Administrowanie serwerem). Kliknij **Manage unique attributes** (Zarządzaj atrybutami unikalnymi).
2. W menu **Available attributes** (Dostępne atrybuty) zaznacz atrybut, który ma zostać dodany jako unikalny. Atrybuty wyświetlone na liście dostępnych atrybutów można określić jako unikalne, na przykład `sn`.
3. Kliknij **Add to cn=localhost** (Dodaj do `cn=localhost`) lub **Add to cn=IBMpolicies** (Dodaj do `cn=IBMpolicies`). Różnica między powyższymi kontenerami jest taka, że pozycje `cn=IBMpolicies` są replikowane, a pozycje `cn=localhost` nie. Atrybut zostanie wyświetlony w odpowiednim oknie listy. Ten sam atrybut można umieścić w obu kontenerach.

**Uwaga:** Jeśli pozycja stworzona zostanie zarówno dla `cn=localhost` jak i `cn=IBMpolicies`, powstała w ten sposób unia tych dwóch pozycji będzie listą atrybutów unikalnych. Na przykład, jeśli atrybuty `cn` i `employeeNumber` są określone jako unikalne w kontenerze `cn=localhost`, a atrybuty `cn` i `telephoneNumber` są określone jako unikalne w kontenerze `cn=IBMpolicies`, serwer traktuje atrybuty `cn`, `employeeNumber` oraz `telephoneNumber` jako unikalne.

4. Powtórz te czynności dla każdego atrybutu, który ma zostać dodany jako atrybut unikalny.
5. Kliknij przycisk **OK**, aby zapisać zmiany.

Jeśli podczas dodawania lub modyfikowania pozycji atrybutu unikalnego ustanowienie ograniczenia przez unikalność dla któregoś z wyświetlonych typów atrybutów unikalnych powoduje błędy, pozycja nie zostanie dodana ani utworzona w katalogu. Błąd musi być usunięty, a komenda dodania lub modyfikacji musi być wprowadzona ponownie zanim pozycję będzie można utworzyć lub zmodyfikować. Na przykład, jeśli podczas dodawania pozycji atrybutu unikalnego do katalogu ustanowienie w tabeli ograniczenia przez unikalność dla jednego z wyświetlonych typów atrybutów unikalnych nie powiedzie się (ze względu na wartości podwójne w bazie danych), pozycja atrybutu unikalnego nie zostanie dodana do katalogu. Wystąpi błąd.

Jeśli aplikacja dokona próby dodania do katalogu pozycji o wartości atrybutu, która duplikuje pozycję istniejącą w katalogu, na serwerze LDAP wystąpi błąd o kodzie 20 (LDAP: kod błędu 20 - Atrybut lub wartość istnieje).

Po uruchomieniu serwer sprawdza listę atrybutów unikalnych i określa, czy dla każdego z nich istnieją ograniczenia DB2. Jeśli ograniczenie dla atrybutu nie istnieje, ponieważ zostało uprzednio usunięte przez narzędzie ładowania masowego lub ręcznie przez użytkownika, jest ono usuwane z listy atrybutów unikalnych, a komunikat o błędzie zostaje zapisany do protokołu błędów `ibmslapd.log`. Na przykład, jeśli atrybut `cn` określony jest jako unikalny w kontenerach `cn=uniqueattributes`, `cn=localhost`, zaś jego ograniczenie DB2 nie istnieje, protokolowany jest następujący komunikat:

Wartości atrybutu CN nie są unikalne.

Atrybut CN został usunięty z pozycji atrybutu unikalnego:

```
CN=UNIQUEATTRIBUTES,CN=LOCALHOST
```

### Pojęcia pokrewne

“Zadania związane z atrybutami unikalnymi” na stronie 141

Ten temat zawiera informacje dotyczące zarządzania atrybutami unikalnymi.

## Usuwanie pozycji z listy atrybutów unikalnych

Ten temat zawiera informacje dotyczące usuwania pozycji z listy atrybutów unikalnych.

Jeśli atrybut unikalny istnieje zarówno w kontenerach `cn=uniqueattribute,cn=localhost` jak i w `cn=uniqueattribute,cn=IBMpolicies` i zostaje usunięty tylko z jednej pozycji, serwer nadal traktował będzie ten atrybut jako unikalny. Atrybut staje się nieunikalny w momencie usunięcia z obydwu pozycji.

1. Rozwiń kategorię **Server administration** (Administrowanie serwerem) w obszarze nawigacyjnym i kliknij **Manage unique attributes** (Zarządzaj atrybutami unikalnymi).
2. Zaznacz atrybut, który ma zostać usunięty z listy atrybutów unikalnych poprzez kliknięcie danego atrybutu w odpowiednim oknie listy.
3. Kliknij przycisk **Remove** (Usuń).
4. Powtórz te czynności dla każdego atrybutu, który ma zostać usunięty z listy.
5. Kliknij przycisk **OK**, aby zapisać zmiany.

**Uwaga:** Usunięcie ostatniego atrybutu unikalnego z okna listy `cn=localhost` lub `cn=IBMpolicies` powoduje w danym oknie automatyczne usunięcie pozycji kontenera `cn=uniqueattribute,cn=localhost` lub `cn=uniqueattribute,cn=IBMpolicies`.

#### Pojęcia pokrewne

“Zadania związane z atrybutami unikalnymi” na stronie 141

Ten temat zawiera informacje dotyczące zarządzania atrybutami unikalnymi.

## Zadania związane z wydajnością

Ten temat zawiera informacje dotyczące dopasowywania ustawień wydajności.

Ustawienia wydajności serwera Directory Server można dopasować, zmieniając dowolny z następujących parametrów:

- Wielkość pamięci podręcznej ACL, wielkość pamięci podręcznej pozycji oraz maksymalną liczbę operacji wyszukiwania i maksymalną wielkość wyników wyszukiwania przechowywanych w pamięci podręcznej filtru.
- Liczba połączeń baz danych i wątków serwera.
- Ustawienia pamięci podręcznej atrybutu
- Ustawienia transakcji serwera

#### Pojęcia pokrewne

“Pamięci podręczne serwera” na stronie 92

Pamięci podręczne LDAP to buforzy szybkiej pamięci używane do przechowywania informacji LDAP, takich jak zapytania, odpowiedzi oraz uwierzytelnienie użytkownika do późniejszego wykorzystania. Strojenie pamięci podręcznych LDAP jest kluczowe dla poprawy wydajności.

## Konfigurowanie połączeń bazy danych i ustawień pamięci podręcznej

Ten temat zawiera informacje dotyczące konfigurowania połączeń bazy danych i ustawień pamięci podręcznej.

Aby ustawić połączenia bazy danych i ustawienia pamięci podręcznej, wykonaj następujące czynności:

1. Rozwiń kategorię **Manage server properties** (Zarządzanie właściwościami serwera) w obszarze nawigacyjnym narzędzia Web Administration i kliknij zakładkę **Performance** (Wydajność) w prawym panelu.
2. Określ wartość w polu **Number of database connections** (Liczba połączeń bazy danych). Określa to liczbę połączeń DB2 używanych przez serwer. Minimalna liczba musi wynosić 4. Ustawieniem domyślnym 15. W przypadku, gdy serwer LDAP odbiera wysoką liczbę żądań klientów lub gdy klienci odbierają błąd typu "odmowa połączenia", zwiększenie liczby połączeń do DB2 wykonywanych przez serwer powinno zapewnić lepsze rezultaty. Maksymalna liczba połączeń jest określona w ustawieniach bazy danych DB2. Serwer nie ogranicza w żaden sposób określanej liczby połączeń, należy jednak pamiętać, że każde połączenie pochłania zasoby.
3. Określ wartość w polu **Number of database connections for replication** (Liczba połączeń bazy danych dla replikacji). Określa to liczbę połączeń DB2 używanych przez serwer dla replikacji. Minimalna liczba musi wynosić 1. Wartością domyślną jest 4.

**Uwaga:** Całkowita liczba połączeń określana dla połączeń bazy danych, w tym połączeń bazy danych dla replikacji, nie może przekraczać liczby połączeń ustawionej w bazie danych DB2.

4. Zaznacz **Cache ACL information** (Informacje o pamięci podręcznej ACL), aby skorzystać z następujących ustawień pamięci podręcznej ACL.
5. Określ wartość w polu **Maximum number of elements in ACL cache** (Maksymalna liczba elementów w pamięci podręcznej ACL). Wartością domyślną jest 25000.
6. Określ wartość w polu **Maximum number of elements in entry cache** (Maksymalna liczba elementów w pamięci podręcznej pozycji). Wartością domyślną jest 25000.
7. Określ wartość w polu **Maximum number of elements in search filter cache** (Maksymalna liczba elementów w pamięci podręcznej filtra wyszukiwania). Wartością domyślną jest 25000. Pamięć podręczna filtra wyszukiwania składa się z bieżących zapytań o filtry żadanego atrybutu i zgodnych z nimi identyfikatorów pozycji wyniku. Operacja aktualizacji unieważnia wszystkie pozycje pamięci podręcznej filtra.
8. Określ wartość w polu **Maximum number of elements from a single search added to search filter cache** (Maksymalna liczba elementów pojedynczego wyszukiwania dodawanych do pamięci podręcznej filtra wyszukiwania). Zaznaczenie **Elements** (Elementy) wymaga podania liczby. Wartością domyślną jest 100. W przeciwnym razie zaznacz **Unlimited** (Nieograniczona). Pozycje wyszukiwania, które zgodne są z większą liczbą pozycji niż liczba tu określona, nie są dodawane do pamięci podręcznej filtra wyszukiwania.
9. Po zakończeniu kliknij przycisk **OK**.
10. Jeśli wprowadzono zmiany w ustawieniach liczby połączeń bazy danych, w celu aktywacji wprowadzonych zmian należy ponownie uruchomić serwer. Jeśli zmodyfikowano jedynie ustawienia pamięci podręcznej, serwer nie wymaga ponownego uruchomienia.

## Konfigurowanie pamięci podręcznej atrybutów

Ten temat zawiera informacje dotyczące konfigurowania pamięci podręcznej atrybutów.

Ustawienia pamięci podręcznej atrybutów można konfigurować za pomocą narzędzia Web Administration oraz programu System i Navigator.

Aby ręcznie dopasować ustawienia pamięci podręcznej atrybutów w narzędziu Web Administration, należy wykonać następujące czynności:

1. Rozwiń kategorię **Server administration** (Administrowanie serwerem) w obszarze nawigacyjnym narzędzia Web Administration i wybierz zakładkę **Attribute cache** (Pamięć podręczna atrybutu) w prawym panelu.

**Uwaga:** Aby zmienić konfigurację serwera za pomocą zadań w kategorii Server administration (Administrowanie serwerem) w narzędziu Web Administration, należy uwierzytelnić się na serwerze jako profil użytkownika systemu i5/OS z uprawnieniami specjalnymi \*ALLOBJ i IOSYSCFG. Można to zrobić, dokonując uwierzytelnienia jako użytkownik rzutowany i używając hasła dla tego profilu. Aby nawiązać połączenie jako użytkownik rzutowany z poziomu narzędzia Web Administration, należy wprowadzić nazwę użytkownika w postaci `os400-profile=MOJANAZWAUŻYTKOWNIKA,cn=accounts,os400-sys=MOJSYSTEM.PL`, gdzie łańcuchy znaków MOJANAZWAUŻYTKOWNIKA i MOJSYSTEM.PL zastępowane są odpowiednio nazwą profilu użytkownika i skonfigurowanym przyrostkiem rzutowania.

2. Zmień wyrażoną w kilobajtach ilość pamięci dostępnej dla pamięci podręcznej katalogu. Wartość domyślna to 16384 kilobajty (16 MB).
3. Zmień wyrażoną w kilobajtach ilość pamięci dostępnej dla pamięci podręcznej protokołu zmian. Wartość domyślna to 16384 kilobajty (16 MB).

**Uwaga:** Jeśli protokół zmian nie został skonfigurowany, wybór jest nieaktywny. Buforowanie atrybutów dla protokołu zmian powinno mieć wartość 0, nie należy też konfigurować żadnych atrybutów, o ile wyszukiwanie w protokole zmian nie jest częstym działaniem, a wydajność tych wyszukiwań nie jest krytyczna.

4. W menu **Available attributes** (Dostępne atrybuty) wybierz atrybut, który ma być buforowany. W menu tym wyświetlone są tylko te atrybuty, które mogą być buforowane, na przykład sn.

**Uwaga:** Atrybut pozostaje na liście dostępnych atrybutów dopóki nie zostanie umieszczony zarówno w kontenerze `cn=directory` jak i `cn=changelog`.

5. Kliknij **Add to cn=directory** (Dodaj do cn=directory) lub **Add to cn=changelog** (Dodaj do cn=changelog). Atrybut zostanie wyświetlony w odpowiednim oknie listy. Ten sam atrybut można umieścić w obu kontenerach.

**Uwaga:** Wybór **Add to cn=changelog** (Dodaj do cn=changelog) jest nieaktywny, jeśli protokół zmian nie został skonfigurowany. Buforowanie atrybutów dla protokołu zmian powinno mieć wartość 0, nie należy też konfigurować żadnych atrybutów, o ile wyszukiwanie w protokole zmian nie jest częstym działaniem, a wydajność tych wyszukiwań nie jest krytyczna.

6. Powtórz te czynności dla każdego atrybutu, który ma zostać dodany do pamięci podręcznej atrybutu.
7. Po zakończeniu kliknij przycisk **OK**.

Aby włączyć automatyczne buforowanie atrybutów w programie System i Navigator, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń pozycję **Sieć**.
2. Rozwiń pozycję **Serwery**.
3. Kliknij **TCP/IP**.
4. Prawym przyciskiem myszy kliknij **IBM Directory Server** i wybierz **Właściwości**.
5. Kliknij zakładkę **Wydajność**.
6. Wybierz opcję **Aktywuj automatyczne buforowanie atrybutów dla Bazy danych** lub **Protokołu zmian** lub dla obydwu. Nie należy aktywować automatycznego buforowania atrybutów dla protokołu zmian o ile wyszukiwanie w protokole nie jest częstym działaniem, a wydajność tych wyszukiwań nie jest krytyczna.
7. Podaj **Czas początkowy** (według czasu miejscowego serwera) i **Interwał** dla każdego z typów buforowania, który ma zostać aktywowany. Na przykład, jeśli po aktywacji buforowania bazy danych czas początkowy ustawiono na godzinę 6 i określono sześciogodzinny interwał, pamięć podręczna będzie automatycznie dopasowywana o godzinie 6, 12, 18 i 24, niezależnie od godziny, w której serwer został uruchomiony i w której dokonano konfiguracji autodopasowania.

**Uwaga:** Automatyczne buforowanie atrybutów będzie aktywne aż do maksymalnej ilości pamięci przeznaczonej do buforowania, jak określono to w narzędziu Web Administration według opisu powyżej.

Tabela 4. Interakcja ustawień pamięci podręcznej atrybutu

Działanie	Zdarzenie
Uruchomienie serwera	Jeśli funkcja automatycznego buforowania atrybutów jest aktualnie włączona, a funkcja automatycznego buforowania była aktywna w momencie ostatniego zatrzymania serwera, wówczas te same atrybuty, które buforowane były w momencie zatrzymania serwera, zostaną utworzone po jego ponownym uruchomieniu. Jeśli dodatkowa pamięć jest nadal dostępna dla buforowania atrybutów, to buforowane będą także atrybuty skonfigurowane ręcznie. Jeśli funkcja automatycznego buforowania atrybutów jest aktualnie włączona, a nie była włączona w momencie ostatniego zatrzymania serwera, atrybuty ręcznie skonfigurowane do buforowania będą buforowane. W obu przypadkach serwer dopasuje automatycznie pamięci podręczne atrybutów w oparciu o określony czas początkowy i interwał. Jeśli funkcja automatycznego buforowania nie jest aktywna, obowiązywać będą ręcznie dopasowane ustawienia pamięci podręcznej.
Aktywacja automatycznego buforowania atrybutów po uruchomieniu serwera	Automatyczne buforowanie atrybutów wystąpi zgodnie z opisem dla uruchomienia serwera. Każda ręcznie skonfigurowana pamięć podręczna atrybutu, która nie mieści się w pamięci skonfigurowanej dla buforowania atrybutów, zostanie usunięta.
Wyłączenie automatycznego buforowania atrybutu po uruchomieniu serwera	Buforowane będą jedynie ręcznie skonfigurowane atrybuty.
Modyfikacja ręcznie buforowanych atrybutów, kiedy po uruchomieniu serwera funkcja automatycznego buforowania jest aktywna	Zmiany bez efektu. Ręczne ustawienia odniosą skutek po wyłączeniu automatycznego buforowania.

Tabela 4. Interakcja ustawień pamięci podręcznej atrybutu (kontynuacja)

Działanie	Zdarzenie
Modyfikacja ilości pamięci dostępnej dla buforowania po uruchomieniu serwera	Jeśli funkcja automatycznego buforowania jest aktywna, serwer przystąpi natychmiast do ponownego buforowania w oparciu o nową wielkość. Jeśli automatyczne buforowanie jest wyłączone, serwer będzie buforował ręcznie skonfigurowane atrybuty aż do nowej wielkości.
Modyfikacja czasu początkowego i interwału po uruchomieniu serwera	Jeśli funkcja automatycznego buforowania jest aktywna, nowe ustawienia zostaną wprowadzone według określonego czasu początkowego lub interwału. Jeśli automatyczne buforowanie jest wyłączone, ustawienia są przechowane i aktywowane w momencie jego ponownej aktywacji.

## Konfigurowanie ustawień transakcji

Ten temat zawiera informacje dotyczące konfigurowania ustawień transakcji.

Aby skonfigurować ustawienia transakcji, wykonaj następujące czynności:

1. Rozwiń kategorię **Manage server properties** (Zarządzanie właściwościami serwera) w obszarze nawigacyjnym narzędzia Web Administration i kliknij zakładkę **Transactions** (Transakcje) w prawym panelu.
2. Zaznacz pole wyboru **Enable transaction processing** (Włącz przetwarzanie transakcji), aby włączyć przetwarzanie transakcji. Jeśli pole **Enable transaction processing** (Włącz przetwarzanie transakcji) nie jest zaznaczone, serwer ignoruje pozostałe opcje dostępne w panelu.
3. Ustaw opcję **Maximum number of transactions** (Maksymalna liczba transakcji). Kliknij przełącznik **Transactions** (Transakcje) lub **Unlimited** (Nieograniczona). Zaznaczenie **Transactions** (Transakcje) wymaga określenia maksymalnej liczby transakcji. Maksymalna liczba transakcji wynosi 2147483647. Ustawieniem domyślnym jest 20 transakcji.
4. Ustaw opcję **Maximum number of operations per transaction** (Maksymalna liczba działań na transakcję). Kliknij przełącznik **Operations** (Działania) lub **Unlimited** (Nieograniczona). Zaznaczenie pola **Operations** (Operacje) wymaga określenia maksymalnej liczby działań dozwolonych dla każdej transakcji. Maksymalna liczba operacji wynosi 2147483647. Im niższa liczba, tym większa wydajność. Ustawieniem domyślnym jest 5 działań.
5. Ustaw opcję **Pending time limit** (Limit czasu oczekiwania). Wybór ten określa w sekundach maksymalną wartość limitu czasu dla oczekującej transakcji. Kliknij przełącznik **Seconds** (Sekundy) lub **Unlimited** (Nieograniczony). Zaznaczenie pola **Seconds** (Sekundy) wymaga określenia maksymalnej liczby sekund dozwolonych dla każdej transakcji. Maksymalna liczba sekund wynosi 2147483647. Transakcje, które nie zostaną zakończone przed upływem tego czasu są anulowane (wycofywane). Wartością domyślną jest 300 sekund.
6. Po zakończeniu kliknij przycisk **OK**.
7. Jeśli obsługa transakcji została włączona, w celu aktywacji wprowadzonych zmian należy ponownie uruchomić serwer. Jeśli modyfikowane były tylko ustawienia, serwer nie wymaga restartowania.

## Zadania związane z replikacją

Ten temat zawiera informacje dotyczące zarządzania replikacją.

Aby zarządzać replikacją, rozwiń kategorię **Replication management** (Zarządzanie replikacją) narzędzia Web Administration.

### Pojęcia pokrewne

“Replikacja” na stronie 37

Replikacja to technika używana przez serwery katalogów do zwiększania wydajności i niezawodności. Proces replikacji synchronizuje dane w wielu katalogach.

## Tworzenie topologii serwer główny - replika

Ten temat zawiera informacje dotyczące tworzenia topologii serwer główny - replika.

Aby zdefiniować podstawową topologię serwer główny - replika:



1. Utwórz serwer główny i określ jego zawartość. Wybierz poddrzewo, które chcesz replikować, i określ serwer jako główny. Więcej informacji zawiera temat “Tworzenie serwera głównego (replikowanego poddrzewa)”.
2. Utwórz referencje, których ma używać serwer wysyłający. Więcej informacji zawiera temat “Tworzenie referencji replikacji” na stronie 149.
3. Utwórz serwer replik. Więcej informacji zawiera temat “Tworzenie serwera replik” na stronie 151.
4. Wyeksportuj topologię z serwera głównego do repliki. Więcej informacji zawiera temat “Kopiowanie danych do repliki” na stronie 153.
5. Zmień konfigurację repliki, aby określała kto ma uprawnienia do replikacji zmian, a następnie dodaj odwołanie do serwera głównego. Więcej informacji zawiera temat “Dodawanie informacji o serwerze wysyłającym do nowej repliki” na stronie 153.

#### Uwaga:

Jeśli pozycja w katalogu głównym poddrzewa do replikacji nie jest przyrostkiem na serwerze, przed użyciem funkcji **Add subtree** (Dodaj poddrzewo) należy sprawdzić, czy zdefiniowano jej listy ACL:

##### Dla niefiltrowanych list ACL:

```
ownersource: <takie samo, jak nazwa wyróżniająca pozycji>
ownerpropagate: TRUE
```

```
acldsource: <takie samo, jak nazwa wyróżniająca pozycji>
aclpropagate: TRUE
```

##### Dla filtrowanych list ACL:

```
ibm-filteraclinherit: FALSE
```

Aby sprostać wymaganiom listy ACL, jeśli pozycja nie jest przyrostkiem na serwerze, należy przeprowadzić edycję listy ACL dla tej pozycji w panelu **Manage entries** (Zarządzaj pozycjami). Po wybraniu pozycji należy kliknąć przycisk **Edit ACL** (Edycja listy ACL). Aby dodać niefiltrowane listy ACL, należy wybrać tę zakładkę i zaznaczyć pole wyboru w celu określenia, czy listy ACL są jawne dla list ACL i właścicieli. Należy sprawdzić, czy zaznaczono pole **Propagate ACLs** (Propaguj listy ACL) i **Propagate owner** (Propaguj właściciela). Aby dodać filtrowane listy ACL, należy wybrać odpowiednią zakładkę i dodać pozycję **cn=this** z rolą **access-id** dla list ACL i właścicieli. Należy sprawdzić, czy pole **Accumulate filtered ACLs** (Kumuluj filtrowane listy ACL) jest odznaczone, a pole **Propagate owner** (Propaguj właściciela) jest zaznaczone. Szczegółowe informacje zawiera temat “Zadania związane z listami kontroli dostępu” na stronie 214.

Początkowo obiekt **ibm-replicagroup** utworzony przez ten proces dziedziczy listę ACL pozycji głównej replikowanego poddrzewa. Te listy ACL mogą być nieodpowiednie do kontroli praw dostępu do informacji o replikacji w katalogu.

## Tworzenie topologii serwer główny - przekazujący - replika

Ten temat zawiera informacje dotyczące tworzenia topologii serwer główny - przekazujący - replika.

Aby zdefiniować topologię serwer główny-przekazujący-replika:

1. Utwórz serwer główny i serwer replik. Więcej informacji zawiera temat “Tworzenie topologii serwer główny - replika” na stronie 146.
2. Utwórz nowy serwer replik dla pierwotnej repliki. Więcej informacji zawiera temat “Tworzenie nowego serwera replik” na stronie 148.
3. Skopiuj dane do repliki. Więcej informacji zawiera temat “Kopiowanie danych do repliki” na stronie 153.

## Tworzenie serwera głównego (replikowanego poddrzewa)

Ten temat zawiera informacje dotyczące tworzenia replikowanego poddrzewa serwera głównego.

**Uwaga:** Aby można było wykonać to zadanie, serwer musi być uruchomiony.

To zadanie określa pozycję jako katalog główny niezależnie replikowanego poddrzewa i tworzy pozycję **ibm-replicasubentry** przedstawiającą ten serwer jako pojedynczy serwer główny dla poddrzewa. Aby utworzyć replikowane poddrzewo, należy wyznaczyć poddrzewo, które ma być replikowane przez serwer.

Rozwiń kategorię Replication management (Zarządzanie replikacją) w obszarze nawigacyjnym i kliknij opcję **Manage topology** (Zarządzaj topologią).

1. Kliknij opcję **Add subtree** (Dodaj poddrzewo).
  2. Wpisz nazwę DN głównej pozycji poddrzewa, które chcesz replikować, lub kliknij przycisk **Browse** (Przełóżaj), aby rozwinąć pozycje i wybrać tę z nich, która ma być początkiem poddrzewa.
  3. Adres URL odwołania do serwera głównego jest wyświetlany w postaci adresu URL LDAP, na przykład:  
`ldap://<nazwa_serwera>.<lokalizacja>.<firma>.pl`
- Uwaga:** Adres URL odwołania do serwera głównego jest opcjonalny. Jest on używany jedynie w następujących sytuacjach:
- Jeśli serwer zawiera (lub będzie zawierał) jakiegokolwiek poddrzewa tylko do odczytu.
  - W celu zdefiniowania adresu URL zwracanego dla aktualizacji do każdego poddrzewa tylko do odczytu na serwerze.
4. Kliknij przycisk **OK**.
  5. Nowy serwer jest wyświetlany w panelu Manage topology (Zarządzaj topologią) pod nagłówkiem **Replicated subtrees** (Replikowane poddrzewa).

## Tworzenie nowego serwera replik

Ten temat zawiera informacje dotyczące tworzenia nowego serwera replik.

Jeśli skonfigurowano topologię replikacji (patrz temat Tworzenie serwera głównego (poddrzewa replikacji)) z serwerem głównym (serwer1) i repliką (serwer2), można zmienić rolę serwera serwer2 na serwer przekazujący. W tym celu należy utworzyć nową replikę (serwer3) pod serwerem serwer2.

1. Podłącz Web Administration do serwera głównego (serwer1).
  2. Rozwiń kategorię Replication management (Zarządzanie replikacją) w obszarze nawigacyjnym i kliknij opcję **Manage topology** (Zarządzaj topologią).
  3. Wybierz poddrzewo, które chcesz replikować, i kliknij opcję **Show topology** (Pokaż topologię).
  4. Kliknij strzałkę obok wyboru **Replication topology** (Topologia replikacji), aby rozwinąć listę serwerów wysyłających.
  5. Kliknij strzałkę obok wyboru **serwer1**, aby rozwinąć listę serwerów.
  6. Wybierz serwer2 i kliknij **Add replica** (Dodaj replikę).
  7. W zakładce **Server** (Serwer) okna **Add replica** (Dodaj replikę):
    - Wprowadź nazwę hosta i numer portu tworzonej repliki (serwer3). Domyślnym numerem portu jest 389 dla połączeń bez użycia protokołu SSL oraz 636 dla połączeń z SSL. Są to pola wymagane.
    - Wybierz komunikację z wykorzystaniem protokołu SSL lub bez niego.
    - Wpisz nazwę repliki lub pozostaw puste pole, aby użyć nazwy hosta.
    - Wpisz identyfikator repliki. Jeśli serwer, na którym tworzona jest replika, jest uruchomiony, kliknij przycisk **Get replica ID** (Pobierz identyfikator repliki), aby automatycznie wypełnić to pole. Jest to pole wymagane, jeśli dodawany serwer ma być serwerem równorzędnym lub przekazującym. Zalecane jest, aby wszystkie serwery były w tej samej wersji.
    - Wpisz opis serwera repliki.
- W zakładce **Additional** (Dodatkowe):
- Podaj referencje, których używa replika do komunikacji z serwerem głównym.

**Uwaga:** Web Administration umożliwia definiowanie referencji w dwóch miejscach:

- **cn=replication,cn=localhost**, w przypadku której referencje są przechowywane tylko na serwerze, który ich używa.
- W replikowanym poddrzewie, w którym to przypadku referencje są replikowane z resztą poddrzewa.

Umieszczanie referencji w pozycji **cn=replication,cn=localhost** jest uważane za bardziej bezpieczne. Referencje umieszczone w poddrzewie replikacji są tworzone na podstawie pozycji **ibm-replicagroup=default** dla tego poddrzewa.

- Kliknij **Select** (Wybierz).
    - Wybierz położenie referencji, których chcesz używać. Preferowanym położeniem jest **cn=replication,cn=localhost**.
    - Kliknij **Show credentials** (Pokaż referencje).
    - Rozwiń listę referencji i wybierz te, których chcesz użyć.
    - Kliknij przycisk **OK**.  
Dodatkowe informacje o referencjach umowy zawiera temat Tworzenie referencji replikacji.
  - Wybierz harmonogram replikacji z listy rozwijanej lub kliknij przycisk **Add** (Dodaj), aby go dodać. Więcej informacji zawiera temat Tworzenie harmonogramów replikacji.
  - Z listy możliwości serwera wysyłającego można usunąć zaznaczenie wszystkich możliwości, które nie mają być replikowane na serwerze odbierającym.  
Jeśli w sieci są różne serwery w różnych wersjach, w nowszych wersjach są dostępne możliwości, których brak w wersjach wcześniejszych. Niektóre możliwości, takie jak filtrowanie list ACL i strategia haseł, używają atrybutów operacyjnych replikowanych z innymi zmianami. W większości przypadków, jeśli te funkcje są używane, wszystkie serwery powinny je obsługiwać. Jeśli nie wszystkie serwery obsługują daną możliwość, lepiej z niej nie korzystać. Na przykład nie powinno być różnych list ACL na każdym serwerze. Jednak zdarzają się przypadki, w których można używać danej możliwości na obsługujących ją serwerach i nie replikować zmian dotyczących tej możliwości na serwery, które jej nie obsługują. W takich przypadkach można używać listy możliwości do oznaczania konkretnych możliwości, które nie będą replikowane.
  - Jako metodę replikacji wybierz opcję **Single threaded** (Jednowątkowa) lub **Multi-threaded** (Wielowątkowa). W przypadku replikacji wielowątkowej należy także podać liczbę (od 2 do 32) połączeń wykorzystywanych do replikacji. Domyślna liczba połączeń to 2.
  - Kliknij **OK**, aby utworzyć replikę.
8. Skopiuj dane z serwera serwer2 do nowej repliki na serwerze serwer3. Odpowiednie informacje zawiera temat Kopiowanie danych do repliki.
  9. Dodaj umowę serwera wysyłającego do serwera serwer3, która czyni serwer2 wysyłającym dla serwera serwer3, a serwer3 odbierającym dla serwera serwer2. Odpowiednie informacje zawiera temat Dodawanie informacji o serwerze wysyłającym do nowej repliki.

W narzędziu Web Administration role serwera są reprezentowane przez ikony. Wybraną topologią jest:

- serwer1 (główny)
  - serwer2 (przekazujący)
  - serwer3 (replika)

## Tworzenie referencji replikacji

Ten temat zawiera informacje dotyczące tworzenia referencji replikacji.

Rozwiń kategorię Replication management (Zarządzanie replikacją) w obszarze nawigacyjnym narzędzia Web Administration i kliknij element **Manage credentials** (Zarządzaj referencjami).

1. Wybierz z listy poddrzew miejsce, w którym chcesz zapisywać referencje. Narzędzie Web Administration umożliwia definiowanie referencji w następujących miejscach:
  - **cn=replication,cn=localhost**, które zawiera referencje tylko na bieżącym serwerze.

**Uwaga:** W większości przypadków replikacji zaleca się umieszczenie referencji w pozycji `cn=replication,cn=localhost`, ponieważ zapewnia to większą ochronę niż replikowane referencje znajdujące się w poddrzewie. Jednak istnieją sytuacje, w których referencje znajdujące się w pozycji `cn=replication,cn=localhost` nie są dostępne.

Podczas dodawania repliki pod serwerem, na przykład o nazwie `serwerA`, jeśli nawiązano połączenie z innym serwerem, `serwerB`, z narzędziem Web Administration, pole **Select credentials** (Wybierz referencje) nie zawiera opcji `cn=replication,cn=localhost`. Jest to spowodowane tym, że nie można odczytać informacji lub ich zaktualizować pod pozycją `cn=localhost` serwera `serwerA` podczas podłączania się do serwera `serwerB`.

Opcja `cn=replication,cn=localhost` jest dostępna tylko wtedy, gdy serwer, pod którym użytkownik próbuje dodać replikę, jest serwerem, do którego jest on podłączony za pomocą narzędzia Web Administration.

- W replikowanym poddrzewie, w którym to przypadku referencje są replikowane z resztą poddrzewa. Referencje umieszczone w poddrzewie replikacji są tworzone na podstawie pozycji `ibm-replicagroup=default` dla tego poddrzewa.

**Uwaga:** Jeśli nie wyświetlono żadnego poddrzewa, w sekcji “Tworzenie serwera głównego (replikowanego poddrzewa)” na stronie 147 znajdują się instrukcje tworzenia poddrzewa, które ma być replikowane.

2. Kliknij przycisk **Add** (Dodaj).
  3. Wprowadź nazwę tworzonej referencji, na przykład `mycreds` (ciąg `cn=` jest już wpisany w tym polu).
  4. Wpisz typ metody uwierzytelniania, która ma być używana, i kliknij przycisk **Next** (Dalej).
- Jeśli wybrano uwierzytelnianie prostego łączenia:
    - a. Wprowadź nazwę wyróżniającą używaną przez serwer do łączenia się z repliką, na przykład `cn=any`
    - b. Wprowadź hasło używane przez serwer podczas łączenia się z repliką, na przykład `secret`.
    - c. Wpisz ponownie hasło w celu potwierdzenia, że nie ma żadnych błędów typograficznych.
    - d. Jeśli chcesz, wpisz krótki opis referencji.
    - e. Kliknij przycisk **Finish** (Zakończ).

**Uwaga:** Warto zapisać nazwę wyróżniającą i hasło łączenia referencji w celu późniejszego wykorzystania. Hasło będzie potrzebne podczas tworzenia umowy replikacji.

- Jeśli wybrano uwierzytelnianie Kerberos:
  - a. Wprowadź nazwę wyróżniającą łączenia Kerberos.
  - b. Wprowadź nazwę tabeli kluczy.
  - c. Jeśli chcesz, wpisz krótki opis referencji. Żadne inne informacje nie są niezbędne. Więcej informacji zawiera temat “Włączanie uwierzytelniania Kerberos na serwerze Directory Server” na stronie 184.
  - d. Kliknij przycisk **Finish** (Zakończ).

Panel **Add Kerberos Credentials** (Dodawanie referencji Kerberos) przyjmuje opcjonalną nazwę wyróżniającą łączenia o postaci `ibm-kr=użytkownika@dziedzina` i opcjonalną nazwę pliku tabeli kluczy (znanego jako plik kluczy). Jeśli nazwa wyróżniająca łączenia jest określona, w celu uwierzytelnienia do serwera odbiorcy serwer używa określonej nazwy użytkownika. W przeciwnym razie użyta jest nazwa usługi Kerberos (`ldap/nazwa_hosta@dziedzina`). Jeśli używana jest tabela kluczy, serwer używa jej w celu uzyskania referencji dla określonej nazwy użytkownika. Jeśli żaden plik tabeli kluczy nie jest określony, serwer używa pliku tabeli kluczy określonego w swojej konfiguracji Kerberos. Jeśli jest wiele serwerów wysyłających, należy określić nazwę użytkownika i plik tabeli kluczy używane przez wszystkie serwery wysyłające.

**Na serwerze, na którym utworzono referencje:**

- a. Rozwiń kategorię **Directory management** (Zarządzanie katalogami) i kliknij **Manage entries** (Zarządzaj pozycjami).
- b. Wybierz poddrzewo, w którym przechowywałaś referencje, na przykład `cn=localhost` i kliknij przycisk **Expand** (Rozwiń).

- c. Wybierz pozycję **cn=replication** i kliknij przycisk **Expand** (Rozwiń).
- d. Wybierz referencje kerberos (ibm-replicationCredentialsKerberos) i kliknij przycisk **Edit attributes** (Edycja atrybutów).
- e. Kliknij zakładkę **Other attributes** (Inne atrybuty).
- f. Wprowadź **replicaBindDN**, na przykład **ibm-  
kn=moja\_nazwa\_uzytkownika@JAKAS.DZIEDZINA**.
- g. Wprowadź parametr **replicaCredentials**. Jest to nazwa tabeli kluczy używane dla nazwy **moja\_nazwa\_uzytkownika**.

**Uwaga:** Ta nazwa użytkownika i hasło powinny być takie same, jak używane do uruchamiania programu **kinit** z wiersza komend.

### W replicie

- a. Kliknij pozycję **Manage replication properties** (Zarządzanie właściwościami replikacji) w obszarze nawigacji.
  - b. Wybierz z rozwijanego menu **Supplier information** (Dane serwera wysyłającego) lub wpisz nazwę replikowanego poddrzewa, dla którego chcesz skonfigurować referencje serwera wysyłającego.
  - c. Kliknij przycisk **Edit** (Edycja).
  - d. Wpisz nazwę wyróżniającą łączenia replikacji. W tym przykładzie jest to **ibm-  
kn=moja\_nazwa\_uzytkownika@JAKAS.DZIEDZINA**.
  - e. Wprowadź i potwierdź **Hasło łączenia replikacji**. Jest to hasło KDC używane dla nazwy **moja\_nazwa\_uzytkownika**.
- Jeśli wybrano uwierzytelnianie SSL z certyfikatami, nie ma potrzeby zapewnienia żadnych dodatkowych informacji, jeśli używany jest certyfikat serwera. W przypadku użycia certyfikatu innego niż certyfikat serwera:
    - a. Wpisz nazwę pliku kluczy.
    - b. Wpisz hasło pliku kluczy.
    - c. Ponownie wprowadź hasło pliku kluczy, aby je potwierdzić.
    - d. Wpisz etykietę klucza.
    - e. Jeśli chcesz, wpisz krótki opis.
    - f. Kliknij przycisk **Finish** (Zakończ).

Więcej informacji zawiera temat “Włączanie SSL i TLS na serwerze Directory Server” na stronie 182.
5. Na serwerze, na którym utworzono referencje, ustaw wartość systemową Zezwól na przechowywanie informacji o ochronie serwera (QRETSVRSEC) na 1 (zachowaj dane). Ponieważ referencje replikacji są przechowywane na liście weryfikacji, umożliwia to serwerowi podczas łączenia się z repliką pobieranie referencji z listy weryfikacji.

## Tworzenie serwera replik

Ten temat zawiera informacje dotyczące tworzenia serwera replik.

**Uwaga:** Aby można było wykonać to zadanie, serwer musi być uruchomiony.

Rozwiń kategorię **Replication management** (Zarządzanie replikacją) w obszarze nawigacyjnym i kliknij **Manage topology** (Zarządzaj topologią).

1. Wybierz poddrzewo, które chcesz replikować, i kliknij opcję **Show topology** (Pokaż topologię).
2. Kliknij strzałkę obok wyboru **Replication topology** (Topologia replikacji), aby rozwinąć listę serwerów wysyłających.
3. Wybierz serwer wysyłający i kliknij **Add replica** (Dodaj replikę).
4. W zakładce **Server** (Serwer) okna **Add replica** (Dodaj replikę):
  - a. Wprowadź nazwę hosta i numer portu tworzonej repliki. Domyślnym numerem portu jest 389 dla połączeń bez użycia protokołu SSL oraz 636 dla połączeń z SSL. Są to pola wymagane.
  - b. Wybierz komunikację z wykorzystaniem protokołu SSL lub bez niego.

- c. Wpisz nazwę repliki lub pozostaw puste pole, aby użyć nazwy hosta.
  - d. Wpisz identyfikator repliki. Jeśli serwer, na którym tworzona jest replika, jest uruchomiony, kliknij przycisk **Get replica ID** (Pobierz identyfikator repliki), aby automatycznie wypełnić to pole. Jest to pole wymagane, jeśli dodawany serwer ma być serwerem równorzędnym lub przekazującym. Zalecane jest, aby wszystkie serwery były w tej samej wersji.
  - e. Wpisz opis serwera repliki.
5. Na karcie **Additional** (Dodatkowe):

- Podaj referencje, których używa replika do komunikacji z serwerem głównym.

**Uwaga:** Narzędzie Web Administration umożliwia definiowanie referencji w następujących miejscach:

- **cn=replication,cn=localhost**, która powoduje przechowywanie referencji tylko na serwerze, który ich używa.
- W replikowanym poddrzewie, w którym to przypadku referencje są replikowane z resztą poddrzewa. Referencje umieszczone w poddrzewie replikacji są tworzone na podstawie pozycji **ibm-replicagroup=default** dla tego poddrzewa.

Umieszczanie referencji w pozycji **cn=replication,cn=localhost** jest uważane za bardziej bezpieczne. Referencje umieszczone w poddrzewie replikacji są tworzone na podstawie pozycji **ibm-replicagroup=default** dla tego poddrzewa.

- Kliknij **Select** (Wybierz).
  - Wybierz położenie referencji, których chcesz używać. Preferowanym położeniem jest **cn=replication,cn=localhost**.
  - Kliknij **Show credentials** (Pokaż referencje).
  - Rozwiń listę referencji i wybierz te, których chcesz użyć.
  - Kliknij przycisk **OK**.

Dodatkowe informacje o referencjach umowy zawiera temat Tworzenie referencji replikacji.

- Wybierz harmonogram replikacji z listy rozwijanej lub kliknij przycisk **Add** (Dodaj), aby go dodać. Więcej informacji zawiera temat Tworzenie harmonogramów replikacji.
- Z listy możliwości serwera wysyłającego można usunąć zaznaczenie wszystkich możliwości, które nie mają być replikowane na serwerze odbierającym.

Jeśli w sieci są różne serwery w różnych wersjach, w nowszych wersjach są dostępne możliwości, których brak w wersjach wcześniejszych. Niektóre możliwości, takie jak filtrowanie list ACL i strategia haseł, używają atrybutów operacyjnych replikowanych z innymi zmianami. W większości przypadków, jeśli te funkcje są używane, wszystkie serwery powinny je obsługiwać. Jeśli nie wszystkie serwery obsługują daną możliwość, lepiej z niej nie korzystać. Na przykład nie powinno być różnych list ACL na każdym serwerze. Jednak zdarzają się przypadki, w których można używać danej możliwości na obsługujących ją serwerach i nie replikować zmian dotyczących tej możliwości na serwery, które jej nie obsługują. W takich przypadkach można używać listy możliwości do oznaczania konkretnych możliwości, które nie będą replikowane.

- Jako metodę replikacji wybierz opcję Single threaded (Jednowątkowa) lub Multi-threaded (Wielowątkowa). W przypadku replikacji wielowątkowej należy także podać liczbę (od 2 do 32) połączeń wykorzystywanych do replikacji. Domyślna liczba połączeń to 2.
- Kliknij **OK**, aby utworzyć replikę.

6. Wyświetlony zostanie komunikat informujący o tym, że należy podjąć dodatkowe działania. Kliknij przycisk **OK**.

**Uwaga:** Jeśli dodajesz kolejne serwery jako dodatkowe repliki lub tworzysz złożoną topologię, nie przechodź do czynności Kopiowanie danych do repliki lub Dodawanie informacji o serwerze wysyłającym do nowej repliki do momentu zakończenia definiowania topologii na serwerze głównym. Jeśli po zakończeniu definiowania topologii utworzony zostanie plik *masterfile.ldif*, zawierać on będzie pozycje katalogu serwera głównego i pełną kopię umów topologii. Podczas ładowania tego pliku na wszystkie serwery, każdy z nich będzie zawierał te same informacje.

## Kopiowanie danych do repliki

Ten temat zawiera informacje dotyczące kopiowania danych do repliki.

Po utworzeniu repliki należy wyeksportować topologię z serwera głównego do repliki.

1. Na serwerze głównym utwórz plik LDIF dla danych. Aby przekopiować wszystkie dane znajdujące się na serwerze głównym, wykonaj następujące czynności:
  - a. W programie System i Navigator rozwiń pozycję **Sieć**.
  - b. Rozwiń pozycję **Serwery**.
  - c. Kliknij **TCP/IP**.
  - d. Prawym przyciskiem myszy kliknij **IBM Directory Server** i wybierz opcję **Narzędzia**, a następnie **Eksportuj plik**.
  - e. Określ nazwę wyjściowego pliku LDIF (na przykład `masterfile.ldif`), opcjonalnie określ poddrzewo do eksportu (na przykład `subtreeDN`), a następnie kliknij przycisk **OK**.
2. Na maszynie, na której tworzysz replikę, wykonaj następujące czynności:
  - a. Sprawdź, czy replikowane przyrostki zostały zdefiniowane w konfiguracji serwera repliki.
  - b. Zatrzymaj serwer replik.
  - c. Przekopiuj plik LDIF do repliki i wykonaj następujące czynności:
    - 1) W programie System i Navigator rozwiń pozycję **Sieć**.
    - 2) Rozwiń pozycję **Serwery**.
    - 3) Kliknij **TCP/IP**.
    - 4) Prawym przyciskiem myszy kliknij element **IBM Directory Server** i wybierz opcję **Narzędzia** (Tools), a następnie opcję **Importuj plik** (Import file).
    - 5) Określ nazwę wejściowego pliku LDIF (na przykład `masterfile.ldif`), opcjonalnie określ, czy chcesz replikować dane, a następnie kliknij przycisk **OK**.Umowy replikacji, harmonogramy i referencje (jeśli są przechowywane w poddrzewie replikacji) oraz dane pozycji zostaną załadowane do repliki.
  - d. Uruchom serwer.

## Dodawanie informacji o serwerze wysyłającym do nowej repliki

W tym temacie opisano dodawanie informacji o serwerze wysyłającym do nowej repliki.

Konfigurację repliki należy zmienić, aby określała kto ma uprawnienia do replikacji zmian, a następnie dodać odwołanie do serwera głównego.

Na maszynie, na której tworzysz replikę:

1. Rozwiń kategorię **Replication management** (Zarządzanie replikacją) w obszarze nawigacyjnym i kliknij **Manage replication properties** (Zarządzaj właściwościami replikacji).

**Uwaga:** Aby możliwa była zmiana ustawień w panelach **Manage replication properties** (Zarządzanie właściwościami replikacji), należy zalogować się do narzędzia Web Administration jako użytkownik rzutowany systemu OS/400 z uprawnieniami specjalnymi `*ALLOBJ` i `*IOSYSCFG`.

2. Kliknij przycisk **Add** (Dodaj).
3. Wybierz z rozwijanego menu **Replicated subtree** (Replikowane poddrzewo) lub wpisz nazwę replikowanego poddrzewa, dla którego chcesz skonfigurować referencje serwera wysyłającego. Podczas edycji referencji serwera wysyłającego pole to jest niedostępne.
4. Wpisz nazwę wyróżniającą łączenia replikacji. W tym przykładzie jest to `cn=any`.

**Uwaga:** W zależności od sytuacji można użyć dowolnej z tych dwóch opcji.

- Ustaw nazwę wyróżniającą łączenia (i hasło) oraz domyślne odwołanie dla wszystkich poddrzew replikowanych na serwerze za pomocą "domyślnych referencji i odwołań". Można tego użyć, gdy wszystkie poddrzewa są replikowane z tego samego serwera wysyłającego.
  - Ustaw nazwę wyróżniającą łączenia i hasło osobno dla każdego replikowanego poddrzewa, dodając dane serwera wysyłającego dla każdego poddrzewa. Można tego użyć, gdy każde poddrzewo ma inny serwer wysyłający (to znaczy inny serwer główny dla każdego poddrzewa).
5. W zależności od typu referencji wprowadź i potwierdź hasło uwierzytelniania (zapisane wcześniej w celu użycia w przyszłości).
- **Proste łączenie** - określa nazwę wyróżniającą i hasło
  - **Kerberos** - jeśli referencje serwera wysyłającego nie identyfikują nazwy użytkownika i hasła, czyli ma zostać użyta własna nazwa użytkownika usługi serwera, to nazwą wyróżniającą łączenia jest `ibm-kn=ldap/<nazwa_serwera@dzielzina>`. Jeśli referencje zawierają nazwę użytkownika, na przykład `<nazwa_uzytkownika@dzielzina>`, należy jej użyć jako nazwy wyróżniającej. W obu przypadkach hasło nie jest wymagane.
  - **Łączenie SSL w/ EXTERNAL** - podaj nazwę wyróżniającą podmiotu dla certyfikatu i nie podawaj hasła. Więcej informacji zawiera temat "Tworzenie referencji replikacji" na stronie 149.
6. Kliknij przycisk **OK**.
7. Aby uaktywnić wprowadzone zmiany, należy zrestartować serwer replik.

Więcej informacji zawiera temat "Zmiana właściwości replikacji" na stronie 161.

Replika jest w stanie zawieszenia i nie jest wykonywana żadna replikacja. Po zakończeniu konfigurowania topologii replikacji należy kliknąć kategorię **Manage queues** (Zarządzaj kolejkami), wybrać replikę i kliknąć przycisk **Suspend/resume** (Wstrzymaj/wznów), aby uruchomić replikację. Szczegółowe informacje zawiera temat "Zarządzanie kolejkami replikacji" na stronie 165. Replika odbiera teraz aktualizacje z serwera głównego.

## Tworzenie prostej topologii z replikacją między serwerami równorzędnymi

Replikacja między serwerami równorzędnymi to topologia replikacji, w której występuje wiele serwerów głównych. Replikacji między serwerami równorzędnymi można używać tylko w środowiskach, w których kierunki aktualizowania są dobrze znane.

Aktualizacje poszczególnych obiektów w katalogu muszą być wprowadzane tylko przez jeden serwer równorzędny. Umożliwia to uniknięcie scenariusza, w którym jeden serwer usuwa obiekt, po czym inny serwer go modyfikuje. Taki scenariusz stwarza możliwość, że serwer równorzędny odbierze komendę usunięcia, a następnie zmodyfikowania tego samego obiektu, co spowoduje konflikt. Replikowane żądania usunięcia i zmiany nazwy są akceptowane w kolejności odbierania bez rozstrzygania konfliktów. Aby dowiedzieć się więcej o rozstrzygnięciu konfliktów replikacji, zapoznaj się z informacjami pokrewnymi wymienionymi poniżej.

Rozwiń kategorię **Replication management** (Zarządzanie replikacją) w obszarze nawigacyjnym i kliknij **Manage topology** (Zarządzaj topologią).

1. Wybierz poddrzewo, które chcesz replikować, i kliknij opcję **Show topology** (Pokaż topologię).
2. Jeśli chcesz wyświetlić istniejącą topologię, kliknij pole obok istniejących serwerów, aby rozwinąć listę serwerów wysyłających.
3. Kliknij opcję **Add master** (Dodaj serwer główny).

Na karcie **Server** (Serwer) w oknie **Add master** (Dodaj serwer główny) wykonaj następujące czynności:

- Wprowadź nazwę hosta i numer portu tworzonego serwera. Domyślnym numerem portu jest 389 dla połączeń bez użycia protokołu SSL oraz 636 dla połączeń z SSL. Są to pola wymagane.
- Wybierz komunikację z wykorzystaniem protokołu SSL lub bez niego.
- Wybierz, czy serwer ma być serwerem-bramą.
- Wpisz nazwę serwera lub pozostaw puste pole, aby użyć nazwy hosta.



- Wpisz identyfikator serwera. Jeśli serwer, na którym tworzony jest serwer równorzędny-główny, jest uruchomiony, kliknij przycisk **Get server ID** (Pobierz identyfikator serwera), aby automatycznie wypełnić to pole. Jeśli identyfikator serwera nie jest znany, wpisz **nieznany**.
- Wpisz opis serwera.
- Należy podać referencje, których serwer używa do komunikacji z serwerem głównym. Kliknij przycisk **Select** (Wybierz).

**Uwaga:** Narzędzie Web Administration umożliwia definiowanie referencji w następujących lokalizacjach:

- **cn=replication,cn=localhost**, w przypadku której referencje są przechowywane tylko na serwerze, który ich używa. Umieszczanie referencji w pozycji **cn=replication,cn=localhost** jest uważane za bardziej bezpieczne.
- **cn=replication,cn=IBMpolicies**, która jest dostępna nawet wtedy, gdy serwer, pod którym użytkownik próbuje dodać replikę, nie jest serwerem, do którego jest on podłączony za pomocą narzędzia Web Administration. Referencje umieszczone w tym miejscu są replikowane na serwery.

**Uwaga:** Lokalizacja **cn=replication,cn=IBMpolicies** jest dostępna tylko wtedy, gdy OID obsługi poddrzewa **IBMpolicies**, 1.3.18.0.2.32.18, jest obecny w atrybucie **ibm-supportedcapabilities** głównego DSE.

- W replikowanym poddrzewie, w którym to przypadku referencje są replikowane z resztą poddrzewa. Referencje umieszczone w poddrzewie replikacji są tworzone na podstawie pozycji **ibm-replicagroup=default** dla tego poddrzewa.
  1. Wybierz położenie referencji, których chcesz używać. Preferowanym położeniem jest **cn=replication,cn=localhost**.
  2. Jeśli utworzono już zestaw referencji, kliknij opcję Show credentials (Pokaż referencje).
  3. Rozwiń listę referencji i wybierz te, których chcesz użyć.
  4. Kliknij przycisk OK.
  5. Jeśli nie ma wcześniejszych referencji, kliknij przycisk Add (Dodaj), aby je utworzyć.

W zakładce **Additional** (Dodatkowe):

1. Wybierz harmonogram replikacji z listy rozwijanej lub kliknij przycisk **Add** (Dodaj), aby go dodać. Więcej informacji zawiera temat Tworzenie harmonogramów replikacji.
2. Z listy możliwości serwera wysyłającego można usunąć zaznaczenie wszystkich możliwości, które nie mają być replikowane na serwerze odbierającym.

Jeśli w sieci są różne serwery w różnych wersjach, w nowszych wersjach są dostępne możliwości, których brak w wersjach wcześniejszych. Niektóre możliwości, takie jak filtrowanie list ACL i strategia haseł, używają atrybutów operacyjnych replikowanych z innymi zmianami. W większości przypadków, jeśli te opcje są używane, wszystkie serwery powinny je obsługiwać. Jeśli nie wszystkie serwery obsługują daną możliwość, lepiej z niej nie korzystać. Na przykład nie powinno być różnych list ACL na każdym serwerze. Jednak zdarzają się przypadki, w których można używać danej możliwości na obsługujących ją serwerach i nie replikować zmian dotyczących tej możliwości na serwery, które jej nie obsługują. W takich przypadkach można używać listy możliwości do oznaczania konkretnych możliwości, które nie będą replikowane.

3. Zaznacz pole wyboru **Add credential information on consumer** (Dodaj informacje o referencjach na serwerze odbierającym), jeśli chcesz włączyć dynamiczne aktualizowanie referencji serwera wysyłającego. Wybór ten automatycznie aktualizuje referencje serwera wysyłającego w pliku konfiguracyjnym serwera odbierającego. Umożliwia to replikację informacji o topologii do serwera.
  - Wpisz nazwę wyróżniającą administratora serwera odbierającego. Na przykład **cn=root**.

**Uwaga:** Jeśli nazwą wyróżniającą administratora utworzoną podczas konfigurowania serwera była **cn=root**, wpisz pełną nazwę wyróżniającą administratora. Nie używaj samego określenia **root**.

- Wpisz hasło administratora serwera odbierającego. Na przykład **tajne\_hasło**.
4. Kliknij przycisk **OK**.

5. Umowy między serwerami wysyłającymi i odbierającymi są wyświetlane między nowym serwerem głównym a istniejącymi serwerami. Anuluj zaznaczenie umów, których nie chcesz tworzyć. Jest to szczególnie ważne podczas tworzenia serwera-bramy.
6. Kliknij przycisk **Continue** (Kontynuuj).
7. Mogą zostać wyświetlone komunikaty informujące o tym, że należy podjąć dodatkowe działania. Wykonaj odpowiednie czynności lub zanotuj je. Po zakończeniu kliknij przycisk **OK**.
8. Dodaj odpowiednie referencje.

**Uwaga:** W niektórych przypadkach zostanie wyświetlony panel Select credentials (Wybór referencji) z zapytaniem o referencje znajdujące się w innym miejscu niż cn=replication,cn=localhost. W takich sytuacjach należy podać obiekt referencji znajdujący się w miejscu innym niż cn=replication,cn=localhost. Należy wybrać referencje dla poddrzewa z istniejących zestawów lub utworzyć nowe referencje.

9. Kliknij przycisk **OK**, aby utworzyć serwer równorzędny-główny.
10. Mogą zostać wyświetlone komunikaty informujące o tym, że należy podjąć dodatkowe działania. Wykonaj odpowiednie czynności lub zanotuj je. Po zakończeniu kliknij przycisk **OK**.

#### Odsyłacze pokrewne

“Replikacja - przegląd” na stronie 37

Poprzez replikację zmiany wprowadzone w jednym katalogu są rozsyłane do jednego lub wielu dodatkowych katalogów. Dzięki temu zmiana w jednym katalogu jest widoczna w wielu różnych katalogach.

## Tworzenie złożonej topologii replikacji

Ten przegląd zawiera wytyczne dotyczące konfigurowania złożonej topologii replikacji.

1. Uruchom wszystkie serwery równorzędne lub te, które mają być replikami. Wymagane jest, aby w programie Web Administration pobrać informacje z serwerów.
2. Uruchom 'pierwszy' serwer główny i skonfiguruj go jako serwer główny dla kontekstu.
3. Załaduj dane dla poddrzewa, które ma być replikowane na 'pierwszym' serwerze głównym, jeśli nie zostały jeszcze załadowane.
4. Wybierz poddrzewo do replikacji.
5. Dodaj wszystkie potencjalne serwery równorzędne jako repliki 'pierwszego' serwera głównego.
6. Dodaj wszystkie pozostałe repliki.
7. Przenieś wszystkie równorzędne serwery główne, aby je awansować.
8. Dodaj umowy replik do wszystkich równorzędnych serwerów głównych.

**Uwaga:** Jeśli referencje mają być tworzone w **cn=replication,cn=localhost**, należy je utworzyć na każdym serwerze po ich zrestartowaniu. Replikacja przez serwery równorzędne nie powiedzie się do momentu utworzenia obiektów referencji.

9. Dodaj umowy replik dla innych serwerów głównych do równorzędnych serwerów głównych. 'Pierwszy' serwer główny zawiera już te informacje.
10. Wygaś replikowane poddrzewo. Zapobiega to aktualizacji podczas kopiowania danych na inne serwery.
11. Użyj zarządzania kolejkami, aby pominąć wszystkie dla każdej kolejki.
12. Wyeksportuj dane dla replikowanego poddrzewa z 'pierwszego' serwera głównego.
13. Cofnij wygaszenie poddrzewa.
14. Zatrzymaj serwery replik i zaimportuj dane dla replikowanego poddrzewa na wszystkie repliki i równorzędne serwery główne. Następnie zrestartuj serwery.
15. Zarządzaj właściwościami replikacji na każdej replice i równorzędnym serwerze głównym, aby ustawić referencje używane przez serwery wysyłające.

## Tworzenie złożonej topologii z replikacją między serwerami równorzędnymi

Ten temat zawiera informacje dotyczące tworzenia złożonej topologii z replikacją między serwerami równorzędnymi.

Replikacja między serwerami równorzędnymi to topologia replikacji, w której występuje wiele serwerów głównych. Jednak w przeciwieństwie do środowiska o wielu serwerach głównych między serwerami równorzędnymi nie ma żadnych konfliktów. Serwery LDAP akceptują aktualizacje udostępniane przez serwery równorzędne i aktualizują ich własne kopie danych. Nie ma żadnego znaczenia kolejność odbieranych aktualizacji lub to, czy wiele aktualizacji powoduje jakikolwiek konflikt.

Aby dodać serwery główne (równorzędne), najpierw należy dodać serwer jako replikę tylko do odczytu istniejących serwerów głównych (patrz sekcja “Tworzenie serwera replik” na stronie 151), zainicjować dane katalogu, a następnie awansować serwer na serwer główny (patrz “Przenoszenie i awansowanie serwera” na stronie 174).

Początkowo obiekt **ibm-replicagroup** utworzony przez ten proces dziedziczy listę ACL pozycji głównej replikowanego poddrzewa. Te listy ACL mogą być nieodpowiednie do kontroli praw dostępu do informacji o replikacji w katalogu.

Aby operacja dodania poddrzewa zakończyła się sukcesem, nazwa wyróżniająca dodawanej pozycji musi mieć odpowiednie listy ACL, jeśli nie jest przyrostkiem na serwerze.

#### W przypadku niefiltrowanych list ACL:

- ownersource : <nazwa wyróżniająca pozycji>
- ownerpropagate : TRUE
- acsource : <nazwa wyróżniająca pozycji>
- acpropagate: TRUE

#### W przypadku filtrowanych list ACL:

- ownersource : <nazwa wyróżniająca pozycji>
- ownerpropagate : TRUE
- ibm-filteraclinherit : FALSE
- ibm-filteraclentry : <dowolna wartość>

Funkcja **Edit ACLs** (Edycja list ACL) programu Web Administration umożliwia ustawienie list ACL dla informacji replikacji powiązanych z nowo tworzonym replikowanym poddrzewem (patrz “Edytowanie list kontroli dostępu” na stronie 176).

Replika jest w stanie zawieszenia i nie jest wykonywana żadna replikacja. Po zakończeniu konfigurowania topologii replikacji należy kliknąć kategorię **Manage queues** (Zarządzaj kolejkami), wybrać replikę i kliknąć przycisk **Suspend/resume** (Wstrzymaj/wznów), aby uruchomić replikację. Szczegółowe informacje zawiera temat “Zarządzanie kolejkami replikacji” na stronie 165. Replika odbiera teraz aktualizacje z serwera głównego.

Replikacji równorzędnej można używać tylko w środowiskach, w których aktualizacje wzorca katalogu są dobrze znane. Aktualizacje poszczególnych obiektów w katalogu muszą być wprowadzane tylko przez jeden serwer równorzędny. Umożliwia to uniknięcie w scenariuszu z jednym serwerem usunięcia obiektu, po którym następuje modyfikacja obiektu przez inny serwer. Ten scenariusz stwarza możliwość, że serwer równorzędny odbierze komendę usunięcia, a następnie modyfikacji, co spowoduje konflikt.

Aby zdefiniować topologię serwer równorzędny-przekazujący-replika składającą się z serwerów równorzędny-główny, dwóch serwerów przekazujących i czterech replik:

1. Utwórz serwer główny i serwer replik. Więcej informacji zawiera temat “Tworzenie topologii serwer główny - replika” na stronie 146.
2. Utwórz dwa dodatkowe serwery replik dla serwera głównego. Więcej informacji zawiera temat “Tworzenie serwera replik” na stronie 151.
3. Utwórz dwie repliki na każdym z dwóch nowo utworzonych serwerów replik.
4. Awansuj pierwotną replikę na serwer główny. Więcej informacji zawiera temat “Awansowanie serwera do serwera równorzędnego” na stronie 158.

**Uwaga:** Serwer, który chcesz awansować do serwera głównego, musi być repliką-liściem bez podrzędnych replik.

5. Skopiuj dane z serwera głównego na nowy serwer główny i repliki. Więcej informacji zawiera temat “Kopiowanie danych do repliki” na stronie 153.

#### Zadania pokrewne

“Przenoszenie i awansowanie serwera” na stronie 174

Ten temat zawiera informacje dotyczące przenoszenia i awansowania serwera.

## Awansowanie serwera do serwera równorzędnego

Ten temat zawiera informacje dotyczące awansowania serwera do serwera równorzędnego.

Używając topologii przekazywania utworzonej w sekcji “Tworzenie topologii serwer główny - przekazujący - replika” na stronie 147, serwer można awansować do serwera równorzędnego. W tym przykładzie przedstawiono awansowanie repliki (serwer3) do serwera równorzędnego na serwerze głównym (serwer1).

1. Podłącz Web Administration do serwera głównego (serwer1).
2. Rozwiń kategorię Replication management (Zarządzanie replikacją) w obszarze nawigacyjnym i kliknij opcję **Manage topology** (Zarządzaj topologią).
3. Wybierz poddrzewo, które chcesz replikować, i kliknij opcję **Show topology** (Pokaż topologię).
4. Kliknij strzałkę obok wyboru **Replication topology** (Topologia replikacji), aby rozwinąć listę serwerów.
5. Kliknij strzałkę obok wyboru **serwer1**, aby rozwinąć listę serwerów.
6. Kliknij strzałkę obok wyboru **serwer2**, aby rozwinąć listę serwerów.
7. Kliknij **serwer1** i kliknij przycisk **Add replica** (Dodaj replikę). Utwórz serwer4. Więcej informacji zawiera temat “Tworzenie serwera replik” na stronie 151. Wykonaj tę samą procedurę, aby utworzyć serwer5. W narzędziu Web Administration role serwera są reprezentowane przez ikony. Wybraną topologią jest:
  - serwer1 (główny)
    - serwer2 (przekazujący)
      - serwer3 (replika)
      - serwer4 (replika)
      - serwer5 (replika)
8. Kliknij **serwer2**, a następnie kliknij przycisk **Add replica** (Dodaj replikę), aby utworzyć serwer6.
9. Kliknij **serwer4**, a następnie kliknij przycisk **Add replica** (Dodaj replikę), aby utworzyć serwer7. Wykonaj tę samą procedurę, aby utworzyć serwer8. Wybraną topologią jest:
  - serwer1 (główny)
    - serwer2 (przekazujący)
      - serwer3 (replika)
      - serwer6 (replika)
    - serwer4 (przekazujący)
      - serwer7 (replika)
      - serwer8 (replika)
    - serwer5 (replika)
10. Wybierz **serwer5** i kliknij przycisk **Move** (Przenieś).

**Uwaga:** Serwer, który chcesz przenieść, musi być repliką-liściem bez podrzędnych replik.

11. Wybierz opcję **Replication topology** (Topologia replikacji), aby awansować replikę do serwera głównego. Kliknij przycisk **Move** (Przenieś).
12. Wyświetlony zostanie panel **Create additional supplier agreements** (Tworzenie dodatkowych umów serwera wysyłającego). Replikacja serwera równorzędnego wymaga, aby każdy serwer główny był serwerem wysyłającym i odbierającym dla wszystkich innych serwerów głównych w topologii i dla każdej z replik pierwszego poziomu, serwer2 i serwer4. Serwer5 jest już serwerem odbierającym serwer1 i teraz musi się stać serwerem wysyłającym dla serwerów serwer1, serwer2 i serwer4. Sprawdź, czy pola umów serwera wysyłającego

są zaznaczone dla:

Tabela 5.

	Serwer wysyłający	Serwer odbierający
✓	serwer5	serwer1
✓	serwer5	serwer2
✓	serwer5	serwer4

Kliknij przycisk **Continue** (Kontynuuj).

**Uwaga:** W niektórych przypadkach wyświetlony zostanie panel wyboru referencji z zapytaniem o referencje znajdujące się w innym miejscu niż `cn=replication,cn=localhost`. W takich sytuacjach należy podać obiekt referencji znajdujący się w miejscu innym niż `cn=replication,cn=localhost`. Wybierz referencje z istniejących zestawów lub utwórz nowe referencje, których poddrzewo ma użyć. Więcej informacji zawiera temat “Tworzenie referencji replikacji” na stronie 149.

13. Kliknij przycisk **OK**. Wybraną topologią jest:

- serwer1 (główny)
  - serwer2 (przekazujący)
  - serwer3 (replika)
  - serwer6 (replika)
  - serwer4 (przekazujący)
  - serwer7 (replika)
  - serwer8 (replika)
  - serwer5 (główny)
- serwer5 (główny)
  - serwer1 (główny)
  - serwer2 (przekazujący)
  - serwer4 (przekazujący)

14. Skopiuj dane z serwera serwer1 do wszystkich serwerów. Informacje, jak to zrobić, zawiera sekcja “Kopiowanie danych do repliki” na stronie 153.

## Konfigurowanie topologii bramy

Ten temat zawiera informacje dotyczące konfigurowania topologii bramy.

Przed rozpoczęciem konfigurowania topologii replikacji, należy utworzyć kopię zapasową oryginalnego pliku `ibmslapd.conf`. Z kopii tej można skorzystać w celu odtworzenia oryginalnej konfiguracji, w przypadku wystąpienia trudności podczas replikacji.

Aby skonfigurować bramę przy użyciu złożonej topologii z replikacją między serwerami równorzędnymi według procedury opisanej w temacie Awansowanie serwera na serwer równorzędny, należy wykonać następujące czynności:

- Dokonaj konwersji istniejącego serwera równorzędnego (peer 1) na serwer-bramę, aby utworzyć ośrodek replikacji 1.
  - Utwórz nowy serwer-bramę dla ośrodka replikacji 2 oraz umowy z serwerem równorzędnym peer 1.
  - Utwórz topologię dla ośrodka replikacji 2 (nie omówione w tym przykładzie).
  - Skopiuj dane z serwera głównego do wszystkich maszyn w topologii.
1. Użyj narzędzia Web Administration, aby zalogować się do serwera głównego (serwer1).
  2. Rozwiń kategorię **Replication management** (Zarządzanie replikacją) w obszarze nawigacyjnym i kliknij **Manage topology** (Zarządzaj topologią).
  3. Wybierz poddrzewo, które chcesz replikować, i kliknij opcję **Show topology** (Pokaż topologię).

4. Aby przekształcić istniejący serwer w serwer-bramę, wybierz pozycję **Manage gateway servers** (Zarządzanie serwerami-bramami). Wybierz **serwer1** lub jego serwer równorzędny **serwer5**. Dla potrzeb tego przykładu wybierz **serwer1** i kliknij **Make gateway** (Wyznacz na bramę).
5. Kliknij przycisk **OK**.

**Uwaga:** Jeśli serwer, który ma zostać użyty jako brama nie jest jeszcze serwerem głównym, musi on być repliką-liściem bez podrzędnych replik, który należy najpierw awansować na serwer główny, a następnie wyznaczyć jako bramę.

6. Aby utworzyć nowy serwer-bramę, kliknij opcję **Add server** (Dodaj serwer).
7. Utwórz nowy serwer o nazwie **serwer9** jako serwer-bramę. Informacje o tej czynności zawiera temat “Dodawanie serwera równorzędny-główny lub serwera-bramy” na stronie 169.
8. Wyświetlony zostanie panel **Create additional supplier agreements** (Tworzenie dodatkowych umów serwera wysyłającego). W tym panelu sprawdź, czy pola umów serwera wysyłającego zaznaczone są tylko dla serwera serwer1. Anuluj wybór pozostałych umów.

	Serwer wysyłający	Serwer odbierający
✓	serwer1	serwer9
✓	serwer9	serwer1
	serwer2	serwer9
	serwer9	serwer2
	serwer4	serwer9
	serwer9	serwer4
	serwer9	serwer5
	serwer5	serwer9

9. Kliknij przycisk **Continue** (Kontynuuj).
10. Kliknij przycisk **OK**.
11. Dodaj odpowiednie referencje i dane serwera odbierającego.

**Uwaga:** W niektórych przypadkach wyświetlony zostanie panel **Select credentials** (Wybór referencji) z zapytaniem o referencje znajdujące się w innym miejscu niż cn=replication,cn=localhost. W takich sytuacjach należy podać obiekt referencji znajdujący się w miejscu innym niż cn=replication,cn=localhost. Należy wybrać referencje dla poddrzewa z istniejących zestawów lub utworzyć nowe referencje. Dodatkowe informacje o referencjach umowy zawiera temat Tworzenie referencji replikacji.

12. Kliknij przycisk **OK**. W narzędziu Web Administration role serwera są reprezentowane przez ikony. Wybraną topologią jest:
  - serwer1 (główny-brama dla ośrodka replikacji 1)
    - serwer2 (przekazujący)
    - serwer3 (replika)
    - serwer6 (replika)
    - serwer4 (przekazujący)
    - serwer7 (replika)
    - serwer8 (replika)
    - serwer5 (główny)
    - serwer9 (główny-brama dla ośrodka replikacji 2)
  - serwer5 (główny)
    - serwer1 (główny)
    - serwer2 (przekazujący)

- | - serwer3 (replika)
  - | - serwer6 (replika)
  - | - serwer4 (przekazujący)
  - | - serwer7 (replika)
  - | - serwer8 (replika)
  - | • serwer9 (główny-brama)
  - | - serwer1 (główny-brama)
- | 13. Dodaj serwery do pozycji **serwer9**, aby utworzyć topologię dla ośrodka replikacji 2. Pamiętaj, aby anulować wybór wszelkich umów nowych serwerów z wszelkimi serwerami znajdującymi się poza ośrodkiem replikacji 2.
  - | 14. Powtórz te czynności, aby utworzyć dodatkowe ośrodki replikacji. Należy pamiętać, aby dla jednego ośrodka replikacji utworzyć tylko jeden serwer-bramę. Każdy serwer-brama musi jednak być obecny w topologiach obejmujących umowy z innymi serwerami tego typu.
  - | 15. Po zakończeniu tworzenia topologii skopiuj dane z serwera serwer1 do wszystkich nowych serwerów we wszystkich nowych ośrodkach replikacji i dodaj informacje o serwerze wysyłającym do wszystkich nowych serwerów. Informacje o tej czynności zawierają tematy Kopiowanie danych na replikę i Dodawanie do nowej repliki informacji o serwerze wysyłającym.

### Zadania pokrewne

“Dodawanie repliki” na stronie 168

Ten temat zawiera informacje dotyczące dodawania repliki.

“Dodawanie serwera równorzędny-główny lub serwera-bramy” na stronie 169

W tym temacie znajdują się informacje o tworzeniu nowego serwera równorzędny-główny lub serwera-bramy.

“Zarządzanie serwerami-bramami” na stronie 172

Ten temat zawiera informacje o zarządzaniu serwerami-bramami. Istnieje możliwość wskazania serwera głównego jako serwera pełniącego funkcję bramy w ośrodku replikacji.

## Zmiana właściwości replikacji

Ten temat zawiera informacje dotyczące modyfikowania właściwości replikacji.

Aby możliwa była zmiana ustawień w panelach **Manage replication properties** (Zarządzanie właściwościami replikacji), należy zalogować się do narzędzia Web Administration jako użytkownik rzutowany o uprawnieniach specjalnych \*ALLOBJ i \*IOSYSCFG.

1. Rozwiń kategorię **Replication management** (Zarządzanie replikacją) w obszarze nawigacyjnym i kliknij opcję **Manage replication properties** (Zarządzaj właściwościami replikacji).
2. Na tym panelu można wykonywać następujące operacje:
  - a. Zmienianie maksymalnej liczby oczekujących zmian zwracanych przez zapytania o status replikacji. Wartością domyślną jest 200.
  - b. Ustaw maksymalną liczbę błędów replikacji, które serwer będzie protokołować podczas replikowania zmian na serwerze odbierającym. Jeśli serwer korzysta z replikacji jednowątkowej i zostanie przekroczona maksymalna liczba błędów, próba aktualizacji będzie okresowo ponawiana, dopóki nie zakończy się powodzeniem lub dopóki administrator nie usunie zawartości protokołu, aby umożliwić dopisanie błędu. Jeśli serwer korzysta z replikacji wielowątkowej i zostanie przekroczona maksymalna liczba błędów, wszelkie błędy replikacji związane z trwającymi operacjami aktualizacji będą protokołowane, a proces replikacji zostanie wstrzymany do czasu usunięcia zawartości protokołu przez administratora. Zawatość protokołu może zostać usunięta poprzez ponowienie lub usunięcie aktualizacji zakończonych niepowodzeniem. Dla każdego serwera odbierającego utrzymywane są osobne protokoły. Wartością domyślną jest zero (brak).

**Uwaga:** Podanie wartości większej od zera oznacza włączenie protokołowania.

  - c. Zmień wielkość pamięci podręcznej kontekstu replikacji (w bajtach). Wielkością domyślną jest 100000 bajtów.

- d. Ustaw maksymalną wielkość pozycji konfliktów replikacji (w bajtach). Jeśli łączna wielkość pozycji (w bajtach) przekracza wartość podaną w tym polu, pozycja nie będzie ponownie wysyłana przez serwer wysyłający w razie wystąpienia konfliktu replikacji po stronie serwera odbierającego. Wartością domyślną jest 0 (bez ograniczeń).
- e. Dodawanie, edytowanie lub usuwanie danych serwera wysyłającego.

**Uwaga:** Nazwa wyróżniająca serwera wysyłającego może być nazwą wyróżniającą profilu użytkownika rzutowanego systemu i5/OS. Profil użytkownika rzutowanego systemu i5/OS nie może mieć uprawnień do administrowania katalogiem LDAP. Użytkownik nie może mieć uprawnień specjalnych \*ALLOBJ i \*IOSYSCFG i nie można mu nadać uprawnień do administrowania poprzez ID aplikacji administratora serwera katalogów.

Więcej informacji zawierają następujące tematy:

- “Dodawanie informacji o serwerze wysyłającym”
- “Edytowanie informacji o serwerze wysyłającym”
- “Usuwanie informacji o serwerze wysyłającym” na stronie 163

## Dodawanie informacji o serwerze wysyłającym

W tym temacie opisano dodawanie informacji o serwerze wysyłającym.

1. Kliknij przycisk **Add** (Dodaj).
2. Wybierz serwer wysyłający z rozwijanego menu lub wpisz nazwę replikowanego poddrzewa, które chcesz dodać jako serwer wysyłający.
3. Wpisz nazwę DN łączenia replikacji dla referencji.

**Uwaga:** W zależności od sytuacji można użyć dowolnej z tych dwóch opcji.

- Ustaw nazwę wyróżniającą łączenia (i hasło) oraz domyślne odwołanie dla wszystkich poddrzew replikowanych na serwerze za pomocą 'domyślnych referencji i odwołań'. Można tego użyć, gdy wszystkie poddrzewa są replikowane z tego samego serwera wysyłającego.
- Ustaw nazwę wyróżniającą łączenia i hasło osobno dla każdego replikowanego poddrzewa, dodając dane serwera wysyłającego dla każdego poddrzewa. Można tego użyć, gdy każde poddrzewo ma inny serwer wysyłający (to znaczy inny serwer główny dla każdego poddrzewa).

4. W zależności od typu referencji wprowadź i potwierdź hasło uwierzytelniania (zapisane wcześniej w celu użycia w przyszłości).
  - **Proste łączenie** - określa nazwę wyróżniającą i hasło
  - **Kerberos** - określa pseudo nazwę wyróżniającą w postaci 'ibm-kn=LDAP-nazwa-usługi@dzieladina' bez hasła.
  - **Łączenie SSL w/ EXTERNAL** - określa nazwę wyróżniającą tematu dla certyfikatu bez hasła.

Więcej informacji zawiera temat “Tworzenie referencji replikacji” na stronie 149.

5. Kliknij przycisk **OK**.

Poddrzewo serwera wysyłającego jest dodawane do listy informacji na temat serwerów wysyłających.

## Edytowanie informacji o serwerze wysyłającym

W tym temacie opisano edytowanie informacji o serwerze wysyłającym.

1. Wybierz poddrzewo serwera wysyłającego do edycji.
2. Kliknij przycisk **Edit** (Edycja).
3. Jeśli edytujesz **Domyślne referencje i odwołania**, które służą do tworzenia pozycji cn=Master Server pod cn=configuration, w polu Default supplier's LDAP URL (Domyślny adres URL LDAP serwera wysyłającego) wpisz adres URL serwera, z którego klient chce otrzymywać aktualizacje replik. Musi to być poprawny adres URL protokołu LDAP (ldap://). W przeciwnym razie przejdź do punktu 4.
4. Wpisz nazwę wyróżniającą łączenia replikacji dla nowych referencji, których chcesz użyć.
5. Wpisz i potwierdź hasło referencji.
6. Kliknij przycisk **OK**.



- | Hasło nazwy wyróżniającej serwera wysyłającego, który uczestniczy w replikacji, można także zmienić za pomocą
- | komendy Zmiana atrybutów serwera katalogów (Change Directory Server Attributes - CHGDIRSVRA). Aby zmienić
- | hasło nazwy wyróżniającej łączenia replikacji cn=master na "nowehaslo", użyj następującej komendy:
- | CHGDIRSVRA INSTANCE(QUSRDIR) DN('cn=master' 'nowehaslo')

## | **Usuwanie informacji o serwerze wysyłającym**

Ten temat zawiera informacje dotyczące usuwania informacji o serwerze wysyłającym.

1. Wybierz poddrzewo serwera wysyłającego do usunięcia.
2. Kliknij przycisk **Delete** (Usuń).
3. Po wyświetleniu żądania potwierdzenie usunięcia kliknij przycisk **OK**.

Poddrzewo zostanie usunięte z listy danych o serwerach wysyłających.

## **Tworzenie harmonogramów replikacji**

Ten temat zawiera informacje dotyczące tworzenia harmonogramów replikacji.

Opcjonalnie można zdefiniować harmonogramy replikacji, aby zaplanować replikację w konkretnych momentach lub aby nie replikować w określonych dniach i godzinach. Jeśli użytkownik nie chce korzystać z harmonogramu, serwer planuje replikację za każdym razem, gdy wprowadzana jest zmiana. Jest to odpowiednikiem określania harmonogramu z natychmiastowym uruchomieniem replikacji codziennie o 0:00.

Rozwiń kategorię **Replication management** (Zarządzanie replikacją) w obszarze nawigacyjnym i kliknij **Manage schedules** (Zarządzaj harmonogramami).

W zakładce **Weekly schedule** (Harmonogram tygodniowy) wybierz poddrzewo, dla którego chcesz utworzyć harmonogram i kliknij **Show schedules** (Pokaż harmonogramy). Wszystkie istniejące harmonogramy zostaną wyświetlone w oknie **Weekly schedules** (Harmonogramy tygodniowe). Aby utworzyć lub dodać nowy harmonogram, należy wykonać następujące czynności:

1. Kliknij przycisk **Add** (Dodaj).
  2. Wpisz nazwę harmonogramu. Na przykład **harmonogram1**.
  3. Dla każdego dnia, od niedzieli do soboty, harmonogram jest określony jako **Brak**. Oznacza to, że nie zaplanowano żadnych aktualizacji replikacji. Nadal aktywne jest ostatnie zdarzenie replikacji, jeśli miało miejsce. Ponieważ jest to nowa replika, nie ma wcześniejszych zdarzeń replikacji, a przez to domyślnie system planuje natychmiastową replikację.
  4. Można wybrać dzień i kliknąć **Add a daily schedule** (Dodaj harmonogram dzienny), aby utworzyć dzienny harmonogram replikacji. Jeśli utworzony zostanie dzienny harmonogram, staje się on domyślnym harmonogramem dla każdego dnia tygodnia. Można wykonać następujące czynności:
    - Pozostawić dzienny harmonogram jako domyślny dla każdego dnia lub wybrać konkretny dzień i zmienić harmonogram z powrotem na brak. Należy pamiętać, że ostatnie zdarzenie replikacji, które wystąpiło, jest wciąż aktywne dla dnia, na który nie zaplanowano zdarzeń replikacji.
    - Zmienić dzienny harmonogram, wybierając dzień i klikając **Edit a daily schedule** (Edycja dziennego harmonogramu). Należy pamiętać, że zmiany dziennego harmonogramu mają wpływ na wszystkie dni, w których używany jest ten harmonogram, a nie tylko na wybrany dzień.
    - Utworzyć dzienny harmonogram, wybierając dzień i klikając **Add a daily schedule** (Dodaj dzienny harmonogram). Po utworzeniu tego harmonogramu jest on dodawany do menu rozwijanego **Daily schedule** (Harmonogram dzienny). Ten harmonogram należy wybrać dla każdego dnia, w którym ma być używany.
- Sekcja "Tworzenie harmonogramu codziennej replikacji" na stronie 164 zawiera więcej informacji na temat konfigurowania harmonogramów dziennych.
5. Po zakończeniu kliknij przycisk **OK**.

### **Zadania pokrewne**

“Wyświetlanie harmonogramu replikacji” na stronie 173

Aby wyświetlić harmonogram replikacji za pomocą narzędzia Web Administration, należy wykonać czynności opisane w tym temacie.

## Tworzenie harmonogramu codziennej replikacji

Ten temat zawiera informacje dotyczące tworzenia harmonogramu codziennej replikacji.

Rozwiń kategorię **Replication management** (Zarządzanie replikacją) w obszarze nawigacyjnym i kliknij **Manage schedules** (Zarządzaj harmonogramami).

W zakładce **Daily schedule** (Harmonogram dzienny) wybierz poddrzewo, dla którego chcesz utworzyć harmonogram i kliknij **Show schedules** (Pokaż harmonogramy). Wszystkie istniejące harmonogramy zostaną wyświetlone w oknie **Daily schedules** (Harmonogramy dzienne). Aby utworzyć lub dodać nowy harmonogram, należy wykonać następujące czynności:

1. Kliknij przycisk **Add** (Dodaj).
2. Wpisz nazwę harmonogramu. Na przykład **poniedziałek1**.
3. Wybierz strefę czasową: UTC lub lokalną.
4. Wybierz typ replikacji z rozwijanego menu.

### **Immediate (Natychmiastowa)**

Wykonuje wszystkie oczekujące aktualizacje pozycji od ostatniej replikacji, a następnie stale aktualizuje pozycje do następnej zaplanowanej aktualizacji.

### **Once (Raz)**

Wykonuje wszystkie oczekujące aktualizacje przed czasem rozpoczęcia. Wszystkie aktualizacje dokonane po czasie rozpoczęcia czekają do czasu następnego zaplanowanego zdarzenia replikacji.

5. Określ czas początkowy (według czasu miejscowego serwera) dla zdarzenia replikacji.
6. Kliknij przycisk **Add** (Dodaj). Wyświetlone zostaną: typ i czas zdarzenia replikacji.
7. Dodaj lub usuń zdarzenia, aby zakończyć harmonogram. Lista zdarzeń zostanie odświeżona w porządku chronologicznym.
8. Po zakończeniu kliknij przycisk **OK**.

Na przykład:

Typ replikacji	Czas uruchomienia
Immediate (Natychmiastowa)	0:00
Once (Raz)	10:00
Once (Raz)	14:00
Immediate (Natychmiastowa)	16:00
Once (Raz)	20:00

W tym harmonogramie pierwsze zdarzenie replikacji występuje o północy i aktualizuje wszystkie oczekujące zmiany. Aktualizacje replikacji są kontynuowane, jeśli zostały wprowadzone do godziny 10:00. Aktualizacje wprowadzone między 10:00 i 14:00 oczekują replikację do 14:00. Wszystkie aktualizacje wprowadzone między 14:00 a 16:00 oczekują na replikację zaplanowaną na 16:00, późniejsze aktualizacje oczekują do następnego zaplanowanego zdarzenia replikacji o 20:00. Wszystkie aktualizacje dokonane po godzinie 20:00 czekają do czasu następnego zaplanowanego zdarzenia replikacji.

**Uwaga:** Jeśli zdarzenia replikacji są zaplanowane zbyt często, replikacja może nie zostać wykonana, jeśli aktualizacje z poprzedniego zdarzenia trwają nadal w chwili, na którą zaplanowane jest następne zdarzenie.

## Zarządzanie kolejkami replikacji

Ten temat zawiera informacje dotyczące monitorowania statusu replikacji dla każdej umowy replikacji (kolejki) używanej przez dany serwer.

1. Rozwiń kategorię **Replication management** (Zarządzanie replikacją) w obszarze nawigacyjnym i kliknij **Manage queues** (Zarządzaj kolejkami).
2. Wybierz replikę, której kolejką chcesz zarządzać.
3. W zależności od statusu repliki kliknij przycisk **Suspend/resume** (Zawieś/wznów), aby zakończyć lub rozpocząć replikację.
4. Kliknij przycisk **Force replication** (Wymuś replikację), aby dokonać replikacji wszystkich zmian bez względu na to, na kiedy zaplanowana jest najbliższa replikacja.
5. Kliknij **Queue details** (Szczegóły kolejki), aby uzyskać pełne informacje na temat kolejki repliki. Kolejka można zarządzać również za pomocą tej opcji.
6. Kliknij opcję **View Errors** (Wyświetl błędy), aby przejść do panelu zarządzania błędami replikacji. Można na nim wyświetlić protokół błędów replikacji, ponowić zmiany, które się nie powiodły, lub usunąć pozycje z protokołu.
7. Kliknij przycisk **Refresh** (Odśwież), aby zaktualizować kolejki i wyzerować komunikaty serwera.

Jeśli kliknięto **Queue details** (Szczegóły kolejki), wyświetlone zostaną trzy zakładki:

- Status
- Last attempted details (Szczegóły dotyczące ostatniej próby)
- Pending changes (Oczekujące zmiany)

Zakładka **Status** zawiera nazwę repliki, jej poddrzewo, status oraz zapis czasów replikacji. Z tego panelu można wstrzymać lub wznowić replikację, klikając przycisk **Resume** (Wznów). Kliknij przycisk **Refresh** (Odśwież), aby zaktualizować informacje na temat kolejki.

Zakładka **Last attempted details** (Szczegóły dotyczące ostatniej próby) zawiera informacje na temat ostatniej próby aktualizacji. Jeśli nie można załadować pozycji, naciśnij przycisk **Skip blocking entry** (Pomiń zablokowaną pozycję), aby kontynuować replikację od następnej oczekującej pozycji. Kliknij przycisk **Refresh** (Odśwież), aby zaktualizować informacje na temat kolejki.

Zakładka **Pending changes** (Oczekujące zmiany) wyświetla wszystkie oczekujące zmiany w replice. Jeśli replikacja jest zablokowana, można usunąć wszystkie oczekujące zmiany, klikając **Skip all** (Pomiń wszystkie). Kliknij przycisk **Refresh** (Odśwież), aby zaktualizować listę oczekujących zmian w celu odzwierciedlenia wszystkich nowo przetworzonych aktualizacji.

**Uwaga:** W przypadku pominięcia wszystkich blokujących zmian należy upewnić się, że serwer odbierający zostanie w końcu zaktualizowany.

### Pojęcia pokrewne

“Tabela błędów replikacji” na stronie 43

W tabeli błędów replikacji protokołowane są niepowodzenia aktualizacji w celu późniejszego odtwarzania. Po rozpoczęciu replikacji liczona jest liczba zaprotokołowanych niepowodzeń dla każdej umowy replikacji. Gdy aktualizacja zakończy się niepowodzeniem, liczba ta jest zwiększana, a do tabeli dodawana jest nowa pozycja.

### Odsyłacze pokrewne

“ldapdiff” na stronie 247

Program narzędziowy wiersza komend do synchronizowania replik LDAP.

## Modyfikowanie ustawień protokołu niedokończonych operacji

W protokole niedokończonych operacji (domyślnie zapisywanym w pliku LostAndFound.log) rejestrowane są błędy, które wystąpiły w wyniku konfliktów replikacji. Dostępne są ustawienia umożliwiające sterowanie obsługą protokołu niedokończonych operacji, w tym określenie położenia i maksymalnej wielkości pliku protokołu oraz zasad archiwizowania starych plików protokołu.

- Aby zmodyfikować ustawienia protokołu niedokończonych operacji, należy wykonać następujące czynności:
1. Korzystając z narzędzia Web Administration produktu IBM Tivoli Directory Server, rozwiń pozycję **Server administration** (Administrowanie serwerem), w obszarze nawigacyjnym wybierz opcję **Logs** (Protokoły) i kliknij opcję **Modify log settings** (Modyfikuj ustawienia protokołów).
  2. Kliknij pozycję **Lost and found log** (Protokół niedokończonych operacji).
  3. Wprowadź ścieżkę i nazwę pliku protokołu błędów. Upewnij się, że plik istnieje na serwerze LDAP, a podana ścieżka jest poprawna. Domyślna ścieżka pliku protokołu to `<napęd>\idslapd-<nazwa-instancji>\logs`, gdzie *napęd* jest napędem dysków wskazanym podczas tworzenia instancji serwera katalogów, a *nazwa-instancji* jest nazwą instancji serwera katalogów. Jeśli zostanie podana niedozwolona nazwa pliku (na przykład jeśli nazwa ma niepoprawną składnię lub jeśli serwer nie posiada uprawnień do utworzenia i/lub modyfikowania pliku), próba zakończy się niepowodzeniem i zwróceniem następującego komunikatu o błędzie: **LDAP Server is unwilling to perform the operation** (Serwer LDAP odmawia wykonania operacji).
  4. Pod nagłówkiem **Log size threshold (MB)** (Wartość progowa wielkości protokołu (MB)) kliknij pierwszy przełącznik i wprowadź maksymalną wielkość pliku protokołu w megabajtach. Jeśli nie chcesz ograniczać wielkości protokołu, kliknij przełącznik **Unlimited** (Bez ograniczeń).
  5. W sekcji **Maximum log archives** (Maksymalna liczba protokołów archiwalnych) wybierz jedną z następujących opcji:
    - Jeśli chcesz określić maksymalną liczbę protokołów archiwalnych, kliknij przełącznik obok pola edycji. Wprowadź maksymalną liczbę protokołów archiwalnych, które mają być składowane. Protokół archiwalny to stary protokół, który osiągnął wartość progową wielkości.
    - Jeśli protokoły nie mają być archiwizowane, wybierz opcję **No archives** (Bez archiwizacji).
    - Jeśli nie chcesz ograniczać liczby protokołów archiwalnych, wybierz opcję **Unlimited** (Bez ograniczeń).
  6. W sekcji **Log archive path** (Ścieżka protokołów archiwalnych) wykonaj jedną z następujących czynności:
    - Jeśli chcesz określić ścieżkę, w której zapisywane będą protokoły archiwalne, kliknij przełącznik obok pola edycji, a następnie wprowadź odpowiednią ścieżkę.
    - Jeśli protokoły archiwalne mają być przechowywane w tym samym katalogu, w którym znajduje się plik protokołu, zaznacz przełącznik **Same directory as log file** (W katalogu pliku protokołu).
  7. Kliknij przycisk **Apply** (Zastosuj), aby zastosować zmiany i kontynuować pracę z protokołami, lub kliknij przycisk **OK**, aby zapisać zmiany i powrócić do ekranu startowego narzędzia Web Administration produktu IBM Tivoli Directory Server. Kliknij przycisk **Cancel** (Anuluj), aby powrócić do ekranu startowego narzędzia Web Administration produktu IBM Tivoli Directory Server bez zapisywania wprowadzonych zmian.

#### Odsyłacze pokrewne

“Replikacja - przegląd” na stronie 37

Poprzez replikację zmiany wprowadzone w jednym katalogu są rozsyłane do jednego lub wielu dodatkowych katalogów. Dzięki temu zmiana w jednym katalogu jest widoczna w wielu różnych katalogach.

## Wyświetlanie pliku protokołu niedokończonych operacji

Plik protokołu niedokończonych operacji replikowania można wyświetlić za pomocą narzędzia IBM Tivoli Directory Server Web Administration lub opcji pliku protokołu w programie narzędziowym ldapexop. Plik protokołu można też przeglądać bezpośrednio.

Aby wyświetlić plik protokołu niedokończonych operacji za pomocą narzędzia Web Administration, rozwiń węzeł **Server Administration** (Administrowanie serwerem) w obszarze nawigacyjnym programu Web Administration, a następnie pozycję **Protocols** (Protokoły) na rozwiniętej liście.

1. Kliknij opcję **View log** (Wyświetl protokół).
2. W panelu **View logs** (Wyświetl protokoły) wybierz element **Lost and found log** (Protokół niedokończonych operacji) i kliknij przycisk **View** (Wyświetl).

**Uwaga:** do tego panelu mają dostęp tylko administrator katalogu i członkowie grupy administracyjnej.

Aby wyświetlić protokół niedokończonych operacji za pomocą programu narzędziowego ldapexop, w powłoce Qshell wpisz komendę:

```
| ldapexop -D -w -op readlog -log LostAndFound -lines all
```

| Aby usunąć zawartość protokołu niedokończonych operacji, wpisz komendę:

```
| ldapexop -D -w -op clearlog -log LostAndFound
```

| **Uwaga:** Jeśli zalogujesz się do systemu i5/OS jako użytkownik z uprawnieniami specjalnymi \*ALLOBJ i \*IOSYSCFG lub jako użytkownik, który ma dostęp administratora do serwera katalogów, możesz użyć programu narzędziowego ldapexop z opcją -m OS400-PRFTKN zamiast podawania nazwy wyróżniającej i hasła administratora. Na przykład:

```
| ldapexop -m OS400-PRFTKN -op readlog -log LostAndFound -lines all
```

#### | **Odsyłacze pokrewne**

| "ldapexop" na stronie 226

| Program narzędziowy wiersza komend do operacji rozszerzonych LDAP.

## **Konfigurowanie replikacji korzystającej z bezpiecznego połączenia**

Ten temat zawiera informacje dotyczące konfigurowania replikacji korzystającej z bezpiecznego połączenia.

Replikacja w połączeniu SSL powinna być skonfigurowana w etapach, aby możliwe było zweryfikowanie poprawności procesu.

Przed dokonaniem próby replikacji w połączeniu chronionym, należy wykonać następujące czynności (w dowolnej kolejności):

- Skonfiguruj replikację w połączeniu bez ochrony.
- Skonfiguruj serwer odbierający, aby akceptował bezpieczne połączenia na bezpiecznym porcie. Sprawdź, czy klient może używać bezpiecznego połączenia z serwerem odbierającym, używając na przykład narzędzia ldapsearch. Jeśli serwer wysyłający ma używać certyfikatu do uwierzytelniania, takiego jak zewnętrzne połączenie SASL poprzez SSL, należy najpierw skonfigurować uwierzytelnianie serwera, a następnie uwierzytelnianie klienta, gdzie "serwer" jest serwerem odbierającym a klient jest serwerem wysyłającym.

**Uwaga:** Po skonfigurowaniu serwera do używania uwierzytelnień klienta i serwera, od wszystkich klientów korzystających z SSL wymagany jest certyfikat klienta.

- Skonfiguruj relacje zaufania serwera wysyłającego dla ośrodka certyfikacji, który wystawił certyfikat klienta.
1. W narzędziu Web Administration kliknij element **Manage topology** (Zarządzaj topologią) w kategorii **Replication management** (Zarządzanie replikacją).
  2. Wybierz jedną z istniejących umów, która ma być chroniona.
  3. Wybierz **Edit agreement...** (Edytuj umowę...) i włącz używanie SSL upewniając się, że używany jest poprawny numer portu. Standardowo numer bezpiecznego portu to 636.
  4. Sprawdź, czy replikacja dla umowy działa poprawnie.

Jeśli dokonywana jest jedynie próba konfiguracji replikacji do uwierzytelniania w bezpiecznym połączeniu za pomocą nazwy wyróżniającej i hasła, czynności te zostały już wykonane w poprzednich punktach. Uwierzytelnianie za pomocą certyfikatu klienta wymaga użycia przez serwer wysyłający innego obiektu referencji w jego umowie, a także skonfigurowania serwera odbierającego do akceptowania tego certyfikatu jako serwera wysyłającego.

## **Zadania związane z topologią replikacji**

Ten temat zawiera informacje dotyczące zarządzania topologiami replikowanych poddrzew.

Topologie są specyficzne dla replikowanych poddrzew.

### **Wyświetlanie topologii**

Ten temat zawiera informacje dotyczące wyświetlania topologii poddrzewa.

**Uwaga:** Aby można było wykonać to zadanie, serwer musi być uruchomiony.

Rozwiń kategorię **Replication management** (Zarządzanie replikacją) w obszarze nawigacyjnym i kliknij **Manage topology** (Zarządzaj topologią).

Wybierz poddrzewo, które chcesz wyświetlić, i kliknij opcję **Show topology** (Pokaż topologię).

Topologia jest wyświetlana na liście topologii replikacji. Można ją rozwinąć poprzez kliknięcie niebieskiego trójkąta. Z listy tej można wykonywać następujące czynności:

- dodawanie repliki,
- edycja informacji na temat istniejącej repliki,
- zmiana serwera wysyłającego wybranej repliki lub awansowanie repliki na serwer główny,
- usunięcie repliki,
- wyświetlenie harmonogramu replikacji.

## Dodawanie repliki

Ten temat zawiera informacje dotyczące dodawania repliki.

**Uwaga:** Opisane tutaj czynności umożliwiają dodanie repliki za pomocą narzędzia Web Administration i są częścią całego procesu obejmującego inne czynności wymagane do prawidłowego zainicjowania nowego serwera. Należy zapoznać się z informacjami na stronach pokrewnych wymienionych poniżej.

**Uwaga:** Aby można było wykonać to zadanie, serwer musi być uruchomiony.

Rozwiń kategorię **Replication management** (Zarządzanie replikacją) w obszarze nawigacyjnym i kliknij **Manage topology** (Zarządzaj topologią).

1. Wybierz poddrzewo, które chcesz replikować, i kliknij opcję **Show topology** (Pokaż topologię).
2. Kliknij strzałkę obok wyboru **Replication topology** (Topologia replikacji), aby rozwinąć listę serwerów wysyłających.
3. Wybierz serwer wysyłający i kliknij **Add replica** (Dodaj replikę).
4. W zakładce **Server** (Serwer) okna **Add replica** (Dodaj replikę):
  - a. Wprowadź nazwę hosta i numer portu tworzonej repliki. Domyślnym numerem portu jest 389 dla połączeń bez użycia protokołu SSL oraz 636 dla połączeń z SSL. Są to pola wymagane.
  - b. Wybierz komunikację z wykorzystaniem protokołu SSL lub bez niego.
  - c. Wpisz nazwę repliki lub pozostaw puste pole, aby użyć nazwy hosta.
  - d. Wpisz identyfikator repliki. Jeśli serwer, na którym tworzona jest replika, jest uruchomiony, kliknij przycisk **Get replica ID** (Pobierz identyfikator repliki), aby automatycznie wypełnić to pole. Jest to pole wymagane, jeśli dodawany serwer ma być serwerem równorzędnym lub przekazującym. Zalecane jest, aby wszystkie serwery były w tej samej wersji.
  - e. Wpisz opis serwera repliki.
5. Na karcie **Additional** (Dodatkowe):
  - Podaj referencje, których używa replika do komunikacji z serwerem głównym.

**Uwaga:** Narzędzie Web Administration umożliwia definiowanie referencji w następujących miejscach:

- **cn=replication,cn=localhost**, która powoduje przechowywanie referencji tylko na serwerze, który ich używa.
- W replikowanym poddrzewie, w którym to przypadku referencje są replikowane z resztą poddrzewa. Referencje umieszczone w poddrzewie replikacji są tworzone na podstawie pozycji **ibm-replicagroup=default** dla tego poddrzewa.

Umieszczanie referencji w pozycji **cn=replication,cn=localhost** jest uważane za bardziej bezpieczne. Referencje umieszczone w poddrzewie replikacji są tworzone na podstawie pozycji **ibm-replicagroup=default** dla tego poddrzewa.

- Kliknij **Select** (Wybierz).
    - Wybierz położenie referencji, których chcesz używać. Preferowanym położeniem jest `cn=replication,cn=localhost`.
    - Kliknij **Show credentials** (Pokaż referencje).
    - Rozwiń listę referencji i wybierz te, których chcesz użyć.
    - Kliknij przycisk **OK**.
- Dodatkowe informacje o referencjach umowy zawiera temat Tworzenie referencji replikacji.
- Wybierz harmonogram replikacji z listy rozwijanej lub kliknij przycisk **Add** (Dodaj), aby go dodać. Więcej informacji zawiera temat Tworzenie harmonogramów replikacji.
  - Z listy możliwości serwera wysyłającego można usunąć zaznaczenie wszystkich możliwości, które nie mają być replikowane na serwerze odbierającym.

Jeśli w sieci są różne serwery w różnych wersjach, w nowszych wersjach są dostępne możliwości, których brak w wersjach wcześniejszych. Niektóre możliwości, takie jak filtrowanie list ACL i strategia haseł, używają atrybutów operacyjnych replikowanych z innymi zmianami. W większości przypadków, jeśli te funkcje są używane, wszystkie serwery powinny je obsługiwać. Jeśli nie wszystkie serwery obsługują daną możliwość, lepiej z niej nie korzystać. Na przykład nie powinno być różnych list ACL na każdym serwerze. Jednak zdarzają się przypadki, w których można używać danej możliwości na obsługujących ją serwerach i nie replikować zmian dotyczących tej możliwości na serwery, które jej nie obsługują. W takich przypadkach można używać listy możliwości do oznaczania konkretnych możliwości, które nie będą replikowane.

- Jako metodę replikacji wybierz opcję **Single threaded** (Jednowątkowa) lub **Multi-threaded** (Wielowątkowa). W przypadku replikacji wielowątkowej należy także podać liczbę (od 2 do 32) połączeń wykorzystywanych do replikacji. Domyślna liczba połączeń to 2.
- Kliknij **OK**, aby utworzyć replikę.

6. Wyświetlony zostanie komunikat informujący o tym, że należy podjąć dodatkowe działania. Kliknij przycisk **OK**.

**Uwaga:** Jeśli dodajesz kolejne serwery jako dodatkowe repliki lub tworzysz złożoną topologię, nie przechodź do czynności Kopiowanie danych do repliki lub Dodawanie informacji o serwerze wysyłającym do nowej repliki do momentu zakończenia definiowania topologii na serwerze głównym. Jeśli po zakończeniu definiowania topologii utworzony zostanie plik *masterfile.ldif*, zawierać on będzie pozycje katalogu serwera głównego i pełną kopię umów topologii. Podczas ładowania tego pliku na wszystkie serwery, każdy z nich będzie zawierał te same informacje.

#### Zadania pokrewne

“Konfigurowanie topologii bramy” na stronie 159

Ten temat zawiera informacje dotyczące konfigurowania topologii bramy.

### Dodawanie serwera równorzędny-główny lub serwera-bramy

W tym temacie znajdują się informacje o tworzeniu nowego serwera równorzędny-główny lub serwera-bramy.

**Uwaga:** Opisane tutaj czynności pozwalają dodać serwer równorzędny-główny lub serwer-bramę przy użyciu zadania narzędzia Web Administration i są częścią całego procesu obejmującego inne czynności wymagane do prawidłowego zainicjowania nowego serwera. Należy zapoznać się z informacjami na stronach pokrewnych wymienionych poniżej.

Rozwiń kategorię **Replication management** (Zarządzanie replikacją) w obszarze nawigacyjnym i kliknij **Manage topology** (Zarządzaj topologią).

1. Wybierz poddrzewo, które chcesz replikować, i kliknij opcję **Show topology** (Pokaż topologię).
2. Jeśli chcesz wyświetlić istniejącą topologię, kliknij pole **Replication topology** (Topologia replikacji), aby rozwinąć listę serwerów wysyłających.
3. Kliknij opcję **Add master** (Dodaj serwer główny).

Na karcie **Server** (Serwer) w oknie **Add master** (Dodaj serwer główny) wykonaj następujące czynności:

- | • Wprowadź nazwę hosta i numer portu tworzonego serwera. Domyślnym numerem portu jest 389 dla połączeń bez użycia protokołu SSL oraz 636 dla połączeń z SSL. Są to pola wymagane.
- | • Wybierz komunikację z wykorzystaniem protokołu SSL lub bez niego.
- | • Wybierz, czy serwer ma być serwerem-bramą.
- | • Wpisz nazwę serwera lub pozostaw puste pole, aby użyć nazwy hosta.
- | • Wpisz **identyfikator serwera**. Jeśli serwer, na którym tworzony jest serwer równorzędny-główny, jest uruchomiony, kliknij przycisk Get server ID (Pobierz identyfikator serwera), aby automatycznie wypełnić to pole.
- | • Wpisz opis serwera.
- | • Należy podać referencje, których serwer używa do komunikacji z innym serwerem głównym. Kliknij **Select** (Wybierz).

| **Uwaga:** Narzędzie Web Administration umożliwia definiowanie referencji w następujących lokalizacjach:

- | – **cn=replication,cn=localhost**, w przypadku której referencje są przechowywane tylko na serwerze, który ich używa. Umieszczanie referencji w pozycji cn=replication,cn=localhost jest uważane za bardziej bezpieczne.
- | – **cn=replication,cn=IBMpolicies**, która jest dostępna nawet wtedy, gdy serwer, pod którym użytkownik próbuje dodać replikę, nie jest serwerem, do którego jest on podłączony za pomocą narzędzia Web Administration. Referencje umieszczone w tym miejscu są replikowane na serwery.

| **Uwaga:** Lokalizacja cn=replication,cn=IBMpolicies jest dostępna tylko wtedy, gdy OID obsługi poddrzewa IBMpolicies, 1.3.18.0.2.32.18, jest obecny w atrybucie ibm-supportedcapabilities głównego DSE.

- | – W replikowanym poddrzewie, w którym to przypadku referencje są replikowane z resztą poddrzewa. Referencje umieszczone w poddrzewie replikacji są tworzone na podstawie pozycji **ibm-replicagroup=default** dla tego poddrzewa.
  - | 1. Wybierz położenie referencji, których chcesz używać. Preferowanym położeniem jest cn=replication,cn=localhost.
  - | 2. Jeśli utworzono już zestaw referencji, kliknij opcję Show credentials (Pokaż referencje).
  - | 3. Rozwiń listę referencji i wybierz te, których chcesz użyć.
  - | 4. Kliknij przycisk OK.
  - | 5. Jeśli nie ma wcześniejszych referencji, kliknij przycisk Add (Dodaj), aby je utworzyć.

| W zakładce **Additional** (Dodatkowe):

- | 1. Wybierz harmonogram replikacji z listy rozwijanej lub kliknij przycisk **Add** (Dodaj), aby go dodać. Więcej informacji zawiera temat Tworzenie harmonogramów replikacji.
- | 2. Z listy możliwości serwera wysyłającego można usunąć zaznaczenie wszystkich możliwości, które nie mają być replikowane na serwerze odbierającym.

| Jeśli w sieci są różne serwery w różnych wersjach, w nowszych wersjach są dostępne możliwości, których brak w wersjach wcześniejszych. Niektóre możliwości, takie jak filtrowanie list ACL (Filtrowane listy kontroli dostępu) i strategia haseł (Ustawianie właściwości strategii haseł), używają atrybutów operacyjnych replikowanych z innymi zmianami. W większości przypadków, jeśli te opcje są używane, wszystkie serwery powinny je obsługiwać. Jeśli nie wszystkie serwery obsługują daną możliwość, lepiej z niej nie korzystać. Na przykład nie powinno być różnych list ACL na każdym serwerze. Jednak zdarzają się przypadki, w których można używać danej możliwości na obsługujących ją serwerach i nie replikować zmian dotyczących tej możliwości na serwery, które jej nie obsługują. W takich przypadkach można używać listy możliwości do oznaczania konkretnych możliwości, które nie będą replikowane.

- | 3. Zaznacz pole wyboru **Add credential information on consumer** (Dodaj informacje o referencjach na serwerze odbierającym), jeśli chcesz włączyć dynamiczne aktualizowanie referencji serwera wysyłającego. Wybór ten automatycznie aktualizuje informacje o serwerze wysyłającym w pliku konfiguracyjnym tworzonego serwera. Umożliwia to replikację informacji o topologii do serwera.
  - | • Wpisz nazwę wyróżniającą serwera odbierającego. Na przykład cn=root.



**Uwaga:** Jeśli nazwą wyróżniającą administratora utworzoną podczas konfigurowania serwera była `cn=root`, wpisz pełną nazwę wyróżniającą administratora. Nie używaj samego określenia `root`.

- Wpisz hasło administratora serwera odbierającego. Na przykład `tajne_hasło`.

4. Kliknij przycisk **OK**.

5. Umowy między serwerami wysyłającymi i odbierającymi są wyświetlane między nowym serwerem głównym a istniejącymi serwerami. Anuluj zaznaczenie umów, których nie chcesz tworzyć. Jest to szczególnie ważne podczas tworzenia serwera-bramy.

6. Kliknij przycisk **Continue** (Kontynuuj).

7. Mogą zostać wyświetlone komunikaty informujące o tym, że należy podjąć dodatkowe działania. Wykonaj odpowiednie czynności lub zanotuj je. Po zakończeniu kliknij przycisk **OK**.

8. Dodaj odpowiednie referencje.

**Uwaga:** W niektórych przypadkach zostanie wyświetlony panel **Select credentials** (Wybór referencji) z zapytaniem o referencje znajdujące się w innym miejscu niż `cn=replication,cn=localhost`. W takich sytuacjach należy podać obiekt referencji znajdujący się w miejscu innym niż `cn=replication,cn=localhost`. Należy wybrać referencje dla poddrzewa z istniejących zestawów lub utworzyć nowe referencje.

9. Zaznacz pole wyboru **Add credential information on consumer** (Dodaj informacje o referencjach na serwerze odbierającym), jeśli chcesz włączyć dynamiczne aktualizowanie referencji serwera wysyłającego. Wybór ten automatycznie aktualizuje informacje o serwerze wysyłającym w pliku konfiguracyjnym tworzonego serwera. Umożliwia to replikację informacji o topologii do serwera.

- Wpisz nazwę wyróżniającą serwera odbierającego. Na przykład `cn=root`.

**Uwaga:** Jeśli nazwą wyróżniającą administratora utworzoną podczas konfigurowania serwera była `cn=root`, wpisz pełną nazwę wyróżniającą administratora. Nie używaj samego określenia `root`.

- Wpisz hasło administratora serwera odbierającego. Na przykład `tajne_hasło`.

10. Kliknij przycisk **OK**, aby utworzyć serwer równorzędny-główny.

11. Mogą zostać wyświetlone komunikaty informujące o tym, że należy podjąć dodatkowe działania. Wykonaj odpowiednie czynności lub zanotuj je. Po zakończeniu kliknij przycisk **OK**.

**Uwaga:** Jeśli podczas dodawania referencji na serwerach odbierających w ramach operacji **Add master** (Dodawanie serwera głównego) w narzędziu **Web Administration** zostanie wybrany zewnętrzny obiekt referencji, to na komputerze, na którym działa serwer **IBM WebSphere Application Server**, trzeba spełnić następujące warunki:

- Katalog `WAS_HOME\java\jre\lib\ext\` musi zawierać następujące pliki JAR:

- `ibmjceprovider.jar`
- `ibmpkcs.jar`
- `ibmjcefw.jar`
- `local_policy.jar`
- `US_export_policy.jar`
- `ibmjlog.jar`
- `gsk7cls.jar`

- Plik `WAS_HOME\java\jre\lib\security\java.security` musi mieć następujące dwa wiersze, aby zarejestrować dostawcę CMS i dostawcę JCE:

```
security.provider.2=com.ibm.spi.IBMCMSProvider
security.provider.3=com.ibm.crypto.provider.IBMJCE
```

- Należy zrestartować serwer **IBM WebSphere Application Server**.
- Musi być zainstalowany pakiet `Gskit`, a katalog `gsk7\lib` musi znajdować się w ścieżce systemowej.

- Aby narzędzie Web Administration mogło odczytać plik kluczy zawierający referencje, których serwer główny używa do łączenia się z repliką, i utworzyć referencje na replice, plik kluczy musi znajdować się w katalogu C:\temp na platformach Windows lub w katalogu /tmp na platformach UNIX.

### Zadania pokrewne

“Konfigurowanie topologii bramy” na stronie 159

Ten temat zawiera informacje dotyczące konfigurowania topologii bramy.

## Zarządzanie serwerami-bramami

Ten temat zawiera informacje o zarządzaniu serwerami-bramami. Istnieje możliwość wskazania serwera głównego jako serwera pełniącego funkcję bramy w ośrodku replikacji.

Aby wyznaczyć serwer główny na bramę, w obszarze nawigacyjnym rozwiń kategorię **Replication management** (Zarządzanie replikacją) i kliknij pozycję **Manage topology** (Zarządzaj topologią).

1. Wybierz poddrzewo, które chcesz wyświetlić, i kliknij opcję **Show topology** (Pokaż topologię).
2. Kliknij opcję **Manage gateway servers** (Zarządzaj serwerami-bramami).
3. W polu **Master servers** (Serwery główne) wybierz serwer, który chcesz wyznaczyć na serwer-bramę.
4. Kliknij opcję **Make gateway** (Zmień funkcję na bramę). Serwer zostanie przeniesiony z pola **Master servers** (Serwery główne) do pola **Gateway servers** (Serwery-bramy).
5. Kliknij przycisk **OK**.

Aby usunąć z serwera głównego rolę serwera-bramy, wykonaj następujące czynności:

1. Kliknij opcję **Manage gateway servers** (Zarządzaj serwerami-bramami).
2. W polu **Gateway servers** (Serwery-bramy) wybierz serwer, który chcesz wyznaczyć na serwer główny.
3. Kliknij opcję **Make master** (Zmień funkcję na główny). Serwer zostanie przeniesiony z pola **Gateway servers** (Serwery-bramy) do pola **Master servers** (Serwery główne).
4. Kliknij przycisk **OK**.

**Uwaga:** Należy pamiętać, że dla każdego ośrodka replikacji może istnieć tylko jeden serwer-brama. Jeśli w używanej topologii zostaną utworzone dodatkowe serwery-bramy, narzędzie Web Administration będzie traktować bramę jako serwer równorzędny i utworzy umowy ze wszystkimi serwerami w topologii. Upewnij się, że zostały anulowane zaznaczenia odpowiadające wszelkim umowom, które nie dotyczą innych serwerów-bram lub wykraczają poza obręb ośrodka replikacji danej bramy.

Więcej informacji można znaleźć w temacie Konfigurowanie topologii bramy, wymienionym poniżej wśród odsyłaczy pokrewnych.

### Zadania pokrewne

“Konfigurowanie topologii bramy” na stronie 159

Ten temat zawiera informacje dotyczące konfigurowania topologii bramy.

## Wyświetlanie informacji o serwerze

Nazwę serwera, nazwę hosta, port, identyfikator serwera, rolę, tryb konfiguracji, nazwę instancji i informacje o bezpieczeństwie można wyświetlać na panelu View server (Wyświetl serwer).

Rozwiń kategorię **Replication management** (Zarządzanie replikacją) w obszarze nawigacyjnym narzędzia Web Administration i kliknij opcję **Manage topology** (Zarządzaj topologią).

1. Wybierz poddrzewo, które chcesz wyświetlić, i kliknij opcję **Show topology** (Pokaż topologię).
2. Wybierz serwer, które chcesz wyświetlić.
3. Kliknij opcję **View server** (Wyświetl serwer), aby wyświetlić panel serwera.

Panel View Server (Widok serwera) zawiera następujące informacje:

#### | **Nazwa serwera**

| To pole zawiera nazwę serwera, na którym działa instancja katalogu. Informacje te są wyświetlane w formacie nazwa\_hosta:port.

#### | **Host name (Nazwa hosta)**

| To pole zawiera nazwę hosta komputera, na którym działa instancja serwera katalogów.

| **Port** To pole zawiera niezabezpieczony port, na którym nasłuchuje serwer.

#### | **Server ID (Identyfikator serwera)**

| To pole zawiera unikalny identyfikator przypisany do serwera w momencie pierwszego uruchomienia. Identyfikator ten jest używany w topologii replikacji w celu ustalenia roli serwera.

#### | **Role (Rola)**

| To pole zawiera rolę skonfigurowaną dla serwera w topologii replikacji.

#### | **Configuration mode (Tryb konfiguracji)**

| To pole określa, czy serwer działa w trybie konfiguracji. Wartość TRUE oznacza, że serwer działa w trybie konfiguracji. Wartość FALSE oznacza, że serwer nie działa w trybie konfiguracji.

#### | **Instance name (Nazwa instancji)**

| To pole zawiera nazwę instancji serwera katalogów działającej na serwerze.

#### | **Security (Bezpieczeństwo)**

| To pole zawiera numer portu zabezpieczonego protokołem SSL, na którym nasłuchuje serwer.

| Wyświetlane są: nazwa, identyfikator i rola serwera oraz informacje o serwerze odbierającym.

### | **Wyświetlanie harmonogramu replikacji**

| Aby wyświetlić harmonogram replikacji za pomocą narzędzia Web Administration, należy wykonać czynności opisane w tym temacie.

| Rozwiń kategorię **Replication management** (Zarządzanie replikacją) w obszarze nawigacyjnym narzędzia Web Administration i kliknij opcję **Manage topology** (Zarządzaj topologią).

- | 1. Wybierz poddrzewo, które chcesz wyświetlić, i kliknij opcję **Show topology** (Pokaż topologię).
- | 2. Wybierz serwer główny lub serwer-bramę, który chcesz wyświetlić.
- | 3. Kliknij opcję **View schedule** (Wyświetl harmonogram).

| Jeśli istnieje harmonogram replikacji obejmujący wybrany serwer i powiązane z nim serwery odbierające, zostanie on wyświetlony. Harmonogramy można modyfikować i usuwać. Jeśli nie istnieje żaden harmonogram i użytkownik chce go utworzyć, powinien użyć funkcji **Manage schedules** (Zarządzaj harmonogramami) w obszarze nawigacyjnym narzędzia Web Administration. Informacje dotyczące zarządzania harmonogramami zawiera temat Tworzenie harmonogramów replikacji, do którego odsyłacz znajduje się poniżej.

#### | **Zadania pokrewne**

| “Tworzenie harmonogramów replikacji” na stronie 163

| Ten temat zawiera informacje dotyczące tworzenia harmonogramów replikacji.

## **Edytowanie umowy**

Ten temat zawiera informacje dotyczące edytowania umowy replikacji.

Dla repliki można zmienić następujące informacje:

1. Na karcie **Server** (Serwer) można zmienić tylko następujące informacje:

- Nazwa hosta
- Port
- Włącz SSL
- Opis

2. Na karcie **Additional** (Dodatkowe) można zmienić tylko takie informacje, jak:

- Referencje - patrz “Tworzenie referencji replikacji” na stronie 149.
  - Harmonogramy replikacji - patrz “Tworzenie harmonogramów replikacji” na stronie 163.
  - Możliwości replikowane do repliki odbierającej. Z listy możliwości serwera wysyłającego można usunąć zaznaczenie wszystkich możliwości, które nie mają być replikowane na serwerze odbierającym.
3. Po zakończeniu kliknij przycisk **OK**.

## Przenoszenie i awansowanie serwera

Ten temat zawiera informacje dotyczące przenoszenia i awansowania serwera.

1. Wybierz serwer i kliknij przycisk **Move** (Przenieś).
2. Wybierz serwer, na który chcesz przenieść replikę, lub wybierz **Replication topology** (Topologię replikacji), aby awansować replikę do serwera głównego. Kliknij przycisk **Move** (Przenieś).
3. W niektórych przypadkach wyświetlony zostanie panel wyboru referencji z zapytaniem o referencje znajdujące się w innym miejscu niż cn=replication,cn=localhost. W takich sytuacjach należy podać obiekt referencji znajdujący się w miejscu innym niż cn=replication,cn=localhost. Wybierz referencje z istniejących zestawów lub utwórz nowe referencje, których poddrzewo ma użyć. Więcej informacji zawiera temat “Tworzenie referencji replikacji” na stronie 149.
4. Wyświetlony zostanie panel **Create additional supplier agreements** (Tworzenie dodatkowych umów serwera wysyłającego). Wybierz umowy serwera wysyłającego odpowiednie dla roli serwera. Na przykład, jeśli serwer replik jest awansowany do serwera równorzędnego, należy utworzyć umowy serwera wysyłającego ze wszystkimi innymi serwerami i ich replikami pierwszego poziomu. Umowy te umożliwiają działanie awansowanego serwera jako serwera wysyłającego dla wszystkich pozostałych serwerów i ich replik. Istniejące umowy serwera wysyłającego z innych serwerów do nowo awansowanego serwera nadal obowiązują i nie ma potrzeby ich ponownego tworzenia.
5. Kliknij przycisk **OK**.

Zmiana w drzewie topologii odzwierciedla przeniesienie serwera.

### Zadania pokrewne

“Tworzenie złożonej topologii z replikacją między serwerami równorzędnymi” na stronie 156

Ten temat zawiera informacje dotyczące tworzenia złożonej topologii z replikacją między serwerami równorzędnymi.

## Degradowanie serwera głównego

Ten temat zawiera informacje dotyczące zmiany roli serwera z serwera głównego na replikę.

Aby zmienić rolę serwera z głównego na serwer replik, wykonaj następujące czynności:

1. Nawiąż połączenie Web Administration z serwerem, który chcesz zdegradować.
2. Kliknij **Manage topology** (Zarządzaj topologią).
3. Wybierz poddrzewo i kliknij **Show topology** (Pokaż topologię).
4. Usuń wszystkie umowy dla serwera, który chcesz zdegradować.
5. Wybierz serwer, który chcesz zdegradować, i kliknij przycisk **Move** (Przenieś).
6. Wybierz serwer, na którym chcesz umieścić zdegradowany serwer, i kliknij przycisk **Move** (Przenieś).
7. Podobnie jak w przypadku nowej repliki, utwórz nowe umowy serwerów wysyłających między zdegradowanym serwerem i jego serwerem wysyłającym. Instrukcje znajdują się w sekcji “Tworzenie serwera replik” na stronie 151.

## Replikowanie poddrzewa

Ten temat zawiera informacje dotyczące replikowania poddrzewa.

**Uwaga:** Aby można było wykonać to zadanie, serwer musi być uruchomiony.

Rozwiń kategorię **Replication management** (Zarządzanie replikacją) w obszarze nawigacyjnym i kliknij **Manage topology** (Zarządzaj topologią).

1. Kliknij opcję **Add subtree** (Dodaj poddrzewo).
2. Wpisz nazwę DN poddrzewa, które chcesz replikować, lub kliknij przycisk **Browse** (Przełóżaj), aby rozwinąć pozycje i wybrać tę z nich, która ma być początkiem poddrzewa.
3. Wpisz adres URL odwołania do serwera głównego. Adres ten musi mieć formę adresu URL LDAP, np.:  
ldap://<nazwa\_serwera>.<lokalizacja>.<firma>.pl
4. Kliknij przycisk **OK**.

Nowy serwer jest wyświetlany w panelu Manage topology (Zarządzaj topologią) pod nagłówkiem **Replicated subtrees** (Replikowane poddrzewa).

## Edytowanie poddrzewa

Ten temat zawiera informacje dotyczące zmiany adresu URL serwera głównego, do którego dane poddrzewo i jego repliki wysyłają aktualizacje. Należy to zrobić w przypadku zmiany numeru portu lub nazwy hosta serwera głównego lub zmiany serwera głównego na inny.

1. Wybierz poddrzewo do edycji.
2. Kliknij przycisk **Edit subtree** (Edycja poddrzewa).
3. Wpisz adres URL odwołania do serwera głównego. Adres ten musi mieć formę adresu URL LDAP, np.:  
ldap://<nazwa\_nowego\_serwera>.<lokalizacja>.<firma>.pl

W zależności od roli pełnionej przez serwer w poddrzewie (czy jest serwerem głównym, repliką czy też serwerem przekazującym), na panelu pojawiają się różne etykiety i przyciski.

- Jeśli rolą poddrzewa jest replika, obok przycisku **Make server a master** (Utwórz serwer serwerem głównym) wyświetlana jest etykieta informująca o tym, że serwer działa jako replika. Po kliknięciu tego przycisku serwer połączony z narzędziem Web Administration staje się serwerem głównym.
- Jeśli poddrzewo jest skonfigurowane tylko dla replikacji poprzez dodanie pomocniczej klasy (brak jest grupy i pozycji podrzędnej), wtedy obok przycisku **Replicate subtree** (Replikuj poddrzewo) wyświetlana jest etykieta **This subtree is not replicated** (To poddrzewo nie jest replikowane). Po kliknięciu tego przycisku dodawana jest domyślna grupa i pozycja podrzędna, przez co serwer połączony do narzędzia Web Administration staje się serwerem głównym.
- Jeśli nie odnaleziono żadnych serwerów głównych, obok przycisku **Make server a master** (Utwórz serwer serwerem głównym) wyświetlana jest etykieta **No master server is defined for this subtree** (Nie zdefiniowano serwera głównego dla tego poddrzewa). Po kliknięciu tego przycisku dodawana jest brakująca pozycja podrzędna, przez co serwer połączony do narzędzia Web Administration staje się serwerem głównym.

## Usuwanie poddrzewa

Ten temat zawiera informacje dotyczące usuwania poddrzewa.

1. Wybierz poddrzewo, które chcesz usunąć.
2. Kliknij przycisk **Delete subtree** (Usuń poddrzewo).
3. Po wyświetleniu żądania potwierdzenie usunięcia kliknij przycisk **OK**.

Poddrzewo zostanie usunięte z listy **Replicated subtree** (Replikowane poddrzewo).

**Uwaga:** Ta operacja zakończy się powodzeniem tylko wtedy, gdy pozycja `ibm-replicaGroup=default` jest pusta.

## Wygaszanie poddrzewa

Ten temat zawiera informacje dotyczące wygaszania poddrzewa.

Funkcja ta jest przydatna podczas obsługi topologii lub dokonywania w niej zmian. Zmniejsza ona liczbę aktualizacji, które można wykonać na serwerze. Wygaszony serwer nie akceptuje żądań klientów. Akceptuje on tylko żądania administratora używającego narzędzi do administrowania serwerem.

Ta funkcja jest typu boolowskiego.

1. Kliknij **Quiesce/Unquiesce** (Wygas/Cofnij wygaszenie), aby wygasić poddrzewo.

2. Po wyświetleniu żądania potwierdzenie operacji kliknij przycisk **OK**.
3. Kliknij **Quiesce/Unquiesce** (Wygaś/Cofnij wygaszenie), aby cofnąć wygaszenie poddrzewa.
4. Po wyświetleniu żądania potwierdzenie operacji kliknij przycisk **OK**.

## Edytowanie list kontroli dostępu

Ten temat zawiera informacje o uprawnieniach wymaganych do edytowania list kontroli dostępu oraz instrukcje dotyczące pracy z listami kontroli dostępu.

Informacje o replikacji (pozycje podrzędne repliki, umowy replikacji, harmonogramy, możliwe referencje) są przechowywane w obiekcie specjalnym **ibm-replicagroup=default**. Obiekt **ibm-replicagroup** znajduje się zaraz pod główną pozycją replikowanego poddrzewa. Domyślnie poddrzewo to dziedziczy listę ACL z głównej pozycji replikowanego poddrzewa. Ta lista ACL może nie być odpowiednia do kontroli dostępu do informacji replikacji.

Wymaganie uprawnienia:

- Sterowanie replikacją - potrzebne są uprawnienia do zapisu do obiektu **ibm-replicagroup=default** (lub prawa właściciela/administratora).
- Kaskadowe sterowanie replikacją - potrzebne są uprawnienia do zapisu do obiektu **ibm-replicagroup=default** (lub prawa właściciela/administratora).
- Sterowanie kolejkami - potrzebne są uprawnienia do zapisu do umowy replikacji.

Aby wyświetlić właściwości listy ACL za pomocą programu narzędziowego Web Administration lub pracować z nimi, należy zapoznać się z sekcją “Zadania związane z listami kontroli dostępu” na stronie 214.

Więcej informacji zawiera temat “Listy kontroli dostępu” na stronie 64.

## Zadania związane z właściwościami bezpieczeństwa

Ten temat zawiera informacje dotyczące zarządzania zadaniami związanymi z właściwościami bezpieczeństwa.

Serwer Directory Server zawiera wiele mechanizmów zapewniających ochronę danych. Obejmują one zarządzanie hasłami, szyfrowanie za pomocą SSL i TLS, uwierzytelnianie Kerberos i uwierzytelnianie DIGEST-MD5. Więcej informacji na temat pojęć związanych z ochroną zawiera sekcja “Bezpieczeństwo serwera Directory Server” na stronie 51.

### Pojęcia pokrewne

“Bezpieczeństwo serwera Directory Server” na stronie 51

Informacje o funkcjach służących do zabezpieczania serwera Directory Server.

## Zadania związane z hasłami

Ten temat zawiera informacje dotyczące zadań związanych z hasłami.

Aby zarządzać hasłami, w obszarze nawigacyjnym narzędzia Web Administration rozwiń kategorię **Manage security properties** (Zarządzanie właściwościami ochrony) i wybierz zakładkę **Password policy** (Strategia haseł).

### Pojęcia pokrewne

“Strategia haseł” na stronie 77

Jeśli serwery LDAP służą do uwierzytelniania, to ważne jest, aby obsługiwały strategię dotyczące wygaśnięcia hasła, zakończonych niepowodzeniem prób zalogowania się i reguł dotyczących haseł. Serwer Directory Server udostępnia konfigurowalną obsługę wszystkich trzech rodzajów strategii.

### Ustawianie właściwości strategii haseł:

Ten temat zawiera informacje dotyczące ustawiania właściwości strategii haseł.

Aby ustawić strategię hasła, wykonaj następujące czynności:

l **Uwaga:** W poniższych punktach opisano konfigurowanie strategii haseł użytkowników. Aby dowiedzieć się więcej o  
l strategii hasła administratora dotyczącej członków grupy administracyjnej, zapoznaj się z tematem  
l Ustawianie hasła administratora i strategii blokowania.

1. W obszarze nawigacyjnym narzędzia Web Administration rozwiń kategorię **Manage security properties** (Zarządzanie właściwościami ochrony) i wybierz zakładkę **Password policy** (Strategia haseł). Panel ten zawiera nieedytowalne pole **Password attribute** (Atrybut hasła) zawierające nazwę atrybutu, którego używa strategia haseł.
2. Z listy rozwijanej wybierz metodę szyfrowania haseł:

l **Brak** Hasła są zapisywane na liście sprawdzania w postaci zaszyfrowanej dwukierunkowo i wczytywane jako  
l część pozycji w pierwotnej postaci jawnego tekstu. Aby możliwe było używanie tego ustawienia,  
l wartość systemowa QRETSVRSEC musi wynosić 1.

**crypt** Hasła są szyfrowane za pomocą algorytmu kodowania crypt systemu UNIX zanim zostaną wprowadzone do katalogu.

**SHA-1** Hasła są szyfrowane za pomocą algorytmu kodowania SHA-1 crypt zanim zostaną wprowadzone do katalogu.

l **MD5** Hasła są szyfrowane za pomocą algorytmu MD5 zanim zostaną wprowadzone do katalogu.

l **AES128**  
Hasła są szyfrowane za pomocą algorytmu AES128 zanim zostaną wprowadzone do katalogu i są wczytywane jako część pozycji w pierwotnej postaci jawnego tekstu.

l **AES192**  
Hasła są szyfrowane za pomocą algorytmu AES192 zanim zostaną wprowadzone do katalogu i są wczytywane jako część pozycji w pierwotnej postaci jawnego tekstu.

l **AES256**  
Hasła są szyfrowane za pomocą algorytmu AES256 zanim zostaną wprowadzone do katalogu i są wczytywane jako część pozycji w pierwotnej postaci jawnego tekstu.

l **Uwaga:** Algorytm AES nie jest obsługiwany na serwerach LDAP w wersji wcześniejszej niż V6R1. W  
l przypadku wyeksportowania zaszyfrowanych algorytmem AES haseł i zaimportowania ich do serwera w  
l wersji wcześniejszej niż V6R1, hasła nie będą nadawały się do użytku.

l W przypadku użycia szyfrowania AES na wielu serwerach wszystkie serwery muszą używać tego samego hasła i  
l klucza dodatkowego AES. Administrator musi śledzić hasło, gdy w oknie konfiguracji serwera wyświetlany jest  
l dostępny skonfigurowany klucz dodatkowy. Konfigurując dodatkowy serwer do korzystania z algorytmu AES,  
l administrator musi wprowadzić prawidłowe hasło i klucz dodatkowy.

l Więcej informacji na ten temat zawiera temat Szyfrowanie haseł, do którego odsyłacz zamieszczono poniżej.

3. Zaznacz pole wyboru **Password policy enabled** (Strategia haseł włączona), aby aktywować strategię haseł.

**Uwaga:** Jeśli strategia haseł nie jest aktywna, pozostałe funkcje w tym panelu i pozostałych panelach związanych z hasłami nie są dostępne. Domyślnie, strategia haseł jest wyłączona.

4. Zaznacz pole wyboru **User can change password** (Użytkownik może zmienić hasło), aby określić, że użytkownik może zmienić hasło.
5. Zaznacz pole wyboru **User must change password after reset** (Użytkownik musi zmienić hasło po wyzerowaniu), aby określić, że użytkownik musi zmienić hasło po zalogowaniu z wyzerowanym hasłem.
6. Zaznacz pole wyboru **User must send password when changing** (Użytkownik musi wysłać hasło podczas zmiany), aby określić, że po początkowym zalogowaniu użytkownik musi podać hasło ponownie, zanim możliwa będzie zmiana hasła.
7. Określ limit ważności hasła. Kliknij przełącznik **Password Never Expires** (Hasło nigdy nie traci ważności), aby określić, że hasło nie musi być zmieniane z określoną częstotliwością lub kliknij przełącznik **Days** (Dni), aby określić częstotliwość zerowania hasła w dniach.
8. Określ, czy system ma wysyłać ostrzeżenie o utracie ważności hasła przed jej utratą.

Po kliknięciu przełącznika **Never warn** (Nigdy nie ostrzegaj), użytkownik nie będzie ostrzegany, że poprzednie hasło traci ważność. Użytkownik nie może uzyskać dostępu do katalogu, zanim administrator nie utworzy nowego hasła.

Po kliknięciu przełącznika **Days before expiration** (Dni przed utratą ważności) i określeni liczby dni (n), użytkownik otrzyma ostrzeżenie i podpowiedź, aby utworzył nowe hasło podczas każdego logowania, począwszy od n dni przed utratą ważności przez hasło. Do momentu utraty ważności przez hasło, użytkownik nadal posiada dostęp do katalogu.

9. Określ liczbę logowań, które użytkownik może wykonać po utracie ważności przez hasło (o ile taka możliwość ma być dostępna). Ten wybór pozwala użytkownikowi uzyskać dostęp do katalogu za pomocą hasła, które utraciło ważność.
10. Kliknij przycisk **OK**.

**Uwaga:** Do ustawienia strategii haseł można również użyć programu narzędziowego ldapmodify (patrz sekcja “ldapmodify i ldapadd” na stronie 218).

Więcej informacji na temat strategii haseł zawiera sekcja “Strategia haseł” na stronie 77.

### Pojęcia pokrewne

“Szyfrowanie haseł” na stronie 54

Serwer IBM Tivoli Directory Server umożliwia zapobieganie nieuprawnionemu dostępowi do haseł użytkowników. Administrator może skonfigurować serwer, aby szyfrował wartości atrybutu userPassword w formacie szyfrowania jednokierunkowego lub dwukierunkowego. Zasyfrowane hasła są oznaczane nazwą algorytmu szyfrującego, dlatego w katalogu mogą istnieć jednocześnie hasła zasyfrowane w różnych formatach. Po zmianie konfiguracji szyfrowania istniejące zasyfrowane hasła pozostaną niezmienione i nadal będą działać.

### Zadania pokrewne

“Ustawianie hasła administratora i strategii blokowania”

Strategię hasła administratora można ustawić tylko za pomocą wiersza komend. Narzędzie Web Administration nie umożliwia pracy ze strategią hasła administratora.

## | Ustawianie hasła administratora i strategii blokowania:

| Strategię hasła administratora można ustawić tylko za pomocą wiersza komend. Narzędzie Web Administration nie umożliwia pracy ze strategią hasła administratora.

| **Uwaga:** Należy uwierzytelnić się jako użytkownik systemu i5/OS z uprawnieniami specjalnymi \*ALLOBJ i \*IOSYSCFG.

| Aby włączyć strategię hasła administratora z bezpieczną konfiguracją EAL4, należy uruchomić następującą komendę:

```
| ldapmodify -D <nazwa_dn_administratora> -w <hasło_administratora> -i <plik>
```

| gdzie <plik> zawiera:

```
| dn: cn=pwdPolicy Admin,cn=Configuration
| changetype: modify
| replace: ibm-slapdConfigPwdPolicyOn
| ibm-slapdConfigPwdPolicyOn: true
```

| Aby włączyć strategię hasła administratora i zmodyfikować ustawienia domyślne, należy uruchomić następującą komendę:

```
| ldapmodify -D <nazwa_dn_administratora> -w <hasło_administratora> -i <plik>
```

| gdzie <plik> zawiera:

```
| dn: cn=pwdPolicyAdmin,cn=Configuration
| changetype: modify
| replace: ibm-slapdConfigPwdPolicyOn
| ibm-slapdConfigPwdPolicyOn: TRUE
| -
```



```

| replace:pwdlockout
| pwdlockout: TRUE
| #wybierz TRUE, aby włączyć, lub FALSE, aby wyłączyć
| -
| replace:pwdmaxfailure
| pwdmaxfailure: 10
| -
| replace:pwdlockoutduration
| pwdlockoutduration: 300
| -
| replace:pwdfailurecountinterval
| pwdfailurecountinterval: 0
| -
| replace:pwdminlength
| pwdminlength: 8
| -
| replace:passwordminalphachars
| passwordminalphachars: 2
| -
| replace:passwordminotherchars
| passwordminotherchars: 2
| -
| replace:passwordmaxrepeatedchars
| passwordmaxrepeatedchars: 2
| -
| replace:passwordmindiffchars
| passwordmindiffchars: 2

```

**Uwaga:** Konta administratorów mogą być blokowane w wyniku nadmiernej ilości niepowodzeń uwierzytelniania. Dotyczy to tylko zdalnych połączeń klientów. Konto jest resetowane podczas uruchamiania serwera.

#### **Zadania pokrewne**

“Ustawianie właściwości strategii haseł” na stronie 176  
 Ten temat zawiera informacje dotyczące ustawiania właściwości strategii haseł.

#### **Ustawianie właściwości blokowania haseł:**

Ten temat zawiera informacje dotyczące ustawiania właściwości blokowania haseł.

1. W obszarze nawigacyjnym narzędzia Web Administration rozwiń kategorię **Manage security properties** (Zarządzanie właściwościami ochrony) i wybierz zakładkę **Password lockout** (Blokowanie haseł).

**Uwaga:** Jeśli strategia haseł nie została aktywowana na serwerze, funkcje znajdujące się w tym panelu nie działają.

2. Określ liczbę sekund, minut, godzin lub dni, które muszą upłynąć zanim hasło będzie mogło zostać zmienione.
3. Określ, czy niepoprawne logowanie ma blokować hasło.
  - Zaznacz przełącznik **Passwords are never locked out** (Hasła nie są nigdy blokowane), a by określić nieograniczoną liczbę prób logowania. Ten wybór wyłącza funkcje blokowania haseł.
  - Zaznacz przełącznik **Attempts (Próby)** i określ liczbę prób logowania dozwolonych przed zablokowaniem hasła. Ten wybór włącza funkcje blokowania haseł.
4. Określ czas trwania blokady. Zaznacz przełącznik **Lockouts never expire** (Blokady nigdy nie tracą ważności), aby określić, że administrator systemu musi wyzerować hasło lub zaznacz przełącznik **Seconds** (Sekundy), aby określić liczbę sekund zanim blokada utraci ważność i można będzie wznowić próby logowania.
5. Określ czas utraty ważności dla niepoprawnego logowania. Kliknij przełącznik **Incorrect logins only cleared with correct password** (Niepoprawne logowanie anulowane jedynie przez poprawne hasło), aby określić, że niepoprawne logowanie jest anulowane jedynie przez poprawne zalogowanie lub kliknij przełącznik **Seconds** (Sekundy) i określ liczbę sekund przed usunięciem nieudanego logowania z pamięci.

**Uwaga:** Opcja ta działa tylko, jeśli hasło nie jest zablokowane.

6. Po zakończeniu kliknij przycisk **Apply** (Zastosuj), aby zachować zmiany nie wychodząc lub kliknij przycisk **OK**, aby zachować zmiany i wyjść lub kliknij przycisk **Cancel** (Anuluj), aby opuścić panel nie zachowując zmian.

#### Ustawianie właściwości sprawdzania haseł:

Ten temat zawiera informacje dotyczące ustawiania właściwości sprawdzania haseł.

1. W obszarze nawigacyjnym narzędzia Web Administration rozwiń kategorię **Manage security properties** (Zarządzanie właściwościami ochrony) i wybierz zakładkę **Password validation** (Sprawdzanie poprawności haseł).

**Uwaga:** Jeśli strategia haseł nie została aktywowana na serwerze, funkcje znajdujące się w tym panelu nie działają.

2. Określ liczbę haseł, które muszą zostać użyte zanim hasło będzie mogło zostać wykorzystane ponownie. Wprowadź liczbę z przedziału od 0 do 30. Jeśli wprowadzona zostanie wartość zero, hasło może być wykorzystywane ponownie bez ograniczeń.
3. Z menu rozwijanego wybierz, czy hasło ma być sprawdzane pod względem składni zdefiniowanej w następujących polach wprowadzania. Można wybrać:

**Do not check syntax (Nie sprawdzaj składni)**

Sprawdzanie składni nie będzie wykonywane.

**Check syntax (except encrypted) (Sprawdzaj składnię (poza hasłami szyfrowanymi))**

Sprawdzanie składni będzie wykonywane dla wszystkich nieszyfrowanych haseł.

**Check syntax (Sprawdzaj składnię)**

Sprawdzanie składni będzie wykonywane dla wszystkich haseł.

4. Określ wartość liczbową minimalnej długości hasła. Jeśli wartość wynosi zero, sprawdzanie składni nie będzie wykonywane.

- Określ wartość liczbową minimalnej liczby znaków alfabetycznych wymaganych w haśle.
- Określ wartość liczbową minimalnej liczby znaków liczbowych i specjalnych wymaganych w haśle.

**Uwaga:** Suma minimalnych liczb znaków alfabetycznych, liczbowych i specjalnych musi być równa lub mniejsza od liczby określonej jako minimalna długość hasła.

5. Określ maksymalną liczbę znaków, które mogą zostać powtórzone w haśle. Opcja ta ogranicza liczbę wystąpień specyficznego znaku w haśle. Jeśli wartość wynosi zero, liczba powtórzonych znaków nie jest sprawdzana.
6. Określ minimalną liczbę znaków, które muszą być różne od znaków użytych w poprzednim haśle oraz liczbę poprzednich haseł określoną w polu **Minimum number of passwords before reuse** (Minimalna liczba haseł przed ponownym użyciem). Jeśli wartość wynosi zero, liczba różnych znaków nie jest sprawdzana.
7. Po zakończeniu kliknij przycisk **Apply** (Zastosuj), aby zachować zmiany nie wychodząc lub kliknij przycisk **OK**, aby zachować zmiany i wyjść lub kliknij przycisk **Cancel** (Anuluj), aby opuścić panel nie zachowując zmian.

#### Wyświetlanie atrybutów strategii haseł:

Ten temat zawiera informacje dotyczące wyświetlania atrybutów strategii haseł.

Atrybuty wykonawcze zwracane są na żądanie wyszukiwania jedynie na szczególne żądanie klienta. Aby użyć tych atrybutów w operacjach wyszukiwania, użytkownik musi posiadać uprawnienie do neuralgicznych atrybutów lub uprawnienie do specyficznych użytych atrybutów.

1. Aby wyświetlić wszystkie atrybuty strategii haseł dla danej pozycji:  

```
> ldapsearch -b "uid=user1,cn=users,o=ibm" -s base "(objectclass=*)"
pwdChangedTime pwdAccountLockedTime pwdExpirationWarned
pwdFailureTime pwdGraceUseTime pwdReset
```
2. Aby wprowadzić zapytanie o pozycje, dla których hasło niedługo utraci ważność, należy użyć atrybutu `pwdChangedTime`. Na przykład, aby wyszukać hasła tracące ważność 26 sierpnia 2004 o strategii utraty ważności haseł 186 dni, należy wprowadzić zapytanie o pozycje, dla których hasło zostało zmienione przynajmniej 186 dni temu (22 lutego 2004):

```
> ldapsearch -b "cn=users,o=ibm" -s sub
"!(pwdChangedTime>20040222000000Z)" 1.1
```

gdzie filtr odpowiada atrybutowi pwdChangedTime północ, 22 lutego 2004.

3. Aby wprowadzić zapytanie o zablokowane konta, należy użyć atrybutu pwdAccountLockedTime:

```
> ldapsearch -b "cn=users,o=ibm" -s sub "(pwdAccountLockedTime=*)" 1.1
```

gdzie "1.1" wskazuje, że zwrócone mają być tylko nazwy wyróżniające pozycji.

4. Aby wprowadzić zapytanie o konta, dla których hasła muszą zostać zmienione, ponieważ hasło zostało wyzerowane, należy użyć atrybutu pwdReset:

```
> ldapsearch -b "cn=users,o=ibm" -s sub "(pwdReset=TRUE)" 1.1
```

### Przesłanie atrybutów strategii hasel:

Ten temat zawiera informacje służące do przesłania atrybutów strategii hasel.

Należy najpierw wykonać następujące czynności.

Administrator katalogu może przesłać zwykłe zachowanie strategii hasel dla określonych pozycji modyfikując atrybuty wykonawcze strategii hasel i używając elementu sterującego administrowania serwerem (opcja -k narzędzi wiersza komend LDAP).

1. Można zapobiec utracie ważności hasła dla określonego konta ustawiając dla atrybutu pwdChangedTime datę odległą w czasie podczas ustawiania atrybutu userPassword. W poniższym przykładzie datę ustawiono na północ, 1 stycznia 2200.

```
> ldapmodify -D cn=root -w ? -k
dn: uid=wasadmin,cn=users,o=ibm
changetype: modify
replace: pwdChangedTime
pwdChangedTime: 22000101000000Z
```

2. Hasło zablokowane z powodu przekroczenia liczby niepoprawnych logowań można odblokować usuwając atrybuty pwdAccountLockedTime i pwdFailureTime attributes:

```
> ldapmodify -D cn=root -w ? -k
dn: uid=user1,cn=users,o=ibm
changetype: modify
delete: pwdAccountLockedTime
-
delete: pwdFailureTime
```

3. Konto, które utraciło ważność można odblokować zmieniając atrybut pwdChangedTime i usuwając atrybuty pwdExpirationWarned i pwdGraceUseTime attributes:

```
> ldapmodify -D cn=root -w ? -k
dn: uid=user1,cn=users,o=ibm
changetype: modify
replace: pwdChangedTime
pwdChangedTime: 20040826000000Z
-
delete: pwdExpirationWarned
-
delete: pwdGraceUseTime
```

4. Status "Hasło musi zostać zmienione" można usunąć lub ustawić określając atrybut pwdReset:

```
> ldapmodify -D cn=root -w ? -k
dn: uid=user1,cn=users,o=ibm
changetype: modify
delete: pwdReset
```

```
> ldapmodify -D cn=root -w ? -k
dn: uid=user2,cn=users,o=ibm
changetype: modify
replace: pwdReset
pwdReset: TRUE
```

5. Konto można zablokować z poziomu administracyjnego ustawiając wartość TRUE dla atrybutu wykonawczego `ibm-pwdAccountLocked`.

Użytkownik zmieniający ten atrybut musi posiadać uprawnienie do zapisu atrybutu `ibm-pwdAccountLocked`, który zdefiniowany jest jako posiadający klasę dostępu CRITICAL (newralgiczny).

```
> ldapmodify -D uid=useradmin,cn=users,o=ibm -w ?
dn: uid=user1,cn=users,o=ibm
changetype: modify
replace: ibm-pwdAccountLocked
ibm-pwdAccountLocked: TRUE
```

6. Konto można odblokować ustawiając wartość atrybutu FALSE. Odblokowanie konta w ten sposób nie wpływa na status konta uzależniony od przekroczenia liczby niepoprawnych haseł lub utraty ważności hasła.

Użytkownik zmieniający ten atrybut musi posiadać uprawnienie do zapisu atrybutu `ibm-pwdAccountLocked`, który zdefiniowany jest jako posiadający klasę dostępu CRITICAL (newralgiczny).

```
> ldapmodify -D uid=useradmin,cn=users,o=ibm -w ?
dn: uid=user1,cn=users,o=ibm
changetype: modify
replace: ibm-pwdAccountLocked
ibm-pwdAccountLocked: FALSE
```

## Włączanie SSL i TLS na serwerze Directory Server

W tym temacie opisano włączanie zabezpieczeń SSL i TLS na serwerze Directory Server.

Jeśli w systemie jest zainstalowany program Digital Certificate Manager, można użyć ochrony SSL (Secure Sockets Layer) w celu zabezpieczenia dostępu do serwera Directory Server. Przed włączeniem SSL na serwerze katalogów pomocne może być zapoznanie się z tematem Protokoły SSL (Secure Sockets Layer) i TLS (Transport Layer Security) na serwerze Directory Server.

Aby włączyć protokół SSL na serwerze LDAP:

### 1. Przypisz certyfikat do serwera Directory Server

- a. Instrukcje dotyczące zarządzania serwerem Directory Server za pomocą programu System i Navigator poprzez połączenie SSL można znaleźć w podręczniku *System i Access for Windows User's Guide* (jest on opcjonalnie instalowany na komputerze PC podczas instalowania programu System i Navigator). Jeśli planowane jest zezwolenie zarówno na połączenia SSL, jak i inne połączenia z serwerem katalogów, można pominąć tę czynność.
- b. Uruchom program IBM Digital Certificate Manager. Więcej informacji zawiera sekcja Uruchamianie programu Digital Certificate Manager w temacie Digital Certificate Manager.
- c. Jeśli chcesz uzyskać lub utworzyć certyfikaty bądź w inny sposób skonfigurować lub zmienić system certyfikatów, zrób to teraz. Więcej informacji o konfigurowaniu systemu certyfikacji zawiera temat Digital Certificate Manager. Do serwera Directory Server przypisane są dwie aplikacje serwera i jedna aplikacja kliencka. Są to:

#### Aplikacja Directory Server

Aplikacja Directory Server jest serwerem.

#### Aplikacja publikowania serwera Directory Server

Aplikacja publikowania serwera Directory Server określa używany certyfikat poprzez jego opublikowanie.

#### Aplikacja kliencka serwera Directory Server

Aplikacja kliencka serwera Directory Server określa domyślny certyfikat stosowany przez aplikacje używające funkcji API ILE klienta LDAP.

- d. Kliknij przycisk **Wybór ośrodka certyfikacji**.
- e. Wybierz **\*SYSTEM**. Kliknij przycisk **Continue** (Kontynuuj).
- f. Wpisz hasło bazy certyfikatów **\*SYSTEM**. Kliknij przycisk **Continue** (Kontynuuj).
- g. Po odświeżeniu menu nawigacji po lewej stronie, rozwiń pozycję **Zarządzanie aplikacjami**.
- h. Kliknij opcję **Aktualizacja przypisania certyfikatu** (Update certificate assignment).

- i. Na następnym ekranie wybierz aplikację **Serwer**. Kliknij przycisk **Continue** (Kontynuuj).
- j. Wybierz **Serwer Directory Server**.
- k. Kliknij opcję **Aktualizacja przypisania certyfikatu** (Update certificate assignment), aby przypisać certyfikat do serwera Directory Server, aby używał go do określania tożsamości klientów System i Access for Windows.

**Uwaga:** Jeśli certyfikat zostanie wybrany z ośrodka CA, którego certyfikatu CA nie ma w bazie danych kluczy klienta System i Access for Windows, należy go dodać, aby korzystać z SSL. Zakończ tę procedurę przed rozpoczęciem następnej.

- l. Wybierz certyfikat z listy, aby przypisać go do serwera.
  - m. Kliknij **Przypisanie nowego certyfikatu**.
  - n. DCM odświeża stronę **Aktualizacja przypisania certyfikatu** i wyświetla komunikat z potwierdzeniem. Po zakończeniu konfigurowania certyfikatów dla serwera Directory Server, kliknij przycisk **Gotowe**.
2. Opcjonalne: **Przypisz certyfikat dla publikowania serwera Directory Server**. Jeśli ma również zostać włączone publikowanie z systemu do serwera Directory Server poprzez połączenie SSL, może być wskazane dodatkowe powiązanie certyfikatu za pomocą funkcji publikowania serwera Directory Server. Określa to domyślny certyfikat i zaufane ośrodki certyfikacji dla aplikacji używającej funkcji API LDAP ILE, które nie określają własnego identyfikatora aplikacji ani alternatywnej bazy danych kluczy.
- a. Uruchom program IBM Digital Certificate Manager.
  - b. Kliknij przycisk **Wybór ośrodka certyfikacji**.
  - c. Wybierz **\*SYSTEM**. Kliknij przycisk **Continue** (Kontynuuj).
  - d. Wpisz hasło bazy certyfikatów **\*SYSTEM**. Kliknij przycisk **Continue** (Kontynuuj).
  - e. Po odświeżeniu menu nawigacji po lewej stronie, rozwiń pozycję **Zarządzanie aplikacjami**.
  - f. Kliknij opcję **Aktualizacja przypisania certyfikatu** (Update certificate assignment).
  - g. Na następnym ekranie wybierz aplikację **Klient**. Kliknij przycisk **Continue** (Kontynuuj).
  - h. Wybierz **Publikowanie serwera Directory Server**.
  - i. Kliknij opcję **Aktualizacja przypisania certyfikatu** (Update certificate assignment), aby przypisać certyfikat do publikowania serwera Directory Server, aby używał go do określania tożsamości.
  - j. Wybierz certyfikat z listy, aby przypisać go do serwera.
  - k. Kliknij **Przypisanie nowego certyfikatu**.
  - l. DCM odświeża stronę **Aktualizacja przypisania certyfikatu** i wyświetla komunikat z potwierdzeniem.

**Uwaga:** W tych instrukcjach przyjęto, że użytkownik publikuje już informacje na serwerze Directory Server za pomocą połączenia bez użycia SSL. Sekcja “Publikowanie informacji na serwerze Directory Server” na stronie 129 zawiera kompletne informacje na temat konfigurowania publikowania.

3. Opcjonalne: **Przypisz certyfikat do klienta serwera Directory Server**. Jeśli istnieją inne aplikacje używające połączeń SSL z serwerem Directory Server, należy również powiązać certyfikat z klientem serwera Directory Server.
- a. Uruchom program IBM Digital Certificate Manager.
  - b. Kliknij przycisk **Wybór ośrodka certyfikacji**.
  - c. Wybierz **\*SYSTEM**. Kliknij przycisk **Continue** (Kontynuuj).
  - d. Wpisz hasło bazy certyfikatów **\*SYSTEM**. Kliknij przycisk **Continue** (Kontynuuj).
  - e. Po odświeżeniu menu nawigacji po lewej stronie, rozwiń pozycję **Zarządzanie aplikacjami**.
  - f. Kliknij opcję **Aktualizacja przypisania certyfikatu** (Update certificate assignment).
  - g. Na następnym ekranie wybierz aplikację **Klient**. Kliknij przycisk **Continue** (Kontynuuj).
  - h. Wybierz **Klient serwera Directory Server**.
  - i. Kliknij opcję **Aktualizacja przypisania certyfikatu** (Update certificate assignment), aby przypisać certyfikat do klienta serwera Directory Server, aby używał go do określania tożsamości.
  - j. Wybierz certyfikat z listy, aby przypisać go do serwera.

k. Kliknij **Przypisanie nowego certyfikatu**.

l. DCM odświeża stronę **Aktualizacja przypisania certyfikatu** i wyświetla komunikat z potwierdzeniem.

Po udostępnieniu SSL można zmienić port używany przez Directory Server do połączeń chronionych.

Aby używać SSL lub TLS, należy aktywować te funkcje w programie System i Navigator.

1. W programie System i Navigator rozwiń pozycję **Sieć**.
2. Rozwiń pozycję **Serwery**.
3. Prawym przyciskiem myszy kliknij **Katalog** i wybierz opcję **Właściwości**.
4. W zakładce **Sieć** zaznacz pole z boku pola **Zabezpiecz**.

Można także określić numer portu, który ma być chroniony. Kliknięcie pola wyboru **Zabezpiecz** wskazuje, że aplikacja może uruchomić połączenie SSL lub TLS na bezpiecznym porcie. Oznacza to również, że aplikacja może wprowadzić działanie StartTLS, aby zezwolić na połączenie TLS na porcie niechronionym. Ewentualnie, ochronę TLS można wywołać za pomocą opcji -Y z poziomu narzędzi wiersza komend klienta. Jeśli używany jest wiersz komend, atrybut `ibm-slapdSecurity` musi być równy TLS lub SSLTLS.

#### Pojęcia pokrewne

“Protokoły SSL (Secure Sockets Layer) i TLS (Transport Layer Security) na serwerze Directory Server” na stronie 52

Aby komunikacja z serwerem Directory Server była bezpieczniejsza, serwer może używać protokołów SSL (Secure Sockets Layer) i TLS (Transport Layer Security).

## Włączanie uwierzytelniania Kerberos na serwerze Directory Server

Ten temat zawiera informacje dotyczące włączania uwierzytelniania Kerberos na serwerze Directory Server.

Jeśli w systemie jest skonfigurowana Sieciowa usługa uwierzytelniania, to serwer Directory Server można skonfigurować tak, aby korzystał z uwierzytelniania protokołem Kerberos. Uwierzytelnianie Kerberos dotyczy użytkowników i administratora. Przed włączeniem protokołu Kerberos na serwerze katalogów przydatne może być zapoznanie się z przeglądem korzystania z protokołu Kerberos na serwerze Directory Server.

Aby włączyć uwierzytelnianie protokołem Kerberos, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń pozycję **Sieć**.
2. Rozwiń pozycję **Serwery**.
3. Kliknij **TCP/IP**.
4. Prawym przyciskiem myszy kliknij **IBM Directory Server** i wybierz **Właściwości**.
5. Kliknij zakładkę **Kerberos**.
6. Zaznacz **Enable Kerberos authentication** (Włącz uwierzytelnianie Kerberos).
7. Na stronie **Kerberos** podaj inne ustawienia, odpowiednio do sytuacji. Informacje dotyczące poszczególnych pól można znaleźć w dokumentacji elektronicznej.

#### Odsyłacze pokrewne

“Uwierzytelnianie” na stronie 80

Uwierzytelnianie umożliwia kontrolę dostępu w ramach serwera Directory Server.

## Konfigurowanie uwierzytelniania DIGEST-MD5 na serwerze Directory Server

Ten temat zawiera informacje dotyczące konfigurowania uwierzytelniania DIGEST-MD5 na serwerze Directory Server.

DIGEST-MD5 jest mechanizmem uwierzytelniania SASL. Jeśli klient używa mechanizmu DIGEST-MD5, hasło zostanie przesłane w tekście zaszyfrowanym, zaś protokół zapobiegnie atakom z powtórzonymi danymi. Do konfigurowania uwierzytelniania DIGEST-MD5 służy narzędzie Web Administration.

1. W obszarze **Server administration** (Administrowanie serwerem) rozwiń kategorię **Manage security properties** (Zarządzanie właściwościami ochrony) i wybierz zakładkę **DIGEST-MD5**.

- Uwaga:** Aby zmienić konfigurację serwera za pomocą zadań w kategorii Server administration (Administrowanie serwerem) w narzędziu Web Administration, należy uwierzytelnić się na serwerze jako profil użytkownika systemu i5/OS z uprawnieniami specjalnymi \*ALLOBJ i IOSYSCFG. Można to zrobić, dokonując uwierzytelnienia jako użytkownik rzutowany i używając hasła dla tego profilu. Aby nawiązać połączenie jako użytkownik rzutowany z poziomu narzędzia Web Administration, należy wprowadzić nazwę użytkownika w postaci `os400-profile=MOJANAZWAUŻYTKOWNIKA,cn=accounts,os400-sys=MÓJSYSTEM.PL`, gdzie łańcuchy znaków MOJANAZWAUŻYTKOWNIKA i MÓJSYSTEM.PL zastępowane są odpowiednio nazwą profilu użytkownika i skonfigurowanym przyrostkiem rzutowania.
2. W polu **Server realm** (Dziedzina serwera), wybierz ustawienie **Default** (Domyślne), które oznacza pełną nazwę hosta serwera lub kliknij przycisk **Realm** (Dziedzina) i wpisz nazwę dziedziny, pod którą ma zostać skonfigurowany serwer. Za pomocą tej nazwy dziedziny klient określa, której nazwy użytkownika i jakiego hasła należy użyć. W przypadku użycia replikacji, wszystkie serwery powinny być skonfigurowane za pomocą tej samej dziedziny.
  3. W polu atrybutu **Username** (Nazwa użytkownika), wybierz ustawienie **Default** (Domyślne), które oznacza uid lub kliknij przycisk **Attribute** (Atrybut) i wpisz nazwę atrybutu, której ma użyć serwer do jednoznacznej identyfikacji pozycji użytkownika podczas połączeń DIGEST-MD5 SASL .
  4. Jeśli użytkownik jest zalogowany jako administrator katalogu, w polu **Administrator username** (Nazwa użytkownika administratora) należy wpisać nazwę użytkownika administratora. Pole to nie może być wypełniane przez członków grupy administracyjnej. Jeśli nazwa użytkownika określona w połączeniu SASL DIGEST-MD5 jest zgodna z podanym ciągiem znaków, administratorem jest użytkownik.

**Uwaga:** W nazwie użytkownika administratora rozróżniana jest wielkość liter.

5. Po zakończeniu kliknij przycisk **OK**.

#### **Odsyłacze pokrewne**

“Uwierzytelnianie” na stronie 80

Uwierzytelnianie umożliwia kontrolę dostępu w ramach serwera Directory Server.

## **Zadania związane ze schematem**

Ten temat zawiera informacje dotyczące zarządzania schematem.

Schematem można zarządzać za pomocą narzędzia Web Administration lub aplikacji LDAP, takiej jak Ldapmodify, w połączeniu z plikami LDIF. Podczas pierwszego definiowania nowych klas obiektu lub atrybutów najwygodniejsze może być użycie programu Web Administration. Do skopiowania nowego schematu na inne serwery (być może jako część wdrażanego produktu lub programu narzędziowego), lepszy może okazać się narzędzie Ldapmodify. Więcej informacji zawiera sekcja “Kopiowanie schematu na inne serwery” na stronie 194.

#### **Pojęcia pokrewne**

“Przyrostek (kontekst nazwy)” na stronie 12

Przyrostek (znany również jako kontekst nazwy) to nazwa DN identyfikująca najwyższą pozycję w lokalnej hierarchii katalogu.

“Schemat” na stronie 14

Schemat jest zestawem reguł określających sposób przechowywania danych w katalogu. Schemat definiuje typ dozwolonych pozycji oraz strukturę i składnię atrybutów.

## **Wyświetlanie klas obiektu**

Ten temat zawiera informacje dotyczące wyświetlania klas obiektu.

Klasy obiektu w schemacie można przeglądać za pomocą narzędzia Web Administration lub za pomocą wiersza komend.

1. Rozwiń kategorię **Schema management** (Zarządzanie schematami) w obszarze nawigacyjnym i kliknij **Manage object classes** (Zarządzaj klasami obiektu). Wyświetlony zostanie panel tylko do odczytu umożliwiający przeglądanie klas obiektu w schemacie i ich parametrów. Klasy obiektu wyświetlane są w porządku alfabetycznym. Poruszanie się pomiędzy stronami możliwe jest poprzez klikanie przycisków Previous (Poprzednia) i Next (Następna). Pole znajdujące się obok tych przycisków określa bieżącą stronę. Zawiera ono także listę rozwijaną,

której można użyć w celu bezpośredniego przejścia do wybranej strony. Pierwsza klasa obiektu na stronie wyświetlana jest razem z numerem strony, co pomaga odnaleźć klasę obiektu, którą chce się przeglądać. Na przykład, jeśli szukana jest klasa obiektu **person** (osoba), należy rozwinąć menu i przewinąć je w dół do miejsca, w którym widoczna będzie **Strona 14 z 16 nsLiServer** i **Strona 15 z 16 printerLPR**. Ponieważ klasa obiektu **person** występuje w porządku alfabetycznym pomiędzy klasami obiektu **nsLiServer** oraz **printerLPR**, należy wybrać stronę 14 i kliknąć przycisk **Go** (Przejdź).

Klasy obiektu można także wyświetlać posortowane według typu. Wybierz opcję **Type** (Typ) i kliknij przycisk **Sort** (Sortuj). Klasy obiektu zostaną posortowane alfabetycznie w ramach typu (abstrakcyjne, pomocnicze i strukturalne). Podobnie można odwrócić porządek listy, wybierając opcję **Descending** (Malejąco) i klikając przycisk **Sort** (Sortuj).

2. Po odnalezieniu poszukiwanej klasy obiektu można wyświetlić jej typ, dziedziczenie i atrybuty wymagane oraz opcjonalne. Aby przejrzeć pełną listę każdej charakterystyki, należy rozwinąć odpowiednie menu zawierające dziedziczenie oraz atrybuty wymagane i opcjonalne. Na pasku narzędzi umieszczonym się po prawej stronie znajdują się operacje, które można wykonać na klasach obiektu:
  - Dodanie
  - Edycja
  - Kopiowanie
  - Usuwanie
3. Po zakończeniu kliknij przycisk **Close** (Zamknij), aby powrócić do panelu **Welcome** (Witamy) serwera IBM Directory Server.

Aby wyświetlić klasy obiektu znajdujące się w schemacie za pomocą wiersza komend, wpisz komendę:

```
ldapsearch -b cn=schema -s base objectclass=* objectclasses
```

## Dodawanie klasy obiektu

Ten temat zawiera informacje dotyczące dodawania klasy obiektu.

Jeśli jeszcze tego nie zrobiono, rozwiń kategorię **Schema management** (Zarządzanie schematami) w obszarze nawigacyjnym, a następnie kliknij przycisk **Manage object classes** (Zarządzanie klasami obiektu). Aby utworzyć nową klasę obiektu:

1. Kliknij przycisk **Add** (Dodaj).

**Uwaga:** Dostęp do tego panelu można również uzyskać, rozwijając kategorię **Schema management** (Zarządzanie schematami) w obszarze nawigacyjnym, a następnie kliknij przycisk **Add an object class** (Dodaj klasę obiektu).

2. W zakładce **General properties** (Właściwości ogólne):
  - Wypełnij pole **Object class name** (Nazwa klasy obiektu). Jest ono wymagane i powinno opisowo określać funkcję klasy obiektu. Na przykład **tempEmployee** może być klasą obiektu używaną do śledzenia informacji na temat tymczasowo zatrudnionych.
  - Wpisz **Description** (Opis) klasy obiektu, np. **klasa obiektu używana dla tymczasowo zatrudnionych**.
  - Wpisz **OID** klasy obiektu. Jest to wymagane pole. Więcej informacji zawiera temat "Identyfikator obiektu (OID)" na stronie 25. Jeśli nie masz identyfikatora OID, użyj **Nazwy klasy obiektu** z dodanym ciągiem znaków **-oid**. Na przykład, jeśli nazwą klasy obiektu jest **tempEmployee**, to identyfikatorem OID jest **tempEmployee-oid**. Wartość w tym polu można zmienić.
  - Wybierz pozycję z listy rozwijanej **Superior object class** (Nadrzędna klasa obiektu). Określa ona klasę obiektu, z której dziedziczone są inne atrybuty. Zwykle **Nadrzędną klasą obiektu** jest **top**, jednak może nią być inna klasa obiektu. Na przykład nadrzędną klasą obiektu dla **tempEmployee** może być **e-osoba**.
  - Wybierz **Object class type** (Typ klasy obiektu). Sekcja "Klasy obiektu" na stronie 17 zawiera dodatkowe informacje na temat typów klas obiektu.



- Kliknij zakładkę **Attributes** (Atrybuty), aby określić wymagane i opcjonalne atrybuty danej klasy obiektu oraz przejrzeć atrybuty dziedziczone, kliknij przycisk **OK**, aby dodać nową klasę obiektu, lub kliknij przycisk **Cancel** (Anuluj), aby powrócić do okna **Manage object classes** (Zarządzanie klasami obiektu) bez wprowadzania żadnych zmian.
3. W zakładce **Attributes** (Atrybuty):
    - Wybierz atrybut z alfabetycznej listy **Available attributes** (Dostępne atrybuty) i kliknij przycisk **Add to required** (Dodaj do wymaganych), aby uczynić dany atrybut wymaganym, lub kliknij przycisk **Add to optional** (Dodaj do opcjonalnych), aby uczynić go atrybutem opcjonalnym klasy obiektu. Atrybut zostanie wyświetlony na właściwej liście wybranych atrybutów.
    - Powtórz te czynności dla wszystkich atrybutów, które chcesz wybrać.
    - Atrybuty można przenosić pomiędzy listami lub kasować z nich, zaznaczając najpierw wybrany atrybut, a następnie klikając przycisk **Move to** (Przenieś) lub **Delete** (Usuń).
    - Można przeglądać listy dziedziczonych atrybutów wymaganych i opcjonalnych. Dziedziczone atrybuty są oparte na nadrzędnej klasie obiektu (**Superior object class**) wybranej w zakładce **General** (Ogólne). Atrybutów dziedziczonych nie można zmieniać. Jeśli jednak zmieni się **Nadrzędną klasę obiektu** w zakładce **General** (Ogólne), wyświetlony zostanie inny zestaw atrybutów dziedziczonych.
  4. Kliknij przycisk **OK**, aby dodać nową klasę obiektu, lub kliknij przycisk **Cancel** (Anuluj), aby powrócić do okna **Manage object classes** (Zarządzanie klasami obiektu) bez dokonywania żadnych zmian.

**Uwaga:** W przypadku kliknięcia przycisku **OK** na zakładce **General** (Ogólne) bez uprzedniego dodania żadnych atrybutów, można dodać je później poprzez dokonanie edycji nowej klasy obiektu.

Aby dodać klasę obiektu za pomocą wiersza komend, należy uruchomić następującą komendę:

```
ldapmodify -D <nazwa_dn_administratora> -w <hasło_administratora> -i <plik>
```

gdzie <plik> zawiera:

```
dn: cn=Schema
changetype: modify
add: objectclasses
objectclasses: ( <klasa_obiektu-oid> NAME '<klasa_obiektu>' DESC '<klasa obiektu
                 zdefiniowana dla aplikacji LDAP>' SUP '<diedziczenie_klasy_obiektu>'
                 <typ_klasy_obiektu> MAY (<atrybut1> $ <atrybut2>))
```

## Edytowanie klasy obiektu

Ten temat zawiera informacje dotyczące edytowania klasy obiektu.

Nie wszystkie zmiany schematu są dozwolone. Ograniczenia dotyczące zmian zawiera sekcja “Niedozwolone zmiany schematu” na stronie 28.

Jeśli jeszcze tego nie zrobiono, rozwiń kategorię **Schema management** (Zarządzanie schematami) w obszarze nawigacyjnym, a następnie kliknij przycisk **Manage object classes** (Zarządzanie klasami obiektu). Aby zmienić klasę obiektu:

1. Zaznacz przełącznik znajdujący się obok klasy obiektu, którą chcesz zmodyfikować.
2. Kliknij przycisk **Edit** (Edycja).
3. Wybierz zakładkę:
  - Na karcie **General** (Ogólne):
    - Zmień opis (**Description**).
    - Zmień nadrzędną klasę obiektu (**Superior object class**). Wybierz pozycję z listy rozwijanej Superior object class (Nadrzędna klasa obiektu). Określa ona klasę obiektu, z której dziedziczone są inne atrybuty. Zwykle **Nadrzędną klasą obiektu** jest **top**, jednak może nią być inna klasa obiektu. Na przykład nadrzędną klasą obiektu dla **tempEmployee** może być **e-osoba**.
    - Zmień **Object class type** (Typ klasy obiektu). Wybierz typ klasy obiektu. Sekcja “Klasy obiektu” na stronie 17 zawiera dodatkowe informacje na temat typów klas obiektu.

- Kliknij zakładkę **Attributes** (Atrybuty), aby zmienić wymagane i opcjonalne atrybuty danej klasy obiektu oraz przejrzeć atrybuty dziedziczone, kliknij przycisk **OK**, aby wprowadzić zmiany w życie, lub kliknij przycisk **Cancel** (Anuluj), aby powrócić do okna **Manage object classes** (Zarządzanie klasami obiektu) bez wprowadzania żadnych zmian.

- W zakładce **Attributes** (Atrybuty):

Wybierz atrybut z alfabetycznej listy **Available attributes** (Dostępne atrybuty) i kliknij przycisk **Add to required** (Dodaj do wymaganych), aby uczynić dany atrybut wymaganym, lub kliknij przycisk **Add to optional** (Dodaj do opcjonalnych), aby uczynić go atrybutem opcjonalnym klasy obiektu. Atrybut zostanie wyświetlony na właściwej liście wybranych atrybutów.

Powtórz te czynności dla wszystkich atrybutów, które chcesz wybrać.

Atrybuty można przenosić pomiędzy listami lub kasować z nich, zaznaczając najpierw wybrany atrybut, a następnie klikając przycisk **Move to** (Przenieś) lub **Delete** (Usuń).

Można przeglądać listy dziedziczonych atrybutów wymaganych i opcjonalnych. Dziedziczone atrybuty są oparte na nadrzędnej klasie obiektu (**Superior object class**) wybranej w zakładce **General** (Ogólne). Atrybutów dziedziczonych nie można zmieniać. Jeśli jednak zmieni się **Nadrzędną klasę obiektu** w zakładce **General** (Ogólne), wyświetlony zostanie inny zestaw atrybutów dziedziczonych.

4. Kliknij przycisk **OK**, aby zmiany wprowadzić w życie, lub kliknij przycisk **Cancel** (Anuluj), aby powrócić do okna **Manage object classes** (Zarządzanie klasami obiektu) bez dokonywania żadnych zmian.

Aby wyświetlić klasy obiektu znajdujące się w schemacie za pomocą wiersza komend, uruchom następującą komendę:

```
ldapsearch -b cn=schema -s base objectclass=* objectclasses
```

Aby przeprowadzić edycję klasy obiektu za pomocą wiersza komend, należy uruchomić następującą komendę:

```
ldapmodify -D <nazwa_dn_administratora> -w <hasło_administratora> -i <plik>
```

gdzie <plik> zawiera:

```
dn: cn=schema
changetype: modify
replace: objectclasses
objectclasses: ( <klasa_obiektu-oid> NAME '<klasa_obiektu>' DESC '<Klasa obiektu
zdefiniowana dla aplikacji LDAP>' SUP '<nowa_nadrzędna_klasa_obiektu>'
<nowy_typ_klasy_obiektu> MAY (atrybut1> $ <atrybut2>
$ <nowy_atrybut3> )
```

## Kopiowanie klasy obiektu

Ten temat zawiera informacje dotyczące kopiowania klasy obiektu.

Jeśli jeszcze tego nie zrobiono, rozwiń kategorię **Schema management** (Zarządzanie schematami) w obszarze nawigacyjnym, a następnie kliknij przycisk **Manage object classes** (Zarządzanie klasami obiektu). Aby skopiować klasę obiektu:

1. Zaznacz przełącznik znajdujący się obok klasy obiektu, którą chcesz skopiować.
2. Kliknij przycisk **Copy** (Kopiuuj).
3. Wybierz zakładkę:
  - Na karcie **General** (Ogólne):
    - Zmień wartość pola **Object class name** (Nazwa klasy obiektu). Nazwą domyślną jest nazwa kopiowanej klasy obiektu z dodanym słowem COPY. Na przykład **tempPerson** jest kopiowana jako **tempPersonCOPY**.
    - Zmień opis (**Description**).
    - Zmień **OID**. Domyślnym OID jest OID kopiowanej klasy obiektu z dodanym słowem COPY. Na przykład **tempPerson-oid** jest kopiowany jako **tempPerson-oidCOPY**.
    - Zmień nadrzędną klasę obiektu (**Superior object class**). Wybierz pozycję z listy rozwijanej nadrzędnych klas obiektu. Określa ona klasę obiektu, z której dziedziczone są inne atrybuty. Zwykle **Nadrzędną klasą obiektu** jest **top**, jednak może nią być inna klasa obiektu. Na przykład, nadrzędną klasą obiektu dla **tempEmployeeCOPY** może być **ePerson**.

- Zmień **Object class type** (Typ klasy obiektu). Wybierz typ klasy obiektu. Sekcja “Klasy obiektu” na stronie 17 zawiera dodatkowe informacje na temat typów klas obiektu.
- Kliknij zakładkę **Attributes** (Atrybuty), aby zmienić wymagane i opcjonalne atrybuty danej klasy obiektu oraz przejrzeć atrybuty dziedziczone, kliknij przycisk **OK**, aby wprowadzić zmiany w życie, lub kliknij przycisk **Cancel** (Anuluj), aby powrócić do okna **Manage object classes** (Zarządzanie klasami obiektu) bez wprowadzania żadnych zmian.

- W zakładce **Attributes** (Atrybuty):

Wybierz atrybut z alfabetycznej listy **Available attributes** (Dostępne atrybuty) i kliknij przycisk **Add to required** (Dodaj do wymaganych), aby uczynić dany atrybut wymaganym, lub kliknij przycisk **Add to optional** (Dodaj do opcjonalnych), aby uczynić go atrybutem opcjonalnym klasy obiektu. Atrybut zostanie wyświetlony na właściwej liście wybranych atrybutów.

Powtórz te czynności dla wszystkich atrybutów, które chcesz wybrać.

Atrybuty można przenosić pomiędzy listami lub kasować z nich, zaznaczając najpierw wybrany atrybut, a następnie klikając przycisk **Move to** (Przenieś) lub **Delete** (Usuń).

Można przeglądać listy dziedziczonych atrybutów wymaganych i opcjonalnych. Dziedziczone atrybuty są oparte na nadrzędnej klasie obiektu (**Superior object class**) wybranej w zakładce **General** (Ogólne). Atrybutów dziedziczonych nie można zmieniać. Jeśli jednak zmieni się **Nadrzędną klasę obiektu** w zakładce **General** (Ogólne), wyświetlony zostanie inny zestaw atrybutów dziedziczonych.

4. Kliknij przycisk **OK**, aby zmiany wprowadzić w życie, lub kliknij przycisk **Cancel** (Anuluj), aby powrócić do okna **Manage object classes** (Zarządzanie klasami obiektu) bez dokonywania żadnych zmian.

Aby wyświetlić klasy obiektu znajdujące się w schemacie za pomocą wiersza komend, uruchom komendę:

```
ldapsearch -b cn=schema -s base objectclass=* objectclasses
```

Wybierz klasę obiektu, którą chcesz skopiować. Użyj edytora w celu zmiany odpowiednich informacji i zapisz zmiany w pliku <plik>. Wprowadź następującą komendę:

```
ldapmodify -D <nazwa_dn_administratora> -w <hasło_administratora> -i <plik>
```

gdzie <plik> zawiera:

```
dn: cn=schema
changetype: modify
add: objectclasses
objectclasses: ( <moja_nowa_klasa_obiektu-oid> NAME '<moja_nowa_klasa_obiektu>'
DESC '<Nowa klasa obiektu
skopiowana z aplikacji LDAP>'
SUP '<obiekt_klasy_nadrzędnej>'<typ_klasy_obiektu> MAY (atrybut1)
$ <atrybut2> $ <atrybut3> )
```

## Usuwanie klasy obiektu

Ten temat zawiera informacje dotyczące usuwania klasy obiektu.

Nie wszystkie zmiany schematu są dozwolone. Ograniczenia dotyczące zmian zawiera sekcja “Niedozwolone zmiany schematu” na stronie 28.

Jeśli jeszcze tego nie zrobiono, rozwiń kategorię **Schema management** (Zarządzanie schematami) w obszarze nawigacyjnym, a następnie kliknij przycisk **Manage object classes** (Zarządzanie klasami obiektu). Aby usunąć klasę obiektu:

1. Zaznacz przełącznik znajdujący się obok klasy obiektu, którą chcesz usunąć.
2. Kliknij przycisk **Delete** (Usuń).
3. Wyświetlony zostanie monit potwierdzenia usunięcia klasy obiektu. Kliknij przycisk **OK**, aby usunąć klasę obiektu, lub kliknij przycisk **Cancel** (Anuluj), aby powrócić do okna **Manage object classes** (Zarządzanie klasami obiektu) bez dokonywania żadnych zmian.

Wyświetl klasy obiektu znajdujące się w schemacie, uruchamiając komendę:

```
ldapsearch -b cn=schema -s base objectclass=* objectclasses
```

Wybierz klasę obiektu do usunięcia i uruchom poniższą komendę:

```
ldapmodify -D <nazwa_dn_administratora> -w <hasło_administratora> -i <plik>
```

gdzie <plik> zawiera:

```
dn: cn=schema
changetype: modify
delete: objectclasses
objectclasses: (<klasa_obiektu-oid>)
```

## Wyświetlanie atrybutów

Ten temat zawiera informacje dotyczące wyświetlania atrybutów.

Atrybuty w schemacie można przeglądać za pomocą narzędzia Web Administration (zalecane) lub za pomocą wiersza komend.

1. Rozwiń kategorię **Schema management** (Zarządzanie schematami) w obszarze nawigacyjnym i kliknij **Manage attributes** (Zarządzaj atrybutami).

Wyświetlony zostanie panel tylko do odczytu umożliwiający przeglądanie atrybutów w schemacie i ich parametrów. Atrybuty wyświetlane są w porządku alfabetycznym. Poruszanie się pomiędzy stronami możliwe jest poprzez klikanie przycisków Previous (Poprzednia) i Next (Następna). Pole znajdujące się obok tych przycisków określa bieżącą stronę. Zawiera ono także listę rozwijaną, której można użyć w celu bezpośredniego przejścia do wybranej strony. Pierwsza klasa obiektu na stronie wyświetlana jest razem z numerem strony, co pomaga odnaleźć klasę obiektu, którą chce się przeglądać. Na przykład, jeśli szukany jest atrybut **authenticationUserID**, należy rozwinąć menu i przewinąć je w dół do miejsca, w którym widoczna będzie **Strona 3 z 62 applSystemHint** oraz **Strona 4 z 62 authorityRevocatonList**. Ponieważ atrybut authenticationUserID występuje w porządku alfabetycznym pomiędzy atrybutami applSystemHint oraz authorityRevocatonList, należy wybrać stronę 3 i kliknąć przycisk **Go** (Przejdź).

Atrybuty można także wyświetlać posortowane według składni. Wybierz opcję **Syntax** (Składnia) i kliknij przycisk **Sort** (Sortuj). Atrybuty zostaną posortowane alfabetycznie według składni. Listę typów składni zawiera sekcja “Składnia atrybutu” na stronie 24. Podobnie można odwrócić porządek listy, wybierając opcję **Descending** (Malejąco) i klikając przycisk **Sort** (Sortuj).

Po odnalezieniu wybranego atrybutu można wyświetlić jego składnię, sprawdzić, czy jest wielowartościowy i wyświetlić klasę obiektu, do której należy. Rozwiń menu rozwijane klas obiektu, aby zobaczyć listę klas obiektu tego atrybutu.

2. Po zakończeniu kliknij przycisk **Close** (Zamknij), aby powrócić do panelu **Welcome** (Witamy) serwera IBM Directory Server.

Aby wyświetlić atrybuty znajdujące się w schemacie, uruchom komendę:

```
ldapsearch -b cn=schema -s base objectclass=* attributeTypes IBMAttributeTypes
```

## Dodawanie atrybutu

Ten temat zawiera informacje dotyczące dodawania atrybutu.

Użyj jednej z poniższych metod, aby utworzyć nowy atrybut. Narzędzie Web Administration jest metodą zalecaną.

Jeśli jeszcze tego nie zrobiono, rozwiń kategorię **Schema management** (Zarządzanie schematami) w obszarze nawigacyjnym, a następnie kliknij przycisk **Manage attributes** (Zarządzanie atrybutami). Aby utworzyć nowy atrybut:

1. Kliknij przycisk **Add** (Dodaj).

**Uwaga:** Dostęp do tego panelu można również uzyskać, rozwijając kategorię **Schema management** (Zarządzanie schematami) w obszarze nawigacyjnym, a następnie kliknij przycisk **Add an attribute** (Dodaj atrybut).

2. Wpisz **Nazwę atrybutu**, np. **tempId**. Jest to pole wymagane, które musi zaczynać się literą.

3. Wpisz **Description** (Opis) atrybutu, np. **identyfikator przypisany tymczasowo zatrudnionemu**.
4. Wpisz **OID** atrybutu. Jest to wymagane pole. Więcej informacji zawiera temat "Identyfikator obiektu (OID)" na stronie 25. Jeśli brak identyfikatora OID, można użyć nazwy atrybutu z końcówką -oid. Na przykład, jeśli nazwą atrybutu jest **tempID**, to domyślnie OID ma wartość **tempID-oid**. Wartość w tym polu można zmienić.
5. Wybierz z listy rozwijanej opcję **Superior attribute** (Atrybut nadrzędny). Atrybut nadrzędny określa atrybut, z którego dziedziczone są właściwości.
6. Wybierz z listy rozwijanej opcję **Syntax** (Składnia). W sekcji "Składnia atrybutu" na stronie 24 znajduje się więcej informacji na temat składni.
7. Wpisz wartość do pola **Długość atrybutu**, która określa maksymalną długość tego atrybutu. Długość jest wyrażana liczbą bajtów.
8. Zaznacz pole wyboru **Allow multiple values** (Dopuszczalne wiele wartości), aby zezwolić na nadawanie atrybutowi wielu wartości.
9. Wybierz regułę sprawdzania zgodności z każdego z rozwijanych menu dla równości, porządkowania i podłańcucha. Pełną listę reguł sprawdzania zgodności zawiera temat "Reguły sprawdzania zgodności" na stronie 21.
10. Kliknij zakładkę **IBM extensions** (Rozszerzenia IBM), aby określić dodatkowe rozszerzenia atrybutu, kliknij przycisk **OK** aby dodać nowy atrybut lub kliknij przycisk **Cancel** (Anuluj), aby powrócić do ekranu **Manage attributes** (Zarządzanie atrybutami) bez dokonywania żadnych zmian.
11. Na karcie **IBM extensions** (Rozszerzenia IBM):
  - Zmień wartość pola **DB2 table name** (Nazwa tabeli DB2). Jeśli pole to pozostanie puste, serwer wygeneruje nazwę tabeli DB2. Wpisanie nazwy tabeli DB2 powoduje konieczność wpisania także nazwy kolumny DB2.
  - Zmień wartość pola **DB2 column name** (Nazwa kolumny DB2). Jeśli pole to pozostanie puste, serwer wygeneruje nazwę kolumny DB2. Wpisanie nazwy kolumny DB2 powoduje konieczność wpisania także nazwy tabeli DB2.
  - Ustaw **Security class** (Klasę ochrony) poprzez wybranie z listy rozwijanej jednej z wartości: **normal** (normalna), **sensitive** (wrażliwa) lub **critical** (newralgiczna).
  - Ustaw **Indexing rules** (Reguły indeksowania) poprzez wybranie jednej lub wielu reguł indeksowania. Temat "Reguły indeksowania" na stronie 22 zawiera dodatkowe informacje o regułach indeksowania.

**Uwaga:** Zaleca się, aby dla każdego atrybutu, który ma zostać użyty w filtrach wyszukiwania, została określona przynajmniej reguła indeksowania równości.
12. Kliknij przycisk **OK**, aby dodać nowy atrybut, lub kliknij przycisk **Cancel** (Anuluj), aby powrócić do okna **Manage attributes** (Zarządzanie atrybutami) bez dokonywania żadnych zmian.

**Uwaga:** W przypadku kliknięcia przycisku OK na zakładce General (Ogólne) bez uprzedniego dodania żadnych rozszerzeń, można dodać je później poprzez dokonanie edycji nowego atrybutu.

Aby dodać atrybut za pomocą wiersza komend, uruchom następującą komendę. Poniższy przykład dodaje definicję typu atrybutu o nazwie "myAttribute", ze składnią Directory String (patrz "Składnia atrybutu" na stronie 24) i z porównaniem Case Ignore Equality (patrz "Reguły sprawdzania zgodności" na stronie 21). Część definicji specyficzna dla IBM stanowi, że dane atrybutu są przechowywane w kolumnie o nazwie "myAttrColumn" w tabeli o nazwie "myAttrTable". Jeśli nazwy te nie zostały określone, zarówno nazwą kolumny, jak i nazwą tabeli domyślnie będzie "myAttribute". Atrybut jest przypisany do klasy dostępu "normal" (normalna), a wartości mają maksymalną długość 200 bajtów.

```
ldapmodify -D <nazwa_dn_administratora> -w <hasło_administratora> -i schemat.ldif
```

gdzie plik **schemat.ldif** zawiera:

```
dn: cn=schema
changetype: modify
add: attributetypes
attributetypes: ( myAttribute-oid NAME ( 'myAttribute' )
DESC 'Atrybut zdefiniowany dla aplikacji LDAP'
EQUALITY 2.5.13.2 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
```

```
USAGE userApplications )
```

```
-  
add: ibmattributetypes  
ibmattributetypes: ( myAttribute-oid DBNAME ( 'myAttrTable' 'myAttrColumn' )  
ACCESS-CLASS normal LENGTH 200 )
```

## Edytowanie atrybutu

Ten temat zawiera informacje dotyczące edytowania atrybutu.

Nie wszystkie zmiany schematu są dozwolone. Ograniczenia dotyczące zmian zawiera sekcja “Niedozwolone zmiany schematu” na stronie 28.

Dowolną część definicji można zmienić przed dodaniem pozycji korzystających z danego atrybutu. Użyj jednej z poniższych metod, aby przeprowadzić edycję atrybutu. Narzędzie Web Administration jest metodą zalecaną.

Jeśli jeszcze tego nie zrobiono, rozwiń kategorię **Schema management** (Zarządzanie schematami) w obszarze nawigacyjnym, a następnie kliknij przycisk **Manage attributes** (Zarządzanie atrybutami). Aby dokonać edycji atrybutu:

1. Zaznacz przełącznik znajdujący się obok atrybutu, który chcesz zmodyfikować.
2. Kliknij przycisk **Edit** (Edycja).
3. Wybierz zakładkę:
  - Na karcie **General** (Ogólne):
    - Wybierz zakładkę:
      - **General** (Ogólne), aby:
        - Zmienić opis (**Description**).
        - Zmienić składnię (**Syntax**).
        - Ustawić długość atrybutu (**Attribute length**).
        - Zmienić ustawienia wartości wielokrotnej (**Multiple value**).
        - Wybrać regułę sprawdzania zgodności (**Matching rule**).
        - Zmienić atrybut nadrzędny (**Superior attribute**).
      - Kliknij zakładkę **IBM extensions** (Rozszerzenia IBM), aby dokonać edycji rozszerzeń atrybutu. Możesz także kliknąć przycisk **OK**, aby zastosować zmiany, lub kliknąć przycisk **Cancel** (Anuluj), aby powrócić do ekranu **Manage attributes** (Zarządzanie atrybutami) bez dokonywania żadnych zmian.
      - **IBM extensions** (Rozszerzenia IBM), jeśli serwer IBM Directory Server używany jest, aby:
        - Zmienić klasę bezpieczeństwa (**Security class**).
        - Zmienić reguły indeksowania (**Indexing rules**).
    - Kliknij przycisk **OK**, aby zastosować zmiany, lub kliknij przycisk **Cancel** (Anuluj), aby powrócić do okna **Manage attributes** (Zarządzanie atrybutami) bez dokonywania żadnych zmian.
4. Kliknij przycisk **OK**, aby zastosować zmiany, lub kliknij przycisk **Cancel** (Anuluj), aby powrócić do okna **Manage attributes** (Zarządzanie atrybutami) bez dokonywania żadnych zmian.

Aby edytować atrybut za pomocą wiersza komend, uruchom następującą komendę. Ten przykład dodaje indeksowanie do atrybutu, co przyspiesza wyszukiwanie. Użyj komendy `ldapmodify` i pliku LDIF, aby zmienić definicję:

```
ldapmodify -D <nazwa_dn_administratora> -w <hasło_administratora> -i zmieniany_schemat.ldif
```

gdzie plik **zmieniany\_schemat.ldif** zawiera:

```
dn: cn=schema  
changetype: modify  
replace: attributetypes  
attributetypes: ( myAttribute-oid NAME ( 'myAttribute' ) DESC 'Atrybut  
zdefiniowany dla aplikacji LDAP' EQUALITY 2.5.13.2  
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 USAGE userApplications )
```

```
replace: ibmattributetypes
ibmattributetypes: ( myAttribute-oid DBNAME ( 'myAttrTable' 'myAttrColumn' )
                    ACCESS-CLASS normal LENGTH 200 EQUALITY SUBSTR )
```

**Uwaga:** Obie części definicji (**attributetypes** i **ibmattributetypes**) muszą być dołączone do operacji zastąpienia, nawet jeśli tylko część **ibmattributetypes** jest zmieniana. Jedyną zmianą jest dodanie "EQUALITY SUBSTR" na końcu definicji w celu uzyskania indeksów służących do określania równości i porównywania podłańcuchów.

## Kopiowanie atrybutu

Ten temat zawiera informacje dotyczące kopiowania atrybutu.

Użyj jednej z poniższych metod, aby skopiować atrybut. Narzędzie Web Administration jest metodą zalecaną.

Jeśli jeszcze tego nie zrobiono, rozwiń kategorię **Schema management** (Zarządzanie schematami) w obszarze nawigacyjnym, a następnie kliknij przycisk **Manage attributes** (Zarządzanie atrybutami). Aby skopiować atrybut:

1. Zaznacz przełącznik znajdujący się obok atrybutu, który chcesz skopiować.
2. Kliknij przycisk **Copy** (Kopiuje).
3. Zmień wartość pola **Attribute name** (Nazwa atrybutu). Nazwą domyślną jest nazwa kopiowanej nazwy atrybutu z dodanym słowem COPY. Na przykład **tempID** jest kopiowana jako **tempIDCOPY**.
4. Zmień **Description** (Opis) atrybutu, na przykład **Numer ID przypisany tymczasowo zatrudnionemu**.
5. Zmień **OID**. Domyślnym OID jest OID kopiowanego atrybutu z dodanym słowem COPYOID. Na przykład **tempID-oid** jest kopiowany jako **tempID-oidCOPYOID**.
6. Wybierz z listy rozwijanej opcję **Superior attribute** (Atrybut nadrzędny). Atrybut nadrzędny określa atrybut, z którego dziedziczone są właściwości.
7. Wybierz z listy rozwijanej opcję **Syntax** (Składnia). W sekcji "Składnia atrybutu" na stronie 24 znajduje się więcej informacji na temat składni.
8. Wpisz wartość do pola **Długość atrybutu**, która określa maksymalną długość tego atrybutu. Długość jest wyrażana liczbą bajtów.
9. Zaznacz pole wyboru **Allow multiple values** (Dopuszczalne wiele wartości), aby zezwolić na nadawanie atrybutowi wielu wartości.
10. Wybierz regułę sprawdzania zgodności z każdego z rozwijanych menu dla równości, porządkowania i podłańcucha. Pełną listę reguł sprawdzania zgodności zawiera temat "Reguły sprawdzania zgodności" na stronie 21.
11. Kliknij zakładkę **IBM extensions** (Rozszerzenia IBM), aby zmodyfikować dodatkowe rozszerzenia atrybutu, kliknij przycisk **OK** aby zastosować zmiany lub kliknij przycisk **Cancel** (Anuluj), aby powrócić do ekranu **Manage attributes** (Zarządzanie atrybutami) bez dokonywania żadnych zmian.
12. Na karcie **IBM extensions** (Rozszerzenia IBM):
  - Zmień wartość pola **DB2 table name** (Nazwa tabeli DB2). Jeśli pole to pozostanie puste, serwer wygeneruje nazwę tabeli DB2. Wpisanie nazwy tabeli DB2 powoduje konieczność wpisania także nazwy kolumny DB2.
  - Zmień wartość pola **DB2 column name** (Nazwa kolumny DB2). Jeśli pole to pozostanie puste, serwer wygeneruje nazwę kolumny DB2. Wpisanie nazwy kolumny DB2 powoduje konieczność wpisania także nazwy tabeli DB2.
  - Zmień wartość pola **Security class** (Klasa ochrony) poprzez wybranie z listy rozwijanej jednej z wartości: **normal** (normalna), **sensitive** (wrażliwa) lub **critical** (newralgiczna).
  - Zmodyfikuj **Indexing rules** (Reguły indeksowania) poprzez wybranie jednej lub wielu reguł indeksowania. Temat "Reguły indeksowania" na stronie 22 zawiera dodatkowe informacje o regułach indeksowania.

**Uwaga:** Zaleca się, aby dla każdego atrybutu, który ma zostać użyty w filtrach wyszukiwania, została określona przynajmniej reguła indeksowania równości.

13. Kliknij przycisk **OK**, aby zastosować zmiany, lub kliknij przycisk **Cancel** (Anuluj), aby powrócić do okna **Manage attributes** (Zarządzanie atrybutami) bez dokonywania żadnych zmian.

**Uwaga:** W przypadku kliknięcia przycisku **OK** na zakładce **General** (Ogólne) bez uprzedniego dodania żadnych rozszerzeń, można je dodać lub zmienić później poprzez dokonanie edycji nowego atrybutu.

Aby wyświetlić atrybuty znajdujące się w schemacie, uruchom komendę:

```
ldapsearch -b cn=schema -s base objectclass=* attributeTypes IBMAttributeTypes
```

Wybierz atrybut, który chcesz skopiować. Użyj edytora w celu zmiany odpowiednich informacji i zapisz zmiany w pliku *<plik>*. Następnie uruchom następującą komendę:

```
ldapmodify -D <nazwa_dn_administratora> -w <hasło_administratora> -i <plik>
```

gdzie *<plik>* zawiera:

```
dn: cn=schema
changetype: modify
add: attributetypes
attributetypes: ( <nowy_atrybut-oid> NAME '<nowy_atrybut>' DESC '<Nowy
                atrybut skopiowany dla aplikacji LDAP > EQUALITY 2.5.13.2
                SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 USAGE userApplications )
-
add: ibmattributetypes
ibmattributetypes: ( myAttribute-oid DBNAME ( 'myAttrTable' 'myAttrColumn' )
                    ACCESS-CLASS normal LENGTH 200 )
```

## Usuwanie atrybutu

Ten temat zawiera informacje dotyczące usuwania atrybutu z drzewa katalogów.

Nie wszystkie zmiany schematu są dozwolone. Ograniczenia dotyczące zmian zawiera sekcja “Niedozwolone zmiany schematu” na stronie 28.

Użyj jednej z poniższych metod, aby usunąć atrybut. Narzędzie Web Administration jest metodą zalecaną.

Jeśli jeszcze tego nie zrobiono, rozwiń kategorię **Schema management** (Zarządzanie schematami) w obszarze nawigacyjnym, a następnie kliknij przycisk **Manage attributes** (Zarządzanie atrybutami). Aby usunąć atrybut:

1. Zaznacz przełącznik znajdujący się obok atrybutu, który chcesz usunąć.
2. Kliknij przycisk **Delete** (Usuń).
3. Wyświetlony zostanie monit potwierdzenia usunięcia atrybutu. Kliknij przycisk **OK**, aby usunąć atrybut, lub kliknij przycisk **Cancel** (Anuluj), aby powrócić do okna **Manage attributes** (Zarządzanie atrybutami) bez dokonywania żadnych zmian.

Aby usunąć atrybut za pomocą wiersza komend, uruchom następującą komendę:

```
ldapmodify -D <nazwa_dn_administratora> -w <hasło_administratora> -i schemat_do_usunięcia.ldif
```

gdzie plik **schemat\_do\_usunięcia.ldif** zawiera:

```
dn: cn=schema
changetype: modify
delete: attributetypes
attributetypes: (<atrybut-oid>)
```

## Kopiowanie schematu na inne serwery

Ten temat zawiera informacje dotyczące kopiowania schematu na inne serwery.

Aby skopiować schemat na inne serwery:

1. Użyj programu narzędziowego ldapsearch, aby skopiować schemat do pliku:  

```
ldapsearch -b cn=schema -L "(objectclass=*)" > schemat.ldif
```
2. Plik schematu będzie zawierał wszystkie klasy obiektu i atrybuty. Można przeprowadzić edycję pliku LDIF, tak aby zawierał tylko wybrane elementy schematu, lub przefiltrować dane wyjściowe komendy ldapsearch za pomocą takiego narzędzia, jak grep. Atrybuty należy umieszczać przed klasami obiektu, które się do nich odwołują. Na



przykład można uzyskać następujący plik (należy zauważyć, że każdy kontynuowany wiersz ma jedną spację na końcu, a wiersz kontynuacji ma przynajmniej jedną spację na początku).

```
attributetypes: ( myattr1-oid NAME 'myattr1' DESC 'Część
informacji.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 EQUALITY 2.5.13.2
USAGE userApplications )
IBMAttributetypes: ( myattr1-oid DBNAME( 'myattr1' 'myattr1' )
ACCESS-CLASS normal LENGTH 500 )
attributetypes: ( myattr2-oid NAME 'myattr2' DESC 'Część
informacji.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 EQUALITY 2.5.13.2
USAGE userApplications )
IBMAttributetypes: ( myattr2-oid DBNAME( 'myattr2' 'myattr2' )
ACCESS-CLASS normal LENGTH 500 )
objectclasses: ( myobject-oid NAME 'myobject' DESC 'Przedstawia
dowolne dane.' SUP 'top' STRUCTURAL MUST ( cn ) MAY ( myattr1 $ myattr2 ) )
```

3. Wstaw wiersz przed każdym wierszem klasy obiektu lub typem atrybutu, aby utworzyć dyrektywy LDIF w celu dodania tych wartości do pozycji cn=schema. Każda klasa obiektu i atrybut muszą być dodane jako pojedyncze modyfikacje.

```
dn: cn=schema
changetype: modify
add: attributetypes ibmattributetypes
attributetypes: ( myattr1-oid NAME 'myattr1' DESC 'Część
informacji.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 EQUALITY 2.5.13.2
USAGE userApplications )
IBMAttributetypes: ( myattr1-oid DBNAME( 'myattr1' 'myattr1' )
ACCESS-CLASS normal LENGTH 500 )

dn: cn=schema
changetype: modify
add: attributetypes ibmattributetypes
attributetypes: ( myattr2-oid NAME 'myattr2' DESC 'Część
informacji.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 EQUALITY 2.5.13.2
USAGE userApplications )
IBMAttributetypes: ( myattr2-oid DBNAME( 'myattr2' 'myattr2' )
ACCESS-CLASS normal LENGTH 500 )

dn: cn=schema
changetype: modify
add: objectclasses
objectclasses: ( myobject-oid NAME 'myobject' DESC 'Przedstawia
dowolne dane.' SUP 'top' STRUCTURAL MUST ( cn ) MAY ( myattr1 $ myattr2 ) )
```

4. Załaduj ten schemat na innych serwerach używających narzędzia ldapmodify:

```
ldapmodify -D cn=administrator -w <hasło> -f schemat.ldif
```

## Zadania związane z pozycjami katalogu

Ten temat zawiera informacje dotyczące zarządzania pozycjami katalogu.

Aby zarządzać pozycjami katalogu, rozwiń kategorię **Directory management** (Zarządzanie katalogiem) w obszarze nawigacji narzędzia Web Administration.

### Pojęcia pokrewne

“Przyrostek (kontekst nazwy)” na stronie 12

Przyrostek (znany również jako kontekst nazwy) to nazwa DN identyfikująca najwyższą pozycję w lokalnej hierarchii katalogu.

“Schemat” na stronie 14

Schemat jest zestawem reguł określających sposób przechowywania danych w katalogu. Schemat definiuje typ dozwolonych pozycji oraz strukturę i składnię atrybutów.

“Prawa własności do obiektów w katalogach LDAP” na stronie 76

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.

## Przeglądanie drzewa katalogów

Ten temat zawiera informacje dotyczące przeglądania drzewa katalogów.

Należy najpierw wykonać następujące czynności.

Przed rozpoczęciem należy wszystko przygotować dokładnie z opisem.

1. Jeśli jeszcze tego nie zrobiono, rozwiń kategorię **Directory management** (Zarządzanie katalogami) w obszarze nawigacyjnym.
2. Kliknij **Manage entries** (Zarządzaj pozycjami).

W celu wybrania pozycji, z którą chce się pracować, można rozwijać różne poddrzewa drzewa katalogu. Z paska narzędzi znajdującego się po prawej stronie można wybrać operację, która ma zostać wykonana.

## Dodawanie pozycji

Ten temat zawiera informacje dotyczące dodawania pozycji do drzewa katalogów.

1. Jeśli jeszcze tego nie zrobiono, rozwiń kategorię **Directory management** (Zarządzanie katalogami) w obszarze nawigacyjnym.
2. Kliknij przycisk **Add an entry** (Dodaj pozycję).
3. Wybierz z listy rozwijanej opcję **Structural object class** (Strukturalna klasa obiektu).
4. Kliknij przycisk **Next** (Dalej).
5. Wybierz w polu Available (Dostępne) dowolne pomocnicze klasy obiektu (**Auxiliary object classes**), których chcesz używać, i kliknij przycisk **Add** (Dodaj). Powtórz te czynności dla każdej pomocniczej klasy obiektu, którą chcesz dodać. Można także skasować pomocnicze klasy obiektu z okna Selected (Wybrane) poprzez zaznaczenie ich i kliknięcie przycisku **Remove** (Usuń).
6. Kliknij przycisk **Next** (Dalej).
7. W polu **Relative DN** (Względna nazwa DN) wpisz względną nazwę wyróżniającą (RDN) pozycji, którą dodajesz, np. cn=Jan Kowalski.
8. W polu **Parent DN** (Nadrzędna nazwa DN) wpisz nazwę wyróżniającą wybranej pozycji drzewa, np. ou=Austin, o=IBM. Możesz także kliknąć przycisk **Browse** (Przeglądaj), aby wybrać z nadrzędną nazwą DN z listy. Wybraną pozycję można rozwinąć w celu przejrzania opcji znajdujących się niżej w poddrzewie. Zaznacz opcję i kliknij przycisk **Select** (Wybierz), aby określić żadaną nadrzędną nazwę DN. Domyślną nadrzędną nazwą wyróżniającą (**Parent DN**) jest pozycja wybrana w drzewie.

**Uwaga:** Jeśli wykonywanie tego zadania zostało rozpoczęte na panelu **Manage entries** (Zarządzanie pozycjami), pole to jest już wypełnione.

9. Na karcie **Required attributes** (Atrybuty wymagane) wpisz wartości atrybutów wymaganych. Jeśli chcesz wpisać więcej niż jedną wartość określonego atrybutu, kliknij przycisk **Multiple values** (Wartości wielokrotne), a następnie dodaj wszystkie wartości, po jednej w wierszu.
10. Kliknij zakładkę **Optional attributes** (Atrybuty opcjonalne).
11. Na karcie **Optional attributes** (Atrybuty opcjonalne) wpisz odpowiednie wartości atrybutów opcjonalnych. Sekcja “Zmiana atrybutów binarnych” na stronie 202 zawiera informacje na temat dodawania wartości binarnych. Jeśli chcesz wpisać więcej niż jedną wartość określonego atrybutu, kliknij przycisk **Multiple values** (Wartości wielokrotne), a następnie dodaj wszystkie wartości, po jednej w wierszu.
12. Kliknij przycisk OK, aby utworzyć pozycję.
13. Kliknij przycisk **ACL**, aby zmodyfikować listę ACL dla danej pozycji. Sekcja “Listy kontroli dostępu” na stronie 64 zawiera informacje na temat list ACL.

14. Po wypełnieniu przynajmniej wymaganych pól kliknij przycisk **Add** (Dodaj), aby dodać nową pozycję, lub kliknij przycisk **Cancel** (Anuluj), aby powrócić do **Browse tree** (Przeglądaj drzewo) bez wprowadzania zmian w katalogu.

## Dodawanie pozycji zawierającej atrybuty ze znacznikami języka

Ten temat zawiera informacje dotyczące tworzenia pozycji zawierającej atrybuty ze znacznikami języka.

Aby utworzyć pozycję zawierającą atrybuty ze znacznikami języka:

1. Włącz znaczniki języka. Więcej informacji zawiera temat “Włączanie znaczników języka” na stronie 126.
2. Rozwiń kategorię **Directory management** (Zarządzanie katalogiem) w obszarze nawigacyjnym i kliknij **Manage entries** (Zarządzaj kolejkami).
3. Kliknij przycisk **Edit attributes** (Edytuj atrybuty).
4. Wybierz atrybut, dla którego ma zostać utworzony znacznik języka.
5. Kliknij przycisk **Language tag value** (Wartość znacznika języka), aby otworzyć panel **Language tag values** (Wartości znaczników języka).
6. W polu **Language tag** (Znacznik języka) wpisz nazwę tworzonego znacznika. Znacznik musi być poprzedzony przyrostkiem lang-.
7. W polu **Value** (Wartość) wprowadź wartość znacznika.
8. Kliknij przycisk **Add** (Dodaj). Znacznik języka i jego wartość są wyświetlone na liście menu.
9. Utwórz dodatkowe znaczniki języka lub zmień istniejące znaczniki języka dla atrybutu, powtarzając punkty 4, 5 i 6. Po utworzeniu żądanych znaczników języka kliknij przycisk **OK**.
10. Rozwiń menu **Display with language tag** (Wyświetl ze znacznikami języka) i wybierz dany znacznik. Kliknij przycisk **Change view** (Zmień widok), aby wyświetlić wartości atrybutu wpisane dla danego znacznika języka. Wartości dodawane lub edytowane na tym ekranie mają zastosowanie jedynie do wybranego znacznika języka.
11. Po zakończeniu kliknij przycisk **OK**.

### Odsyłacze pokrewne

“Znaczniki języka” na stronie 49

Termin *znaczniki języka* oznacza mechanizm, dzięki któremu serwer Directory Server może przypisać kody języka naturalnego wartościom przechowywanym w katalogu. Pozwalają one wprowadzać klientom zapytania o wartości w katalogu spełniające określone wymagania języka naturalnego.

## Usuwanie pozycji

Ten temat zawiera informacje dotyczące usuwania pozycji z drzewa katalogów.

1. Jeśli jeszcze tego nie zrobiono, rozwiń kategorię **Directory management** (Zarządzanie katalogami) w obszarze nawigacyjnym, a następnie kliknij przycisk **Manage entries** (Zarządzanie pozycjami). W celu wybrania pozycji, przyrostka lub poddrzewa, z którym chce się pracować, można rozwijać różne poddrzewa drzewa katalogu. Kliknij przycisk **Delete** (Usuń) znajdujący się na pasku narzędzi umieszczonym po prawej stronie.
2. Zostanie wyświetlony monit o potwierdzenie kasowania pozycji. Kliknij przycisk **OK**. Pozycja zostanie usunięta z katalogu i ponownie zostanie wyświetlona lista pozycji.

## Edytowanie pozycji

Ten temat zawiera informacje dotyczące edytowania pozycji w drzewie katalogów.

1. Jeśli jeszcze tego nie zrobiono, rozwiń kategorię **Directory management** (Zarządzanie katalogami) w obszarze nawigacyjnym, a następnie kliknij przycisk **Manage entries** (Zarządzanie pozycjami). W celu wybrania pozycji, z którą chce się pracować, można rozwijać różne poddrzewa drzewa katalogu. Kliknij przycisk **Edit attributes** (Edycja atrybutów) znajdujący się na pasku narzędzi umieszczonym po prawej stronie.
2. Na karcie **Required attributes** (Atrybuty wymagane) wpisz wartości atrybutów wymaganych. Sekcja “Zmiana atrybutów binarnych” na stronie 202 zawiera informacje na temat dodawania wartości binarnych. Jeśli chcesz wpisać więcej niż jedną wartość określonego atrybutu, kliknij przycisk **Multiple values** (Wartości wielokrotne), a następnie dodaj wszystkie wartości, po jednej w wierszu.
3. Kliknij zakładkę **Optional attributes** (Atrybuty opcjonalne).

4. Na karcie **Optional attributes** (Atrybuty opcjonalne) wpisz odpowiednie wartości atrybutów opcjonalnych. Jeśli chcesz wpisać więcej niż jedną wartość określonego atrybutu, kliknij przycisk **Multiple values** (Wartości wielokrotne), a następnie dodaj wszystkie wartości, po jednej w wierszu.
5. Kliknij zakładkę **Memberships** (Przynależność do grup).
6. Jeśli utworzono grupy, to na karcie **Memberships** (Przynależność do grup):
  - Wybierz grupę z listy **Available groups** (Dostępne grupy) i kliknij przycisk **Add** (Dodaj), aby przypisać pozycję do wybranej grupy statycznej (**Static group membership**).
  - Wybierz grupę z listy **Static group memberships** (Członkostwo w grupach statycznych) i kliknij przycisk **Remove** (Usuń), aby usunąć pozycję z wybranej grupy.
7. Jeśli jest to pozycja grupowa, dostępna będzie zakładka **Members** (Elementy). Zakładka **Members** (Elementy) zawiera elementy wybranej grupy. Elementy można dodawać do grupy oraz ich z niej usuwać.
  - Aby dodać element do grupy:
    - a. Kliknij opcję **Multiple values** (Wiele wartości) obok zakładki **Members** (Elementy) lub na zakładce **Members** (Elementy) kliknij opcję **Members** (Elementy).
    - b. W polu Member (Element) wprowadź wprowadź nazwę wyróżniającą pozycji, którą chcesz dodać.
    - c. Kliknij przycisk **Add** (Dodaj).
    - d. Kliknij przycisk **OK**.
  - Aby usunąć element z grupy:
    - a. Kliknij opcję **Multiple values** (Wiele wartości) obok zakładki **Members** (Elementy) lub na zakładce **Members** (Elementy) kliknij opcję **Members** (Elementy).
    - b. Wybierz pozycję do usunięcia.
    - c. Kliknij przycisk **Remove** (Usuń).
    - d. Kliknij przycisk **OK**.
  - Aby odświeżyć listę elementów, kliknij przycisk **Update** (Aktualizuj).
8. Kliknij przycisk **OK**, aby zmodyfikować pozycję.

## Kopiowanie pozycji

Ten temat zawiera informacje dotyczące kopiowania pozycji w drzewie katalogów.

Funkcja ta jest przydatna podczas tworzenia podobnych pozycji. Kopia dziedziczy wszystkie atrybuty oryginału. Trzeba tylko zmienić nazwę nowej pozycji.

1. Jeśli jeszcze tego nie zrobiono, rozwiń kategorię **Directory management** (Zarządzanie katalogami) w obszarze nawigacyjnym, a następnie kliknij przycisk **Manage entries** (Zarządzanie pozycjami). Aby wybrać pozycję, z którą chcesz pracować, na przykład Jan Kowalski, możesz rozwijać różne poddrzewa. Kliknij przycisk **Copy** (Kopiuj) znajdujący się na pasku narzędzi umieszczonym po prawej stronie.
2. Zmień pozycję RDN w polu DN (Nazwa wyróżniająca). Na przykład zmień cn=Jan Kowalski na cn=Tomasz Nowak.
3. Na zakładce wymaganych atrybutów zmień pozycję cn na nową nazwę RDN. W tym przykładzie jest to Tomasz Nowak.
4. Zmień odpowiednie inne wymagane atrybuty. W tym przykładzie zmień atrybut z Kowalski na Nowak.
5. Po zakończeniu wprowadzania niezbędnych zmian kliknij przycisk **OK**, aby utworzyć nową pozycję. Nowa pozycja Tomasz Nowak zostanie dodana na końcu listy pozycji.

**Uwaga:** Ta procedura kopiuje tylko atrybuty pozycji. Przypisania pierwotnej pozycji do grupy nie są kopiowane do nowej pozycji. Użyj funkcji edycji atrybutów, aby dodać przypisania.

## Edytowanie list kontroli dostępu

Ten temat zawiera informacje dotyczące zarządzania listami kontroli dostępu.

Aby wyświetlić właściwości list ACL za pomocą narzędzia Web Administration lub pracować z listami ACL, należy zapoznać się z tematem “Zadania związane z listami kontroli dostępu” na stronie 214.

## Pojęcia pokrewne

“Listy kontroli dostępu” na stronie 64

Listy kontroli dostępu (ACL) stanowią ochronę informacji zapisanych w katalogu LDAP. Za pomocą list ACL administratorzy ograniczają dostęp do różnych części katalogu lub konkretnych jego pozycji.

## Dodawanie pomocniczej klasy obiektu

Ten temat zawiera informacje dotyczące dodawania pomocniczej klasy obiektu.

Przycisk **Add auxiliary class** (Dodaj klasę pomocniczą) na pasku narzędzi umożliwia dodanie pomocniczej klasy obiektu do istniejącej pozycji w drzewie katalogów. Pomocnicza klasa obiektu udostępnia dodatkowe atrybuty pozycji, do której jest dodawana.

Jeśli jeszcze tego nie zrobiono, rozwiń kategorię **Directory management** (Zarządzanie katalogami) w obszarze nawigacyjnym, a następnie kliknij przycisk **Manage entries** (Zarządzanie pozycjami). Aby wybrać pozycję, z którą chcesz pracować, na przykład Jan Kowalski, możesz rozwijać różne poddrzewa. Kliknij przycisk **Add auxiliary class** (Dodaj klasę pomocniczą) znajdujący się na pasku narzędzi umieszczonym po prawej stronie.

1. Wybierz w polu Available (Dostępne) dowolne pomocnicze klasy obiektu (**Auxiliary object classes**), których chcesz używać, i kliknij przycisk **Add** (Dodaj). Powtórz te czynności dla każdej pomocniczej klasy obiektu, którą chcesz dodać. Można także skasować pomocnicze klasy obiektu z okna Selected (Wybrane) poprzez zaznaczenie ich i kliknięcie przycisku **Remove** (Usuń).
2. Na karcie **Required attributes** (Atrybuty wymagane) wpisz wartości atrybutów wymaganych. Jeśli chcesz wpisać więcej niż jedną wartość określonego atrybutu, kliknij przycisk **Multiple values** (Wartości wielokrotne), a następnie dodaj wszystkie wartości, po jednej w wierszu.
3. Kliknij zakładkę **Optional attributes** (Atrybuty opcjonalne).
4. Na karcie **Optional attributes** (Atrybuty opcjonalne) wpisz odpowiednie wartości atrybutów opcjonalnych. Jeśli chcesz wpisać więcej niż jedną wartość określonego atrybutu, kliknij przycisk **Multiple values** (Wartości wielokrotne), a następnie dodaj wszystkie wartości, po jednej w wierszu.
5. Kliknij zakładkę **Memberships** (Przynależność do grup).
6. Jeśli utworzono grupy, to na karcie **Memberships** (Przynależność do grup):
  - Wybierz grupę z listy **Available groups** (Dostępne grupy) i kliknij przycisk **Add** (Dodaj), aby przypisać pozycję do wybranej grupy statycznej (**Static group membership**).
  - Wybierz grupę z listy **Static group memberships** (Członkostwo w grupach statycznych) i kliknij przycisk **Remove** (Usuń), aby usunąć pozycję z wybranej grupy.
7. Kliknij przycisk **OK**, aby zmodyfikować pozycję.

## Usuwanie klasy pomocniczej

Ten temat zawiera informacje dotyczące usuwania klasy pomocniczej.

Mimo iż klasę pomocniczą można usunąć w ramach procedury dodawania pomocniczej klasy, łatwiej jest użyć funkcji usuwania klasy pomocniczej, jeśli z pozycji ma zostać usunięta pojedyncza klasa pomocnicza. Jeśli jednak użytkownik chce usunąć z pozycji wiele klas pomocniczych, wygodniejsze może być użycie procedury dodawania klasy pomocniczej.

1. Jeśli jeszcze tego nie zrobiono, rozwiń kategorię **Directory management** (Zarządzanie katalogami) w obszarze nawigacyjnym, a następnie kliknij przycisk **Manage entries** (Zarządzanie pozycjami). Aby wybrać pozycję, z którą chcesz pracować, na przykład Jan Kowalski, możesz rozwijać różne poddrzewa. Kliknij przycisk **Delete auxiliary class** (Usuń klasę pomocniczą) znajdujący się na pasku narzędzi umieszczonym po prawej stronie.
2. Z listy klas pomocniczych wybierz tę, którą chcesz usunąć, i naciśnij przycisk **OK**.
3. Po wyświetleniu żądania potwierdzenia usunięcia kliknij przycisk **OK**.
4. Klasa pomocnicza zostanie usunięta z drzewa i ponownie zostanie wyświetlona lista pozycji.

Powtórz te czynności dla każdej klasy pomocniczej, którą chcesz usunąć.

## Zmiana członkostwa w grupie

Ten temat zawiera informacje dotyczące dokonywania zmian członkostwa w grupie.

Jeśli jeszcze tego nie zrobiono, rozwiń kategorię **Directory management** (Zarządzanie katalogami) w obszarze nawigacyjnym.

1. Kliknij **Manage entries** (Zarządzaj pozycjami).
2. Wybierz użytkownika z drzewa katalogów i kliknij ikonę **Edit attributes** (Edycja atrybutów) na pasku narzędzi.
3. Kliknij zakładkę **Memberships** (Przynależność do grup).
4. Zmień przypisanie użytkownika do grupy. Panel **Change memberships** (Zmiana przypisania) zawiera **Available groups** (Dostępne grupy), do których można dodać użytkownika, jak również **Static Group Memberships** (Przypisania do grup statycznych) pozycji.
  - Wybierz grupę z listy **Available groups** (Dostępne grupy) i kliknij przycisk **Add** (Dodaj), aby przypisać pozycję do wybranej grupy.
  - Wybierz grupę z listy **Static Group Memberships** (Członkostwo w grupach statycznych) i kliknij przycisk **Remove** (Usuń), aby usunąć pozycję z wybranej grupy.
5. Kliknij przycisk **OK**, aby zapisać zmiany, lub kliknij przycisk **Cancel** (Anuluj), aby powrócić do poprzedniego panelu bez zapisywania zmian.

## Wyszukiwanie pozycji w katalogu

Ten temat zawiera informacje dotyczące wyszukiwania pozycji w katalogu.

Istnieją trzy możliwości wyszukiwania w drzewie katalogów:

- Proste wyszukiwanie przy użyciu wcześniej zdefiniowanego zestawu kryteriów wyszukiwania.
- Zaawansowane wyszukiwanie przy użyciu zdefiniowanego przez użytkownika zestawu kryteriów wyszukiwania.
- Wyszukiwanie ręczne.

Opcje wyszukiwania są dostępne po rozwinięciu kategorii **Directory management** (Zarządzanie katalogiem) w obszarze nawigacji i kliknięciu przycisku **Find entries** (Znajdź pozycje). Należy wybrać zakładkę **Search filters** (Filtry wyszukiwania) lub **Options** (Opcje).

**Uwaga:** Pozycje binarne, na przykład hasła, nie podlegają wyszukiwaniu.

Proste wyszukiwanie używa domyślnych kryteriów wyszukiwania:

- Podstawowa nazwa wyróżniająca to **Wszystkie przyrostki**
- Zasięgiem wyszukiwania jest **Poddrzewo**
- Wielkość wyszukiwania jest **Nieograniczona**
- Limit czasu jest **Nieograniczony**
- Wyłuskiwanie aliasów nie jest przeprowadzane **nigdy**
- Podążanie za odwołaniami jest wyłączone

Zaawansowane wyszukiwanie umożliwia określenie ograniczeń wyszukiwania i użycie filtrów wyszukiwania. Aby zastosować kryteria domyślne, użyj prostego wyszukiwania.

1. Aby przeprowadzić proste wyszukiwanie:
  - a. W zakładce **Search filter** (Filtr wyszukiwania) kliknij opcję **Simple search** (Proste wyszukiwanie).
  - b. Wybierz klasę obiektu z listy rozwijanej.
  - c. Wybierz konkretny atrybut wybranego typu pozycji. W przypadku wyszukiwania konkretnego atrybutu wybierz atrybut z listy rozwijanej i wpisz jego wartość w polu **Is equal to** (Jest równy). Jeśli nie zostanie podany atrybut, operacja wyszukiwania zwraca wszystkie pozycje katalogu dla wybranego typu pozycji.
2. Aby przeprowadzić zaawansowane wyszukiwanie:

- a. W zakładce **Search filter** (Filtr wyszukiwania) kliknij opcję **Advanced search** (Zaawansowane wyszukiwanie).
  - b. Wybierz z listy rozwijanej **Atrybut**.
  - c. Wybierz operator **porównania**.
  - d. Wpisz **Wartość** do porównania.
  - e. W przypadku złożonych zapytań skorzystaj z przycisków operatorów wyszukiwania.
    - Jeśli podano już przynajmniej jeden filtr wyszukiwania, określ dodatkowe kryterium i kliknij przycisk **AND** (ORAZ). Komenda **AND** zwraca pozycje zgodne z oboma zestawami kryteriów wyszukiwania.
    - Jeśli podano już przynajmniej jeden filtr wyszukiwania, określ dodatkowe kryterium i kliknij przycisk **OR** (LUB). Komenda **OR** zwraca pozycje zgodne z dowolnym zestawem kryteriów wyszukiwania.
    - Kliknij przycisk **Add** (Dodaj), aby dodać kryterium filtru wyszukiwania do zaawansowanego wyszukiwania.
    - Kliknij przycisk **Delete** (Usuń), aby usunąć kryterium filtru wyszukiwania z zaawansowanego wyszukiwania.
    - Kliknij przycisk **Reset** (Resetuj), aby skasować wszystkie filtry wyszukiwania.
3. Aby przeprowadzić wyszukiwanie ręczne, utwórz filtr wyszukiwania.

Na przykład, aby wyszukiwać nazwiska, wpisz w tym polu `sn=*`. Jeśli wyszukiwanie odbywa się na podstawie wielu atrybutów, należy użyć składni filtru wyszukiwania. Na przykład, aby wyszukać nazwiska z konkretnego departamentu, wprowadź:

```
(&(sn=*)(dept=<nazwa_działu>))
```

W zakładce **Options** (Opcje):

- **Search base DN** (Bazowa nazwa wyróżniająca wyszukiwania) - wybierz z listy rozwijanej przyrostek, w ramach którego przeprowadzane będzie wyszukiwanie.

**Uwaga:** Jeśli wykonywanie tego zadania zostało rozpoczęte na panelu **Manage entries** (Zarządzanie pozycjami), pole to jest już wypełnione. Opcję **Parent DN** (Nadrzędna nazwa DN) wybrano przed kliknięciem przycisku **Add** (Dodaj) w celu rozpoczęcia procesu dodawania pozycji.

Można także wybrać opcję **All suffixes** (Wszystkie przyrostki), aby przeszukiwać całe drzewo.

**Uwaga:** Wyszukiwanie w poddrzewie z aktywną opcją **All suffixes** (Wszystkie przyrostki) nie zwraca informacji o schematach lub protokole zmian, nie zwraca też niczego z systemowego mechanizmu rzutowania.

- **Zasięg wyszukiwania**
  - Wybierz opcję **Object** (Obiekt), aby przeprowadzić wyszukiwanie tylko w ramach wybranego obiektu.
  - Wybierz opcję **Single level** (Jeden poziom), aby przeprowadzić wyszukiwanie w ramach bezpośrednich obiektów potomnych wybranej pozycji.
  - Wybierz opcję **Subtree** (Poddrzewo), aby przeprowadzić wyszukiwanie w ramach wszystkich obiektów potomnych wybranej pozycji.
- **Search size limit** (Limit wielkości wyszukiwania) - wpisz maksymalną liczbę wyszukanych pozycji lub wybierz opcję **Unlimited** (Nieograniczona).
- **Search time limit** (Limit czasu wyszukiwania) - wpisz maksymalny czas wyszukiwania w sekundach lub wybierz opcję **Unlimited** (Nieograniczony).
- Z listy rozwijanej wybierz typ **Alias dereferencing** (Wyłuskiwania aliasów).
  - **Never** (Nigdy) - jeśli wybrana pozycja jest aliasem, nie jest wyłuskiwana do wyszukiwania, tzn. wyszukiwanie ignoruje odniesienie do tego aliasu.
  - **Finding** (Znajdując) - jeśli wybrana pozycja jest aliasem, wyszukiwanie wyłuskuje ten alias i kontynuuje działanie od miejsca jego położenia.
  - **Searching** (Wyszukując) - wybrana pozycja nie jest wyłuskiwana, ale są wyłuskiwane wszystkie znalezione pozycje.
  - **Always** (Zawsze) - wszystkie napotkane aliasy są wyłuskiwane.

- Zaznacz pole wyboru **Chase referrals** (Podążaj za odwołaniami), aby przenosić wyszukiwanie do innego serwera, jeśli w wyniku wyszukiwania zwrócone zostanie odwołanie do niego. Kiedy odwołanie przenosi wyszukiwanie do innego serwera, połączenie z tym serwerem wykorzystuje bieżące referencje. W przypadku zalogowania jako użytkownik Anonimowy (anonimowy) może być konieczne zalogowanie się na serwerze za pomocą uwierzytelnionej nazwy DN.

#### Zadania pokrewne

“Dopasowywanie ustawień wyszukiwania” na stronie 127

Ten temat zawiera informacje dotyczące określania możliwości użytkowników w zakresie wyszukiwania.

#### Odsyłacze pokrewne

“Parametry wyszukiwania” na stronie 47

Aby ograniczyć ilość zasobów używanych przez serwer, administrator może ustawić parametry wyszukiwania tak, aby ograniczyć możliwości wyszukiwania przez użytkowników. Możliwości wyszukiwania mogą także zostać rozszerzone dla specjalnych użytkowników.

## Zmiana atrybutów binarnych

Ten temat zawiera informacje dotyczące importowania, eksportowania i usuwania danych binarnych.

Jeśli atrybut wymaga danych binarnych, obok pola atrybutu wyświetlany jest przycisk **Binary data** (Dane binarne). Jeśli atrybut nie zawiera danych, pole jest puste. Ponieważ atrybuty binarne nie są wyświetlane, jeśli atrybut zawiera dane binarne, pole zawiera **Binary Data - 1** (Dane binarne - 1). Jeśli atrybut zawiera wiele wartości, pole to wyświetlane jest jako lista rozwijana.

Kliknij przycisk **Binary data** (Dane binarne), aby pracować z atrybutami binarnymi.

Dane binarne można importować, eksportować i usuwać.

1. Aby dodać dane binarne do atrybutu:
  - a. Kliknij przycisk **Binary data** (Dane binarne).
  - b. Kliknij przycisk **Import** (Importuj).
  - c. Możesz wprowadzić nazwę ścieżki wybranego pliku lub kliknąć przycisk **Browse** (Przeglądaj), aby znaleźć i wybrać plik binarny.
  - d. Kliknij przycisk **Submit file** (Wyślij plik). Wyświetlony zostanie komunikat File uploaded (Plik wysłany).
  - e. Kliknij przycisk **Close** (Zamknij). W polu **Binary data entries** (Pozycje danych binarnych) wyświetlona jest teraz informacja **Binary Data - 1** (Dane binarne - 1).
  - f. Powtórz proces importu dla wszystkich dodawanych plików binarnych. Kolejnymi pozycjami są **Binary Data - 2** (Dane binarne - 2), **Binary Data - 3** (Dane binarne - 3) i tak dalej.
  - g. Po zakończeniu dodawania danych binarnych kliknij przycisk **OK**.
2. Aby wyeksportować dane binarne:
  - a. Kliknij przycisk **Binary data** (Dane binarne).
  - b. Kliknij przycisk **Export** (Eksportuj).
  - c. Kliknij odsyłacz **Binary data to download** (Dane binarne do pobrania).
  - d. Postępuj zgodnie ze wskazówkami kreatora, aby wyświetlić plik binarny lub zapisać go w nowym położeniu.
  - e. Kliknij przycisk **Close** (Zamknij).
  - f. Powtórz proces eksportu dla wszystkich eksportowanych plików binarnych.
  - g. Po zakończeniu eksportowania danych binarnych kliknij przycisk **OK**.
3. Aby usunąć dane binarne:
  - a. Kliknij przycisk **Binary data** (Dane binarne).
  - b. Zaznacz plik danych binarnych do usunięcia. Można zaznaczyć kilka plików.
  - c. Kliknij przycisk **Delete** (Usuń).
  - d. Po wyświetleniu monitu o potwierdzenie usunięcia kliknij przycisk **OK**. Dane binarne oznaczone do usunięcia są usuwane z listy.



- e. Po zakończeniu usuwania danych kliknij przycisk **OK**.

**Uwaga:** Atrybuty binarne można wyszukiwać jedynie w oparciu o istnienie.

## Zadania związane z użytkownikami i grupami

Ten temat zawiera informacje dotyczące zarządzania użytkownikami i grupami.

Aby zarządzać użytkownikami i grupami, rozwiń kategorię **Users and groups** (Użytkownicy i grupy) w obszarze nawigacyjnym narzędzia Web Administration.

### Pojęcia pokrewne

“Grupy i role” na stronie 56

Wykorzystanie grup i ról pozwala organizować i kontrolować uprawnienia dostępu poszczególnych członków grup.

## Zadania związane z użytkownikami

Ten temat zawiera informacje dotyczące zarządzania użytkownikami.

Po skonfigurowaniu dziedzin i szablonów można wypełnić je użytkownikami.

### Odsyłacze pokrewne

“Uwierzytelnianie” na stronie 80

Uwierzytelnianie umożliwia kontrolę dostępu w ramach serwera Directory Server.

### Dodawanie użytkowników:

Ten temat zawiera informacje dotyczące dodawania użytkowników.

Rozwiń kategorię **Users and groups** (Użytkownicy i grupy) w obszarze nawigacyjnym narzędzia Web Administration.

1. Kliknij przycisk **Add user** (Dodaj użytkownika) lub kliknij opcję **Managing users** (Zarządzanie użytkownikami) i przycisk **Add** (Dodaj).
2. Wybierz z menu rozwijanego dziedzinę, do której chcesz dodać użytkownika.
3. Kliknij przycisk **Next** (Dalej). Wyświetlony zostanie szablon powiązany z tą dziedziną. Wypełnij wymagane pola oznaczone gwiazdką (\*) oraz dowolne z pozostałych pól zakładek. Jeśli grupy są już utworzone w dziedzinie, można również dodać użytkownika do jednej lub kilku z nich.
4. Po zakończeniu kliknij przycisk **Finish** (Zakończ).

### Wyszukiwanie użytkowników w dziedzinie:

Ten temat zawiera informacje dotyczące wyszukiwania użytkowników w dziedzinie.

Rozwiń kategorię **Users and groups** (Użytkownicy i grupy) w obszarze nawigacyjnym narzędzia Web Administration.

1. Kliknij przycisk **Find user** (Znajdź użytkownika) lub kliknij opcję **Manage users** (Zarządzanie użytkownikami) i przycisk **Find** (Znajdź).
2. W polu **Select realm** (Wybierz dziedzinę) wybierz dziedzinę, w której chcesz wyszukiwać.
3. W polu **Naming attribute** (Atrybut nazewnictwa) wpisz wyszukiwany łańcuch. Obsługiwane są znaki zastępcze, na przykład jeśli wprowadzony zostanie łańcuch **\*smith**, wynikiem będą wszystkie pozycje zawierające atrybut nazwy kończący się na smith.
4. Dla wybranego użytkownika można wykonać następujące operacje:
  - **Edycja** - patrz “Edytowanie informacji o użytkowniku”.
  - **Kopiowanie** - patrz “Kopiowanie użytkownika” na stronie 204.
  - **Usuwanie** - patrz “Usuwanie użytkownika” na stronie 204.
5. Po zakończeniu kliknij przycisk **OK**.

### Edytowanie informacji o użytkowniku:

Ten temat zawiera informacje dotyczące edytowania informacji o użytkowniku.

Rozwiń kategorię **Users and groups** (Użytkownicy i grupy) w obszarze nawigacyjnym narzędzia Web Administration.

1. Kliknij **Manage users** (Zarządzaj użytkownikami).
2. Z menu rozwijanego wybierz dziedzinę. Kliknij **View users** (Przeglądaj użytkowników), jeśli użytkownicy nie zostali wyświetleni w polu **Users** (Użytkownicy).
3. Wybierz użytkownika do edycji i kliknij przycisk **Edit** (Edycja).
4. Zmień dane w zakładkach i zmień przypisanie do grupy.
5. Po zakończeniu kliknij przycisk **OK**.

#### **Kopiowanie użytkownika:**

Ten temat zawiera informacje dotyczące kopiowania użytkownika.

Aby utworzyć wielu w zasadzie podobnych użytkowników, można utworzyć dodatkowych użytkowników, kopiując początkowego użytkownika i zmieniając informacje.

Rozwiń kategorię **Users and groups** (Użytkownicy i grupy) w obszarze nawigacyjnym narzędzia Web Administration.

1. Kliknij **Manage users** (Zarządzaj użytkownikami).
2. Z menu rozwijanego wybierz dziedzinę. Kliknij **View users** (Przeglądaj użytkowników), jeśli użytkownicy nie zostali wyświetleni w polu **Users** (Użytkownicy).
3. Wybierz użytkownika do skopiowania i kliknij przycisk **Copy** (Kopiuj).
4. Zmień odpowiednie informacje dla nowego użytkownika, na przykład wymagane informacje identyfikujące konkretnego użytkownika, takie jak sn lub cn. Nie zmieniaj informacji wspólnych dla obu użytkowników.
5. Po zakończeniu kliknij przycisk **OK**.

#### **Usuwanie użytkownika:**

Ten temat zawiera informacje dotyczące usuwania użytkownika.

Rozwiń kategorię **Users and groups** (Użytkownicy i grupy) w obszarze nawigacyjnym narzędzia Web Administration.

1. Kliknij **Manage users** (Zarządzaj użytkownikami).
2. Z menu rozwijanego wybierz dziedzinę. Kliknij **View users** (Przeglądaj użytkowników), jeśli użytkownicy nie zostali wyświetleni w polu **Users** (Użytkownicy).
3. Wybierz użytkownika do usunięcia i kliknij przycisk **Delete** (Usuń).
4. Po wyświetleniu monitu o potwierdzenie usunięcia kliknij przycisk **OK**.
5. Użytkownik zostanie usunięty z listy użytkowników.

### **Zadania związane z grupami**

Ten temat zawiera informacje dotyczące zarządzania grupami.

Po skonfigurowaniu dziedzin i schematów można utworzyć grupy.

#### **Dodawanie grup:**

Ten temat zawiera informacje dotyczące dodawania grup.

Rozwiń kategorię **Users and groups** (Użytkownicy i grupy) w obszarze nawigacyjnym narzędzia Web Administration.

1. Kliknij przycisk **Add group** (Dodaj grupę) lub kliknij opcję **Manage groups** (Zarządzanie grupami) i przycisk **Add** (Dodaj).
2. Wprowadź nazwę grupy, którą chcesz utworzyć.
3. Wybierz z rozwijanego menu dziedzinę, do której ma zostać dodana grupa.

4. Kliknij przycisk **Finish** (Zakończ), aby utworzyć grupę. Jeśli w dziedzinie znajdują się już użytkownicy, kliknij przycisk **Next** (Dalej) i wybierz użytkowników, którzy zostaną dodani do grupy. Następnie kliknij przycisk **Finish** (Zakończ).

#### Pojęcia pokrewne

“Grupy i role” na stronie 56

Wykorzystanie grup i ról pozwala organizować i kontrolować uprawnienia dostępu poszczególnych członków grup.

#### Wyszukiwanie grup w dziedzinie:

Ten temat zawiera informacje dotyczące wyszukiwania grup w dziedzinie.

Rozwiń kategorię **Users and groups** (Użytkownicy i grupy) w obszarze nawigacyjnym narzędzia Web Administration.

1. Kliknij przycisk **Find group** (Znajdź grupę) lub kliknij opcję **Manage groups** (Zarządzanie grupami) i przycisk **Find** (Znajdź).
2. W polu **Select realm** (Wybierz dziedzinę) wybierz dziedzinę, w której chcesz wyszukiwać.
3. W polu **Naming attribute** (Atrybut nazewnictwa) wpisz wyszukiwany łańcuch. Obsługiwane są znaki zastępcze, na przykład jeśli wprowadzany jest łańcuch **\*club**, wynikiem są wszystkie grupy zawierające atrybut kończący się na **club**, na przykład **book club**, **chess club**, **garden club** i tak dalej.
4. Dla wybranej grupy można wykonać następujące operacje:
  - **Edycja** - patrz “Edytowanie informacji o grupie”.
  - **Kopiowanie** - patrz “Kopiowanie grupy”.
  - **Usuwanie** - patrz “Usuwanie grupy” na stronie 206.
5. Po zakończeniu kliknij przycisk **Close** (Zamknij).

#### Edytowanie informacji o grupie:

W tym temacie opisano edytowanie informacji o grupie.

Rozwiń kategorię **Users and groups** (Użytkownicy i grupy) w obszarze nawigacyjnym narzędzia Web Administration.

1. Kliknij **Manage groups** (Zarządzaj grupami).
2. Z menu rozwijanego wybierz dziedzinę. Kliknij opcję **View groups** (Przeglądaj grupy), jeśli grupy nie zostały wyświetlone w polu **Groups** (Grupy).
3. Wybierz grupę do edycji i kliknij przycisk **Edit** (Edycja).
4. Możesz kliknąć opcję **Filter** (Filtr), aby ograniczyć liczbę **dostępnych użytkowników**. Na przykład wprowadzenie **\*smith** w polu nazwiska ogranicza dostępnych użytkowników do tych, których imię i nazwisko kończy się na **smith**, na przykład **Ann Smith**, **Bob Smith**, **Joe Goldsmith** i tak dalej.
5. Można dodawać lub usuwać użytkowników z grupy.
6. Po zakończeniu kliknij przycisk **OK**.

#### Kopiowanie grupy:

Ten temat zawiera informacje dotyczące kopiowania grupy.

Aby utworzyć wiele grup zawierających w większości te same elementy, można utworzyć dodatkowe grupy, kopiując początkową grupę i zmieniając informacje.

Rozwiń kategorię **Users and groups** (Użytkownicy i grupy) w obszarze nawigacyjnym narzędzia Web Administration.

1. Kliknij **Manage groups** (Zarządzaj grupami).
2. Z menu rozwijanego wybierz dziedzinę. Kliknij **View groups** (Przeglądaj grupy), jeśli użytkownicy nie zostali wyświetleni w polu **Groups** (Grupy).
3. Wybierz grupę do skopiowania i kliknij przycisk **Copy** (Kopiuuj).

4. Zmień nazwę grupy w polu **Group name** (Nazwa grupy). Nowa grupa ma te same elementy, co oryginalna grupa.
5. Można modyfikować elementy grupy.
6. Po zakończeniu kliknij przycisk **OK**. Zostanie utworzona nowa grupa zawierająca te same elementy, co grupa oryginalna, ze wszystkimi zmianami polegającymi na dodaniu lub usunięciu wprowadzonymi podczas kopiowania.

### Usuwanie grupy:

Ten temat zawiera informacje dotyczące usuwania grupy.

Rozwiń kategorię **Users and groups** (Użytkownicy i grupy) w obszarze nawigacyjnym narzędzia Web Administration.

1. Kliknij **Manage groups** (Zarządzaj grupami).
2. Z menu rozwijanego wybierz dziedzinę. Kliknij opcję **View groups** (Przeglądaj grupy), jeśli grupy nie zostały wyświetlone w polu **Groups** (Grupy).
3. Wybierz grupę do usunięcia i kliknij przycisk **Delete** (Usuń).
4. Po wyświetleniu monitu o potwierdzenie usunięcia kliknij przycisk **OK**.
5. Grupa zostanie usunięta z listy grup.

## Zadania związane z dziedzinami i szablonami użytkowników

Ten temat zawiera informacje dotyczące zarządzania dziedzinami i szablonami użytkowników.

Aby zarządzać dziedzinami i szablonami użytkowników, kliknij kategorię **Realms and templates** (Dziedziny i szablony) w obszarze nawigacji narzędzia Web Administration. Dziedziny i szablony użytkowników ułatwiają innym wprowadzanie danych do katalogu.

### Pojęcia pokrewne

“Dziedziny i szablony użytkowników” na stronie 46

Dzięki obiektom dziedziny i szablonu użytkowników znajdującym się w narzędziu Web Administration użytkownik nie musi w pełni znać niektórych niskopoziomowych zagadnień związanych z protokołem LDAP.

## Tworzenie dziedziny

Ten temat zawiera informacje dotyczące tworzenia dziedziny.

Aby utworzyć dziedzinę:

1. Rozwiń kategorię **Realms and templates** (Dziedziny i szablony) znajdującą się w obszarze nawigacyjnym narzędzia Web Administration.
2. Kliknij przycisk **Add realm** (Dodaj dziedzinę).
  - Wpisz nazwę dziedziny. Na przykład **dziedzina1**.
  - Wpisz nadrzędną nazwę DN, która identyfikuje położenie dziedziny. Wpis ten ma postać przyrostka, np. **o=ibm,c=us**. Ta pozycja może być przyrostkiem lub dowolną pozycją w katalogu. Można także kliknąć przycisk **Browse** (Przeglądaj), aby wybrać wymagane położenie poddrzewa.
3. Kliknij **Next** (Dalej), aby kontynuować, lub kliknij **Finish** (Zakończ).
4. Po kliknięciu przycisku **Next** (Dalej) przejrzyj informacje. W tym momencie nie utworzono jeszcze dziedziny, więc opcje **User template** (Szablon użytkowników) i **User search filter** (Filtr wyszukiwania użytkowników) można zignorować.
5. Kliknij przycisk **Finish** (Zakończ), aby utworzyć dziedzinę.

### Pojęcia pokrewne

“Dziedziny i szablony użytkowników” na stronie 46

Dzięki obiektom dziedziny i szablonu użytkowników znajdującym się w narzędziu Web Administration użytkownik nie musi w pełni znać niektórych niskopoziomowych zagadnień związanych z protokołem LDAP.

## Tworzenie administratora dziedziny

Ten temat zawiera informacje dotyczące tworzenia administratora dziedziny.

Aby utworzyć administratora dziedziny, należy najpierw utworzyć grupę administrowania dla dziedziny, wykonując następujące operacje:

1. Utwórz grupę administrowania dziedziny.
  - a. Rozwiń kategorię **Directory management** (Zarządzanie katalogiem) w obszarze nawigacyjnym narzędzia Web Administration.
  - b. Kliknij **Manage entries** (Zarządzaj pozycjami).
  - c. Rozwiń drzewo i wybierz utworzoną dziedzinę **cn=realm1,o=ibm,c=us**.
  - d. Kliknij przycisk **Edit ACL** (Edycja listy ACL).
  - e. Kliknij zakładkę **Owners** (Właściciele).
  - f. Sprawdź, czy zaznaczono pole **Propagate owner** (Propagacja właściciela).
  - g. Wprowadź nazwę wyróżniającą dla dziedziny **cn=realm1,o=ibm,c=us**.
  - h. Zmień **Type** (Typ) na grupę.
  - i. Kliknij przycisk **Add** (Dodaj).
2. Utwórz pozycję administratora. Jeśli jeszcze nie ma pozycji użytkownika dla administratora, należy ją utworzyć.
  - a. Rozwiń kategorię **Directory management** (Zarządzanie katalogiem) w obszarze nawigacyjnym narzędzia Web Administration.
  - b. Kliknij **Manage entries** (Zarządzaj pozycjami).
  - c. Rozwiń drzewo do położenia, w którym ma znajdować się pozycja administratora.

**Uwaga:** Umieszczenie pozycji administratora poza dziedziną pozwala uniknąć przypadkowego usunięcia go przez niego samego. W tym przykładzie położeniem może być **o=ibm,c=us**.
  - d. Kliknij przycisk **Add** (Dodaj).
  - e. Wybierz **Structural object class** (Strukturalną klasę obiektu), na przykład **inetOrgPerson**.
  - f. Kliknij przycisk **Next** (Dalej).
  - g. Wybierz pomocniczą klasę obiektu, którą chcesz dodać.
  - h. Kliknij przycisk **Next** (Dalej).
  - i. Wprowadź atrybuty wymagane dla pozycji. Na przykład:
    - **RDN** cn=JanKowalski
    - **DN** o=ibm,c=us
    - **cn** Jan Kowalski
    - **sn** Kowalski
  - j. Na karcie **Other attributes** (Inne atrybuty) sprawdź, czy użytkownik ma przypisane hasło.
  - k. Po zakończeniu kliknij przycisk **Finish** (Zakończ).
3. Dodaj administratora do grupy administrowania.
  - a. Rozwiń kategorię **Directory management** (Zarządzanie katalogiem) w obszarze nawigacyjnym narzędzia Web Administration.
  - b. Kliknij **Manage entries** (Zarządzaj pozycjami).
  - c. Rozwiń drzewo i wybierz utworzoną dziedzinę **cn=realm1,o=ibm,c=us**.
  - d. Kliknij przycisk **Edit attributes** (Edycja atrybutów).
  - e. Kliknij zakładkę **Members** (Elementy).
  - f. Kliknij **Members** (Elementy).
  - g. W polu **Members** (Elementy) wprowadź nazwę wyróżniającą administratora, w tym przykładzie **cn=Jan Kowalski,o=ibm,c=us**.
  - h. Kliknij przycisk **Add** (Dodaj). Nazwa wyróżniająca jest wyświetlana na liście **Members** (Elementy).
  - i. Kliknij przycisk **OK**.
  - j. Kliknij przycisk **Update** (Aktualizuj). Nazwa wyróżniająca jest wyświetlana na liście **Current members** (Bieżące elementy).

- k. Kliknij przycisk **OK**.
4. Utworzono administratora, który może zarządzać pozycjami w dziedzinie.

## Tworzenie szablonu

Ten temat zawiera informacje dotyczące tworzenia szablonu.

Po utworzeniu dziedziny następną czynnością jest utworzenie szablonu użytkownika. Szablon pomaga w organizowaniu informacji, które będą wprowadzane. Rozwiń kategorię **Realms and templates** (Dziedziny i szablony) znajdującą się w obszarze nawigacyjnym narzędzia Web Administration.

1. Kliknij przycisk **Add user template** (Dodaj szablon użytkownika).
  - Wprowadź nazwę szablonu, na przykład **szablon1**.
  - Wpisz położenie, w którym będzie się znajdował szablon. Do celów replikacji zlokalizuj szablon w poddrzewie dziedziny, która ma używać tego szablonu. Na przykład w dziedzinie utworzonej w poprzednich operacjach **cn=realm1,o=ibm,c=us**. Można także kliknąć przycisk **Browse** (Przełóżaj), aby wybrać inne poddrzewo do umieszczenia szablonu.
2. Kliknij przycisk **Next** (Dalej). Możesz kliknąć przycisk **Finish** (Zakończ), aby utworzyć pusty szablon. Później możesz dodać informacje do szablonu. Patrz sekcja “Edytowanie szablonu” na stronie 213.
3. Jeśli kliknięto przycisk **Next** (Dalej), wybierz strukturalną klasę obiektu szablonu, np. **inetOrgPerson**. Możesz także dodać dowolne pomocnicze klasy obiektu.
4. Kliknij przycisk **Next** (Dalej).
5. W szablonie utworzona została karta **Required** (Wymagane). Informacje znajdujące się na tej karcie można zmieniać.
  - a. Wybierz element **Required** (Wymagane) w menu kart i kliknij przycisk **Edit** (Edycja). Wyświetlony zostanie panel **Edit tab** (Edycja zakładki). Widoczna będzie nazwa karty **Required** (Wymagane) i wybrane atrybuty, które są wymagane przez klasę obiektu **inetOrgPerson**:
    - \*sn - nazwisko
    - \*cn - nazwa zwykła

**Uwaga:** Gwiazdka (\*) oznacza wymagane informacje.

  - b. Aby wprowadzić dodatkowe informacje na tej karcie, wybierz atrybut z menu **Attributes** (Atrybuty). Na przykład wybierz atrybut **departmentNumber** i kliknij przycisk **Add** (Dodaj). Wybierz atrybut **employeeNumber** i kliknij przycisk **Add** (Dodaj). Wybierz atrybut **title** i kliknij przycisk **Add** (Dodaj). Menu **Selected attributes** (Wybrane atrybuty) wygląda teraz następująco:
    - title
    - employeeNumber
    - departmentNumber
    - \*sn
    - \*cn
  - c. Można zmienić sposób wyświetlania tych pól w szablonie, podświetlając wybrany atrybut i klikając opcję **Move up** (Przesuń w górę) lub **Move down** (Przesuń w dół). Spowoduje to przesunięcie atrybutu o jedną pozycję. Powtarzaj tę procedurę do czasu uzyskania wymaganej kolejności atrybutów. Na przykład:
    - \*sn
    - \*cn
    - title
    - employeeNumber
    - departmentNumber
  - d. Można również zmienić wszystkie wybrane atrybuty.
    - 1) Zaznacz atrybut w polu **Selected attributes** (Wybrane atrybuty) i kliknij przycisk **Edit** (Edycja).

- 2) Można zmienić wyświetlaną nazwę pola używaną w szablonie. Na przykład, aby **departmentNumber** wyświetlać jako **Numer departamentu**, należy wprowadzić ją w polu **Display name** (Nazwa wyświetlana).
  - 3) Można również podać wartość domyślną, aby wstępnie wypełnić pole atrybutu w szablonie. Na przykład, jeśli większość użytkowników, którzy mają być wprowadzeni, są członkami grupy Department 789, jako wartość domyślną można wprowadzić 789. Pole w szablonie jest uzupełniane wartością 789. Wartość można zmienić podczas dodawania właściwych danych użytkownika.
  - 4) Kliknij przycisk **OK**.
- e. Kliknij przycisk **OK**.
6. Aby utworzyć inną dodatkową kategorię zakładek dla dodatkowych informacji, kliknij przycisk **Add** (Dodaj).
    - Wprowadź nazwę nowej zakładki. Na przykład adres.
    - Dla tej zakładki wybierz atrybuty z menu **Attributes** (Atrybuty). Na przykład zaznacz atrybut **homePostalAddress** i kliknij przycisk **Add** (Dodaj). Wybierz atrybut **postOfficeBox** i kliknij **Add** (Dodaj). Wybierz atrybut **telephoneNumber** i kliknij przycisk **Add** (Dodaj). Wybierz atrybut **homePhone** i kliknij **Add** (Dodaj). Wybierz atrybut **facsimileTelephoneNumber** i kliknij **Add** (Dodaj). Menu **Selected attributes** (Wybrane atrybuty) wygląda następująco:
      - homePostalAddress
      - postOfficeBox
      - telephoneNumber
      - homePhone
      - facsimileTelephoneNumber
    - Można zmienić sposób wyświetlania tych pól w szablonie, podświetlając wybrany atrybut i klikając opcję **Move up** (Przesuń w górę) lub **Move down** (Przesuń w dół). Spowoduje to przesunięcie atrybutu o jedną pozycję. Powtarzaj tę procedurę do czasu uzyskania wymaganej kolejności atrybutów. Na przykład:
      - homePostalAddress
      - postOfficeBox
      - telephoneNumber
      - facsimileTelephoneNumber
      - homePhone
    - Kliknij przycisk **OK**.
  7. Powtórz ten proces dla wszystkich tworzonych kart. Po zakończeniu kliknij przycisk **Finish** (Zakończ), aby utworzyć szablon.

## Dodawanie szablonu do dziedziny

Ten temat zawiera informacje dotyczące dodawania szablonu do dziedziny.

Po utworzeniu dziedziny i szablonu należy dodać szablon do dziedziny. Rozwiń kategorię **Realms and templates** (Dziedziny i szablony) znajdującą się w obszarze nawigacyjnym narzędzia Web Administration.

1. Kliknij **Manage realms** (Zarządzaj dziedzinaми).
2. Wybierz dziedzinę, do której chcesz dodać szablonu, w tym przykładzie **cn=realm1,o=ibm,c=us** i kliknij przycisk **Edit** (Edycja).
3. Przewiń ekran do pozycji **User template** (Szablon użytkownika) i rozwiń menu.
4. Wybierz szablon, w tym przykładzie **cn=template1,cn=realm1,o=ibm,c=us**.
5. Kliknij przycisk **OK**.
6. Kliknij przycisk **Close** (Zamknij).

## Tworzenie grup

Ten temat zawiera informacje dotyczące tworzenia grup.

Rozwiń kategorię **Users and groups** (Użytkownicy i grupy) w obszarze nawigacyjnym narzędzia Web Administration.

1. Kliknij przycisk **Add group** (Dodaj grupę).

2. Wprowadź nazwę grupy, którą chcesz utworzyć. Na przykład **grupa1**.
3. Wybierz z menu rozwijanego dziedzinę, do której chcesz dodać użytkownika. W tym przypadku **dziedzina1**.
4. Kliknij przycisk **Finish** (Zakończ), aby utworzyć grupę. Jeśli w dziedzinie znajdują się już użytkownicy, kliknij przycisk **Next** (Dalej) i wybierz użytkowników, którzy zostaną dodani do grupy grupa1. Następnie kliknij przycisk **Finish** (Zakończ).

#### Pojęcia pokrewne

“Grupy i role” na stronie 56

Wykorzystanie grup i ról pozwala organizować i kontrolować uprawnienia dostępu poszczególnych członków grup.

## Dodawanie użytkownika do dziedziny

Ten temat zawiera informacje dotyczące dodawania użytkownika do dziedziny.

Rozwiń kategorię **Users and groups** (Użytkownicy i grupy) w obszarze nawigacyjnym narzędzia Web Administration.

1. Kliknij przycisk **Add user** (Dodaj użytkownika).
2. Wybierz z menu rozwijanego dziedzinę, do której chcesz dodać użytkownika. W tym przypadku **dziedzina1**.
3. Kliknij przycisk **Next** (Dalej). Wyświetlony jest utworzony właśnie szablon szablon1. Wypełnij wymagane pola oznaczone gwiazdką (\*) oraz dowolne z pozostałych pól zakładek. Jeśli grupy są już utworzone w dziedzinie, można również dodać użytkownika do jednej lub kilku z nich.
4. Po zakończeniu kliknij przycisk **Finish** (Zakończ).

## Zadania związane z dziedzinaми

Ten temat zawiera informacje dotyczące zarządzania dziedzinaми.

Po skonfigurowaniu i wypełnieniu początkowej dziedziny można dodać więcej dziedzin lub zmienić istniejące.

Rozwiń kategorię **Realms and templates** (Dziedziny i szablony) w obszarze nawigacyjnym i kliknij przycisk **Manage realms** (Zarządzaj dziedzinaми). Wyświetlona zostanie lista istniejących dziedzin. Z tego panelu można dodawać, edytować i usuwać dziedzinę lub przeprowadzać edycję listy ACL dziedziny.

### Dodawanie dziedziny:

Ten temat zawiera informacje dotyczące dodawania dziedziny.

Rozwiń kategorię **Realms and templates** (Dziedziny i szablony) znajdującą się w obszarze nawigacyjnym narzędzia Web Administration.

1. Kliknij przycisk **Add realm** (Dodaj dziedzinę).
  - Wpisz nazwę dziedziny. Na przykład **dziedzina2**.
  - Jeśli istnieją inne dziedziny, na przykład **dziedzina1**, możesz wybrać jedną z nich, aby skopiować jej ustawienia do tworzonej dziedziny.
  - Wpisz nadrzędną nazwę DN, która identyfikuje położenie dziedziny. Wpis ten ma postać przyrostka, np. **o=ibm,c=us**. Można także kliknąć przycisk **Browse** (Przeglądaj), aby wybrać wymagane położenie poddrzewa.
2. Kliknij **Next** (Dalej), aby kontynuować, lub kliknij **Finish** (Zakończ).
3. Po kliknięciu przycisku **Next** (Dalej) przejrzyj informacje.
4. Wybierz **User template** (Szablon użytkownika) z rozwijanego menu. Jeśli ustawienia zostały skopiowane z wcześniej istniejącej dziedziny, jej szablon jest wstępnie wpisany w tym polu.
5. Wpisz **User search filter** (Filtr wyszukiwania użytkowników).
6. Kliknij przycisk **Finish** (Zakończ), aby utworzyć dziedzinę.

### Edytowanie dziedziny:

Ten temat zawiera informacje dotyczące edytowania dziedziny.



Rozwiń kategorię **Realms and templates** (Dziedziny i szablony) znajdującą się w obszarze nawigacyjnym narzędzia Web Administration.

- Kliknij **Manage realms** (Zarządzaj dziedzinami).
- Wybierz z listy dziedzinę do edycji.
- Kliknij przycisk **Edit** (Edycja).
  - Przyciski **Browse** (Przeglądaj) umożliwiają zmianę następujących atrybutów:
    - Grupa administratorów
    - Pojemnik grup
    - Pojemnik użytkowników
  - Można wybrać inny szablon z menu rozwijanego.
  - Kliknij przycisk **Edit** (Edytuj), aby zmienić **User search filter** (Filtr wyszukiwania użytkownika).
- Po zakończeniu wprowadzania ustawień kliknij **OK**.

#### **Usuwanie dziedziny:**

Ten temat zawiera informacje dotyczące usuwania dziedziny.

Rozwiń kategorię **Realms and templates** (Dziedziny i szablony) znajdującą się w obszarze nawigacyjnym narzędzia Web Administration.

1. Kliknij **Manage realms** (Zarządzaj dziedzinami).
2. Wybierz dziedzinę do usunięcia.
3. Kliknij przycisk **Delete** (Usuń).
4. Po wyświetleniu monitu o potwierdzenie usunięcia kliknij przycisk **OK**.
5. Dziedzina zostanie usunięta z listy dziedzin.

#### **Edytowanie list ACL w dziedzinie:**

Ten temat zawiera informacje dotyczące edytowania list ACL w dziedzinie.

Aby wyświetlić właściwości list ACL za pomocą narzędzia Web Administration lub pracować z listami ACL, należy zapoznać się z tematem “Zadania związane z listami kontroli dostępu” na stronie 214.

#### **Pojęcia pokrewne**

“Listy kontroli dostępu” na stronie 64

Listy kontroli dostępu (ACL) stanowią ochronę informacji zapisanych w katalogu LDAP. Za pomocą list ACL administratorzy ograniczają dostęp do różnych części katalogu lub konkretnych jego pozycji.

#### **Zadania związane z szablonami**

Ten temat zawiera informacje dotyczące zarządzania szablonami.

Po utworzeniu początkowego szablonu można dodać kolejne lub zmienić istniejące szablony.

Rozwiń kategorię **Realms and templates** (Dziedziny i szablony) w obszarze nawigacyjnym i kliknij przycisk **Manage user templates** (Zarządzaj szablonami użytkowników). Wyświetlona zostanie lista istniejących szablonów. Z tego panelu można dodawać, edytować i usuwać szablon lub przeprowadzać edycję listy ACL szablonu.

#### **Dodawanie szablonu użytkownika:**

Ten temat zawiera informacje dotyczące dodawania szablonu użytkownika.

Rozwiń kategorię **Realms and templates** (Dziedziny i szablony) znajdującą się w obszarze nawigacyjnym narzędzia Web Administration.

1. Kliknij przycisk **Add user template** (Dodaj szablon użytkownika) lub **Manage user templates** (Zarządzaj szablonami użytkowników) i kliknij przycisk **Next** (Dodaj).
  - Wprowadź nazwę nowego szablonu. Na przykład **szablon2**.
  - Jeśli istnieją inne szablony, na przykład **szablon1**, można wybrać jeden z nich, aby skopiować jego ustawienia do tworzonego szablonu.
  - Wpisz nadrzędną nazwę DN, która identyfikuje położenie szablonu. Ta pozycja ma postać nazwy wyróżniającej, na przykład **cn=realm1,o=ibm,c=us**. Można także kliknąć przycisk **Browse** (Przeglądaj), aby wybrać wymagane położenie poddrzewa.
2. Kliknij przycisk **Next** (Dalej). Możesz kliknąć przycisk **Finish** (Zakończ), aby utworzyć pusty szablon. Później możesz dodać informacje do szablonu. Patrz sekcja “Edytowanie szablonu” na stronie 213.
3. Jeśli kliknięto przycisk **Next** (Dalej), wybierz strukturalną klasę obiektu szablonu, np. **inetOrgPerson**. Możesz także dodać dowolne pomocnicze klasy obiektu.
4. Kliknij przycisk **Next** (Dalej).
5. W szablonie utworzona została karta **Required** (Wymagane). Informacje znajdujące się na tej karcie można zmieniać.
  - a. Wybierz element **Required** (Wymagane) w menu kart i kliknij przycisk **Edit** (Edycja). Wyświetlony zostanie panel **Edit tab** (Edycja zakładki). Widoczna będzie nazwa karty **Required** (Wymagane) i wybrane atrybuty, które są wymagane przez klasę obiektu **inetOrgPerson**:
    - \*sn - nazwisko
    - \*cn - nazwa zwykła

**Uwaga:** Gwiazdka (\*) oznacza wymagane informacje.
  - b. Aby wprowadzić dodatkowe informacje na tej karcie, wybierz atrybut z menu **Attributes** (Atrybuty). Na przykład wybierz atrybut **departmentNumber** i kliknij przycisk **Add** (Dodaj). Wybierz atrybut **employeeNumber** i kliknij przycisk **Add** (Dodaj). Wybierz atrybut **title** i kliknij przycisk **Add** (Dodaj). Menu **Selected attributes** (Wybrane atrybuty) wygląda teraz następująco:
    - title
    - employeeNumber
    - departmentNumber
    - \*sn
    - \*cn
  - c. Można zmienić sposób wyświetlania tych pól w szablonie, podświetlając wybrany atrybut i klikając opcję **Move up** (Przesuń w górę) lub **Move down** (Przesuń w dół). Spowoduje to przesunięcie atrybutu o jedną pozycję. Powtarzaj tę procedurę do czasu uzyskania wymaganej kolejności atrybutów. Na przykład:
    - \*sn
    - \*cn
    - title
    - employeeNumber
    - departmentNumber
  - d. Można również zmienić wszystkie wybrane atrybuty.
    - 1) Zaznacz atrybut w polu **Selected attributes** (Wybrane atrybuty) i kliknij przycisk **Edit** (Edycja).
    - 2) Można zmienić wyświetlaną nazwę pola używaną w szablonie. Na przykład, aby **departmentNumber** wyświetlać jako **Numer departamentu**, należy wprowadzić ją w polu **Display name** (Nazwa wyświetlana).
    - 3) Można również podać wartość domyślną, aby wstępnie wypełnić pole atrybutu w szablonie. Na przykład, jeśli większość użytkowników, którzy mają być wprowadzeni, są członkami grupy Department 789, jako wartość domyślną można wprowadzić 789. Pole w szablonie jest uzupełniane wartością 789. Wartość można zmienić podczas dodawania właściwych danych użytkownika.
    - 4) Kliknij przycisk **OK**.

- e. Kliknij przycisk **OK**.
6. Aby utworzyć inną dodatkową kategorię zakładek dla dodatkowych informacji, kliknij przycisk **Add** (Dodaj).
- Wprowadź nazwę nowej zakładki. Na przykład adres.
  - Dla tej zakładki wybierz atrybut z menu **Attributes** (Atrybuty). Na przykład zaznacz atrybut **homePostalAddress** i kliknij przycisk **Add** (Dodaj). Wybierz atrybut **postOfficeBox** i kliknij **Add** (Dodaj). Wybierz atrybut **telephoneNumber** i kliknij przycisk **Add** (Dodaj). Wybierz atrybut **homePhone** i kliknij **Add** (Dodaj). Wybierz atrybut **facsimileTelephoneNumber** i kliknij **Add** (Dodaj). Menu **Selected attributes** (Wybrane atrybuty) wygląda następująco:
    - homePostalAddress
    - postOfficeBox
    - telephoneNumber
    - homePhone
    - facsimileTelephoneNumber
  - Można zmienić sposób wyświetlania tych pól w szablonie, podświetlając wybrany atrybut i klikając opcję **Move up** (Przesuń w górę) lub **Move down** (Przesuń w dół). Spowoduje to przesunięcie atrybutu o jedną pozycję. Powtarzaj tę procedurę do czasu uzyskania wymaganej kolejności atrybutów. Na przykład:
    - homePostalAddress
    - postOfficeBox
    - telephoneNumber
    - facsimileTelephoneNumber
    - homePhone
  - Kliknij przycisk **OK**.
7. Powtórz ten proces dla wszystkich tworzonych kart. Po zakończeniu kliknij przycisk **Finish** (Zakończ), aby utworzyć szablon.

### Edytowanie szablonu:

Ten temat zawiera informacje dotyczące edytowania szablonu.

Rozwiń kategorię **Realms and templates** (Dziedziny i szablony) znajdującą się w obszarze nawigacyjnym narzędzia Web Administration.

- Kliknij **Manage user templates** (Zarządzaj szablonami użytkowników).
- Wybierz z listy dziedzinę do edycji.
- Kliknij przycisk **Edit** (Edycja).
- Jeśli istnieją inne szablony, na przykład szablon1, możesz wybrać jeden z nich aby skopiować jego ustawienia do edytowanego szablonu.
- Kliknij przycisk **Next** (Dalej).
  - Można użyć menu rozwijanego w celu zmiany strukturalnej klasy obiektu szablonu.
  - Możesz dodać lub usunąć pomocnicze klasy obiektu.
- Kliknij przycisk **Next** (Dalej).
- Można zmodyfikować zakładki i atrybuty zawarte w szablonie. Sekcja 5 na stronie 212 zawiera informacje na temat modyfikacji zakładek.
- Po zakończeniu kliknij przycisk **Finish** (Zakończ).

### Usuwanie szablonu:

Ten temat zawiera informacje dotyczące usuwania szablonu.

Rozwiń kategorię **Realms and templates** (Dziedziny i szablony) znajdującą się w obszarze nawigacyjnym narzędzia Web Administration.

1. Kliknij **Manage user templates** (Zarządzaj szablonami użytkowników).
2. Wybierz szablon do usunięcia.
3. Kliknij przycisk **Delete** (Usuń).
4. Po wyświetleniu monitu o potwierdzenie usunięcia kliknij przycisk **OK**.
5. Szablon jest usuwany z listy szablonów.

#### **Edytowanie list ACL w szablonie:**

Ten temat zawiera informacje dotyczące edytowania list ACL w szablonie.

Rozwiń kategorię **Realms and templates** (Dziedziny i szablony) znajdującą się w obszarze nawigacyjnym narzędzia Web Administration.

1. Kliknij **Manage user templates** (Zarządzaj szablonami użytkowników).
2. Wybierz szablon, dla którego chcesz edytować listy ACL.
3. Kliknij przycisk **Edit ACL** (Edycja listy ACL).

Aby wyświetlić właściwości list ACL za pomocą narzędzia Web Administration lub pracować z listami ACL, należy zapoznać się z tematem “Zadania związane z listami kontroli dostępu”.

#### **Pojęcia pokrewne**

“Listy kontroli dostępu” na stronie 64

Listy kontroli dostępu (ACL) stanowią ochronę informacji zapisanych w katalogu LDAP. Za pomocą list ACL administratorzy ograniczają dostęp do różnych części katalogu lub konkretnych jego pozycji.

## **Zadania związane z listami kontroli dostępu**

Ten temat zawiera informacje dotyczące zarządzania listami kontroli dostępu.

#### **Pojęcia pokrewne**

“Listy kontroli dostępu” na stronie 64

Listy kontroli dostępu (ACL) stanowią ochronę informacji zapisanych w katalogu LDAP. Za pomocą list ACL administratorzy ograniczają dostęp do różnych części katalogu lub konkretnych jego pozycji.

## **Wyświetlanie praw dostępu do wybranej efektywnej listy ACL**

Ten temat zawiera informacje dotyczące wyświetlania praw dostępu do wybranej efektywnej listy ACL.

Efektywnymi listami ACL są jawne i odziedziczone listy ACL wybranej pozycji.

1. Wybierz pozycję katalogu. Na przykład cn=Jan Kowalski,ou=Advertising,o=ibm,c=US.
2. Kliknij przycisk **Edit ACL** (Edycja listy ACL). Zostanie wyświetlony panel Edit ACL (Edycja listy ACL) z wybraną wstępnie zakładką **Effective ACLs** (Efektywne listy ACL). Karta **Effective ACLs** (Efektywne listy ACL) zawiera informacje tylko do odczytu dotyczące list ACL.
3. Wybierz konkretną efektywną listę ACL i kliknij przycisk **View** (Wyświetl). Powoduje to otwarcie panelu **View access rights** (Przeglądanie praw dostępu).
4. Kliknij przycisk **OK**, aby powrócić do zakładki Effective ACLs (Efektywne listy ACL).
5. Kliknij opcję **Cancel** (Anuluj), aby powrócić do panelu Edit ACL (Edycja listy ACL).

## **Wyświetlanie efektywnych właścicieli**

Ten temat zawiera informacje dotyczące wyświetlania efektywnych właścicieli.

Efektywnymi właścicielami są jawni i odziedziczeni właściciele wybranej pozycji.

1. Wybierz pozycję katalogu. Na przykład cn=Jan Kowalski,ou=Advertising,o=ibm,c=US.
2. Kliknij przycisk **Edit ACL** (Edycja listy ACL).
3. Kliknij zakładkę **Effective owners** (Efektywni właściciele). Karta **Effective owners** (Efektywni właściciele) zawiera informacje tylko do odczytu dotyczące list ACL.

4. Kliknij opcję **Cancel** (Anuluj), aby powrócić do panelu Edit ACL (Edycja listy ACL).

## Dodawanie, edytowanie i usuwanie niefiltrowanych list kontroli dostępu

Ten temat zawiera informacje dotyczące zarządzania niefiltrowanymi listami kontroli dostępu.

Do pozycji można dodać nowe niefiltrowane listy ACL lub dokonać edycji istniejących.

Niefiltrowane listy ACL można propagować. Oznacza to, że informacje o kontroli dostępu zdefiniowane dla jednej pozycji można zastosować do wszystkich jej pozycji podrzędnych. Źródło ACL jest źródłem bieżącej listy ACL wybranej pozycji. Jeśli dana pozycja nie ma listy ACL, dziedziczy ją od obiektów nadrzędnych na podstawie ustawień listy ACL dla obiektów nadrzędnych.

Wprowadź poniższe informacje w zakładce **Non-filtered ACLs** (Niefiltrowane listy ACL):

- Wykonaj propagację list ACL - zaznacz pole wyboru **Propagate** (Propagacja), aby zezwolić pozycjom potomnym o nieokreślonej jawnie ACL dziedziczyć ją od tej pozycji. Jeśli pole wyboru jest zaznaczone, podrzędne obiekty dziedziczą listy ACL z tej pozycji i jeśli dla pozycji potomnej lista ACL jest zdefiniowana jawnie, to lista ACL dziedziczona z nadrzędnej jest zastępowana nową dodaną listą ACL. Jeśli to pole wyboru nie jest zaznaczone, pozycje potomne bez jawnie określonej listy ACL dziedziczą je od pozycji nadrzędnej, która ma włączoną tę opcję.
- DN (Nazwa wyróżniająca) - wpisz **nazwę wyróżniającą** jednostki żądającej dostępu do wybranej pozycji w celu wykonania na niej operacji, na przykład cn=Grupa Marketingu.
- Type (Typ) - wpisz **Typ** nazwy wyróżniającej. Na przykład jeśli nazwa wyróżniająca określa użytkownika, wybierz typ access-id.

Kliknij przycisk **Add** (Dodaj), aby dodać nazwę wyróżniającą w polu DN (Nazwa wyróżniająca) do listy kontroli dostępu, lub przycisk Edit (Edycja), aby zmodyfikować listy kontroli dostępu istniejącej nazwy wyróżniającej.

Panele **Add access rights** (Dodaj prawa dostępu) i **Edit access rights** (Edycja prawa dostępu) umożliwiają ustawienie praw dostępu dla nowych lub istniejących list ACL. Pole **Type** (Typ) przyjmuje domyślnie wartość wybraną w panelu **Edit ACL** (Edycja listy ACL). W przypadku dodawania listy ACL wszystkie pozostałe pola będą domyślnie puste. W przypadku edycji listy ACL pola zawierają wartości ustawione w czasie ostatniej modyfikacji tej listy.

Można wykonać następujące czynności:

- zmienić typ listy ACL,
- ustawić uprawnienia do dodawania i usuwania,
- ustawić prawa dostępu klas bezpieczeństwa.

Aby ustawić prawa dostępu:

1. W polu **Type** (Typ), wybierz typ pozycji dla listy ACL. Na przykład jeśli nazwa wyróżniająca określa użytkownika, wybierz typ access-id.
2. W sekcji **Rights** (Prawa) znajdują się prawa do dodawania i usuwania posiadane przez podmiot.
  - Opcja **Add child** (Dodanie elementu potomnego) umożliwia nadanie lub odebranie podmiotowi prawa dodawania do katalogu pozycji znajdującej się poniżej pozycji zaznaczonej.
  - Opcja **Delete entry** (Usuwanie pozycji) umożliwia nadanie lub odebranie podmiotowi prawa do usuwania wybranej pozycji.
3. Sekcja **Security class** (Klasa bezpieczeństwa) definiuje uprawnienia klas atrybutów. Atrybuty grupowane są w klasy bezpieczeństwa:
  - **Normal** (Normalna) - normalne klasy atrybutów wymagają najmniejszego poziomu bezpieczeństwa, na przykład atrybut commonName (nazwa zwykła).
  - **Sensitive** (Wrażliwa) - wrażliwe klasy atrybutów wymagają większego poziomu bezpieczeństwa, na przykład homePhone (telefon domowy).
  - **Critical** (Newralgiczna) - newralgiczne klasy atrybutów wymagają największego poziomu bezpieczeństwa, na przykład atrybut userpassword (hasło użytkownika).

- **System** (Systemowe) - atrybuty systemowe są atrybutami tylko do odczytu, utrzymywanymi przez serwer.
- **Restricted** (Ograniczone) - atrybuty ograniczone określają kontrolę dostępu.

Każda klasa bezpieczeństwa ma powiązane ze sobą uprawnienia.

- Read (Odczyt) - podmiot może odczytywać atrybuty.
- Write (Zapis) - podmiot może modyfikować atrybuty.
- Search (Wyszukiwanie) - podmiot może przeszukiwać atrybuty.
- Compare (Porównywanie) - podmiot może porównywać atrybuty.

Ponadto można określać prawa dostępu w oparciu o atrybut zamiast klasy ochrony, do której należy dany atrybut. Sekcja atrybutu znajduje się poniżej **Critical security class** (Newralgicznej klasy ochrony).

- Wybierz atrybut z listy rozwijanej **Define an attribute** (Definiuj atrybut).
- Kliknij przycisk **Define** (Zdefiniuj). Wyświetlony zostanie atrybut z tabelą uprawnień.
- Określ, czy nadać czy cofnąć uprawnienia każdej z czterech klas ochrony powiązanych z atrybutem.
- Tę procedurę możesz powtórzyć dla wielu atrybutów.
- Aby usunąć atrybut, zaznacz go i kliknij przycisk **Delete** (Usuń).
- Po zakończeniu kliknij przycisk **OK**.

Listy ACL można usuwać na dwa sposoby:

- Zaznacz przełącznik znajdujący się obok listy ACL, którą chcesz usunąć. Kliknij przycisk **Remove** (Usuń).
- Kliknij przycisk **Remove all** (Usuń wszystkie), aby usunąć wszystkie nazwy wyróżniające z listy.

## Dodawanie, edytowanie i usuwanie filtrowanych list kontroli dostępu

Ten temat zawiera informacje dotyczące wyświetlania praw dostępu związanych z filtrowaną listą kontroli dostępu.

Do pozycji można dodać nowe filtrowane listy ACL lub dokonać edycji istniejących.

Filtrowane listy ACL korzystają z porównywania opartego na filtrze, używając określonego filtru obiektów, w celu uzgadniania obiektów z efektywnymi prawami dostępu, które ich dotyczą.

Domyślnie listy ACL oparte na filtrach kumulują się, poczynając od najniższej pozycji zawierającej taką listę, w górę łańcucha pozycji nadrzędnych do najwyższej pozycji w drzewie DIT zawierającej taką listę. Efektywne prawa dostępu są obliczane jako iloczyn mnogościowy praw dostępu nadanych lub odebranych pozycjom nadrzędnym. Istnieje wyjątek od tej reguły. W celu zapewnienia zgodności z funkcją replikacji poddrzewa oraz zwiększenia kontroli administracyjnej wprowadzono atrybut ceiling służący do zatrzymania kumulacji na pozycji, w której znajduje się ten atrybut.

Wprowadź poniższe informacje w zakładce Filtered ACLs (Filtrowane listy ACL):

- Accumulate filtered ACLs (Kumuluj filtrowane listy ACL):
  - Wybierz przełącznik **Not specified** (Nieokreślone), aby usunąć atrybut `ibm-filterACLInherit` z wybranej pozycji.
  - Wybierz przełącznik **True** (Prawda), aby zezwolić listom ACL wybranej pozycji na ich kumulowanie się poczynając od wybranej, w górę łańcucha pozycji nadrzędnych do najwyższej pozycji w drzewie informacji katalogu zawierającej filtrowaną listę ACL.
  - Wybierz przełącznik **False** (Fałsz), aby zatrzymać kumulowanie się filtrowanych list ACL na wybranej pozycji.
- DN (Nazwa wyróżniająca) - wpisz **nazwę wyróżniającą** jednostki żądającej dostępu do wybranej pozycji w celu wykonania na niej operacji, na przykład `cn=Grupa Marketingu`.
- Type (Typ) - wpisz **Typ** nazwy wyróżniającej. Na przykład jeśli nazwa wyróżniająca określa użytkownika, wybierz typ `access-id`.

Kliknij przycisk **Add** (Dodaj), aby dodać nazwę wyróżniającą w polu DN (Nazwa wyróżniająca) do listy kontroli dostępu, lub przycisk **Edit** (Edycja), aby zmodyfikować listy kontroli dostępu istniejącej nazwy wyróżniającej.

Panele **Add access rights** (Dodaj prawa dostępu) i **Edit access rights** (Edycja prawa dostępu) umożliwiają ustawienie praw dostępu dla nowych lub istniejących list ACL. Pole **Type** (Typ) przyjmuje domyślnie wartość wybraną w panelu **Edit ACL** (Edycja listy ACL). W przypadku dodawania listy ACL wszystkie pozostałe pola będą domyślnie puste. W przypadku edycji listy ACL pola zawierają wartości ustawione w czasie ostatniej modyfikacji tej listy.

Można wykonać następujące czynności:

- zmienić typ listy ACL,
- ustawić uprawnienia do dodawania i usuwania,
- ustawić filtr obiektów dla filtrowanych list ACL,
- ustawić prawa dostępu klas bezpieczeństwa.

Aby ustawić prawa dostępu:

1. W polu **Type** (Typ), wybierz typ pozycji dla listy ACL. Na przykład jeśli nazwa wyróżniająca określa użytkownika, wybierz typ **access-id**.
2. W sekcji **Rights** (Prawa) znajdują się prawa do dodawania i usuwania posiadane przez podmiot.
  - Opcja **Add child** (Dodanie elementu potomnego) umożliwia nadanie lub odebranie podmiotowi prawa dodawania do katalogu pozycji znajdującej się poniżej pozycji zaznaczonej.
  - Opcja **Delete entry** (Usuwanie pozycji) umożliwia nadanie lub odebranie podmiotowi prawa do usuwania wybranej pozycji.
3. Ustaw filtr obiektu dla porównywania opartego na filtrze. W polu **Object filter** (Filtr obiektów) wpisz wybrany filtr obiektów dla wybranej listy ACL. Kliknij przycisk **Edit filter** (Edycja filtru), aby uzyskać pomoc w tworzeniu łańcucha filtru wyszukiwania. Bieżąca filtrowana lista ACL jest propagowana do podrzędnego obiektu w powiązonym poddrzewie zgodnym z filtrem w tym polu.
4. Sekcja **Security class** (Klasa bezpieczeństwa) definiuje uprawnienia klas atrybutów. Atrybuty grupowane są w klasy bezpieczeństwa:
  - **Normal** (Normalna) - normalne klasy atrybutów wymagają najmniejszego poziomu bezpieczeństwa, na przykład atrybut **commonName** (nazwa zwykła).
  - **Sensitive** (Wrażliwa) - wrażliwe klasy atrybutów wymagają większego poziomu bezpieczeństwa, na przykład **homePhone** (telefon domowy).
  - **Critical** (Newralgiczna) - newralgiczne klasy atrybutów wymagają największego poziomu bezpieczeństwa, na przykład atrybut **userpassword** (hasło użytkownika).
  - **System** (Systemowe) - atrybuty systemowe są atrybutami tylko do odczytu, utrzymywanymi przez serwer.
  - **Restricted** (Ograniczone) - atrybuty ograniczone określają kontrolę dostępu.

Każda klasa bezpieczeństwa ma powiązane ze sobą uprawnienia.

- **Read** (Odczyt) - podmiot może odczytywać atrybuty.
- **Write** (Zapis) - podmiot może modyfikować atrybuty.
- **Search** (Wyszukiwanie) - podmiot może przeszukiwać atrybuty.
- **Compare** (Porównywanie) - podmiot może porównywać atrybuty.

Ponadto można określać prawa dostępu w oparciu o atrybut zamiast klasy ochrony, do której należy dany atrybut. Sekcja atrybutu znajduje się poniżej **Critical security class** (Newralgicznej klasy ochrony).

- Wybierz atrybut z listy rozwijanej **Define an attribute** (Definiuj atrybut).
- Kliknij przycisk **Define** (Zdefiniuj). Wyświetlony zostanie atrybut z tabelą uprawnień.
- Określ, czy nadać czy cofnąć uprawnienia każdej z czterech klas ochrony powiązanych z atrybutem.
- Tę procedurę możesz powtórzyć dla wielu atrybutów.
- Aby usunąć atrybut, zaznacz go i kliknij przycisk **Delete** (Usuń).
- Po zakończeniu kliknij przycisk **OK**.

Listy ACL można usuwać na dwa sposoby:

- Zaznacz przełącznik znajdujący się obok listy ACL, którą chcesz usunąć. Kliknij przycisk **Remove** (Usuń).

- Kliknij przycisk **Remove all** (Usuń wszystkie), aby usunąć wszystkie nazwy wyróżniające z listy.

## Dodawanie i usuwanie właścicieli

Ten temat zawiera informacje dotyczące dodawania i usuwania właścicieli.

Właściciele pozycji mają pełne uprawnienia do wykonywania wszystkich operacji. Właściciele pozycji mogą być jawni lub propagowani (odziedziczeni).

Wprowadź poniższe informacje w zakładce **Owners** (Właściciele):

1. Zaznacz pole wyboru **Propagate owners** (Propagacja właścicieli), aby zezwolić pozycjom potomnym o nieokreślonym jawnie właścicielu dziedziczyć go od tej pozycji. Jeśli to pole wyboru nie jest zaznaczone, pozycje potomne bez jawnie określonego właściciela dziedziczą go od pozycji nadrzędnej, która ma włączoną tę opcję.
2. DN (Nazwa wyróżniająca) - wpisz **nazwę wyróżniającą** jednostki żądającej dostępu do wybranej pozycji w celu wykonania na niej operacji, na przykład `cn=Marketing Group`. Użycie pozycji `cn=this` z obiektami przekazującymi swoje prawa własności do innych obiektów ułatwia tworzenie poddrzewa katalogu, w którym obiekt należy sam do siebie.
3. Type (Typ) - wpisz **Typ** nazwy wyróżniającej. Na przykład jeśli nazwa wyróżniająca określa użytkownika, wybierz typ `access-id`.

Aby dodać właściciela, kliknij przycisk **Add** (Dodaj) w celu dodania nazwy wyróżniającej DN z pola **DN** (Nazwa wyróżniająca) do listy.

Właściciela można usunąć na dwa sposoby:

- Zaznacz przełącznik obok nazwy wyróżniającej właściciela, którego chcesz usunąć. Kliknij przycisk **Remove** (Usuń).
- Kliknij przycisk **Remove all** (Usuń wszystkie), aby usunąć wszystkie nazwy wyróżniające właścicieli z listy.

---

## Informacje dodatkowe

Materiały referencyjne dotyczące serwera Directory Server, takie jak informacje dotyczące narzędzi wiersza komend i formatu LDIF.

Poniższe sekcje zawierają informacje uzupełniające.

## Programy narzędziowe wiersza komend serwera Directory Server

W tym temacie opisano programy narzędziowe serwera Directory Server, które można uruchamiać ze środowiska komend Qshell.

Należy zaznaczyć, że niektóre łańcuchy trzeba ująć w cudzysłów, aby były prawidłowo przetwarzane w środowisku komend Qshell. Dotyczy to zwykle łańcuchów, które są nazwami wyróżniającymi, filtrami wyszukiwania i listą atrybutów zwracanych przez `ldapsearch`. Oto przykłady:

- Łańcuchy zawierające spacje: `"cn=John Smith,cn=users"`
- Łańcuchy zawierające znaki zastępcze: `"**"`
- Łańcuchy zawierające nawiasy: `"(objectclass=person)"`

Więcej informacji o środowisku komend Qshell zawiera temat "Qshell".

Więcej informacji zawierają opisy poniższych komend:

## Idapmodify i Idapadd

Programy narzędziowe wiersza komend służące do dodawania i modyfikowania pozycji w katalogu LDAP.

## Składnia



```
ldapmodify [-a] [-b] [-c] [-C zestaw_znaków] [-d poziom_debugowania] [-D nazwa_wyróżniająca_łączenia]
[-e plik_błędów] [-g] [-f plik] [-F] [-g] [-G dziedzina] [-h host_ldap] [-i plik] [-k] [-K plik_kluczy]
[-m mechanizm] [-M] [-n] [-N nazwa_certyfikatu] [-O maksymalna_liczba_przeskoków] [-p port_ldap]
[-P hasło_pliku_kluczy] [-r] [-R] [-U nazwa_użytkownika] [-v] [-V] [-w hasło | ?]
[-y nazwa_wyróżniająca_proxy]
[-Y] [-Z]
```

```
ldapadd [-a] [-b] [-c] [-C zestaw_znaków] [-d poziom_debugowania] [-D nazwa_wyróżniająca_łączenia]
[-e plik_błędów] [-g] [-f plik] [-F] [-g] [-G dziedzina] [-h host_ldap] [-i plik] [-k] [-K plik_kluczy]
[-m mechanizm] [-M] [-n] [-N nazwa_certyfikatu] [-O maksymalna_liczba_przeskoków] [-p port_ldap]
[-P hasło_pliku_kluczy] [-r] [-R] [-U nazwa_użytkownika] [-v] [-V] [-w hasło | ?]
[-y nazwa_wyróżniająca_proxy]
[-Y] [-Z]
```

## Opis

Komenda **ldapmodify** to interfejs wiersza komend do funkcji API `ldap_modify`, `ldap_add`, `ldap_delete` i `ldap_rename`. Komenda **ldapadd** to zaimplementowana pod inną nazwą wersja komendy `ldapmodify`. Po jej wywołaniu jako `ldapadd` opcja **-a** (dodaj nową pozycję) jest automatycznie włączana.

Komenda **ldapmodify** otwiera połączenie z serwerem LDAP i łączy się z serwerem. Komendy **ldapmodify** można użyć do modyfikowania i dodawania pozycji. Informacje o pozycji są odczytywane ze standardowego wejścia lub z pliku poprzez użycie opcji **-i**.

Aby wyświetlić pomoc dotyczącą składni komendy **ldapmodify** lub **ldapadd**, wpisz

```
ldapmodify -?
```

lub

```
ldapadd -?
```

## Opcje

- a** Dodaje nowe pozycje. Domyślnym działaniem komendy **ldapmodify** jest zmiana istniejących pozycji. W przypadku wywołania komendy jako **ldapadd** ta opcja jest zawsze ustawiona.
- b** Przyjmuje, że wszystkie wartości zaczynające się od "/" są wartościami binarnymi i że rzeczywista wartość znajduje się w pliku, którego ścieżka została określona w miejscu wartości.
- c** Tryb działania ciągłego. Błędy są zgłaszane, ale komenda **ldapmodify** nadal wprowadza zmiany. W przeciwnym razie domyślną operacją jest wyjście po zgłoszeniu błędu.
- C zestaw\_znaków**  
Określa, że łańcuchy dostarczone jako dane wejściowe do narzędzi **ldapmodify** i **ldapadd** są reprezentowane w lokalnym zestawie znaków i należy je przekształcić do UTF-8. Opcji **-C zestaw\_znaków** używa się, gdy strona kodowa wejściowego łańcucha znaków różni się od strony kodowej zadania. Opis funkcji API `ldap_set_iconv_local_charset()` zawiera obsługiwane wartości zestawów znaków.
- d poziom\_debugowania**  
Ustawia poziom debugowania LDAP na `poziom_debugowania`.
- D nazwa\_wyróżniająca\_łączenia**  
Parametr ***nazwa\_wyróżniająca\_łączenia*** umożliwia utworzenie łączenia z katalogiem LDAP. ***nazwa\_wyróżniająca\_łączenia*** jest nazwą wyróżniającą w postaci łańcucha znaków. Jeśli używana jest wraz z **-m DIGEST-MD5**, wykorzystywana jest do określenia identyfikatora autoryzacji. Nazwa ta może być nazwą wyróżniającą lub łańcuchem `authzId` rozpoczynającym się od "u:" lub "dn:".
- e plik\_błędów**  
Określa plik, do którego będą zapisywane odrzucone pozycje. Opcja ta wymaga podania opcji **-c** (ciągłe działanie). W przypadku niepowodzenia przetwarzania pozycji, pozycja ta jest zapisywana w pliku

odrzuconych i zwiększany jest licznik odrzuconych pozycji. Jeśli dane wejściowe komendy ldapmodify lub ldapadd pochodzą z pliku, po zakończeniu przetwarzania tego pliku zwracana jest informacja o łącznej liczbie pozycji zapisanych w pliku odrzuconych.

**-f plik** Odczytuje informacje dotyczące modyfikacji pozycji z pliku LDIF zamiast ze standardowego wejścia. Jeśli plik LDIF nie zostanie podany, rekordy aktualizacji w formacie LDIF należy wprowadzić na standardowym wejściu. Plik wejściowy można wskazać za pomocą opcji **-i** lub **-f**; działanie obu opcji jest identyczne.

**-F** Wymusza aplikację wszystkich zmian niezależnie od zawartości wierszy wejściowych rozpoczynających się od repliki: (domyślnie, replika: wiersze są porównywane względem używanego hosta serwera LDAP i portu, aby zdecydować, czy zapis protokołu replikacji powinien rzeczywiście zostać zastosowany).

**-g** Nie należy umieszczać spacji na końcu wartości atrybutów.

**-G** Określa dziedzinę. Parametr ten jest opcjonalny. Jeśli używany jest wraz z **-m DIGEST-MD5**, wartość przekazywana jest do serwera podczas połączenia.

#### **-h host\_ldap**

Określa alternatywny host, na którym działa serwer ldap.

**-i plik** Odczytuje informacje dotyczące modyfikacji pozycji z pliku LDIF zamiast ze standardowego wejścia. Jeśli plik LDIF nie zostanie podany, rekordy aktualizacji w formacie LDIF należy wprowadzić na standardowym wejściu. Plik wejściowy można wskazać za pomocą opcji **-i** lub **-f**; działanie obu opcji jest identyczne.

**-k** Określa, czy używać elementu sterującego administrowania serwerem.

#### **-K plik\_kluczy**

Określa nazwę pliku bazy danych kluczy SSL z domyślnym rozszerzeniem **kdb**. Jeśli plik bazy danych kluczy nie znajduje się w bieżącym katalogu, należy podać jego nazwę z pełną ścieżką. Jeśli nazwa pliku bazy danych kluczy nie zostanie podana, to narzędzie najpierw poszuka zmiennej środowiskowej **SSL\_KEYRING**, która powinna zawierać nazwę pliku. Jeśli nie zdefiniowano zmiennej środowiskowej, **SSL\_KEYRING**, użyty zostanie systemowy plik kluczy, jeśli istnieje.

Parametr ten udostępnia opcję **-Z**. W przypadku serwera Directory Server w systemie i5/OS, jeśli użyta została opcja **-Z** i nie użyto opcji **-K** ani **-N**, wykorzystany zostanie certyfikat powiązany z identyfikatorem aplikacji Directory Services Client.

**-l** Zapobiega replikowaniu zmiany. Opcja "nie replikuj" umożliwia wskazanie, że określona zmiana nie ma być replikowana. Opcja ta jest przeznaczona przede wszystkim do użytku przez topologię replikacji w celu wyłączenia replikowania przez serwer docelowy zmian wprowadzanych w ramach synchronizowania topologii replikacji. Pozwala to zapobiec propagowaniu zmian na inne serwery. Z opcji może też korzystać klient administracyjny.

#### **-m mechanizm**

Parametr **mechanizm** określa mechanizm SASL używany do łączenia z serwerem. Używana jest funkcja API `ldap_sasl_bind_s()`. Parametr **-m** jest ignorowany, jeśli ustawiony zostanie parametr **-V 2**. Jeśli parametr **-m** nie jest określony, użyte zostanie proste uwierzytelnianie. Poprawne mechanizmy to:

- **CRAM-MD5** - chroni hasło wysyłane na serwer.
- **EXTERNAL** - używa certyfikatu SSL. Wymaga opcji **-Z**.
- **GSSAPI** - używa referencji Kerberos użytkownika.
- **DIGEST-MD5** - wymaga od klienta wysłania do serwera wartości nazwy użytkownika. Wymaga opcji **-U**. Parametr **-D** (zwykle nazwa wyróżniająca łączenia) określa identyfikator autoryzacji. Może być nazwą wyróżniającą lub łańcuchem `authId` rozpoczynającym się od `u:` lub `dn:`.
- **OS400\_PRFTKN** - dokonuje uwierzytelnienia na lokalnym serwerze LDAP jako bieżący użytkownik systemu i5/OS za pomocą nazwy wyróżniającej użytkownika w systemowym mechanizmie rzutowania. Nie należy określać parametrów **-D** (nazwy wyróżniającej łączenia) oraz **-w** (hasła).

**-M** Zarządza obiektami odwołania tak jak zwykłymi pozycjami.

**-n** Podanie opcji wyłączenia operacji pozwala zapoznać się z działaniem wydawanej komendy bez faktycznego wykonywania działań na katalogu. Zmiany, które zostałyby wprowadzone, są wypisywane na standardowe

wyjście poprzedzone znakiem wykrzyknika. Wszelkie błędy składniowe, które zostaną wykryte podczas przetwarzania pliku wejściowego, ale przed wywołaniem funkcji dokonujących zmian w katalogu, są wypisywane na standardowe wyjście błędów. Opcja ta jest szczególnie użyteczna w połączeniu z opcją `-v` w przypadku konieczności debugowania ewentualnych błędów.

**-N** *nazwa\_certyfikatu*

Określa etykietę powiązaną z certyfikatem klienta w pliku 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 może być certyfikat klienta. Parametr *nazwa\_certyfikatu* nie jest wymagany, jeśli określono domyślną parę certyfikat/klucz prywatny dla pliku bazy danych kluczy. Podobnie parametr *nazwa\_certyfikatu* nie jest wymagany, jeśli w wyznaczonej bazie danych kluczy znajduje się pojedyncza para certyfikat/klucz prywatny. Parametr ten jest ignorowany, gdy nie zostanie podana opcja `-Z` lub `-K`. W przypadku serwera Directory Server w systemie i5/OS, jeśli użyta została opcja `-Z` i nie użyto opcji `-K` ani `-N`, wykorzystany zostanie certyfikat powiązany z identyfikatorem aplikacji Directory Services Client.

**-O** *maksymalna\_liczba\_przeskoków*

Parametr *maksymalna\_liczba\_przeskoków* określa maksymalną liczbę przeskoków, którą wykona biblioteka klienta podczas przeglądania odwołań. Domyślna liczba przeskoków jest równa 10.

**-p** *port\_ldap*

Określa alternatywny port TCP, na którym serwer ldap prowadzi nasłuch. Domyślnym portem LDAP jest 389. Jeśli nie podano opcji `-p`, a podano `-Z`, używany jest domyślny port 636 SSL LDAP.

**-P** *hasło\_pliku\_kluczy*

Określa hasło bazy danych kluczy. Hasło to jest wymagane w celu uzyskania dostępu do szyfrowanych informacji w pliku bazy danych kluczy, który może zawierać jeden lub wiele kluczy prywatnych. Jeśli z plikiem bazy danych kluczy jest związany plik ukrytych haseł, hasło jest otrzymywane z niego pliku i parametr `-P` nie jest wymagany. Parametr ten jest ignorowany, gdy nie zostanie podana opcja `-Z` lub `-K`.

**-r** Wszystkie wartości zastępuje wartościami domyślnymi.

**-R** Określa, że odwołania nie mają następować automatycznie.

**-U** Określa nazwę użytkownika. Wymagane w przypadku określenia opcji `-m DIGEST-MD5` i ignorowane w przypadku pozostałych mechanizmów.

**-v** Używa trybu szczegółowego z wieloma komunikatami diagnostycznymi wysyłanymi na wyjście standardowe.

**-V** *wersja*

Określa wersję LDAP używaną przez komendę `ldapmodify` podczas łączenia się z serwerem LDAP. Domyślnie nawiązywane jest połączenie LDAP V3. Aby jawnie wybrać LDAP V3, należy podać wartość `-V 3`. Aby uruchomić jako aplikację LDAP V2, należy podać `-V 2`.

**-w** *hasło | ?*

Do uwierzytelniania zostanie użyte podane *hasło*. Użyj `?` w celu wywołania zachęty do wpisania hasła.

**-y** *nazwa\_wyróżniająca\_proxy*

Ustawia ID proxy dla opcji autoryzacji proxy.

**-Y** Używa bezpiecznego połączenia LDAP (TLS).

**-Z** Używa bezpiecznego połączenia SSL w komunikacji z serwerem LDAP. W przypadku serwera Directory Server w systemie i5/OS, jeśli użyta została opcja `-Z` i nie użyto opcji `-K` ani `-N`, wykorzystany zostanie certyfikat powiązany z identyfikatorem aplikacji Directory Services Client.

## Format wejściowy

Zawartość pliku (lub standardowego wejścia, jeśli w wierszu komend nie określono opcji `-i`) powinna odpowiadać formatowi LDIF.

## Przykłady

Zakładając, że plik /tmp/entrymods istnieje i że zawiera:

```
dn: cn=Zmień Mnie, o=University of Higher Learning, c=US
changetype: modify
replace: mail
mail: zmień_mnie@student.of.life.edu
-
add: title
title: Słynna osoba
-
add: jpegPhoto
jpegPhoto: /tmp/zmień_mnie.jpeg
-
delete: description
-
```

komenda:

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

zastąpi dane atrybutu poczty pozycji Zmień Mnie wartością zmień\_mnie@student.of.life.edu, doda tytuł Słynna osoba oraz dane z pliku /tmp/modme.jpeg jako jpegPhoto, a także całkowicie usunie atrybut opisu. Te same zmiany można wprowadzić, używając starszego formatu wejściowego ldapmodify:

```
cn=Zmień Mnie, o=University of Higher Learning, c=US
mail=zmień_mnie@student.of.life.edu
+title=Słynna osoba
+jpegPhoto=/tmp/zmień_mnie.jpeg
-description
```

i komendy:

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

Zakładając, że plik /tmp/newentry istnieje i że zawiera:

```
dn: cn=Jan Kowalski, o=University of Higher Learning, c=US
objectClass: person
cn: Jan Kowalski
cn: Janek
sn: Kowalski
title: Najsłynniejsza fikcyjna osoba na świecie
mail: jankowalski@student.of.life.edu
uid: jkowalski
```

komenda:

```
ldapadd -i /tmp/newentry
```

doda nową pozycję dla Jana Kowalskiego, używając wartości z pliku /tmp/newentry.

## Uwagi

Jeśli dane pozycji nie zostały podane w pliku poprzez użycie opcji **-i**, komenda **ldapmodify** będzie czekać na wprowadzenie pozycji z wejścia standardowego.

## Diagnostyka

Jeśli nie wystąpiły żadne błędy, statusem wyjścia jest 0. Wystąpienie błędu powoduje zwrócenie niezerowego statusu wyjścia i wypisanie komunikatu diagnostycznego na standardowe wyjście błędów.

### Pojęcia pokrewne

“Przyrostek (kontekst nazwy)” na stronie 12

Przyrostek (znany również jako kontekst nazwy) to nazwa DN identyfikująca najwyższą pozycję w lokalnej hierarchii katalogu.

Funkcje API protokołu LDAP

Temat Funkcje API protokołu LDAP zawiera więcej informacji o funkcjach API serwera katalogów.

“Schemat konfiguracji serwera Directory Server” na stronie 258

W tych informacjach opisano drzewo informacji katalogu (Directory Information Tree - DIT) oraz atrybuty używane do konfigurowania pliku `ibmslapd.conf`.

### Odsyłacze pokrewne

“Format wymiany danych LDAP (LDIF)” na stronie 251

Format wymiany danych LDAP (LDAP Data Interchange Format - LDIF) to standardowy format używany do tekstowego zapisu reprezentacji obiektów LDAP i operacji na obiektach LDAP (dodawanie, modyfikowanie, usuwanie, zmiana nazwy wyróżniającej). Pliki zawierające rekordy LDIF mogą być używane do przenoszenia danych między serwerami katalogów lub podawane jako dane wejściowe programów narzędziowych LDAP, takich jak `ldapadd` i `ldapmodify`.

## ldapdelete

Program narzędziowy wiersza komend do usuwania pozycji LDAP.

### Składnia

```
ldapdelete [-c] [-C zestaw_znaków] [-d poziom_debugowania] [-D nazwa_wyróżniająca_łączenia] [-f plik]
[-G dziedzina] [-h host_ldap] [-i plik] [-k] [-K plik_kluczy] [-m mechanizm]
[-M] [-n] [-N nazwa_certyfikatu] [-O maksymalna_liczba_przeskoków] [-p port_ldap]
[-P hasło_pliku_kluczy] [-R] [-s] [-U nazwa_użytkownika] [-v] [-V wersja]
[-w hasło | ?] [-y nazwa_wyróżniająca_proxy] [-Y] [-Z] [nazwa_wyróżniająca].....
```

### Opis

Komenda **ldapdelete** to interfejs wiersza komend do funkcji API `ldap_delete`.

Komenda **ldapdelete** otwiera połączenie z serwerem LDAP, łączy się i usuwa jedną lub wiele pozycji. Jeśli podano co najmniej jeden argument nazwy wyróżniającej, pozycje z tymi nazwami są usuwane. Każda nazwa wyróżniająca ma postać łańcucha. Jeśli nie podano argumentu nazwy wyróżniającej, lista nazw wyróżniających jest odczytywana ze standardowego wejścia lub z pliku, jeśli użyta zostanie opcja **-i**.

Aby wyświetlić pomoc dotyczącą składni komendy **ldapdelete**, wpisz:

```
ldapdelete -?
```

### Opcje

**-c** Tryb działania ciągłego. Błędy są raportowane, ale komenda **ldapdelete** kontynuuje usuwanie. W przeciwnym razie domyślną operacją jest wyjście po zgłoszeniu błędu.

**-C zestaw\_znaków**

Określa, że nazwy wyróżniające podane jako dane wejściowe w programie narzędziowym **ldapdelete** są przedstawiane w określonym lokalnym zestawie znaków. Opcji **-C zestaw\_znaków** używa się, gdy strona kodowa wejściowego łańcucha znaków różni się od strony kodowej zadania. Opis funkcji API `ldap_set_iconv_local_charset()` zawiera obsługiwane wartości zestawów znaków.

**-d poziom\_debugowania**

Ustawia poziom debugowania LDAP na `poziom_debugowania`.

**-D nazwa\_wyróżniająca\_łączenia**

Parametr ***nazwa\_wyróżniająca\_łączenia*** umożliwia utworzenie łączenia z katalogiem LDAP.

***nazwa\_wyróżniająca\_łączenia*** jest nazwą wyróżniającą w postaci łańcucha znaków. Jeśli używana jest wraz z **-m DIGEST-MD5**, wykorzystywana jest do określenia identyfikatora autoryzacji. Nazwa ta może być nazwą wyróżniającą lub łańcuchem `authzId` rozpoczynającym się od "u:" lub "dn:".

**-f plik** Odczytuje wiersze z pliku, wykonując dla każdego z nich operację usunięcia LDAP. Każdy wiersz powinien zawierać pojedynczą nazwę wyróżniającą.

**-G dziedzina**

Określa dziedzinę. Parametr ten jest opcjonalny. Jeśli używany jest wraz z **-m DIGEST-MD5**, wartość przekazywana jest do serwera podczas połączenia.

**-h host\_ldap**

Określa alternatywnego hosta, na którym działa serwer LDAP.

**-i plik** Odczytuje wiersze z pliku, wykonując dla każdego z nich operację usunięcia LDAP. Każdy wiersz powinien zawierać jedną nazwę wyróżniającą.

**-k** Określa, czy używać elementu sterującego administrowania serwerem.

**-K plik\_kluczy**

Określa nazwę pliku bazy danych kluczy SSL. Jeśli plik bazy danych kluczy nie znajduje się w bieżącym katalogu, należy podać jego nazwę z pełną ścieżką.

Jeśli narzędzie nie może znaleźć bazy danych kluczy, użyje wkompiowanego na stałe zestawu domyślnych zaufanych głównych ośrodków certyfikacji. Plik bazy danych kluczy zazwyczaj zawiera jeden lub więcej certyfikatów ośrodków certyfikacji (CA), do których klient ma zaufanie. Tego typu certyfikaty X.509 zwane są także użytkownikami zaufanymi.

Parametr ten udostępnia opcję **-Z**. W przypadku serwera Directory Server w systemie i5/OS, jeśli użyta została opcja **-Z** i nie użyto opcji **-K** ani **-N**, stosowany będzie certyfikat powiązany z ID aplikacji Directory Services Client.

**-m mechanizm**

Parametr **mechanizm** określa mechanizm SASL używany do łączenia z serwerem. Używana jest funkcja API `ldap_sasl_bind_s()`. Parametr **-m** jest ignorowany, jeśli ustawiony zostanie parametr **-V 2**. Jeśli parametr **-m** nie jest określony, użyte zostanie proste uwierzytelnianie. Poprawne mechanizmy to:

- CRAM-MD5 - chroni hasło wysyłane na serwer.
- EXTERNAL - używa certyfikatu SSL. Wymaga opcji **-Z**.
- GSSAPI - używa referencji Kerberos użytkownika.
- DIGEST-MD5 - wymaga od klienta wysłania do serwera wartości nazwy użytkownika. Wymaga opcji **-U**. Parametr **-D** (zwykle nazwa wyróżniająca łączenia) określa identyfikator autoryzacji. Może być nazwą wyróżniającą lub łańcuchem `authzId` rozpoczynającym się od `u:` lub `dn:`.
- OS400\_PRFTKN - dokonuje uwierzytelnienia na lokalnym serwerze LDAP jako bieżący użytkownik systemu i5/OS za pomocą nazwy wyróżniającej użytkownika w systemowym mechanizmie rzutowania. Nie należy określać parametrów **-D** (nazwy wyróżniającej łączenia) oraz **-w** (hasła).

**-M** Zarządza obiektami odwołania tak jak zwykłymi pozycjami.

**-n** Pokazuje, co byłoby wykonane, ale nie modyfikuje pozycji. Opcja przydatna podczas debugowania w połączeniu z parametrem **-v**.

**-N nazwa\_certyfikatu**

Określa etykietę powiązaną z certyfikatem klienta w pliku 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 może być certyfikat klienta. Parametr **nazwa\_certyfikatu** nie jest wymagany, jeśli określono domyślną parę certyfikat/klucz prywatny. Podobnie parametr **nazwa\_certyfikatu** nie jest wymagany, jeśli w wyznaczonej bazie danych kluczy znajduje się pojedyncza para certyfikat/klucz prywatny. Parametr ten jest ignorowany, gdy nie zostanie podana opcja **-Z** lub **-K**. W przypadku serwera Directory Server w systemie i5/OS, jeśli użyta została opcja **-Z** i nie użyto opcji **-K** ani **-N**, wykorzystany zostanie certyfikat powiązany z identyfikatorem aplikacji Directory Services Client.

**-O maksymalna\_liczba\_przeskoków**

Parametr **maksymalna\_liczba\_przeskoków** określa maksymalną liczbę przeskoków, którą wykona biblioteka klienta podczas przeglądania odwołań. Domyślna liczba przeskoków jest równa 10.

**-p** *port\_ldap*

Określa alternatywny port TCP, na którym serwer LDAP prowadzi nasłuch. Domyślnym portem LDAP jest 389. Jeśli nie podano opcji **-p**, a podano **-Z**, używany jest domyślny port 636 SSL LDAP.

**-P** *hasło\_pliku\_kluczy*

Określa hasło bazy danych kluczy. Hasło to jest wymagane w celu uzyskania dostępu do szyfrowanych informacji w pliku bazy danych kluczy, który może zawierać jeden lub wiele kluczy prywatnych. Jeśli z plikiem bazy danych kluczy jest związany plik ukrytych haseł, hasło jest otrzymywane z niego pliku i parametr **-P** nie jest wymagany. Parametr ten jest ignorowany, gdy nie zostanie podana opcja **-Z** lub **-K**.

**-R** Określa, że odwołania nie mają następować automatycznie.

**-s** Ta opcja służy do usuwania poddrzewa, którego katalogiem głównym jest określona pozycja.

**-U** *nazwa\_użytkownika*

Określa nazwę użytkownika. Wymagane w przypadku określenia opcji **-m** DIGEST-MD5 i ignorowane w przypadku pozostałych mechanizmów.

**-v** Używa trybu szczegółowego z wieloma komunikatami diagnostycznymi wysyłanymi na wyjście standardowe.

**-V** *wersja*

Określa wersję LDAP używaną przez komendę **ldapdelete** podczas łączenia się z serwerem LDAP.

Domyślnie nawiązywane jest połączenie LDAP V3. Aby jawnie wybrać LDAP V3, należy podać wartość **-V 3**. Aby uruchomić jako aplikację LDAP V2, należy podać **-V 2**.

**-w** *hasło | ?*

Do uwierzytelniania zostanie użyte podane **hasło**. Podanie wartości **?** spowoduje wywołanie zachęty do wpisania hasła.

**-y** *nazwa\_wyróżniająca\_proxy*

Ustawia ID proxy dla działania autoryzacji proxy.

**-Y** Używa bezpiecznego połączenia LDAP (TLS).

**-Z** Używa bezpiecznego połączenia SSL w komunikacji z serwerem LDAP. W przypadku serwera Directory Server w systemie i5/OS, jeśli użyta została opcja **-Z** i nie użyto opcji **-K** ani **-N**, wykorzystany zostanie certyfikat powiązany z identyfikatorem aplikacji Directory Services Client.

**dn** Określa jeden lub kilka argumentów nazwy wyróżniającej. Każda nazwa wyróżniająca powinna mieć postać łańcucha.

## Przykłady

Następująca komenda:

```
ldapdelete -D cn=adminstrator -w sekret "cn=Usuń mnie, o=University of Life, c=US"
```

próbuje usunąć pozycję o nazwie zwykłej "Usuń mnie", znajdującą się bezpośrednio pod pozycją organizacyjną University of Life.

## Uwagi

Jeśli nie podano żadnych argumentów nazwy wyróżniającej, komenda **ldapdelete** czeka na odczytanie listy nazw wyróżniających.

## Diagnostyka

Jeśli nie wystąpiły żadne błędy, statusem wyjścia jest 0. Wystąpienie błędu powoduje zwrócenie niezerowego statusu wyjścia i wypisanie komunikatu diagnostycznego na standardowe wyjście błędów.

### Pojęcia pokrewne

Funkcje API serwera Directory Server

## Idapexop

Program narzędziowy wiersza komend do operacji rozszerzonych LDAP.

### Składnia

```
ldapexop [-C zestaw_znaków] [-d poziom_debugowania] [-D nazwa_wyróżniająca_łączenia] [-e] [-G dziedzina]
[-h host_ldap] [-pomoc] [-K plik_kluczy] [-m mechanizm] [-N nazwa_certyfikatu]
[-p port_ldap]
[-P hasło_pliku_kluczy] [-?] [-U] [-v] [-w hasło | ?] [-Y] [-Z]
-op {cascrepl | controlqueue | controlrepl | getAttributes |
getusertype | quiesce | readconfig | uniqueattr}
```

### Opis

Komenda **ldapexop** umożliwia powiązanie z serwerem katalogów i wykonanie pojedynczej rozszerzonej operacji z danymi składającymi się na rozszerzoną wartość operacji.

Narzędzie **ldapexop** obsługuje standardowe opcje hosta, portu, SSL i uwierzytelniania używane przez wszystkie narzędzia klienckie LDAP. Poza tym zdefiniowano zestaw opcji do określenia operacji, która ma zostać wykonana, oraz argumenty dla każdej rozszerzonej operacji.

Aby wyświetlić pomoc dotyczącą składni komendy **ldapexop**, wpisz:

```
ldapexop -?
```

lub

```
ldapexop -help
```

### Opcje

Opcje komendy **ldapexop** są podzielone na dwie kategorie:

1. Ogólne opcje określające sposób łączenia się z serwerem katalogów. Opcje te należy określać przed opcjami specyficznymi dla operacji.
2. Rozszerzone opcje operacji określające rozszerzoną operację, która ma być wykonana.

### Ogólne opcje

Opcje te określają metody łączenia się z serwerem i należy je zdefiniować przed opcją **-op**.

#### **-C** *zestaw\_znaków*

Określa, że nazwy wyróżniające podane jako dane wejściowe w programie narzędziowym **ldapexop** są przedstawiane w określonym lokalnym zestawie znaków. Opcji **-C** *zestaw\_znaków* używa się, gdy strona kodowa wejściowego łańcucha znaków różni się od strony kodowej zadania. Opis funkcji API `ldap_set_iconv_local_charset()` zawiera obsługiwane wartości zestawów znaków.

#### **-d** *poziom\_debugowania*

Ustawia poziom debugowania LDAP na *poziom\_debugowania*.

#### **-D** *nazwa\_wyróżniająca\_łączenia*

Parametr *nazwa\_wyróżniająca\_łączenia* umożliwia utworzenie łączenia z katalogiem LDAP. *nazwa\_wyróżniająca\_łączenia* jest nazwą wyróżniającą w postaci łańcucha znaków. Jeśli używana jest wraz z **-m** DIGEST-MD5, wykorzystywana jest do określenia identyfikatora autoryzacji. Nazwa ta może być nazwą wyróżniającą lub łańcuchem `authzId` rozpoczynającym się od "u:" lub "dn:".

**-e** Wyświetla informacje o wersji biblioteki LDAP i kończy pracę.

**-G** Określa dziedzinę. Parametr ten jest opcjonalny. Jeśli używany jest wraz z **-m** DIGEST-MD5, wartość przekazywana jest do serwera podczas połączenia.

#### **-h** *host\_ldap*

Określa alternatywnego hosta, na którym działa serwer LDAP.



**-help** Wyświetla składnię komendy i informacje o użyciu.

**-K** *plik\_kluczy*

Określa nazwę pliku bazy danych kluczy SSL. Jeśli plik bazy danych kluczy nie znajduje się w bieżącym katalogu, należy podać jego nazwę z pełną ścieżką.

Jeśli narzędzie nie może zlokalizować bazy danych kluczy, zostanie użyta systemowa baza danych kluczy. Plik bazy danych kluczy zazwyczaj zawiera jeden lub więcej certyfikatów ośrodków certyfikacji (CA), do których klient ma zaufanie. Tego typu certyfikaty X.509 zwane są także użytkownikami zaufanymi.

Parametr ten udostępnia opcję **-Z**. W przypadku serwera Directory Server w systemie i5/OS, jeśli użyta została opcja **-Z** i nie użyto opcji **-K** ani **-N**, wykorzystany zostanie certyfikat powiązany z identyfikatorem aplikacji Directory Services Client.

**-m** *mechanizm*

Parametr **mechanizm** określa mechanizm SASL używany do łączenia z serwerem. Używana jest funkcja API `ldap_sasl_bind_s()`. Parametr **-m** jest ignorowany, jeśli ustawiony zostanie parametr **-V 2**. Jeśli parametr **-m** nie jest określony, użyte zostanie proste uwierzytelnianie. Poprawne mechanizmy to:

- CRAM-MD5 - chroni hasło wysyłane na serwer.
- EXTERNAL - używa certyfikatu SSL. Wymaga opcji **-Z**.
- GSSAPI - używa referencji Kerberos użytkownika.
- DIGEST-MD5 - wymaga od klienta wysłania do serwera wartości nazwy użytkownika. Wymaga opcji **-U**. Parametr **-D** (zwykle nazwa wyróżniająca łączenia) określa identyfikator autoryzacji. Może być nazwą wyróżniającą lub łańcuchem `authzId` rozpoczynającym się od `u:` lub `dn:`.
- OS400\_PRFTKN - dokonuje uwierzytelnienia na lokalnym serwerze LDAP jako bieżący użytkownik systemu i5/OS za pomocą nazwy wyróżniającej użytkownika w systemowym mechanizmie rzutowania. Nie należy określać parametrów **-D** (nazwy wyróżniającej łączenia) oraz **-w** (hasła).

**-N** *nazwa\_certyfikatu*

Określa etykietę powiązaną z certyfikatem klienta w pliku 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 może być certyfikat klienta. Parametr **nazwa\_certyfikatu** nie jest wymagany, jeśli określono domyślną parę certyfikat/klucz prywatny. Podobnie parametr **nazwa\_certyfikatu** nie jest wymagany, jeśli w wyznaczonej bazie danych kluczy znajduje się pojedyncza para certyfikat/klucz prywatny. Parametr ten jest ignorowany, gdy nie zostanie podana opcja **-Z** lub **-K**. W przypadku serwera Directory Server w systemie i5/OS, jeśli użyta została opcja **-Z** i nie użyto opcji **-K** ani **-N**, wykorzystany zostanie certyfikat powiązany z identyfikatorem aplikacji Directory Services Client.

**-p** *port\_ldap*

Określa alternatywny port TCP, na którym serwer LDAP prowadzi nasłuch. Domyślnym portem LDAP jest 389. Jeśli nie podano opcji **-p**, a podano **-Z**, używany jest domyślny port 636 SSL LDAP.

**-P** *hasło\_pliku\_kluczy*

Określa hasło bazy danych kluczy. Hasło to jest wymagane w celu uzyskania dostępu do szyfrowanych informacji w pliku bazy danych kluczy, który może zawierać jeden lub wiele kluczy prywatnych. Jeśli z plikiem bazy danych kluczy jest związany plik ukrytych haseł, hasło jest otrzymywane z niego pliku i parametr **-P** nie jest wymagany. Parametr ten jest ignorowany, gdy nie zostanie podana opcja **-Z** lub **-K**.

**-?** Wyświetla składnię komendy i informacje o użyciu.

**-U** Określa nazwę użytkownika. Wymagane w przypadku określenia opcji **-m DIGEST-MD5** i ignorowane w przypadku pozostałych mechanizmów.

**-v** Używa trybu szczegółowego z wieloma komunikatami diagnostycznymi wysyłanymi na wyjście standardowe.

**-w** *hasło | ?*

Do uwierzytelniania zostanie użyte podane **hasło**. Podanie wartości **?** spowoduje wywołanie zachęty do wpisania hasła.

**-Y** Używa bezpiecznego połączenia LDAP (TLS).

- Z Używa bezpiecznego połączenia SSL w komunikacji z serwerem LDAP. W przypadku serwera Directory Server w systemie i5/OS, jeśli użyta została opcja -Z i nie użyto opcji -K ani -N, wykorzystany zostanie certyfikat powiązany z identyfikatorem aplikacji Directory Services Client.

## Opcja rozszerzonych operacji

Opcja **-op** określa rozszerzoną operację, która ma być wykonana. Rozszerzona operacja może mieć jedną z następujących wartości:

- **acctstatus**: operacja rozszerzona statusu konta. Wyświetla status określonego konta.  
| ldapexop -op acctstatus -d <nazwa\_wyróżniająca>  
|  
| -d nazwa\_wyróżniająca  
| Określa nazwę wyróżniającą pozycji, dla której ma być pobrany status konta.  
| Możliwe statusy konta to otwarte (open), zablokowane (locked) lub wygasłe (expired).
- **cascrepl**: kaskadowe sterowanie replikacją. Żądana operacja dotyczy określonego serwera i jest także przekazywana do wszystkich replik w danym poddrzewie. Jeśli któraś z nich jest replika przekazująca, to wykonuje ona operację rozszerzoną na wszystkich swoich replikach. Operacja tworzy kaskadę dla całej topologii replikacji.

### **-action quiesce | unquiesce | replnow | wait**

Ten atrybut jest wymagany i określa działanie do wykonania.

#### **quiesce**

Kolejne aktualizacje są zabronione z wyjątkiem replikacji.

#### **unquiesce**

Wznowienie normalnej operacji, akceptowane są aktualizacje klienta.

#### **replnow**

Natychmiast replikuje wszystkie zmiany w kolejce do wszystkich serwerów replik, bez względu na harmonogram.

**wait** Czeka na replikację wszystkich aktualizacji w replikach.

### **-rc nazwa\_wyróżniająca\_kontekstu**

To jest atrybut wymagany określający katalog główny poddrzewa.

### **-timeout sekundy**

Ten atrybut jest opcjonalny. Jeśli został zdefiniowany, określa limit czasu w sekundach. Jeśli go nie podano lub wpisano 0, operacja oczekuje w nieskończoność.

### **Przykład:**

```
ldapexop -op cascrepl -action -quiesce -rc "o=acme,c=us" -timeout 60
```

- **clearlog | getlogsize | readlog -log ...**  
| Te trzy operacje umożliwiają obsługę nowego pliku protokołu:  
| LostAndFound  
| Operacje te mogą być używane z serwerem katalogów i5/OS (wersja V6R1 i późniejsze), ale obsługiwane są tylko określone typy plików protokołu:  
| LostAndFound – plik protokołu niedokończonych operacji.
  - **controlqueue**: steruje kolejką replikacji. Ta operacja umożliwia usunięcie oczekujących zmian z listy zmian replikacji znajdujących się kolejce, a które nie zostały wykonane z powodu awarii replikacji. Operacja ta przydaje się, gdy dane repliki są definiowane ręcznie. Następnie można jej użyć do pominięcia niektórych awarii w kolejce.
- skip all | ID\_zmiany**  
Ten atrybut jest wymagany.
- wartość **-skip all** określa pominięcie wszystkich oczekujących zmian dla tej umowy.
  - **ID\_zmiany** określa pojedynczą zmianę do pominięcia. Jeśli serwer nie replikuje w danej chwili tej zmiany, żądanie zakończy się niepowodzeniem.

**-ra nazwa\_wyróżniająca\_umowy**

To jest atrybut wymagany określający nazwę wyróżniającą umowy replikacji.

**Przykłady:**

```
ldapexop -op controlqueue -skip all -ra "cn=serwer3,  
ibm-replicaSubentry=master1-id,ibm-replicaGroup=default,  
o=acme,c=us"
```

```
ldapexop -op controlqueue -skip 2185 -ra "cn=serwer3,  
ibm-replicaSubentry=master1-id,ibm-replicaGroup=default,  
o=acme,c=us"
```

- **controlrepl:** steruje replikacją.

**-action suspend | resume | replnow**

Ten atrybut jest wymagany i określa działanie do wykonania.

**-rc nazwa\_wyróżniająca\_kontekstu | -ra nazwa\_wyróżniająca\_umowy**

Opcja **-rc nazwa\_wyróżniająca\_kontekstu** określa nazwę wyróżniającą kontekstu replikacji. Operacja jest wykonywana dla wszystkich umów dla tego kontekstu. Opcja **-ra nazwa\_wyróżniająca\_umowy** określa nazwę wyróżniającą umowy replikacji. Operacja jest wykonywana dla określonej umowy replikacji.

**Przykład:**

```
ldapexop -op controlrepl -action suspend -ra "cn=serwer3,  
ibm-replicaSubentry=master1-id,ibm-replicaGroup=default,  
o=acme,c=us"
```

- **controlreplerr**

Operacja rozszerzona controlreplerr umożliwia zarządzanie tabelą błędów replikacji na serwerze i5/OS V6R1 (lub IBM Tivoli Directory Server v6.0) oraz wersjach późniejszych. Dostępne opcje to:

```
ldapexop -op controlreplerr -show <identyfikator_błędu> -ra <nazwa_wyróżniająca_umowy>
```

Umożliwia przeglądanie pozycji w tabeli błędów replikacji.

**<identyfikator\_błędu>**

Identyfikator błędu. Podanie wartości 0 spowoduje wyświetlenie wszystkich pozycji.

**<nazwa\_wyróżniająca\_umowy>**

Umowa replikacji, z którą powiązana jest pozycja.

```
ldapexop -op controlreplerr -delete <identyfikator_błędu> -ra <nazwa_wyróżniająca_umowy>
```

Umożliwia usuwanie pozycji z tabeli błędów replikacji.

**<identyfikator\_błędu>**

Identyfikator błędu. Podanie wartości 0 spowoduje wyświetlenie wszystkich pozycji.

**<nazwa\_wyróżniająca\_umowy>**

Umowa replikacji, z którą powiązana jest pozycja.

```
ldapexop -op controlreplerr -retry <identyfikator_błędu> -ra <nazwa_wyróżniająca_umowy>
```

Umożliwia ponowienie operacji określonej przez pozycję w tabeli błędów replikacji.

**<identyfikator\_błędu>**

Identyfikator błędu. Podanie wartości 0 spowoduje wyświetlenie wszystkich pozycji.

**<nazwa\_wyróżniająca\_umowy>**

Umowa replikacji, z którą powiązana jest pozycja.

- **evaluateGroups**

Program narzędziowy ldapexop obsługuje nową operację evaluateGroups:

```
ldapexop -op evaluateGroups -d <nazwa_wyróżniająca_użytkownika> \  
-a <lista rozdzielanych spacjami par atrybutów i wartości>
```

Umożliwia wyświetlenie listy grup, do których należy określona nazwa\_wyróżniająca\_użytkownika.

Opcja "-a" umożliwia określenie wartości atrybutów pozycji oraz pobranie grup dynamicznych, które odpowiadają pozycji. Jeśli opcja "-a" nie zostanie podana, żądanie zostanie przesłane do serwera wyłącznie w odniesieniu do

| grup statycznych. Ta operacja rozszerzona służy do pobierania informacji o przynależności do grupy dla nazwy  
| wyróżniającej użytkownika, która nie istnieje na serwerze (na przykład gdy odpowiada ona zdalnemu członkowi  
| grupy). Do wyświetlenia informacji o przynależności do grup na serwerze zawierającym podaną nazwę  
| wyróżniającą użytkownika służy atrybut operacyjny `ibm-allGroups`.

| **Przykład:**

| Sprawdzenie przynależności do grupy dla pozycji `uid=przykład,cn=users,o=ibm` na podstawie wartości atrybutów  
| `departmentnumber` i `objectclass` pozycji:

| `ldapexop -op evaluateGroups -d uid=przykład,cn=users,o=ibm -a objectclass=person`  
| `departmentnumber=abc`

| **Uwaga:** Do takiej operacji rozszerzonej przekazywane są najczęściej wszystkie wartości atrybutów dotyczących  
| przedmiotowej pozycji.

- **getattributes -attrType<typ> -matches bool<wartość>**

**-attrType {operational | language\_tag | attribute\_cache | unique | configuration}**

To jest atrybut wymagany określający typ żadanego atrybutu.

**-matches bool {true | false}**

Określa zgodność listy zwróconych atrybutów z typem atrybutu określonym przez opcję `-attrType<`.

**Przykład:**

`ldapexop -op getattributes -attrType unique -matches bool true`

Zwraca listę wszystkich atrybutów określonych jako unikalne.

`ldapexop -op getattributes -attrType unique -matches bool false`

Zwraca listę wszystkich atrybutów, które nie zostały określone jako unikalne.

- **getusertype:** żądanie rozszerzonej operacji typu użytkownika

Ta rozszerzona operacja zwraca typ użytkownika w oparciu o przypisaną nazwę wyróżniającą.

**Przykład:**

`ldapexop - D <nazwa_wyróżniająca_administratora> -w <hasło_administratora> -op getusertype`  
zwraca:

User : root\_administrator

Role(s) : server\_config\_administrator directory\_administrator

| User : global\_admin\_group\_member

| Role(s) : directory\_administrator

- **quiesce:** wygaszenie lub cofnięcie wygaszenia replikacji poddrzewa.

**-rc nazwa\_wyróżniająca\_kontekstu**

To jest atrybut wymagany określający nazwę wyróżniającą kontekstu replikacji (poddrzewa), która ma być wygaszona lub której wygaszenie ma być cofnięte.

**-end** Opcjonalny atrybut określający cofnięcie wygaszenia poddrzewa. Jeśli nie podano inaczej, domyślnym działaniem jest wygaszenie poddrzewa.

**Przykłady:**

`ldapexop -op quiesce -rc "o=acme,c=us"`

`ldapexop -op quiesce -end -rc "o=ibm,c=us"`

- **readconfig:** ponowne odczytanie pliku konfiguracyjnego.

**-scope entire | single<nazwa\_wyróżniająca\_pozycji><atrybut>**

Ten atrybut jest wymagany.

– **entire** określa ponowne odczytanie całego pliku konfiguracyjnego.

– **single** oznacza odczytanie pojedynczej pozycji i podanego atrybutu.

**Przykłady:**

```
ldapexop -op readconfig -scope entire
```

```
ldapexop -op readconfig -scope single "cn=configuration" ibm-slapdAdminPW
```

**Uwaga:** Poniższe pozycje oznaczone za pomocą:

- <sup>1</sup> są wykonywane natychmiast po odczytaniu konfiguracji
- <sup>2</sup> są wykonywane w nowej operacji
- <sup>3</sup> są wykonywane zaraz po zmianie hasła (nie jest wymagane odczytanie konfiguracji)
- <sup>4</sup> są obsługiwane przez ten sam program narzędziowy wiersza komend w systemie i5/OS, ale nie są obsługiwane przez serwer Directory Server w systemie operacyjnym i5/OS

```
cn=Configuration  
ibm-slapdadmin2  
ibm-slapdadminpw2, 3  
ibm-slapderrorlog1, 4  
ibm-slapdpwencryption1  
ibm-slapdsizelimit1  
ibm-slapdsysloglevel1, 4  
ibm-slapdtimelimit1
```

```
cn=Front End, cn=Configuration  
ibm-slapdaclcache1  
ibm-slapdaclcachesize1  
ibm-slapdentrycachesize1  
ibm-slapdfiltercachebypasslimit1  
ibm-slapdfiltercachesize1  
ibm-slapdidletimeout1
```

```
cn=Event Notification, cn=Configuration  
ibm-slapdmaxeventspersconnection2  
ibm-slapdmaxeventstotal2
```

```
cn=Transaction, cn=Configuration  
ibm-slapdmaxnumoftransactions2  
ibm-slapdmaxoppertransaction2  
ibm-slapdmaxtimelimitoftransactions2
```

```
cn=ConfigDB, cn=Config Backends, cn=IBM SecureWay, cn=Schemas, cn=Configuration  
ibm-slapdreadonly2
```

```
cn=Directory, cn=RDBM Backends, cn=IBM SecureWay, cn=Schemas, cn=Configuration  
ibm-slapdbulkloaderrors1, 4  
ibm-slapdclierrors1, 4  
ibm-slapdpagedresallownonadmin2  
ibm-slapdpagedreslmt2  
ibm-slapdpagesizelmt2  
ibm-slapdreadonly2  
ibm-slapdsortkeylimit2  
ibm-slapdsortsrchallownonadmin2  
ibm-slapdsuffix2
```

| • **repltopology -rc [opcje]:**

| operacja rozszerzona repltopology służy do dopasowania danych topologii replikacji na serwerze odbierającym do topologii na serwerze wysyłającym.

| ldapexop -op repltopology -rc [-timeout sekundy] [-ra nazwa\_wyróżniająca\_umowy]

| gdzie

| **-rc nazwa\_wyróżniająca\_kontekstu**

| To jest atrybut wymagany określający katalog główny poddrzewa.

| **-timeout sekundy**

| Ten atrybut jest opcjonalny. Jeśli został zdefiniowany, określa limit czasu w sekundach. Jeśli go nie podano lub wpisano 0, operacja oczekuje w nieskończoność.

### **-ra nazwa\_wyróżniająca\_umowy**

Opcja **-ra nazwa\_wyróżniająca\_umowy** określa nazwę wyróżniającą umowy replikacji. Operacja jest wykonywana dla określonej umowy replikacji. Jeśli opcja **-ra** nie zostanie podana, operacja zostanie wykonana dla wszystkich umów replikacji zdefiniowanych w ramach kontekstu.

### **Przykład:**

```
ldapexop -op repltopology -rc "o=acme,c=us" -ra "cn=server3,  
ibm-replicaSubentry=master1-id,ibm-replicaGroup=default,  
o=acme,c=us"-timeout 60
```

Serwer wysyłający tworzy powiązanie z serwerem odbierającym na podstawie skonfigurowanych referencji replikacji. Nazwy wyróżniające serwerów wysyłających mają uprawnienia do dodawania przyrostków do konfiguracji serwerów odbierających (replik). Możliwość ta jest wykorzystywana przez serwer wysyłający w ramach operacji rozszerzonej Replication Topology (Topologia replikacji) w celu dodawania brakujących przyrostków do serwera odbierającego. Nazwy wyróżniające serwerów wysyłających mają też uprawnienia do tworzenia nowego, zreplikowanego poddrzewa w przypadku przyrostków, dla których nie istnieje pozycja contextDN (nazwa wyróżniająca kontekstu). Jeśli pozycja contextDN już istnieje, musi być uprzednio zdefiniowana jako element główny zreplikowanego poddrzewa, tzn. jej klasą obiektu musi być `ibm-replicationcontext`.

- **unbind** {**-dn**<określona\_nazwa\_wyróżniająca>|**-ip**<adres\_IP\_źródła>|**-dn**<określona\_nazwa\_wyróżniająca>**-ip**<adres\_IP\_źródła>|**all**}

rozłącza połączenia oparte na nazwie wyróżniającej, adresie IP, DN/IP lub rozłącza wszystkie połączenia. Wszystkie bezczynne połączenia oraz wszystkie połączenia zawierające działania znajdujące się w kolejce roboczej zostaną natychmiast zakończone. Jeśli w połączeniu działa aktualnie proces roboczy, zostanie ono zakończone po zakończeniu działania przez proces roboczy.

#### **-dn**<określona\_nazwa\_wyróżniająca>

Wprowadza żądanie zakończenia połączenia wyłącznie według nazwy wyróżniającej. W rezultacie wszystkie połączenia oparte na określonej nazwie wyróżniającej zostaną usunięte.

#### **-ip**<adres\_IP\_źródła>

Wprowadza żądanie zakończenia połączenia wyłącznie według adresu IP. W rezultacie wszystkie połączenia pochodzące z określonego źródła IP zostaną usunięte.

#### **-dn**<określona\_nazwa\_wyróżniająca> **-ip**<adres\_IP\_źródła>

Wysyła żądanie zakończenia połączenia określonego przez parę nazwa wyróżniająca/adres IP. W rezultacie wszystkie połączenia oparte na określonej nazwie wyróżniającej i pochodzące z określonego źródła IP zostaną usunięte.

**-all** Wprowadza żądanie zakończenia wszystkich połączeń. W rezultacie wszystkie połączenia za wyjątkiem tego, w którym żądanie zostało wystawione, zostaną usunięte. Atrybut ten nie może zostać użyty wraz z atrybutami **-D** lub **-IP**.

### **Przykłady:**

```
ldapexop -op unbind -dn cn=john  
ldapexop -op unbind -ip 9.182.173.43  
ldapexop -op unbind -dn cn=john -ip 9.182.173.43  
ldapexop -op unbind -all
```

- **uniqueattr -a <typ\_atributu>**: identyfikuje wszystkie wartości nieunikalne dla określonego atrybutu.

#### **-a** <atribut>

Określa atrybut, dla którego wszystkie wartości sprzeczne zostaną wyświetlone.

**Uwaga:** Wartości podwójne dla atrybutów binarnych, wykonawczych i konfiguracyjnych, a także dla atrybutu klasy obiektu nie zostaną wyświetlone. Atrybuty te są rozszerzonymi operacjami nieobsługiwanymi dla atrybutów unikalnych.

### **Przykład:**

```
ldapexop -op uniqueattr -a "uid"
```

Dodaje następujący wiersz do pliku konfiguracyjnego w pozycji "cn=Directory,cn=RDBM Backends,cn=IBM Directory,cn=schema,cn=Configuration" dla poniższej operacji rozszerzonej:

```
ibm-slapdPlugin: extendedop /QSYS.LIB/QGLDRDBM.SRVPGM initUniqueAttr
```

## Diagnostyka

Jeśli nie wystąpiły żadne błędy, statusem wyjścia jest 0. Wystąpienie błędu powoduje zwrócenie niezerowego statusu wyjścia i wypisanie komunikatu diagnostycznego na standardowe wyjście błędów.

### Pojęcia pokrewne

Funkcje API serwera Directory Server

“Tabela błędów replikacji” na stronie 43

W tabeli błędów replikacji protokołowane są niepowodzenia aktualizacji w celu późniejszego odtwarzania. Po rozpoczęciu replikacji liczona jest liczba zaprotokołowanych niepowodzeń dla każdej umowy replikacji. Gdy aktualizacja zakończy się niepowodzeniem, liczba ta jest zwiększana, a do tabeli dodawana jest nowa pozycja.

### Zadania pokrewne

“Wyświetlanie pliku protokołu niedokończonych operacji” na stronie 166

Plik protokołu niedokończonych operacji replikowania można wyświetlić za pomocą narzędzia IBM Tivoli Directory Server Web Administration lub opcji pliku protokołu w programie narzędziowym ldapexop. Plik protokołu można też przeglądać bezpośrednio.

## ldapmodrdn

Program narzędziowy wiersza komend do modyfikowania pozycji z nazwami RDN.

### Składnia

```
ldapmodrdn [-c] [-C zestaw_znaków] [-d poziom_debugowania] [-D nazwa_wyróżniająca_łączenia]
[-f plik] [-G dziedzina] [-h host_ldap] [-i plik] [-k] [-K plik_kluczy]
[-m mechanizm] [-M] [-n]
[-N nazwa_certyfikatu] [-O liczba_przeskoków]
[-p port_ldap] [-P hasło_pliku_kluczy] [-r] [-R]
[-U nazwa_użytkownika] [-v] [-V wersja]
[-w hasło | ?] [-y nazwa_wyróżniająca_proxy] [-Y] [-Z]
[dn nowa_nazwa_rdn | [-i plik]]
```

### Opis

- | Komenda **ldapmodrdn** to interfejs wiersza komend do funkcji API ldap\_rename.
- | Komenda **ldapmodrdn** otwiera połączenie z serwerem LDAP, łączy się i przenosi pozycje lub zmienia ich nazwy.
- | Informacje o pozycji są odczytywane z wejścia standardowego, z pliku za pomocą opcji **-f** lub z pary dn i rdn wiersza komend. Gdy opcja **-s** jest używana do przenoszenia pozycji, ma ona zastosowanie do wszystkich pozycji, na których jest wykonywana komenda.

Aby wyświetlić pomoc dotyczącą składni komendy **ldapmodrdn**, wpisz:

```
ldapmodrdn -?
```

### Opcje

**-c** Tryb działania ciągłego. Błędy są zgłaszane, ale komenda **ldapmodrdn** nadal wprowadza zmiany. W przeciwnym razie domyślną operacją jest wyjście po zgłoszeniu błędu.

**-C zestaw\_znaków**

Określa, że łańcuchy podane jako dane wejściowe w programie narzędziowym **ldapmodrdn** są przedstawiane w określonym lokalnym zestawie znaków. Opcji **-C zestaw\_znaków** używa się, gdy strona kodowa wejściowego łańcucha znaków różni się od strony kodowej zadania. Opis funkcji API ldap\_set\_iconv\_local\_charset() zawiera obsługiwane wartości zestawu znaków. Należy zauważyć, że obsługiwane wartości zestawu znaków są tymi samymi wartościami, które są obsługiwane dla znacznika zestawu znaków opcjonalnie zdefiniowanego w plikach LDIF w wersji 1.

**-d poziom\_debugowania**

Ustawia poziom debugowania LDAP na poziom\_debugowania.

**-D** *nazwa\_wyróżniająca\_łączenia*

Parametr *nazwa\_wyróżniająca\_łączenia* umożliwia utworzenie łączenia z katalogiem LDAP.

*nazwa\_wyróżniająca\_łączenia* powinna być nazwą wyróżniającą w postaci łańcucha znaków. Jeśli używana jest wraz z -m DIGEST-MD5, wykorzystywana jest do określenia identyfikatora autoryzacji. Nazwa ta może być nazwą wyróżniającą lub łańcuchem authzId rozpoczynającym się od "u:" lub "dn:".

**-f** *plik* Odczytuje dane o modyfikacjach pozycji z pliku LDIF zamiast ze standardowych danych wejściowych lub wiersza komend (przez określenie nazwy\_wyróżniającej lub nowej\_nazwy\_rdn). Standardowe dane wejściowe mogą być także dostarczane z pliku (< plik).

**-G** *dziedzina*

Określa dziedzinę. Parametr ten jest opcjonalny. Jeśli używany jest wraz z -m DIGEST-MD5, wartość przekazywana jest do serwera podczas połączenia.

**-h** *host\_ldap*

Określa alternatywny host, na którym działa serwer ldap.

**-i** *plik* Odczytuje dane na temat modyfikacji pozycji z pliku zamiast z wejścia standardowego lub wiersza komend (parametr rdn i newrdn). Wejście standardowe można także umieścić w pliku, podając ("*< file*").

**-k** Określa, czy używać elementu sterującego administrowania serwerem.

**-K** *plik\_kluczy*

Określa nazwę pliku bazy danych kluczy SSL. Jeśli plik bazy danych kluczy nie znajduje się w bieżącym katalogu, należy podać jego nazwę z pełną ścieżką.

Jeśli narzędzie nie może znaleźć bazy danych kluczy, użyje skompilowanego na stałe zestawu domyślnych zaufanych głównych ośrodków certyfikacji. Plik bazy danych kluczy zazwyczaj zawiera jeden lub więcej certyfikatów ośrodków certyfikacji (CA), do których klient ma zaufanie. Tego typu certyfikaty X.509 zwane są także użytkownikami zaufanymi.

Parametr ten udostępnia opcję **-Z**. W przypadku serwera Directory Server w systemie i5/OS, jeśli użyta została opcja **-Z** i nie użyto opcji **-K** ani **-N**, wykorzystany zostanie certyfikat powiązany z identyfikatorem aplikacji Directory Services Client.

**-m** *mechanizm*

Parametr *mechanizm* określa mechanizm SASL używany do łączenia z serwerem. Używana jest funkcja API ldap\_sasl\_bind\_s(). Parametr **-m** jest ignorowany, jeśli ustawiony zostanie parametr **-V 2**. Jeśli parametr **-m** nie jest określony, użyte zostanie proste uwierzytelnianie. Poprawne mechanizmy to:

- CRAM-MD5 - chroni hasło wysyłane na serwer.
- EXTERNAL - używa certyfikatu SSL. Wymaga opcji **-Z**.
- GSSAPI - używa referencji Kerberos użytkownika.
- DIGEST-MD5 - wymaga od klienta wysłania do serwera wartości nazwy użytkownika. Wymaga opcji **-U**. Parametr **-D** (zwykle nazwa wyróżniająca łączenia) określa identyfikator autoryzacji. Może być nazwą wyróżniającą lub łańcuchem authzId rozpoczynającym się od u: lub dn:.
- OS400\_PRFTKN - dokonuje uwierzytelnienia na lokalnym serwerze LDAP jako bieżący użytkownik systemu i5/OS za pomocą nazwy wyróżniającej użytkownika w systemowym mechanizmie rzutowania. Nie należy określać parametrów **-D** (nazwy wyróżniającej łączenia) oraz **-w** (hasła).

**-M** Zarządza obiektami odwołania tak jak zwykłymi pozycjami.

**-n** Pokazuje, co byłoby wykonane, ale nie modyfikuje pozycji. Opcja przydatna podczas debugowania w połączeniu z parametrem **-v**.

**-N** *nazwa\_certyfikatu*

Określa etykietę powiązaną z certyfikatem klienta w pliku 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 może być certyfikat klienta. Parametr *nazwa\_certyfikatu* nie jest wymagany, jeśli określono domyślną parę certyfikat/klucz prywatny. Podobnie parametr *nazwa\_certyfikatu* nie jest wymagany, jeśli w wyznaczonej bazie danych kluczy znajduje się pojedyncza para certyfikat/klucz prywatny. Parametr ten jest ignorowany, gdy nie zostanie podana opcja **-Z**



lub **-K**. W przypadku serwera Directory Server w systemie i5/OS, jeśli użyta została opcja **-Z** i nie użyto opcji **-K** ani **-N**, wykorzystany zostanie certyfikat powiązany z identyfikatorem aplikacji Directory Services Client.

**-O liczba\_przeskoków**

Parametr **liczba\_przeskoków** określa maksymalną liczbę przeskoków, którą wykona biblioteka klienta podczas przeglądania odwołań. Domyślna liczba przeskoków jest równa 10.

**-p port\_ldap**

Określa alternatywny port TCP, na którym serwer ldap prowadzi nasłuch. Domyślnym portem LDAP jest 389. Jeśli go nie podano tej opcji, a podano **-Z**, używany jest domyślny port 636 SSL LDAP.

**-P hasło\_pliku\_kluczy**

Określa hasło bazy danych kluczy. Hasło to jest wymagane w celu uzyskania dostępu do szyfrowanych informacji w pliku bazy danych kluczy, który może zawierać jeden lub wiele kluczy prywatnych. Jeśli z plikiem bazy danych kluczy jest związany plik ukrytych haseł, hasło jest otrzymywane z niego pliku i parametr **-P** nie jest wymagany. Parametr ten jest ignorowany, gdy nie zostanie podana opcja **-Z** lub **-K**.

**-r** Usuwa stare wartości nazw RDN z pozycji. Domyślnie stare wartości są zachowywane.

**-R** Określa, że odwołania nie mają następować automatycznie.

**-s nowa\_pozycja\_nadrzędna**

Określa nazwę wyróżniającą nowej pozycji nadrzędnej, pod którą zostanie przemieszczona pozycja ze zmienioną nazwą. Argumentem **nowa\_pozycja\_nadrzędna** może być łańcuch o zerowej długości (**-s ""**).

**Uwaga:** Opcja nowej pozycji nadrzędnej nie jest obsługiwana w przypadku łączenia się z serwerem w wersji wcześniejszej niż V6R1 (ITDS v6.0). Opcja ta jest poprawna wyłącznie w przypadku pozycji liścia.

**-U nazwa\_użytkownika**

Określa nazwę użytkownika. Wymagane w przypadku określenia opcji **-m DIGEST-MD5** i ignorowane w przypadku pozostałych mechanizmów.

**-v** Używa trybu szczegółowego z wieloma komunikatami diagnostycznymi wysyłanymi na wyjście standardowe.

**-V wersja**

Określa wersję LDAP używaną przez komendę **ldapmodrdn** podczas łączenia się z serwerem LDAP. Domyślnie nawiązywane jest połączenie LDAP V3. Aby jawnie wybrać LDAP V3, należy podać wartość **-V 3**. Aby uruchomić jako aplikację LDAP V2, należy podać **-V 2**. Aplikacja, na przykład **ldapmodrdn**, wybiera LDAP V3 jako preferowany protokół, używając funkcji **ldap\_init** zamiast **ldap\_open**.

**-w hasło | ?**

Do uwierzytelniania zostanie użyte podane **hasło**. Podanie wartości **?** spowoduje wywołanie zachęty do wpisania hasła.

**-y nazwa\_wyróżniająca\_proxy**

Ustawia ID proxy dla działania autoryzacji proxy.

**-Y** Używa bezpiecznego połączenia LDAP (TLS).

**-Z** Używa bezpiecznego połączenia SSL w komunikacji z serwerem LDAP. W przypadku serwera Directory Server w systemie i5/OS, jeśli użyta została opcja **-Z** i nie użyto opcji **-K** ani **-N**, wykorzystany zostanie certyfikat powiązany z identyfikatorem aplikacji Directory Services Client.

**dn newrdn**

Poniższa sekcja, "Format danych wejściowych dla pozycji **dn newrdn**" zawiera więcej informacji.

## Format danych wejściowych dla pozycji **dn newrdn**

Jeśli podano argumenty wiersza komend **dn** i **newrdn**, **argument newrdn** zastępuje nazwę RDN pozycji określonej przez nazwę wyróżniającą **dn**. W przeciwnym razie zawartość pliku (lub standardowego wejścia, jeśli nie podano opcji **-i**) składa się z jednej lub kilku pozycji:

Nazwa wyróżniająca (DN)

Relative Distinguished Name (RDN)

Jeden lub więcej pustych wierszy może służyć do oddzielania każdej pary nazwy wyróżniającej i nazwy RDN.

## Przykłady

Zakładając, że plik /tmp/entrymods istnieje i że zawiera:

```
cn=Zmień Mnie, o=University of Life, c=US
cn=Nowy Ja
```

komenda:

```
ldapmodrdn -r -i /tmp/entrymods
```

zmienia nazwę RDN pozycji Zmień mnie ze Zmień mnie na Nowy ja, a stara pozycja cn - Zmień mnie - jest usuwana.

## Uwagi

Jeśli informacji o pozycji nie podano z pliku za pomocą opcji **-i** (ani z pary wiersza komend *dn* i *rdn*), komenda **ldapmodrdn** czeka na odczyt pozycji ze standardowego wejścia.

## Diagnostyka

Jeśli nie wystąpiły żadne błędy, statusem wyjścia jest 0. Wystąpienie błędu powoduje zwrócenie niezerowego statusu wyjścia i wypisanie komunikatu diagnostycznego na standardowe wyjście błędów.

### Pojęcia pokrewne

Funkcje API serwera Directory Server

“Nazwy wyróżniające (DN)” na stronie 9

Każda pozycja w katalogu ma nazwę wyróżniającą (DN). Nazwa DN jednoznacznie identyfikuje pozycję w katalogu. Pierwszy komponent nazwy DN jest nazywany względną nazwą wyróżniającą (RDN).

## Idapsearch

Program narzędziowy wiersza komend do wyszukiwania w katalogu LDAP.

### Składnia

```
ldapsearch [-a wyłuskiwanie_aliasów [-A] [-b baza_wyszukiwania] [-B] [-C zestaw_znaków]
[-d poziom_debugowania] [-D nazwa_wyróżniająca_łączenia] [-e] [-f plik] [-F separator]
[-G dziedzina] [-h host_ldap] [-i plik] [-K plik_kluczy] [-l limit_czasu] [-L]
[-m mechanizm] [-M] [-n] [-N nazwa_certyfikatu] [-o typ_atrybutu]
[-O maksymalna_liczba_przeskoków] [-p port_ldap] [-P hasło_pliku_kluczy]
[-q wielkość_strony] [-R] [-s zasięg] [-t] [-T sekundy] [-U nazwa_użytkownika]
[-v] [-V wersja] [-w hasło | ?] [-z limit_wielkości] [-y nazwa_wyróżniająca_proxy]
[-Y] [-Z] filtr [-9 p] [-9 s] [atrybuty...]
```

### Opis

Komenda **ldapsearch** jest interfejsem wiersza komend dla funkcji API `ldap_search`.

Komenda **ldapsearch** otwiera połączenie z serwerem LDAP, łączy i przeprowadza wyszukiwanie za pomocą filtru. Filtr powinien odpowiadać reprezentacji łańcucha dla filtrów LDAP (patrz opis funkcji `ldap_search` w sekcji Funkcje API serwera Directory Server, aby uzyskać więcej informacji a temat filtrów).

Jeśli komenda **ldapsearch** znajduje jedną lub kilka pozycji, podane atrybuty są pobierane, a pozycje i wartości są drukowane na standardowym wyjściu. Jeśli nie zostanie podany żaden atrybut, zwrócone zostaną wszystkie atrybuty.

Aby wyświetlić pomoc dotyczącą składni komendy **ldapsearch**, wpisz **ldapsearch -?**

## Opcje

### -a wyluskiwanie\_aliasów

Określa, w jaki sposób są podstawiane aliasy. Parametr wyluskiwanie\_aliasów powinien mieć wartość never, always, search lub find, określającą odpowiednio, że aliasy mają być podstawiane: nigdy, zawsze, podczas wyszukiwania lub tylko podczas określania położenia obiektu podstawowego do wyszukiwania. Wartością domyślną jest never (nigdy).

**-A** Pobiera tylko atrybuty (nie wartości). Jest to przydatne do sprawdzania, czy pozycja zawiera podany atrybut, gdy nie jest potrzebna konkretna wartość.

### -b baza\_wyszukiwania

Używa bazy wyszukiwania jako początkowego punktu wyszukiwania zamiast punktu domyślnego. Jeśli nie określono opcji **-b**, to narzędzie sprawdza zmienną środowiskową LDAP\_BASEDN i szuka definicji podstawy wyszukiwania. Jeśli nie ustawiono żadnego z powyższych, domyślna podstawa jest ustawiana na "".

**-B** Wyświetla wartości w kodzie innym niż ASCII. Jest to użyteczne w przypadku pracy z wartościami, które występują w innych zestawach znaków, takich jak ISO-8859-1. Ta opcja jest także włączana przez opcję **-L**.

### -C zestaw\_znaków

Określa, że łańcuchy znaków dostarczone do narzędzia ldapsearch jako wejściowe są przedstawione w lokalnym zestawie znaków (określonym przez wartość zestaw\_znaków). Łańcuch wejściowy zawiera filtr, nazwę DN łączenia i podstawową nazwę DN. Podobnie, podczas wyświetlania danych narzędzie ldapsearch przekształca otrzymane z serwera LDAP dane do określonego zestawu znaków. Opcji **-C zestaw\_znaków** używa się, gdy strona kodowa wejściowego łańcucha znaków różni się od strony kodowej zadania. Opis funkcji API ldap\_set\_iconv\_local\_charset() zawiera obsługiwane wartości zestawów znaków. Również jeśli obie opcje: **-C** i **-L** są określone, przyjmuje się, że dane wejściowe są w podanym zestawie znaków, ale dane wyjściowe narzędzia ldapsearch są zawsze pozostawiane w reprezentacji UTF-8 lub w postaci zakodowanej algorytmem base-64, gdy wykryto znaki niedrukowalne. Wynika to z tego, że standardowe pliki LDIF zawierają reprezentacje danych łańcuchowych tylko w formacie UTF-8 (lub UTF-8 zakodowanym algorytmem base-64). Należy zauważyć, że obsługiwane wartości zestawu znaków są tymi samymi wartościami, które są obsługiwane dla znacznika zestawu znaków, który jest opcjonalnie definiowany w plikach LDIF w wersji 1.

### -d poziom\_debugowania

Ustawia poziom debugowania LDAP na poziom\_debugowania.

### -D nazwa\_wyróżniająca\_łączenia

Określa nazwę wyróżniającą do łączenia z katalogiem LDAP. *Nazwa\_wyróżniająca\_łączenia* powinna być nazwą wyróżniającą w postaci łańcucha znaków (więcej informacji zawiera temat Nazwy wyróżniające LDAP). Jeśli używana jest wraz z **-m DIGEST-MD5**, wykorzystywana jest do określenia identyfikatora autoryzacji. Nazwa ta może być nazwą wyróżniającą lub łańcuchem authzId rozpoczynającym się od "u:" lub "dn:".

**-e** Wyświetla informacje o wersji biblioteki LDAP i kończy pracę.

### -F separator

Określa separator pola pomiędzy nazwami i wartościami atrybutów. Separatorem domyślnym jest '=', chyba że została określona flaga **-L**, wówczas opcja ta jest ignorowana.

### -G dziedzina

Określa dziedzinę. Parametr ten jest opcjonalny. Jeśli używany jest wraz z **-m DIGEST-MD5**, wartość przekazywana jest do serwera podczas połączenia.

### -h host\_ldap

Określa alternatywny host, na którym działa serwer ldap.

**-i plik** Odczytuje wiersze z pliku, wykonując dla każdego z nich operację wyszukiwania LDAP. W tym przypadku

filtr określony w wierszu komend jest traktowany jako wzorzec, w którym pierwsze wystąpienie znaku %s jest zastępowane wierszem z pliku. Jeśli plik ma postać jednego znaku "-", wiersze są odczytywane ze standardowego wejścia.

#### **-K plik\_kluczy**

Określa nazwę pliku bazy danych kluczy SSL. Jeśli plik bazy danych kluczy nie znajduje się w bieżącym katalogu, należy podać jego nazwę z pełną ścieżką.

Jeśli narzędzie nie może znaleźć bazy danych kluczy, użyje wkompiowanego na stałe zestawu domyślnych zaufanych głównych ośrodków certyfikacji. Plik bazy danych kluczy zazwyczaj zawiera jeden lub więcej certyfikatów ośrodków certyfikacji (CA), do których klient ma zaufanie. Tego typu certyfikaty X.509 zwane są także użytkownikami zaufanymi.

Parametr ten udostępnia opcję **-Z**. W przypadku serwera Directory Server w systemie i5/OS, jeśli użyta została opcja **-Z** i nie użyto opcji **-K** ani **-N**, wykorzystany zostanie certyfikat powiązany z identyfikatorem aplikacji Directory Services Client.

#### **-l limit\_czasu**

Czeka maksymalnie limit\_czasu sekund na zakończenie wyszukiwania.

**-L** Wyświetla wyniki wyszukiwania w formacie LDIF. Opcja ta włącza także opcję **-Bi** powoduje ignorowanie opcji **-F**.

#### **-m mechanizm**

Parametr *mechanizm* określa mechanizm SASL używany do łączenia z serwerem. Używana jest funkcja API ldap\_sasl\_bind\_s(). Parametr **-m** jest ignorowany, jeśli ustawiony zostanie parametr **-V 2**. Jeśli parametr **-m** nie jest określony, użyte zostanie proste uwierzytelnianie. Poprawne mechanizmy to:

- CRAM-MD5 - chroni hasło wysyłane na serwer.
- EXTERNAL - używa certyfikatu SSL. Wymaga opcji **-Z**.
- GSSAPI - używa referencji Kerberos użytkownika.
- DIGEST-MD5 - wymaga od klienta wysłania do serwera wartości nazwy użytkownika. Wymaga opcji **-U**. Parametr **-D** (zwykle nazwa wyróżniająca łączenia) określa identyfikator autoryzacji. Może być nazwą wyróżniającą lub łańcuchem authzId rozpoczynającym się od u: lub dn:.
- OS400\_PRFTKN - dokonuje uwierzytelnienia na lokalnym serwerze LDAP jako bieżący użytkownik systemu i5/OS za pomocą nazwy wyróżniającej użytkownika w systemowym mechanizmie rzutowania. Nie należy określać parametrów **-D** (nazwy wyróżniającej łączenia) oraz **-w** (hasła).

**-M** Zarządza obiektami odwołania tak jak zwykłymi pozycjami.

**-n** Pokazuje, co byłoby wykonane, ale nie modyfikuje pozycji. Opcja przydatna podczas debugowania w połączeniu z parametrem **-v**.

#### **-N nazwa\_certyfikatu**

Określa etykietę powiązaną z certyfikatem klienta w pliku bazy danych kluczy.

**Uwaga:** 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 może być certyfikat klienta. Parametr *nazwa\_certyfikatu* nie jest wymagany, jeśli określono domyślną parę certyfikat/klucz prywatny. Podobnie parametr *nazwa\_certyfikatu* nie jest wymagany, jeśli w wyznaczonej bazie danych kluczy znajduje się pojedyncza para certyfikat/klucz prywatny. Parametr ten jest ignorowany, gdy nie zostanie podana opcja **-Z** lub **-K**.

W przypadku serwera Directory Server w systemie i5/OS, jeśli użyta została opcja **-Z** i nie użyto opcji **-K** ani **-N**, wykorzystany zostanie certyfikat powiązany z identyfikatorem aplikacji Directory Services Client.

#### **-o typ\_atributu**

Aby określić atrybut używany jako kryterium sortowania wyników wyszukiwania, można użyć parametru **-o** (porządek). Kolejnych parametrów **-o** można używać do dalszego definiowania kolejności sortowania. W poniższym przykładzie wyniki wyszukiwania są sortowane najpierw według nazwiska (sn), a następnie w odwrotnej kolejności według imienia (givenname), co określa znak minus (-):

-o sn -o -givenname

Przez to składnia parametru sortowania jest następująca:

[< ->]<nazwa atrybutu>[:<OID reguły sprawdzania zgodności>]

gdzie

- nazwa atrybutu jest nazwą atrybutu, według którego ma się odbywać sortowanie.
- OID reguły sprawdzania zgodności jest opcjonalnym OID reguły sprawdzania zgodności, które mają być używane podczas sortowania. Atrybut reguły zgodności OID nie jest obsługiwany przez serwer Directory Server, jednak inne serwery LDAP mogą go obsługiwać.
- Znak minus ( - ) oznacza, że wyniki muszą być sortowane w odwrotnej kolejności.
- Newralgiczność jest zawsze istotna.

Domyślnym działaniem komendy ldapsearch jest brak sortowania zwróconych wyników.

#### **-O maksymalna\_liczba\_przeskoków**

Parametr maksymalna\_liczba\_przeskoków określa maksymalną liczbę przeskoków, którą wykona biblioteka klienta podczas przeglądania odwołań. Domyślna liczba przeskoków jest równa 10.

#### **-p port\_ldap**

Określa alternatywny port TCP, na którym serwer ldap prowadzi nasłuch. Domyślnym portem LDAP jest 389. Jeśli go nie podano tej opcji, a podano -Z, używany jest domyślny port 636 SSL LDAP.

#### **-P hasło\_pliku\_kluczy**

Określa hasło bazy danych kluczy. Hasło to jest wymagane w celu uzyskania dostępu do szyfrowanych informacji w pliku bazy danych kluczy, który może zawierać jeden lub wiele kluczy prywatnych. Jeśli z plikiem bazy danych kluczy jest związany plik ukrytych haseł, hasło jest otrzymywane z niego pliku i parametr -P nie jest wymagany. Parametr ten jest ignorowany, gdy nie zostanie podana opcja -Z lub -K.

#### **-q wielkość\_strony**

Aby określić podział na strony wyników wyszukiwania, można użyć dwóch parametrów: -q (wielkość strony zapytania) i -T (czas między operacjami wyszukiwania w sekundach). W poniższym przykładzie wyniki wyszukiwania zwracają stronę (25 pozycji) naraz, co 15 sekund, do momentu aż zwrócone zostaną wszystkie wyniki tego wyszukiwania. Klient ldapsearch obsługuje wszystkie kontynuacje połączenia dla każdego żądania strony wyników przez cały czas wykonywania operacji wyszukiwania.

Parametry te przydają się, gdy klient ma ograniczone zasoby lub jeśli połączenie ma małą przepustowość. Ogólnie umożliwia sterowanie szybkością zwracania danych z żądania wyszukiwania. Zamiast odbierania wszystkich wyników za jednym razem, można je pobierać w kilku częściach (stronach). Poza tym można sterować opóźnieniem między żądaniami poszczególnych stron, dając klientowi czas na przetworzenie żądań.

-q 25 -T 15

Jeśli określono parametr -v (tryb szczegółowy), narzędzie ldapsearch wyświetla po każdej stronie pozycji zwróconych z serwera liczbę pozycji zwróconych dotychczas, na przykład **Łączna liczba zwróconych pozycji: 30**.

Dopuszczalnych jest wiele parametrów -q, aby można było określać różne wielkości stron w ramach jednej operacji wyszukiwania. W poniższym przykładzie pierwsza strona zawiera 15 pozycji, druga 20, a trzeci parametr kończy operację wyszukiwania/podziału na strony:

-q 15 -q 20 -q 0

W poniższym przykładzie pierwsza strona zawiera 15 pozycji, a wszystkie pozostałe strony zawierają 20 pozycji, licząc od ostatniej określonej wartości -q do zakończenia operacji wyszukiwania:

-q 15 -q 20

Domyślnym działaniem narzędzia ldapsearch jest zwrócenie wszystkich pozycji w pojedynczym żądaniu. Domyślnie komenda ldapsearch zwraca dane bez podziału na strony.

- R** Określa, że odwołania nie mają następować automatycznie.
- s zasięg**  
Określa zasięg wyszukiwania. Parametr zasięg może mieć wartość base, one lub sub, aby określić, czy wyszukiwanie ma być podstawowe, jednopoziomowe czy w poddrzewie. Wartością domyślną jest sub.
- t** Zapisuje pobrane wartości do zestawu plików tymczasowych. Jest to użyteczne podczas pracy z wartościami innymi niż ASCII, takimi jak jpegPhoto lub danymi dźwiękowymi.
- T sekundy**  
Czas między operacjami wyszukiwania (w sekundach). Opcja **-T** jest obsługiwana tylko wtedy, gdy podano opcję **-q**.
- U nazwa\_użytkownika**  
Określa nazwę użytkownika. Wymagane w przypadku określenia opcji **-m DIGEST-MD5** i ignorowane w przypadku pozostałych mechanizmów.
- v** Używa trybu szczegółowego z wieloma komunikatami diagnostycznymi wysyłanymi na wyjście standardowe.
- V** Określa wersję LDAP używaną przez komendę `ldapmodify` podczas łączenia się z serwerem LDAP. Domyślnie nawiązywane jest połączenie LDAP V3. Aby jawnie wybrać LDAP V3, należy podać `"-V 3"`. Aby operację wykonać jako aplikację LDAP V2, należy podać `"-V 2"`. Aplikacja, na przykład `ldapmodify`, wybiera LDAP V3 jako preferowany protokół, używając funkcji `ldap_init` zamiast `ldap_open`.
- w hasło | ?**  
Do uwierzytelniania zostanie użyte podane **hasło**. Podanie wartości **?** spowoduje wywołanie zachęty do wpisania hasła.
- y nazwa\_wyróżniająca\_proxy**  
Ustawia ID proxy dla działania autoryzacji proxy.
- Y** Używa bezpiecznego połączenia LDAP (TLS).
- z limit\_wielkości**  
Ogranicza wyniki wyszukiwania do maksymalnie `limit_wielkości` pozycji. Umożliwia to określenie górnej granicy liczby pozycji zwracanych podczas operacji wyszukiwania.
- Z** Używa bezpiecznego połączenia SSL w komunikacji z serwerem LDAP. W przypadku serwera Directory Server w systemie i5/OS, jeśli użyta została opcja **-Z** i nie użyto opcji **-K** ani **-N**, wykorzystany zostanie certyfikat powiązany z identyfikatorem aplikacji Directory Services Client.
- filtr** Określa reprezentację łańcucha filtru stosowanego w operacji wyszukiwania. Proste filtry można określać w postaci `typ_atrybutu=wartość_atrybutu`. Bardziej złożone filtry są określane za pomocą notacji przyrostka zgodnie z następującą gramatyką Backus Naur Form (BNF):
 

```

<filtr> ::= '(' <porównanie_filtru> ')'
<porównanie_filtru> ::= <koniunkcja> | <alternatywa> | <negacja> | <prosty>
<koniunkcja> ::= '&' <lista_filtrów>
<alternatywa> ::= '|' <lista_filtrów>
<negacja> ::= '!' <filtr>
<lista_filtrów> ::= <filtr> | <filtr> <lista_filtrów>
<prosty> ::= <typ_atrybutu> <typ_filtru>
<wartość_atrybutu>
<typ_filtru> ::= '=' | '~=' | '<' | '>'
```

Operator `'~='` służy do określania przybliżonej równości. Reprezentacje wartości `<typ_atrybutu>` i `<wartość_atrybutu>` odpowiadają definicjom w dokumencie RFC 2252 "LDAP V3 Attribute Syntax Definitions". Ponadto, jeśli typem filtru jest `'='`, jako `<wartość_atrybutu>` można podać jeden znak `*`, aby sprawdzić, czy atrybut istnieje, lub tekst zawierający gwiazdki (`*`) w celu sprawdzenia dopasowania podłańcucha.

Na przykład filtr `"mail=*"` wyszukuje wszystkie pozycje zawierające atrybut poczty. Filtr `"mail=@student.of.life.edu"` znajduje wszystkie pozycje zawierające atrybut poczty kończący się podanym łańcuchem. Aby wstawić nawiasy w filtrze, należy użyć ukośnika odwrotnego (`\`).

**Uwaga:** W katalogu IBM Directory filtr "cn=Jan \*", ze spacją między słowem Jan a gwiazdką ( \* ) jest zgodny z wartością "Jan Nowak", ale nie z "Janek Nowak". Spacja między słowem "Jan" a znakiem wieloznacznym ( \* ) ma wpływ na wynik wyszukiwania przy użyciu tego filtru.

Bardziej szczegółowy opis dozwolonych filtrów można znaleźć w dokumencie RFC 2254 "A String Representation of LDAP Search Filters".

## Format wyjściowy

Jeśli odnaleziona zostanie jedna lub więcej pozycji, każda z nich jest zapisywana na standardowe wyjście w następującej postaci:

Nazwa wyróżniająca (DN)

nazwa\_atrybutu=wartość

nazwa\_atrybutu=wartość

nazwa\_atrybutu=wartość

...

Pozycje oddzielane są od siebie pojedynczym pustym wierszem. Jeśli w opcji **-F** określono znak separatora, zostanie on użyty zamiast znaku '='. Jeśli użyto opcji **-t**, zamiast wartości użyta zostanie nazwa pliku tymczasowego. Jeśli podano opcję **-A**, zapisywana jest tylko część "nazwa\_atrybutu".

## Przykłady

Poniższa komenda:

```
ldapsearch "cn=jan kowalski" cn telephoneNumber
```

wykonuje operację wyszukiwania w poddrzewie (używając domyślnej podstawy wyszukiwania) pozycji z atrybutem commonName o wartości "jan kowalski". Wartości commonName i telephoneNumber są pobierane i drukowane na standardowe wyjście. Jeśli odnalezione zostaną dwie pozycje, dane wyjściowe będą podobne do poniższych:

```
cn=Jan E Kowalski, ou="College of Literature, Science, and the Arts",  
ou=Students, ou=People, o=University of Higher Learning, c=US
```

```
cn=Jan Kowalski
```

```
cn=Jan Edward Kowalski
```

```
cn=Jan E Kowalski 1
```

```
cn=Jan E Kowalski
```

```
telephoneNumber=+1 313 555-5432
```

```
cn=Jan B Kowalski, ou=Information Technology Division,  
ou=Faculty and Staff, ou=People, o=University of Higher Learning, c=US
```

```
cn=Jan Kowalski
```

```
cn=Jan B Kowalski 1
```

```
cn=Jan B Kowalski
```

```
telephoneNumber=+1 313 555-1111
```

Komenda:

```
ldapsearch -t "uid=jed" jpegPhoto audio
```

wykonuje operację wyszukiwania w poddrzewie, używając domyślnej podstawy wyszukiwania pozycji z identyfikatorem użytkownika "jed". Wartości atrybutów jpegPhoto i audio są pobierane i zapisywane do plików tymczasowych. Dane wyjściowe mogą być podobne do poniższych, jeśli odnaleziona zostanie jedna pozycja z jedną wartością dla każdego atrybutu:

```
cn=Jan E Kowalski, 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
```

Komenda:

```
ldapsearch -L -s one -b "c=US" "o=university*" o description
```

wykonuje jednopoziomowe wyszukiwanie na poziomie c=US dla wszystkich organizacji, których organizationName zaczyna się od słowa university. Wyniki wyszukiwania zostaną wyświetlone w formacie LDIF (patrz LDAP Data Interchange Format). Wartości atrybutów organizationName i description zostaną pobrane i wydrukowane na standardowym wyjściu i będą podobne do poniższych:

```
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: UF1  
  
description: Shaper of young minds
```



...

Komenda:

```
ldapsearch -b "c=US" -o ibm-slapdDN "objectclass=person" ibm-slapdDN
```

wykonuje wyszukiwanie na poziomie poddrzewa na poziomie c=US dla wszystkich osób. Ten atrybut specjalny (ibm-slapdDN), jeśli jest używany w operacjach wyszukiwania z sortowaniem, sortuje wyniki wyszukiwania według reprezentacji łańcucha nazwy wyróżniającej. Dane wyjściowe mogą być następujące:

```
cn=Al Edwards,ou=Widget Division,ou=Austin,o=IBM,c=US
```

```
cn=Al Garcia,ou=Home Entertainment,ou=Austin,o=IBM,c=US
```

```
cn=Amy Nguyen,ou=In Flight Systems,ou=Austin,o=IBM,c=US
```

```
cn=Arthur Edwards,ou=Widget Division,ou=Austin,o=IBM,c=US
```

```
cn=Becky Garcia,ou=In Flight Systems,ou=Austin,o=IBM,c=US
```

```
cn=Ben Catu,ou=In Flight Systems,ou=Austin,o=IBM,c=US
```

```
cn=Ben Garcia Jr,ou=Home Entertainment,ou=Austin,o=IBM,c=US
```

```
cn=Bill Keller Jr.,ou=In Flight Systems,ou=Austin,o=IBM,c=US
```

```
cn=Bob Campbell,ou=In Flight Systems,ou=Austin,o=IBM,c=US
```

Komenda:

```
ldapsearch -h nazwa_hosta -o sn -b "o=ibm,c=pl" "title=inzynier"
```

zwraca z katalogu pracowników IBM wszystkie pozycje pracowników o tytule "inzynier", a wyniki są sortowane według nazwiska.

Komenda:

```
ldapsearch -h nazwa_hosta -o -sn -o cn -b "o=ibm,c=pl" "title=inzynier"
```

zwraca z katalogu pracowników IBM wszystkie pozycje pracowników o tytule "inzynier", a wyniki są sortowane według nazwiska (malejąco), a następnie według imienia(rosnąco).

Komenda:

```
ldapsearch -h nazwa_hosta -q 5 -T 3 -b o=ibm,c=pl "title=inzynier"
```

zwraca po pięć pozycji na stronie z opóźnieniem 3 sekund między stronami dla wszystkich pozycji pracowników o tytule "inzynier" w katalogu pracowników IBM.

Przykład ten przedstawia wyszukiwanie, w którym bierze udział obiekt odwołania. Katalogi LDAP serwera Directory Server mogą zawierać obiekty odwołania, o ile zawierają one wyłącznie:

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

Przypuśćmy, 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 'System\_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
```

Jeśli użytkownik wysyła żądanie do systemu 'System\_A', serwer LDAP w tym systemie wysyła do klienta odpowiedź zawierającą adres URL:

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

Klient za pomocą tej informacji wysyła żądanie do systemu System\_B. Jeśli pozycja w systemie System\_A zawiera jakieś atrybuty oprócz dn, objectclass i ref, serwer ignoruje je (chyba że użyta zostanie opcja **-R**, aby nie używać odwołań).

Gdy klient odbierze z serwera odpowiedź na odwołanie, wysyła ponownie żądanie, tym razem do serwera, na który wskazuje zwrócony adres URL. Nowe żądanie ma ten sam zakres co oryginalne. Wyniki tego wyszukiwania zależą od wartości podanej jako zasięg wyszukiwania (**-b**).

Jeśli podano parametr **-s base**, jak poniżej:

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

w wynikach wyszukiwania zostaną zwrócone wszystkie atrybuty dla wszystkich pozycji z 'sn=Jensen', które znajdują się w pozycji 'ou=Rochester, o=Big Company, c=US' w systemach System\_A i System\_B.

Jeśli podano parametr **-s sub**, jak poniżej:

```
ldapsearch -s sub "cn=John"
```

serwer wyszuka wszystkie przyrostki i zwróci wszystkie pozycje określone jako "cn=John". Jest to wyszukiwanie w poddrzewie bazy zerowej. Wyszukiwanie w całym katalogu jest realizowane dzięki pojedynczemu działaniu wyszukiwania, co pozwala uniknąć konieczności korzystania z opcji wielokrotnego wyszukiwania (z których każde posiada odmienny przyrostek jako bazę wyszukiwania). Ten typ wyszukiwania trwa dłużej i pochłania więcej zasobów systemu, ponieważ wyszukuje w całym katalogu (wszystkie przyrostki).

**Uwaga:** Wyszukiwanie w poddrzewie bazy zerowej nie zwraca informacji o schematach lub protokole zmian, nie zwraca też żadnych danych z systemowego mechanizmu rzutowania.

Jeśli podano parametr **-s sub**, jak poniżej:

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

w wynikach wyszukiwania zostaną zwrócone wszystkie atrybuty dla wszystkich pozycji z 'sn=Jensen', które znajdują się w pozycji 'ou=Rochester, o=Big Company, c=US' w systemach System\_A i System\_B lub pod nią.

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 zwróci 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
```

Klient z kolei wysyła żądanie:

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

Nie daje to żadnych wyników, ponieważ pozycja

```
dn: cn=Barb Jensen, ou=Rochester, o=Big Company, c=US
```

znajduje się w

```
ou=Rochester, o=Big Company, c=US
```

Operacja wyszukiwania z `-s one` próbuje odnaleźć pozycje na poziomie znajdującym się zaraz pod pozycją

```
ou=Rochester, o=Big Company, c=US
```

## Diagnostyka

Jeśli nie wystąpiły żadne błędy, statusem wyjścia jest 0. Wystąpienie błędu powoduje zwrócenie niezerowego statusu wyjścia i wypisanie komunikatu diagnostycznego na standardowe wyjście błędów.

### Pojęcia pokrewne

Funkcje API serwera Directory Server

“Odwołania do katalogu LDAP” na stronie 50

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

### Odsyłacze pokrewne

“Format wymiany danych LDAP (LDIF)” na stronie 251

Format wymiany danych LDAP (LDAP Data Interchange Format - LDIF) to standardowy format używany do tekstowego zapisu reprezentacji obiektów LDAP i operacji na obiektach LDAP (dodawanie, modyfikowanie, usuwanie, zmiana nazwy wyróżniającej). Pliki zawierające rekordy LDIF mogą być używane do przenoszenia danych między serwerami katalogów lub podawane jako dane wejściowe programów narzędziowych LDAP, takich jak `ldapadd` i `ldapmodify`.

### Informacje pokrewne



RFC 2252, LDAP V3 Attribute Syntax Definitions



RFC 2254, A String Representation of LDAP Search Filters

## ldapchangepwd

Program narzędziowy wiersza komend do zmiany haseł LDAP.

### Składnia

```
ldapchangepwd -D nazwa_wyróżniająca_łączenia -w hasło | ? -n nowe_hasło | ?  
[-C zestaw_znaków] [-d poziom_debugowania] [-G dziedzina] [-h host_ldap]  
[-K plik_kluczy] [-m mechanizm] [-M] [-N nazwa_certyfikatu]  
[-O maksymalna_liczba_przeskoków] [-p port_ldap] [-P hasło_pliku_kluczy] [-R]  
[-U nazwa_użytkownika] [-v] [-V wersja] [-y nazwa_wyróżniająca_proxy] [-Y] [-Z] [-?]
```

### Opis

Wysyła żądanie zmiany hasła do serwera LDAP. Umożliwia zmianę hasła dla pozycji katalogu.

### Opcje

`-C zestaw_znaków`

Określa, że nazwy wyróżniające podane jako dane wejściowe w programie narzędziowym `ldapdelete` są przedstawiane w określonym lokalnym zestawie znaków. Opcji `-C zestaw_znaków` używa się, gdy strona

kodowa wejściowego łańcucha znaków różni się od strony kodowej zadania. Opis funkcji API `ldap_set_iconv_local_charset()` zawiera obsługiwane wartości zestawów znaków.

**-d** *poziom\_debugowania*

Ustawia poziom debugowania LDAP na *poziom\_debugowania*.

**-D** *nazwa\_wyróżniająca\_łączenia*

Parametr *nazwa\_wyróżniająca\_łączenia* umożliwia utworzenie łączenia z katalogiem LDAP.

*nazwa\_wyróżniająca\_łączenia* jest nazwą wyróżniającą w postaci łańcucha znaków. Jeśli używana jest wraz z `-m DIGEST-MD5`, wykorzystywana jest do określenia identyfikatora autoryzacji. Nazwa ta może być nazwą wyróżniającą lub łańcuchem `authzId` rozpoczynającym się od "u:" lub "dn:".

**-G** *dziedzina*

Określa dziedzinę. Parametr ten jest opcjonalny. Jeśli używany jest wraz z `-m DIGEST-MD5`, wartość przekazywana jest do serwera podczas połączenia.

**-h** *host\_ldap*

Określa alternatywny host, na którym działa serwer ldap.

**-K** *plik\_kluczy*

Określa nazwę pliku bazy danych kluczy SSL. Jeśli plik bazy danych kluczy nie znajduje się w bieżącym katalogu, należy podać jego nazwę z pełną ścieżką.

Jeśli narzędzie nie może znaleźć bazy danych kluczy, użyje wkompiowanego na stałe zestawu domyślnych zaufanych głównych ośrodków certyfikacji. Plik bazy danych kluczy zazwyczaj zawiera jeden lub więcej certyfikatów ośrodków certyfikacji (CA), do których klient ma zaufanie. Tego typu certyfikaty X.509 zwane są także użytkownikami zaufanymi.

Parametr ten udostępnia opcję `-Z`. W przypadku serwera Directory Server w systemie i5/OS, jeśli użyta została opcja `-Z` i nie użyto opcji `-K` ani `-N`, wykorzystany zostanie certyfikat powiązany z identyfikatorem aplikacji Directory Services Client.

**-m** *mechanizm*

Parametr *mechanizm* określa mechanizm SASL używany do łączenia z serwerem. Używana jest funkcja API `ldap_sasl_bind_s()`. Parametr `-m` jest ignorowany, jeśli ustawiony zostanie parametr `-V 2`. Jeśli parametr `-m` nie jest określony, użyte zostanie proste uwierzytelnianie. Poprawne mechanizmy to:

- CRAM-MD5 - chroni hasło wysyłane na serwer.
- EXTERNAL - używa certyfikatu SSL. Wymaga opcji `-Z`.
- GSSAPI - używa referencji Kerberos użytkownika.
- DIGEST-MD5 - wymaga od klienta wysłania do serwera wartości nazwy użytkownika. Wymaga opcji `-U`. Parametr `-D` (zwykle nazwa wyróżniająca łączenia) określa identyfikator autoryzacji. Może być nazwą wyróżniającą lub łańcuchem `authzId` rozpoczynającym się od u: lub dn:.

**-M** Zarządza obiektami odwołania tak jak zwykłymi pozycjami.

**-n** *nowe\_haslo | ?*

Określa nowe hasło. Podanie wartości `?` spowoduje wywołanie zachęty do wpisania hasła.

**-N** *nazwa\_certyfikatu*

Określa etykietę powiązaną z certyfikatem klienta w pliku 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 może być certyfikat klienta. Parametr *nazwa\_certyfikatu* nie jest wymagany, jeśli określono domyślną parę certyfikat/klucz prywatny. Podobnie parametr *nazwa\_certyfikatu* nie jest wymagany, jeśli w wyznaczonej bazie danych kluczy znajduje się pojedyncza para certyfikat/klucz prywatny. Parametr ten jest ignorowany, gdy nie zostanie podana opcja `-Z` lub `-K`. W przypadku serwera Directory Server w systemie i5/OS, jeśli użyta została opcja `-Z` i nie użyto opcji `-K` ani `-N`, wykorzystany zostanie certyfikat powiązany z identyfikatorem aplikacji Directory Services Client.

**-O** *maksymalna\_liczba\_przeskoków*

Parametr *maksymalna\_liczba\_przeskoków* określa maksymalną liczbę przeskoków, którą wykona biblioteka klienta podczas przeglądania odwołań. Domyślna liczba przeskoków jest równa 10.

**-p** *port\_ldap*

Określa alternatywny port TCP, na którym serwer ldap prowadzi nasłuch. Domyślnym portem LDAP jest 389. Jeśli nie podano opcji **-p**, a podano **-Z**, używany jest domyślny port 636 SSL LDAP.

**-P** *hasło\_pliku\_kluczy*

Określa hasło bazy danych kluczy. Hasło to jest wymagane w celu uzyskania dostępu do szyfrowanych informacji w pliku bazy danych kluczy, który może zawierać jeden lub wiele kluczy prywatnych. Jeśli z plikiem bazy danych kluczy jest związany plik ukrytych haseł, hasło jest otrzymywane z niego pliku i parametr **-P** nie jest wymagany. Parametr ten jest ignorowany, gdy nie zostanie podana opcja **-Z** lub **-K**.

**-R** Określa, że odwołania nie mają następować automatycznie.

**-U** *nazwa\_użytkownika*

Określa nazwę użytkownika. Wymagane w przypadku określenia opcji **-m** DIGEST-MD5 i ignorowane w przypadku pozostałych mechanizmów.

**-v** Używa trybu szczegółowego z wieloma komunikatami diagnostycznymi wysyłanymi na wyjście standardowe.

**-V** *wersja*

Określa wersję LDAP używaną przez komendę **ldapdchangepwd** podczas łączenia się z serwerem LDAP. Domyślnie nawiązywane jest połączenie LDAP V3. Aby jawnie wybrać LDAP V3, należy podać wartość **-V 3**. Aby uruchomić jako aplikację LDAP V2, należy podać **-V 2**. Aplikacja, na przykład **ldapdchangepwd**, wybiera LDAP V3 jako preferowany protokół, używając funkcji `ldap_init` zamiast `ldap_open`.

**-w** *hasło | ?*

Do uwierzytelniania zostanie użyte podane **hasło**. Podanie wartości **?** spowoduje wywołanie zachęty do wpisania hasła.

**-y** *nazwa\_wyróżniająca\_proxy*

Ustawia ID proxy dla działania autoryzacji proxy.

**-Y** Używa bezpiecznego połączenia LDAP (TLS).

**-Z** Używa bezpiecznego połączenia SSL w komunikacji z serwerem LDAP. W przypadku serwera Directory Server w systemie i5/OS, jeśli użyta została opcja **-Z** i nie użyto opcji **-K** ani **-N**, wykorzystany zostanie certyfikat powiązany z identyfikatorem aplikacji Directory Services Client.

**-?** Wyświetla pomoc dotyczącą składni komendy `ldapdchangepwd`.

## Przykłady

Następująca komenda:

```
ldapdchangepwd -D cn=Jan Kowalski -w a1b2c3d4 -n wxyz9876
```

zmienia hasło dla pozycji o nazwie `commonName "Jan Kowalski"` z `a1b2c3d4` na `wxyz9876`

## Diagnostyka

Jeśli nie wystąpiły żadne błędy, statusem wyjścia jest 0. Wystąpienie błędu powoduje zwrócenie niezerowego statusu wyjścia i wypisanie komunikatu diagnostycznego na standardowe wyjście błędów.

### Pojęcia pokrewne

Funkcje API protokołu LDAP

Temat Funkcje API protokołu LDAP zawiera więcej informacji o funkcjach API serwera katalogów.

## Idapdiff

Program narzędziowy wiersza komend do synchronizowania replik LDAP.

**Uwaga:** Ta komenda może działać przez długi czas w zależności od liczby pozycji (i atrybutów tych pozycji), które są replikowane.

## Składnia

(Porównuje i synchronizuje dane między dwoma serwerami w środowisku replikacji).

```
ldapdiff -b nazwa_wyróżniająca_bazy -sh host -ch host [-a] [-C liczba_pozycji]
[-cD dn] [-cK baza_kluczy] [-cw hasło] [-cN etykieta_klucza]
[-cp port] [-cP hasło_bazy_kluczy] [-cZ] [-F] [-L nazwa_pliku] [-sD dn] [-sK baza_kluczy]
[-sw hasło] [-sN etykieta_klucza] [-sp port] [-sP hasło_bazy_kluczy]
[-sZ] [-v]
```

lub

(Porównuje schemat między dwoma serwerami).

```
ldapdiff -S -sh host -ch host [-a] [-C liczba_pozycji] [-cD dn]
[-cK baza_kluczy] [-cw hasło] [-cN etykieta_klucza] [-cp port]
[-cP hasło_bazy_kluczy] [-cZ] [-L nazwa_pliku] [-sD dn]
[-sK baza_kluczy] [-sw hasło] [-sN etykieta_klucza] [-sp port]
[-sP hasło_pliku_kluczy] [-sZ] [-v]
```

## Opis

To narzędzie synchronizuje serwer replik z serwerem głównym. Aby wyświetlić pomoc dotyczącą składni komendy **ldapdiff**, wpisz:

```
ldapdiff -?
```

## Opcje

Poniższe opcje dotyczą komendy **ldapdiff**. Istnieją dwie podgrupy: jedna dotyczy serwera wysyłającego, druga serwera odbierającego.

- a** Określa użycie elementu sterującego administracją serwerem dla operacji zapisu w replice tylko do odczytu.
- b** *nazwa\_wyróżniająca\_bazy* Używa bazy wyszukiwania jako początkowego punktu wyszukiwania zamiast punktu domyślnego. Jeśli nie określono opcji **-b**, to narzędzie sprawdza zmienną środowiskową LDAP\_BASEDN i szuka definicji podstawy wyszukiwania.
- C** *liczba\_pozycji* Określa liczbę pozycji do poprawy. Jeśli wystąpi więcej niezgodności niż określono w tej opcji, narzędzie kończy pracę.
- F** To jest opcja poprawki. Jeśli będzie określona, zawartość repliki odbierającej zostanie zmieniona na zgodną z zawartością serwera wysyłającego. Nie można jej używać, jeśli określono również opcję **-S**.
- L** Jeśli nie podano opcji **-F**, należy użyć tej opcji do wygenerowania pliku LDIF z danymi wyjściowymi. Pliku LDIF można używać do aktualizowania serwera odbierającego w celu wyeliminowania różnic.
- S** Umożliwia porównanie schematów na obu serwerach.
- v** Używa trybu szczegółowego z wieloma komunikatami diagnostycznymi wysyłanymi na wyjście standardowe.

## Opcje dla serwera wysyłającego replikacji

Poniższe opcje dotyczą serwera wysyłającego i są oznaczone literą 's' na początku nazwy opcji.

- sD** *nazwa\_wyróżniająca* Parametr *nazwa\_wyróżniająca* umożliwia utworzenie łączenia z katalogiem LDAP. *nazwa\_wyróżniająca* jest nazwą DN w postaci łańcucha znaków.
- sh** *host* Określa nazwę hosta.

**-sK** *plik\_kluczy*

Określa nazwę pliku bazy danych kluczy SSL z domyślnym rozszerzeniem **kdb**. Jeśli nie podano tego parametru lub wartość jest łańcuchem pustym (-sK""), używana jest systemowa baza kluczy. Jeśli plik bazy danych kluczy nie znajduje się w bieżącym katalogu, należy podać jego nazwę z pełną ścieżką.

**-sN** *etykieta\_klucza*

Określa etykietę powiązaną z certyfikatem klienta w pliku bazy danych kluczy. Jeśli etykietę określono bez określania pliku kluczy, etykieta jest identyfikatorem aplikacji w Menedżerze certyfikatów cyfrowych. Domyślną etykietą (identyfikatorem aplikacji) jest QIBM\_GLD\_DIRSRV\_CLIENT. 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 *etykieta\_klucza* nie jest wymagany, jeśli określono domyślną parę certyfikat/klucz prywatny. Podobnie parametr *etykieta\_klucza* nie jest wymagany, jeśli w wyznaczonej bazie danych kluczy znajduje się pojedyncza para certyfikat/klucz prywatny. Parametr ten jest ignorowany, gdy nie zostanie podana opcja **-Z** ani **-sK**.

**-sp** *port\_ldap*

Określa alternatywny port TCP, na którym serwer ldap prowadzi nasłuch. Domyślnym portem LDAP jest 389. Jeśli nie podano opcji **-sp**, a podano parametr **-sZ**, używany jest domyślny port 636 SSL LDAP.

**-sP** *haslo\_pliku\_kluczy*

Określa hasło bazy danych kluczy. Hasło to jest wymagane w celu uzyskania dostępu do szyfrowanych informacji w pliku bazy danych kluczy, który może zawierać jeden lub wiele kluczy prywatnych. Jeśli z plikiem bazy danych kluczy jest związany plik ukrytych haseł, hasło jest otrzymywane z niego pliku i parametr **-sP** nie jest wymagany. Parametr ten jest ignorowany, gdy nie zostanie podana opcja **-Z** ani **-sK**. Hasło nie jest używane, jeśli dla używanej bazy kluczy istnieje plik ukrytych haseł.

**-st** *typ\_zaufanej\_bazy*

Określa etykietę związaną z certyfikatem klienta w pliku zaufanej bazy danych. 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 może być certyfikat klienta. Parametr *typ\_zaufanej\_bazy* nie jest wymagany, jeśli określono domyślną parę certyfikat/klucz prywatny. Podobnie parametr *typ\_zaufanej\_bazy* nie jest wymagany, jeśli w wyznaczonej bazie danych kluczy znajduje się pojedyncza para certyfikat/klucz prywatny. Parametr ten jest ignorowany, gdy nie zostanie podana opcja **-Z** ani **-sT**.

**-sZ** Używa bezpiecznego połączenia SSL w komunikacji z serwerem LDAP.

## Opcje dla serwera odbierającego replikacji

Poniższe opcje dotyczą serwera odbierającego i są oznaczone literą 'c' na początku nazwy opcji. Jeśli **-cZ** podano bez określania wartości dla opcji **-cK**, **-cN** lub **-cP**, opcje te używają tej samej wartości określonej dla opcji SSL serwera wysyłającego. Aby zastąpić opcje serwera wysyłającego i użyć ustawień domyślnych, należy podać **-cK ""** **-cN ""** **-cP ""**.

**-cD** *nazwa\_wyróżniająca*

Parametr *nazwa\_wyróżniająca* umożliwia utworzenie łączenia z katalogiem LDAP. *nazwa\_wyróżniająca* jest nazwą DN w postaci łańcucha znaków.

**-ch** *host*

Określa nazwę hosta.

**-cK** *plik\_kluczy*

Określa nazwę pliku bazy danych kluczy SSL z domyślnym rozszerzeniem **kdb**. Jeśli wartość jest łańcuchem pustym (-sK""), używana jest systemowa baza kluczy. Jeśli plik bazy danych kluczy nie znajduje się w bieżącym katalogu, należy podać jego nazwę z pełną ścieżką.

**-cN** *etykieta\_klucza*

Określa etykietę powiązaną z certyfikatem klienta w pliku bazy danych kluczy. Jeśli serwer LDAP jest skonfigurowany tylko do uwierzytelniania serwera, certyfikat klienta nie jest wymagany. Jeśli etykietę

określono bez określania pliku kluczy, etykieta jest identyfikatorem aplikacji w Menedżerze certyfikatów cyfrowych. Domyślną etykietą (identyfikatorem aplikacji) jest QIBM\_GLD\_DIRSrv\_CLIENT. Jeśli serwer LDAP jest skonfigurowany do uwierzytelniania klienta i serwera, wymagany jest certyfikat klienta. Parametr *etykieta\_klucza* nie jest wymagany, jeśli określono domyślną parę certyfikat/klucz prywatny. Podobnie parametr *etykieta\_klucza* nie jest wymagany, jeśli w wyznaczonej bazie danych kluczy znajduje się pojedyncza para certyfikat/klucz prywatny. Parametr jest ignorowany, gdy nie zostanie podana opcja **-cZ** lub **-cK**.

**-cp** *port\_ldap*

Określa alternatywny port TCP, na którym serwer ldap prowadzi nasłuch. Domyślnym portem LDAP jest 389. Jeśli nie podano opcji **-cp**, a podano parametr **-cZ**, używany jest domyślny port 636 SSL LDAP.

**-cP** *hasło\_bazy\_kluczy*

Określa hasło bazy danych kluczy. Hasło to jest wymagane w celu uzyskania dostępu do szyfrowanych informacji w pliku bazy danych kluczy, który może zawierać jeden lub wiele kluczy prywatnych. Jeśli z plikiem bazy danych kluczy jest związany plik ukrytych haseł, hasło jest otrzymywane z niego pliku i parametr **-cP** nie jest wymagany. Parametr jest ignorowany, gdy nie zostanie podana opcja **-cZ** lub **-cK**.

**-cw** *hasło* | ?

Do uwierzytelniania używa podanego *hasła*. Podanie wartości ? spowoduje wywołanie zachęty do wpisania hasła.

**-cZ** Używa bezpiecznego połączenia SSL w komunikacji z serwerem LDAP.

## Przykłady

```
ldapdiff -b <nazwa_wyróżniająca_bazy> -sh <nazwa_hosta_wysyłającego> \  
-ch <nazwa_hosta_odbierającego> [opcje]
```

lub

```
ldapdiff -S -sh <nazwa_hosta_wysyłającego> -ch <nazwa_hosta_odbierającego> [opcje]
```

## Diagnostyka

Jeśli nie wystąpiły żadne błędy, statusem wyjścia jest 0. Wystąpienie błędu powoduje zwrócenie niezerowego statusu wyjścia i wypisanie komunikatu diagnostycznego na standardowe wyjście błędów.

### Zadania pokrewne

“Zarządzanie kolejkami replikacji” na stronie 165

Ten temat zawiera informacje dotyczące monitorowania statusu replikacji dla każdej umowy replikacji (kolejki) używanej przez dany serwer.

### Odsyłacze pokrewne

“Replikacja - przegląd” na stronie 37

Poprzez replikację zmiany wprowadzone w jednym katalogu są rozsyłane do jednego lub wielu dodatkowych katalogów. Dzięki temu zmiana w jednym katalogu jest widoczna w wielu różnych katalogach.

## Używanie protokołu SSL z programami narzędziowymi LDAP wiersza komend

Ten temat zawiera informacje o używaniu protokołu SSL podczas pracy z programami narzędziowymi LDAP wiersza komend.

W temacie “Protokoły SSL (Secure Sockets Layer) i TLS (Transport Layer Security) na serwerze Directory Server” na stronie 52 omówiono używanie protokołu SSL z serwerem LDAP Directory Server. Informacje te obejmują tworzenie zaufanych ośrodków certyfikacji dla programu DCM i zarządzanie nimi.

Niektóre serwery LDAP, z których korzysta klient, używają wyłącznie uwierzytelniania serwera. W przypadku tych serwerów należy tylko zdefiniować jeden lub kilka certyfikatów użytkowników zaufanych 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 także dostarczonych w funkcjach API referencji LDAP, które służą do łączenia z serwerem katalogów. Na przykład, jeśli serwer LDAP używa certyfikatu Verisign o wysokim zaufaniu, należy:

1. Uzyskać z Verisign certyfikat CA.
2. Użyć programu DCM do zaimportowania go do bazy certyfikatów.
3. Użyć programu 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. Dotyczy to także dostarczonych w funkcjach API referencji LDAP, które służą do łączenia z serwerem katalogów.
- Utworzyć parę kluczy i zażądać certyfikatu klienta z ośrodka certyfikacji. Po otrzymaniu podpisanego certyfikatu z ośrodka certyfikacji należy go przesłać do pliku kluczy w systemie klienta.

#### Pojęcia pokrewne

“Protokoły SSL (Secure Sockets Layer) i TLS (Transport Layer Security) na serwerze Directory Server” na stronie 52

Aby komunikacja z serwerem Directory Server była bezpieczniejsza, serwer może używać protokołów SSL (Secure Sockets Layer) i TLS (Transport Layer Security).

## Format wymiany danych LDAP (LDIF)

Format wymiany danych LDAP (LDAP Data Interchange Format - LDIF) to standardowy format używany do tekstowego zapisu reprezentacji obiektów LDAP i operacji na obiektach LDAP (dodawanie, modyfikowanie, usuwanie, zmiana nazwy wyróżniającej). Pliki zawierające rekordy LDIF mogą być używane do przenoszenia danych między serwerami katalogów lub podawane jako dane wejściowe programów narzędziowych LDAP, takich jak **ldapadd** i **ldapmodify**.

Rekordy treści w formacie LDIF reprezentują zawartość katalogu LDAP. Każdy rekord składa się z wiersza identyfikującego obiekt, po którym następują wiersze zawierające pary atrybut-wartość dotyczące tego obiektu. Pliki tego typu są używane przez program narzędziowy **ldapadd** powłoki Qshell, jak również przez narzędzia importu i eksportu katalogów w programie System i Navigator oraz komendy CL CPYFRMLDIF (LDIF2DB) i CPYTOLDIF (DB2LDIF).

**Uwaga:** Zaleca się wykonywanie komendy DB2LDIF w ramach jednego, autonomicznego zadania.

Rekordy zmian w formacie LDIF reprezentują operacje aktualizowania katalogu. Każdy taki rekord składa się z wiersza identyfikującego obiekt w katalogu, po którym następują wiersze opisujące zmiany wprowadzane w tym obiekcie. Zmiany te mogą polegać na dodawaniu, usuwaniu lub przenoszeniu obiektów bądź zmianie ich nazw, jak również modyfikowaniu istniejących obiektów.

Oba typy rekordów mogą być zapisywane w dwóch formatach wejściowych: standardowym formacie LDIF, zdefiniowanym w dokumencie RFC 2849 (The LDAP Data Interchange Format (LDIF) - Technical Specification), oraz starszym, niestandardowym formacie modyfikowania. Zaleca się korzystanie ze standardowego formatu LDIF. Starszy format jest tu opisany wyłącznie dla potrzeb obsługi starszych narzędzi, które generują lub przyjmują dane w tym formacie.

## | **Formaty danych wejściowych**

| Programy narzędziowe powłoki Qshell **ldapmodify** i **ldapadd** akceptują dwa formaty danych wejściowych. Typ danych wejściowych jest określany na podstawie formatu pierwszego wiersza danych przekazanych do programu **ldapmodify** lub **ldapadd**.

| Pierwszy wiersz danych wejściowych przekazywanych do komendy ldapmodify lub ldapadd musi określać nazwę wyróżniającą pozycji w katalogu, która będzie dodawana lub modyfikowana. Wiersz ten musi mieć następującą postać:  
| dn: nazwa\_wyróżniająca

| lub  
| nazwa\_wyróżniająca

| gdzie dn: jest literałem łańcuchowym, a nazwa\_wyróżniająca jest nazwą wyróżniającą pozycji w katalogu, która ma być zmodyfikowana (lub dodana). Jeśli zostanie znaleziony łańcuch dn:, ustawiany jest format wejściowy LDIF zgodny z RFC 2849. Jeśli łańcuch ten nie zostanie znaleziony, ustawiany jest niestandardowy format modyfikowania.

### | **Uwaga:**

- | 1. Komenda **ldapadd** ma działanie równoważne z wywołaniem komendy **ldapmodify -a**.
- | 2. Programy narzędziowe **ldapmodify** i **ldapadd** nie obsługują nazw wyróżniających w kodowaniu base64.

### | **Odsyłacze pokrewne**

| "ldapmodify i ldapadd" na stronie 218  
| Programy narzędziowe wiersza komend służące do dodawania i modyfikowania pozycji w katalogu LDAP.  
| "ldapsearch" na stronie 236  
| Program narzędziowy wiersza komend do wyszukiwania w katalogu LDAP.

## | **Standardowy format LDIF zgodny z dokumentem RFC 2849**

| Zalecane jest użycie standardowego formatu LDIF zdefiniowanego w dokumencie RFC 2849 "The LDAP Data Interchange Format (LDIF)". Plik LDIF może zaczynać się od opcjonalnych dyrektyw **version** i **charset**: np. version: 1 oraz charset: ISO-8859-1.

| Dyrektywa **charset** przydaje się w przypadku użycia systemów plików na innych platformach, które nie obsługują oznaczania plików identyfikatorem CCSID. W systemie i5/OS standardowym działaniem jest otwieranie plików LDIF przy użyciu kodowania UTF-8 (CCSID 1208) i zezwolenie systemowi plików na przekształcenie danych z identyfikatora CCSID pliku do UTF-8, dlatego dyrektywa **charset** zazwyczaj nie jest potrzebna.

| Po opcjonalnych wierszach **version** i **charset** następuje opisana poniżej seria rekordów zmian.

| W przypadku formatu LDIF zgodnego z dokumentem RFC 2849 typy i wartości atrybutów są oddzielone pojedynczym dwukropkiem (:) lub podwójnym dwukropkiem (::). Ponadto pojedyncze zmiany w wartościach atrybutów są oddzielone wierszem wejściowym **changetype:**. Ogólna postać wierszy wejściowych w pliku LDIF zgodnym z RFC 2849 jest następująca:

```
| rekord_zmiany  
| <pusty wiersz>  
| rekord_zmiany  
| <pusty wiersz>  
| .  
| .  
| .
```

| Plik wejściowy w formacie LDIF zgodnym z dokumentem RFC 2849 składa się z jednego lub wielu zestawów wierszy rekordów zmian oddzielonych pojedynczym pustym wierszem. Każdy rekord\_zmiany ma następującą postać:

```
| dn: <nazwa_wyróżniająca>  
| [changetype: {modify|add|modrdn|moddn|delete}]  
| klauzula_zmiany
```

```
| klauzula_zmiany  
| .  
| .  
| .
```

Zatem rekord\_zmiany składa się z wiersza wskazującego nazwę wyróżniającą pozycji katalogu do zmodyfikowania, opcjonalnego wiersza wskazującego typ modyfikacji pozycji w katalogu oraz jednego lub wielu zestawów wierszy klauzula\_zmiany. Jeśli wiersz changetype: zostanie pominięty, zakłada się, że typ zmiany to modify (modyfikacja), o ile wywołanie komendy nie miało postaci ldapmodify -a lub ldapadd, w którym to przypadku zakłada się, że typ\_zmiany to add (dodanie).

Kiedy typem zmiany jest modify (modyfikacja), każda klauzula\_zmiany jest definiowana jako zestaw wierszy w postaci:

```
| add: {typ_atrybutu}  
| {typ_atrybutu}{separator}{wartość}  
| .  
| .  
| .  
| -
```

lub

```
| replace: {typ_atrybutu}  
| {typ_atrybutu}{separator}{wartość}  
| .  
| .  
| .  
| -
```

lub

```
| delete: {typ_atrybutu}  
| [{typ_atrybutu}{separator}{wartość}]  
| .  
| .  
| .  
| -
```

lub

```
| {typ_atrybutu}{separator}{wartość}  
| .  
| .  
| .
```

Podanie dyrektywy replace (zastąpienie) powoduje zastąpienie wszystkich istniejących wartości atrybutu podanym zestawem atrybutów. Podanie dyrektywy add (dodanie) powoduje dodanie wartości do istniejącego zestawu wartości atrybutu. Podanie dyrektywy delete (usunięcie) bez rekordów par atrybut-wartość powoduje usunięcie wszystkich wartości podanego atrybutu. Podanie dyrektywy delete z jedną lub wieloma parami atrybut-wartość powoduje usunięcie tylko wartości podanych w rekordach par atrybut-wartość.

Jeśli zostanie podany dowolny z wierszy add: typ\_atrybutu, replace: typ\_atrybutu lub delete: typ\_atrybutu (indykator zmiany), jako ogranicznik zmian dla tego typu\_atrybutu oczekiwany jest wiersz zawierający łącznik (-). Par atrybut-wartość oczekuje się w wierszach wejściowych, które znajdują się między indykatorem zmiany a wierszem z łącznikiem. Jeśli wiersz typ\_zmiany zostanie pominięty, zakłada się, że typ\_zmiany to add dla komendy ldapadd i replace dla komendy ldapmodify.

Wartość atrybutu można określić jako łańcuch tekstowy, wartość zakodowaną w formacie base-64 lub adres URL pliku zgodnie z użytym separatorem (separator).

**attrtype: wartość**

Pojedynczy dwukropek (:) określa, że wartością jest łańcuch wartość.

#### | **attrtype:: łańcuch\_base64**

| Podwójny dwukropek (::) określa, że *łańcuch\_base64* jest zakodowaną w formacie base-64 reprezentacją wartości binarnej lub łańcucha UTF-8, który zawiera znaki wielobajtowe.

#### | **attrtype:< adres\_URL\_pliku**

| Dwukropek i lewy nawias trójkątny (:<) oznacza, że wartość należy odczytać z pliku określonego przez adres\_URL\_pliku. Przykładem wiersza z adresem URL pliku określającego, że wartość atrybutu jpegPhoto znajduje się w pliku /tmp/photo.jpg jest

| jpegphoto:< file:///tmp/photo.jpg

| Wszelkie białe znaki między separatorem a wartością atrybutu są ignorowane. Wartości atrybutów można rozłożyć na wiele wierszy, używając znaku pojedynczej spacji jako pierwszego znaku w następnym wierszu wejściowym. W przypadku użycia podwójnego dwukropka jako separatora oczekiwane są dane wejściowe w formacie base64. W tym formacie kodowania każdym trzem binarnym bajtom odpowiadają cztery znaki tekstowe.

| Aby podać wiele wartości atrybutu, można użyć wielu specyfikacji {typ\_atrybutu}{separator}{wartość}.

| Kiedy typem zmiany jest add (dodanie), każda klauzula\_zmiany jest definiowana jako zestaw wierszy w postaci:

| {typ\_atrybutu}{separator}{wartość}

| Podobnie jak w przypadku typu zmiany modify separatorem (separator) może być pojedynczy dwukropek (:), podwójny dwukropek (::) lub dwukropek i lewy nawias trójkątny (:<). Wszelkie białe znaki między separatorem a wartością atrybutu są ignorowane. Wartości atrybutów można rozłożyć na wiele wierszy, używając znaku pojedynczej spacji jako pierwszego znaku w następnym wierszu wejściowym. W przypadku użycia podwójnego dwukropka jako separatora oczekiwane są dane wejściowe w formacie base64.

| Kiedy typem zmiany jest modrdn lub moddn, każda klauzula\_zmiany jest definiowana jako zestaw wierszy w postaci:

| newrdn: wartość  
| deleteoldrdn:{0|1}  
| [newsuperior: nowa\_nadrzędna\_nazwa\_wyróżniająca]

| Są to parametry, które można określić dla operacji LDAP modify RDN (zmiana nazwy) lub modifyDN (przeniesienie). Wartością ustawienia newrdn jest nowa nazwa RDN, która zostanie użyta podczas wykonywania operacji modify RDN. Jako wartość ustawienia deleteoldrdn należy określić 0, aby zapisać atrybut w starej nazwie RDN, lub 1, aby usunąć wartości atrybutów ze starej nazwy RDN. Wartością ustawienia nowa\_nadrzędna\_nazwa\_wyróżniająca jest nazwa wyróżniająca nowego elementu nadrzędnego podczas przenoszenia pozycji.

| Kiedy typem zmiany jest delete, nie określa się klauzuli\_zmiany.

#### | **Przykład formatu LDIF:**

| W tym temacie przedstawiono przykłady poprawnych danych wejściowych dla komendy **ldapmodify** z wykorzystaniem formatu LDIF zdefiniowanego w dokumencie RFC 2849.

#### | **Dodawanie nowej pozycji**

| Następujący przykład ilustruje dodawanie nowej pozycji do katalogu przy użyciu nazwy cn=Tomek Kowalski, ou=Dział, o=Firma, c=PL, zakładając, że wywoływana jest komenda **ldapadd** lub **ldapmodify -a**:

| dn:cn=Tomek Kowalski, ou=Dział, o=Firma, c=PL  
| changetype:add  
| cn: Tomek Kowalski  
| sn: Kowalski  
| objectclass: organizationalperson  
| objectclass: person  
| objectclass: top

| Następujący przykład ilustruje dodawanie nowej pozycji do katalogu przy użyciu nazwy `cn=Tomek Kowalski`,  
| `ou=Dział`, `o=Firma`, `c=PL`, zakładając, że wywoływana jest komenda **ldapadd** lub **ldapmodify -a**. Należy zauważyć,  
| że atrybut `jpegphoto` jest ładowany z pliku `/tmp/tomekkowalski.jpg`.

```
| dn:cn=Tomek Kowalski, ou=Dział, o=Firma, c=PL
| changetype:add
| cn: Tomek Kowalski
| sn: Kowalski
| jpegphoto:< file:///tmp/tomekkowalski.jpg
| objectclass: inetorgperson
| objectclass: organizationalperson
| objectclass: person
| objectclass: top
```

### | **Dodawanie typów atrybutów**

| Następujący przykład ilustruje dodawanie dwóch nowych typów atrybutów do istniejącej pozycji. Należy zwrócić  
| uwagę, że atrybutowi `registeredaddress` przypisywane są dwie wartości:

```
| dn:cn=Tomek Kowalski, ou=Dział, o=Firma, c=PL
| changetype: modify
| add: telephonenumber
| telephonenumber: 888 555 1234
| -
| add: registeredaddress
| registeredaddress: tk@firma.pl
| registeredaddress: trk@firma.pl
```

### | **Zmiana nazwy pozycji**

| Następujący przykład ilustruje zmianę nazwy istniejącej pozycji na `cn=Tomek Romek Kowalski`, `ou=Dział`,  
| `o=Firma`, `c=PL`. Stara nazwa RDN, `cn=Tomek Kowalski`, jest zachowywana jako dodatkowa wartość atrybutu `cn`.  
| Nowa nazwa RDN, `cn=Tomek Romek Kowalski`, jest przez serwer LDAP automatycznie dodawana do wartości  
| atrybutu `cn` pozycji:

```
| dn:cn=Tomek Kowalski, ou=Dział, o=Firma, c=PL
| changetype:modrdn
| newrdn: cn=Tomek Romek Kowalski
| deleteoldrdn: 0
```

| Następujący przykład ilustruje przeniesienie pracownika `cn=Tomek Kowalski` do działu `ou=Nowy dział`; nazwa RDN  
| (`cn=Tomek Kowalski`) pozostaje bez zmian.

```
| dn:cn=Tomek Kowalski, ou=Dział, o=Firma, c=PL
| changetype:moddn
| newrdn: cn=Tomek Kowalski
| deleteoldrdn: 0
| newsuperior: ou=Nowy dział, o=Firma, c=PL
```

### | **Zastępowanie wartości atrybutów**

| W następującym przykładzie wartości atrybutów `telephonenumber` i `registeredaddress` zostają zastąpione  
| podanymi wartościami.

```
| dn: cn=Tomek Romek Kowalski, ou=Dział, o=Firma, c=PL
| changetype: modify
| replace: telephonenumber
| telephonenumber: 888 555 4321
| -
| replace: registeredaddress
| registeredaddress: tomek@firma.pl
| registeredaddress: tomekrk@firma.pl
```

## | Usuwanie i dodawanie atrybutów

| Następujący przykład ilustruje usunięcie atrybutu `telephonenumber`, usunięcie jednej z wartości atrybutu `registeredaddress` i dodanie atrybutu `description`:

```
| dn: cn=Tomek Romek Kowalski, ou=Dział, o=Firma, c=PL
| changetype: modify
| add: description
| description: To bardzo długa wartość atrybutu,
| kontynuowana w kolejnych wierszach.
| Spacje poprzedzające kolejne wiersze
| sygnalizują, że pierwszy wiersz jest
| kontynuowany.
| -
| delete: telephonenumber
| -
| delete: registeredaddress
| registeredaddress: tomek@firma.pl
```

## | Usuwanie pozycji

| Następujący przykład ilustruje usuwanie pozycji katalogu o nazwie `cn=Tomek Romek Kowalski, ou=Dział, o=Firma, c=PL`:

```
| dn: cn=Tomek Romek Kowalski, ou=Dział, o=Firma, c=PL
| changetype:delete
```

## | Niestandardowy format modyfikowania rekordów

| Starszy, niestandardowy format danych wejściowych dla komend `ldapmodify` i `ldapadd` nie jest tak elastyczny, jak format LDIF zdefiniowany w dokumencie RFC 2849, jednak w niektórych sytuacjach jest łatwiejszy w użyciu.

| W niestandardowym formacie danych wejściowych typy i wartości atrybutów są rozdzielane znakiem równości (=). Ogólna postać wierszy wejściowych formatu niestandardowego wygląda następująco:

```
| rekord_zmiany
| <pusty wiersz>
| rekord_zmiany
| <pusty wiersz>
| .
| .
| .
```

| Plik danych wejściowych w formacie niestandardowym zawiera jedną lub wiele grup wierszy *rekord\_zmian*, rozdzielanych pojedynczymi pustymi wierszami. Każdy *rekord\_zmian* ma następującą postać:

```
| nazwa_wyróżniająca
| [+|-]{typ_atrybutu} = {wartość_wiersz1[\
| wartość_wiersz2[\
| ...wartość_wierszN]}}
```

| Każdy *rekord\_zmian* składa się zatem z wiersza określającego nazwę wyróżniającą pozycji w katalogu, która ma zostać zmodyfikowana, po którym następuje jeden lub wiele wierszy modyfikowania atrybutów. Każdy wiersz modyfikowania atrybutu składa się z opcjonalnego indykatora dodawania lub usuwania (+ lub -), typu atrybutu i wartości atrybutu. Jeśli zostanie podany plus (+), typ modyfikacji zostanie ustawiony na **add** (dodawanie). Jeśli zostanie podany minus (-), typ modyfikacji zostanie ustawiony na **delete** (usuwanie). W przypadku usuwania usunięcie całego atrybutu można osiągnąć poprzez pominięcie znaku równości (=) i *wartości* atrybutu. Jeśli nie zostanie podany indykator dodawania ani usuwania, typ modyfikacji zostanie ustawiony na dodawanie, chyba że zostanie podana opcja `-r`, co spowoduje ustawienie typu modyfikacji **replace** (zastępowanie). Z wartości atrybutów usuwane są wszelkie początkowe i końcowe białe znaki. Jeśli wymagana jest obecność końcowych białych znaków w wartościach atrybutów, należy używać formatu danych wejściowych LDIF zgodnego z RFC 2849. Wiersze można kontynuować poprzez podanie ukośnika odwrotnego (\) jako ostatniego znaku wiersza. Podczas przetwarzania wiersza

| kontynuowanego znaku ukośnika odwrotnego jest usuwany, a kolejny wiersz jest dopisywany bezpośrednio po znaku  
| poprzedzającym ukośnik odwrotny. Znak nowego wiersza kończący wiersz wejściowy nie jest włączany do wynikowej  
| wartości atrybutu.

| Do definiowania wielu wartości atrybutu należy używać wielu osobnych definicji *typ\_atributu=wartość*.

| Jeśli zostanie podana opcja obsługi wartości binarnych pobieranych z plików (-b), *wartość* rozpoczynająca się znakiem  
| '/' jest interpretowana jako nazwa pliku. Na przykład następujący wiersz oznacza, że wartość atrybutu jpegphoto ma  
| zostać pobrana z pliku /tmp/photo.jpg:

| jpegphoto=/tmp/photo.jpg

### | **Przykłady niestandardowego formatu modyfikowania rekordów:**

| W tym temacie przedstawiono przykłady poprawnych danych wejściowych dla komendy **ldapmodify** w  
| niestandardowym formacie modyfikowania.

### | **Dodawanie nowej pozycji**

| Następujący przykład ilustruje dodawanie nowej pozycji do katalogu przy użyciu nazwy cn=Tomek Kowalski,  
| ou=Dział, o=Firma, c=PL:

```
| cn=Tomek Kowalski, ou=Dział, o=Firma, c=PL  
| cn=Tomek Kowalski  
| sn=Kowalski  
| objectclass=organizationalperson  
| objectclass=person  
| objectclass=top
```

### | **Dodawanie nowego typu atrybutu**

| Następujący przykład ilustruje dodawanie dwóch nowych typów atrybutów do istniejącej pozycji. Należy zwrócić  
| uwagę, że atrybutowi **registeredaddress** przypisywane są dwie wartości:

```
| cn=Tomek Kowalski, ou=Dział, o=Firma, c=PL  
| +telephonenumber=888 555 1234  
| +registeredaddress=tk@firma.pl  
| +registeredaddress=trk@firma.pl
```

### | **Zastępowanie wartości atrybutów**

| Przypuśćmy, że wywołanie komendy miało postać:

```
| ldapmodify -r ...
```

| W następującym przykładzie wartości atrybutów **telephonenumber** i **registeredaddress** zostają zastąpione  
| podanymi wartościami. Jeśli opcja wiersza komend **-r** nie zostanie podana, wartości atrybutów zostaną dodane do  
| istniejącego zestawu wartości atrybutów.

```
| cn=Tomek Kowalski, ou=Dział, o=Firma, c=PL  
| telephonenumber=888 555 4321  
| registeredaddress: tomek@firma.pl  
| registeredaddress: tomekrk@firma.pl
```

### | **Usuwanie typu atrybutu**

| Następujący przykład ilustruje usunięcie jednej z wartości atrybutu **registeredaddress** z istniejącej pozycji.

```
| cn=Tomek Kowalski, ou=Dział, o=Firma, c=PL  
| -registeredaddress=tomek@firma.pl
```

## I Dodawanie atrybutu

I Następujący przykład ilustruje dodanie atrybutu `description`. Wartość atrybutu `description` obejmuje wiele wierszy:

```
I cn=Tomek Kowalski, ou=Dział, o=Firma, c=PL
I +description=To jest bardzo długa wartość atrybutu \
I kontynuowana w kolejnych wierszach. \
I Ukośnik odwrotny na końcu każdego wiersza \
I sygnalizuje, że wiersz będzie \
I kontynuowany.
```

## I Schemat konfiguracji serwera Directory Server

W tych informacjach opisano drzewo informacji katalogu (Directory Information Tree - DIT) oraz atrybuty używane do konfigurowania pliku `ibmslapd.conf`.

W poprzednich wersjach ustawienia konfiguracji katalogu przechowywane były w zastrzeżonym formacie w pliku konfiguracyjnym. Obecnie ustawienia katalogu są przechowywane w formacie LDIF w pliku konfiguracyjnym.

Plik konfiguracyjny ma nazwę `ibmslapd.conf`. Obecnie dostępny jest także schemat używany przez plik konfiguracyjny. Typy atrybutów znajdują się w pliku `v3.config.at`, a klasy obiektu w pliku `v3.config.oc`. Atrybuty można modyfikować za pomocą komendy `ldapmodify`.

### Pojęcia pokrewne

“Sprawdzanie schematu” na stronie 31

Po zainicjowaniu serwera pliki schematu są odczytywane oraz sprawdzana jest ich spójność i poprawność.

### Odsyłacze pokrewne

“`ldapmodify` i `ldapadd`” na stronie 218

Programy narzędziowe wiersza komend służące do dodawania i modyfikowania pozycji w katalogu LDAP.

## Drzewo informacji katalogu

W tym temacie opisano drzewo informacji katalogu serwera Directory Server.

`cn=Configuration`

- `cn=Admin`
- `cn=Event Notification`
- `cn=Front End`
- `cn=Kerberos`
- `cn=Master Server`
- `cn=Referral`
- `cn=Schema`
  - `cn=IBM Directory`
    - `cn=Config Backends`
      - `cn=ConfigDB`
    - `cn=RDBM Backends`
      - `cn=Directory`
      - `cn=ChangeLog`
    - `cn=LDCF Backends`
      - `cn=SchemaDB`
- `cn=SSL`
  - `cn=CRL`
- `cn=Transaction`



## **cn=Configuration**

### **Nazwa wyróżniająca**

cn=Configuration

**Opis** Jest to pozycja najwyższego poziomu w drzewie DIT konfiguracji. Zawiera ona dane o znaczeniu globalnym dla serwera, choć w praktyce może zawierać także inne informacje. Każdy atrybut w tej pozycji pochodzi z pierwszej sekcji (sekcji globalnej) pliku ibmslapd.conf.

**Liczba** 1 (wymagane)

### **Klasa obiektu**

ibm-slapdTop

### **Atrybuty obowiązkowe**

- cn
- ibm-slapdAdminDN
- ibm-slapdAdminPW
- ibm-slapdErrorLog
- ibm-slapdPort
- ibm-slapdPwEncryption
- ibm-slapdSizeLimit
- ibm-slapdSysLogLevel
- ibm-slapdTimeLimit
- objectClass

### **Atrybuty opcjonalne**

- ibm-slapdACLAccess
- ibm-slapdACIMechanism
- ibm-slapdConcurrentRW (należy unikać)
- ibm-slapdMaxPendingChangesDisplayed
- ibm-slapdServerId
- ibm-slapdSupportedWebAdmVersion
- ibm-slapdVersion

## **cn=Admin**

### **Nazwa wyróżniająca**

cn=Admin, cn=Configuration

**Opis** Globalne ustawienia konfiguracyjne demona IBM Admin

**Liczba** 1 (wymagane)

### **Klasa obiektu**

ibm-slapdAdmin

### **Atrybuty obowiązkowe**

- cn
- ibm-slapdErrorLog
- ibm-slapdPort

### **Atrybuty opcjonalne**

- ibm-slapdSecurePort

## **cn=Event Notification**

### **Nazwa wyróżniająca**

cn=Event Notification, cn=Configuration

**Opis** Globalne ustawienia powiadamiania o zdarzeniach dla serwera Directory Server

**Liczba** 0 lub 1 (opcjonalne, potrzebne tylko w przypadku włączenia powiadamiania o zdarzeniach)

### **Klasa obiektu**

ibm-slapdEventNotification

### **Atrybuty obowiązkowe**

- cn
- ibm-slapdEnableEventNotification
- objectClass

### **Atrybuty opcjonalne**

- ibm-slapdMaxEventsPerConnection
- ibm-slapdMaxEventsTotal

## **cn=Front End**

### **Nazwa wyróżniająca**

cn=Front End, cn=Configuration

**Opis** Globalne ustawienia dotyczące środowiska używane przez serwer w momencie uruchomienia.

**Liczba** 0 lub 1 (opcjonalne)

### **Klasa obiektu**

ibm-slapdFrontEnd

### **Atrybuty obowiązkowe**

- cn
- objectClass

### **Atrybuty opcjonalne**

- ibm-slapdACLCache
- ibm-slapdACLCacheSize
- ibm-slapdDB2CP
- ibm-slapdEntryCacheSize
- ibm-slapdFilterCacheBypassLimit
- ibm-slapdFilterCacheSize
- ibm-slapdPlugin
- ibm-slapdSetenv
- ibm-slapdIdleTimeOut

## **cn=Kerberos**

### **Nazwa wyróżniająca**

cn=Kerberos, cn=Configuration

**Opis** Globalne ustawienia uwierzytelniania Kerberos dla serwera Directory Server.

**Liczba** 0 lub 1 (opcjonalne)

### **Klasa obiektu**

ibm-slapdKerberos

### Atrybuty obowiązkowe

- cn
- ibm-slapdKrbEnable
- ibm-slapdKrbRealm
- ibm-slapdKrbKeyTab
- ibm-slapdKrbIdentityMap
- ibm-slapdKrbAdminDN
- objectClass

### Atrybuty opcjonalne

- Brak

## cn=Master Server

### Nazwa wyróżniająca

cn=Master Server, cn=Configuration

**Opis** Podczas konfigurowania repliki pozycja ta zawiera referencje do łączenia oraz adres URL odwołania do serwera głównego.

**Liczba** 0 lub 1 (opcjonalne)

### Klasa obiektu

ibm-slapdReplication

### Atrybuty obowiązkowe

- cn
- ibm-slapdMasterPW (Obowiązkowy, gdy nie korzysta się z uwierzytelniania Kerberos).

### Atrybuty opcjonalne

- ibm-slapdMasterDN
- ibm-slapdMasterPW (Opcjonalny, gdy używa się uwierzytelniania Kerberos).
- ibm-slapdMasterReferral
- objectClass

## cn=Referral

### Nazwa wyróżniająca

cn=Referral, cn=Configuration

**Opis** Pozycja ta zawiera wszystkie pozycje odwołań z pierwszej sekcji (sekcji globalnej) pliku ibmslapd.conf. Jeśli nie ma żadnych odwołań (domyślnie nie ma żadnych), pozycja ta jest opcjonalna.

**Liczba** 0 lub 1 (opcjonalne)

### Klasa obiektu

ibm-slapdReferral

### Atrybuty obowiązkowe

- cn
- ibm-slapdReferral
- objectClass

### Atrybuty opcjonalne

- Brak

## cn=Schemas

### Nazwa wyróżniająca

cn=Schemas, cn=Configuration

**Opis** Pozycja ta służy jako kontener na schematy. Nie jest ona niezbędna, ponieważ schematy można rozróżnić na podstawie ich klasy obiektu `ibm-slapdSchema`. Została ona włączona w celu poprawy czytelności drzewa informacji katalogu.

Obecnie dozwolona jest tylko jedna pozycja schematu: `cn=IBM Directory`.

**Liczba** 1 (wymagane)

### Klasa obiektu

Kontener

### Atrybuty obowiązkowe

- `cn`
- `objectClass`

### Atrybuty opcjonalne

- Brak

## cn=IBM Directory

### Nazwa wyróżniająca

cn=IBM Directory, cn=Schemas, cn=Configuration

**Opis** Pozycja ta zawiera wszystkie dane konfiguracyjne schematu z pierwszej sekcji (sekcji globalnej) pliku `ibmslapd.conf`. Służy także jako kontener dla wszystkich postprocesorów używających schematu. Obecnie wiele schematów nie jest obsługiwanych, ale jeśli występują, wtedy dla każdego z nich istnieje pozycja `ibm-slapdSchema`. Należy zauważyć, że schematy wielokrotne uważane są za niekompatybilne. Dlatego postprocesor można skojarzyć tylko z jednym schematem.

**Liczba** 1 (wymagane)

### Klasa obiektu

`ibm-slapdSchema`

### Atrybuty obowiązkowe

- `cn`
- `ibm-slapdSchemaCheck`
- `ibm-slapdIncludeSchema`
- `objectClass`

### Atrybuty opcjonalne

- `ibm-slapdSchemaAdditions`

## cn=Config Backends

### Nazwa wyróżniająca

cn=Config Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

**Opis** Pozycja ta służy jako pojemnik dla postprocesorów konfiguracyjnych.

**Liczba** 1 (wymagane)

### Klasa obiektu

Kontener

### Atrybuty obowiązkowe

- `cn`

- objectClass

#### Atrybuty opcjonalne

Brak

### cn=ConfigDB

#### Nazwa wyróżniająca

cn=ConfigDB, cn=Config Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

**Opis** Postprocessor konfiguracji serwera IBM Directory Server

**Liczba** 0 - n (opcjonalne)

#### Klasa obiektu

ibm-slapdConfigBackend

#### Atrybuty obowiązkowe

- ibm-slapdSuffix
- ibm-slapdPlugin

#### Atrybuty opcjonalne

- ibm-slapdReadOnly

### cn=RDBM Backends

#### Nazwa wyróżniająca

cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

**Opis** Pozycja ta służy jako pojemnik dla postprocesorów RDBM. Zastępuje ona efektywnie wiersz database rdbm w pliku ibmslapd.conf, identyfikując wszystkie podpozycje jako postprocesory DB2. Nie jest ona niezbędna, ponieważ postprocesory RDBM można rozróżnić na podstawie ich klasy obiektu ibm-slapdRdbmBackend. Została ona włączona w celu poprawy czytelności drzewa informacji katalogu.

**Liczba** 0 lub 1 (opcjonalne)

#### Klasa obiektu

Kontener

#### Atrybuty obowiązkowe

- cn
- objectClass

#### Atrybuty opcjonalne

- Brak

### cn=Directory

#### Nazwa wyróżniająca

cn=Directory, cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

**Opis** Pozycja ta zawiera wszystkie ustawienia konfiguracyjne bazy danych domyślnego postprocesora RDBM.

Chociaż można utworzyć wiele postprocesorów o dowolnych nazwach, Administrowanie serwerem zakłada, że "cn=Directory" jest głównym postprocesorem katalogu, oraz że "cn=ChangeLog Log" jest opcjonalnym postprocesorem protokołu zmian. Tylko przyrostki wyświetlane w "cn=Directory" są konfigurowalne za pomocą Administrowania serwerem (z wyjątkiem przyrostka protokołu zmian, który ustawiany jest w sposób przezroczysty przez włączenie protokołu zmian).

**Liczba** 0 - n (opcjonalne)

#### Klasa obiektu

ibm-slapdRdbmBackend

### Atrybuty obowiązkowe

- cn
- ibm-slapdDbInstance
- ibm-slapdDbName
- ibm-slapdDbUserID
- objectClass

### Atrybuty opcjonalne

- ibm-slapdBulkloadErrors
- ibm-slapdChangeLogMaxEntries
- ibm-slapdCLIErrors
- ibm-slapdDBAlias
- ibm-slapdDB2CP
- ibm-slapdDbConnections
- ibm-slapdDbLocation
- ibm-slapdPagedResAllowNonAdmin
- ibm-slapdPagedResLmt
- ibm-slapdPageSizeLmt
- ibm-slapdPlugin
- ibm-slapdReadOnly
- ibm-slapdReplDbConns
- ibm-slapdSortKeyLimit
- ibm-slapdSortSrchAllowNonAdmin
- ibm-slapdSuffix
- ibm-slapdUseProcessIdPw

**Uwaga:** W przypadku użycia atrybutu **ibm-slapdUseProcessIdPw**, należy zmodyfikować schemat, aby atrybut **ibm-slapdDbUserPW** był opcjonalny.

## cn=Change Log

### Nazwa wyróżniająca

cn=Change Log, cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

**Opis** Pozycja ta zawiera wszystkie ustawienia konfiguracyjne bazy danych postprocesora protokołu zmian.

**Liczba** 0 - n (opcjonalne)

### Klasa obiektu

ibm-slapdRdbmBackend

### Atrybuty obowiązkowe

- cn
- ibm-slapdDbInstance
- ibm-slapdDbName
- ibm-slapdDbUserID
- objectClass

### Atrybuty opcjonalne

- ibm-slapdBulkloadErrors
- ibm-slapdChangeLogMaxEntries
- ibm-slapdCLIErrors

- ibm-slapdDBAlias
- ibm-slapdDB2CP
- ibm-slapdDbConnections
- ibm-slapdDbLocation
- ibm-slapdPagedResAllowNonAdmin
- ibm-slapdPagedResLmt
- ibm-slapdPageSizeLmt
- ibm-slapdPlugin
- ibm-slapdReadOnly
- ibm-slapdReplDbConns
- ibm-slapdSortKeyLimit
- ibm-slapdSortSrchAllowNonAdmin
- ibm-slapdSuffix
- ibm-slapdUseProcessIdPw

**Uwaga:** W przypadku użycia atrybutu **ibm-slapdUseProcessIdPw**, należy zmodyfikować schemat, aby atrybut **ibm-slapdDbUserPW** był opcjonalny.

## cn=LDCF Backends

### Nazwa wyróżniająca

cn=LDCF Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

**Opis** Pozycja ta służy jako pojemnik dla postprocesorów LDCF. Zastępuje ona efektywnie wiersz database ldcf w pliku ibmslapd.conf, identyfikując wszystkie podpozycje jako postprocesory LDCF. Nie jest ona niezbędna, ponieważ postprocesory LDCF można rozróżniać na podstawie ich klasy obiektu ibm-slapdLdcfBackend. Została ona włączona w celu poprawy czytelności drzewa informacji katalogu.

**Liczba** 1 (wymagane)

### Klasa obiektu

Kontener

### Atrybuty obowiązkowe

- cn
- objectClass

### Atrybuty opcjonalne

- ibm-slapdPlugin

## cn=SchemaDB

### Nazwa wyróżniająca

cn=SchemaDB, cn=LDCF Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

**Opis** Pozycja ta zawiera wszystkie ustawienia konfiguracyjne bazy danych z sekcji database ldcf pliku ibmslapd.conf.

**Liczba** 1 (wymagane)

### Klasa obiektu

ibm-slapdLdcfBackend

### Atrybuty obowiązkowe

- cn
- objectClass

### Atrybuty opcjonalne

- ibm-slapdPlugin
- ibm-slapdSuffix

## cn=SSL

### Nazwa wyróżniająca

cn=SSL, cn=Configuration

**Opis** Globalne ustawienia połączenia SSL dla serwera Directory Server.

**Liczba** 0 lub 1 (opcjonalne)

### Klasa obiektu

ibm-slapdSSL

### Atrybuty obowiązkowe

- cn
- ibm-slapdSecurity
- ibm-slapdSecurePort
- ibm-slapdSslAuth
- objectClass

### Atrybuty opcjonalne

- ibm-slapdSslCertificate
- ibm-slapdSslCipherSpec

**Uwaga:** Użycie atrybutu **ibm-slapdSslCipherSpecs** nie jest zalecane. Należy zamiast niego używać atrybutu **ibm-slapdSslCipherSpec**. W przypadku użycia atrybutu **ibm-slapdSslCipherSpecs** serwer przekształca go w atrybut obsługiwany.

- ibm-slapdSslKeyDatabase
- ibm-slapdSslKeyDatabasePW

## cn=CRL

### Nazwa wyróżniająca

cn=CRL, cn=SSL, cn=Configuration

**Opis** Pozycja ta zawiera dane z listy odwołań certyfikatów z pierwszej sekcji (globalnej) pliku ibmslapd.conf. Jest ona potrzebna tylko wtedy, gdy określono "ibm-slapdSslAuth = serverclientauth" w pozycji cn=SSL i wydano certyfikaty klienta do weryfikacji CRL.

**Liczba** 0 lub 1 (opcjonalne)

### Klasa obiektu

ibm-slapdCRL

### Atrybuty obowiązkowe

- cn
- ibm-slapdLdapCrlHost
- ibm-slapdLdapCrlPort
- objectClass

### Atrybuty opcjonalne

- ibm-slapdLdapCrlUser
- ibm-slapdLdapCrlPassword



## cn=Transaction

### Nazwa wyróżniająca

cn = Transaction, cn = Configuration

**Opis** Określa globalne ustawienia dotyczące obsługi transakcji. Obsługa transakcji udostępniana jest za pomocą modułu dodatkowego:

```
extendedop /QSYS.LIB/QGLDTRANEX.SRVPGM tranExtOpInit 1.3.18.0.2.12.5  
1.3.18.0.2.12.6
```

Serwer (**slapd**) ładuje ten moduł dodatkowy automatycznie podczas startu, jeśli określono **ibm-slapdTransactionEnable = TRUE**. Modułu dodatkowego nie trzeba jawnie dodawać do pliku **ibmslapd.conf**.

**Liczba** 0 lub 1 (opcjonalne, wymagane tylko w przypadku używania transakcji)

### Klasa obiektu

ibm-slapdTransaction

### Atrybuty obowiązkowe

- cn
- ibm-slapdMaxNumOfTransactions
- ibm-slapdMaxOpPerTransaction
- ibm-slapdMaxTimeLimitOfTransactions
- ibm-slapdTransactionEnable
- objectClass

### Atrybuty opcjonalne

- Brak

## Atrybuty

W tym temacie opisano atrybuty serwera Directory Server używane do konfigurowania pliku **ibmslapd.conf**.

- cn
- ibm-slapdACIMechanism
- ibm-slapdACLAccess
- ibm-slapdACLCache
- ibm-slapdACLCacheSize
- ibm-slapdAdminDN
- ibm-slapdAdminGroupEnabled
- ibm-slapdAdminPW
- ibm-slapdAllowAnon
- ibm-slapdAllReapingThreshold
- ibm-slapdAnonReapingThreshold
- ibm-slapdBoundReapingThreshold
- ibm-slapdBulkloadErrors
- ibm-slapdCachedAttribute
- ibm-slapdCachedAttributeAutoAdjust
- ibm-slapdCachedAttributeAutoAdjustTime
- ibm-slapdCachedAttributeAutoAdjustTimeInterval
- ibm-slapdCachedAttributeSize
- ibm-slapdChangeLogMaxEntries
- ibm-slapdCLIErrors

- ibm-slapdConcurrentRW
- ibm-slapdDB2CP
- ibm-slapdDBAlias
- ibm-slapdDbConnections
- ibm-slapdDbInstance
- ibm-slapdDbLocation
- ibm-slapdDbName
- ibm-slapdDbUserID
- ibm-slapdDbUserPW
- ibm-slapdDerefAliases
- ibm-slapdDigestAdminUser
- ibm-slapdDigestAttr
- ibm-slapdDigestRealm
- ibm-slapdEnableEventNotification
- ibm-slapdEntryCacheSize
- ibm-slapdErrorLog
- ibm-slapdESizeThreshold
- ibm-slapdEThreadActivate
- ibm-slapdEThreadEnable
- ibm-slapdETimeThreshold
- ibm-slapdFilterCacheBypassLimit
- ibm-slapdFilterCacheSize
- ibm-slapdIdleTimeOut
- ibm-slapdIncludeSchema
- ibm-slapdKrbAdminDN
- ibm-slapdKrbEnable
- ibm-slapdKrbIdentityMap
- ibm-slapdKrbKeyTab
- ibm-slapdKrbRealm
- ibm-slapdLanguageTagsEnabled
- ibm-slapdLdapCrlHost
- ibm-slapdLdapCrlPassword
- ibm-slapdLdapCrlPort
- ibm-slapdLdapCrlUser
- ibm-slapdMasterDN
- ibm-slapdMasterPW
- ibm-slapdMasterReferral
- ibm-slapdMaxEventsPerConnection
- ibm-slapdMaxEventsTotal
- ibm-slapdMaxNumOfTransactions
- ibm-slapdMaxOpPerTransaction
- ibm-slapdMaxPendingChangesDisplayed
- ibm-slapdMaxTimeLimitOfTransactions
- ibm-slapdPagedResAllowNonAdmin
- ibm-slapdPagedResLmt

- ibm-slapdPageSizeLmt
- ibm-slapdPlugin
- ibm-slapdPort
- ibm-slapdPwEncryption
- ibm-slapdReadOnly
- ibm-slapdReferral
- ibm-slapdReplDbConns
- ibm-slapdReplicaSubtree
- ibm-slapdSchemaAdditions
- ibm-slapdSchemaCheck
- ibm-slapdSecurePort
- ibm-slapdSecurity
- ibm-slapdServerId
- ibm-slapdSetenv
- ibm-slapdSizeLimit
- ibm-slapdSortKeyLimit
- ibm-slapdSortSrchAllowNonAdmin
- ibm-slapdSslAuth
- ibm-slapdSslCertificate
- ibm-slapdSslCipherSpec
- ibm-slapdSslKeyDatabase
- ibm-slapdSslKeyDatabasePW
- ibm-slapdSslKeyRingFile
- ibm-slapdSuffix
- ibm-slapdSupportedWebAdmVersion
- ibm-slapdSysLogLevel
- ibm-slapdTimeLimit
- ibm-slapdTransactionEnable
- ibm-slapdUseProcessIdPw
- ibm-slapdVersion
- ibm-slapdWriteTimeout
- objectClass

## **cn**

**Opis** Jest to atrybut nazwy zwykłej X.500, który zawiera nazwę obiektu.

### **Składnia**

Ciąg znaków katalogu

### **Maksymalna długość**

256

### **Wartość**

Wielowartościowy

## **ibm-slapdACIMechanism**

**Opis** Określa, którego modelu ACL używa serwer. (Obsługiwany tylko w systemie i5/OS i OS/400 od wersji 3.2, ignorowany na innych platformach.)

- 1.3.18.0.2.26.1 = model listy ACL IBM SecureWay v3.1
- 1.3.18.0.2.26.2 = model listy ACL IBM SecureWay v3.2

**Wartość domyślna**

1.3.18.0.2.26.2 = model listy ACL IBM SecureWay v3.2

**Składnia**

Ciąg znaków katalogu

**Maksymalna długość**

256

**Wartość**

Wielowartościowy

**ibm-slapdACLAccess**

**Opis** Określa, czy włączony jest dostęp do list ACL. Wartość TRUE oznacza, że dostęp do list ACL jest włączony. Wartość FALSE oznacza, że dostęp do list ACL jest wyłączony.

**Wartość domyślna**

TRUE

**Składnia**

Boolowski

**Maksymalna długość**

5

**Wartość**

Jednowartościowy

**ibm-slapdACLCache**

**Opis** Określa, czy serwer buforuje informacje z list ACL w pamięci podręcznej.

- Wartość TRUE oznacza, że serwer buforuje informacje z list ACL w pamięci podręcznej.
- Wartość FALSE oznacza, że serwer nie buforuje informacji z list ACL w pamięci podręcznej.

**Wartość domyślna**

TRUE

**Składnia**

Boolowski

**Maksymalna długość**

5

**Wartość**

Jednowartościowy

**ibm-slapdACLCacheSize**

**Opis** Maksymalna liczba pozycji przechowywanych w pamięci podręcznej ACL.

**Wartość domyślna**

25000

**Składnia**

Liczba całkowita

**Maksymalna długość**

11

**Wartość**

Jednowartościowy

## **ibm-slapdAdminDN**

**Opis** Nazwa wyróżniająca łączenia administratora dla serwera Directory Server.

**Wartość domyślna**

cn=root

**Składnia**

Nazwa wyróżniająca

**Maksymalna długość**

Nieograniczona

**Wartość**

Jednowartościowy

## **ibm-slapdAdminGroupEnabled**

**Opis** Określa, czy grupa administracyjna jest aktualnie włączona. Ustawienie TRUE powoduje, że serwer zezwala użytkownikom grupy administracyjnej na zalogowanie się.

**Wartość domyślna**

FALSE

**Składnia**

Boolowski

**Maksymalna długość**

128

**Wartość**

Jednowartościowy

## **ibm-slapdAdminPW**

**Opis** Hasło łączenia administratora dla serwera Directory Server.

**Wartość domyślna**

secret

**Składnia**

Kod binarny

**Maksymalna długość**

128

**Wartość**

Jednowartościowy

## **ibm-slapdAllowAnon**

**Opis** Określa, czy anonimowe łączenia są dozwolone.

**Wartość domyślna**

True

**Składnia**

Boolowski

**Maksymalna długość**

128

**Wartość**

Jednowartościowy

### **ibm-slapdAllReapingThreshold**

**Opis** Określa liczbę obsługiwanych połączeń na serwerze zanim zarządzanie połączeniem zostanie aktywowane.

**Wartość domyślna**

1200

**Składnia**

Ciąg znaków katalogu (z rozróżnianiem wielkości liter).

**Maksymalna długość**

1024

**Wartość**

Jednowartościowy

### **ibm-slapdAnonReapingThreshold**

**Opis** Określa liczbę obsługiwanych połączeń na serwerze zanim zarządzanie połączeniem dla połączeń anonimowych zostanie aktywowane.

**Wartość domyślna**

0

**Składnia**

Ciąg znaków katalogu (z rozróżnianiem wielkości liter).

**Maksymalna długość**

1024

**Wartość**

Jednowartościowy

### **ibm-slapdBoundReapingThreshold**

**Opis** Określa liczbę obsługiwanych połączeń na serwerze zanim zarządzanie połączeniem dla połączeń anonimowych i przypisanych zostanie aktywowane.

**Wartość domyślna**

1100

**Składnia**

Ciąg znaków katalogu (z rozróżnianiem wielkości liter).

**Maksymalna długość**

1024

**Wartość**

Jednowartościowy

### **ibm-slapdBulkloadErrors**

**Opis** Ścieżka do pliku lub urządzenie maszyny hosta ibmslapd, do którego mają być zapisywane komunikaty o błędach ładowania masowego.

**Wartość domyślna**

/var/bulkload.log

**Składnia**

Ciąg znaków katalogu (z rozróżnianiem wielkości liter)

**Maksymalna długość**

1024

**Wartość**

Jednowartościowy

## **ibm-slapdCachedAttribute**

**Opis** Zawiera nazwy atrybutów przeznaczonych do przechowania w pamięci podręcznej atrybutu (po jednej nazwie atrybutu dla każdej wartości).

**Wartość domyślna**

Brak

**Składnia**

Ciąg znaków katalogu

**Maksymalna długość**

256

**Wartość**

Wielowartościowy

## **ibm-slapdCachedAttributeAutoAdjust**

**Opis** Określa, czy serwer ma automatycznie dopasować pamięci podręczne atrybutów według skonfigurowanych częstotliwości zdefiniowanych w `ibm-slapdCachedAttributeAutoAdjustTime` oraz `ibm-slapdCachedAttributeAutoAdjustTimeInterval`.

**Wartość domyślna**

FALSE

**Składnia**

Boolowski

**Maksymalna długość**

5

**Wartość**

Jednowartościowy

## **ibm-slapdCachedAttributeAutoAdjustTime**

**Opis** Jeśli `ibm-slapdCachedAttributeAutoAdjust` ma wartość TRUE, określa godzinę, w której serwer rozpoczyna automatyczne dopasowywanie pamięci podręcznych.

Minimum = T000000

Maksimum = T235959

**Wartość domyślna**

T000000

**Składnia**

Czas wojskowy

**Maksymalna długość**

7

**Wartość**

Jednowartościowy

## **ibm-slapdCachedAttributeAutoAdjustTimeInterval**

**Opis** Jeśli `ibm-slapdCachedAttributeAutoAdjust` ma wartość TRUE, określa częstotliwość automatycznych dopasowań pamięci podręcznej atrybutu.

Minimum = 1

Maksimum = 24

**Wartość domyślna**

2

**Składnia**

Liczba całkowita

**Maksymalna długość**

2

**Wartość**

Jednowartościowy

**ibm-slapdCachedAttributeSize**

**Opis** Ilość pamięci, wyrażona w bajtach, która może zostać użyta przez pamięć podręczną atrybutu. Wartość 0 oznacza, że pamięć podręczna atrybutu nie jest używana.

**Wartość domyślna**

0

**Składnia**

Liczba całkowita

**Maksymalna długość**

11

**Wartość**

Jednowartościowy.

**ibm-slapdChangeLogMaxEntries**

**Opis** Atrybut ten używany jest przez moduł dodatkowy protokołu zmian do określania maksymalnej liczby pozycji protokołu zmian dozwolonych w bazie danych RDBM. Każdy protokół zmian ma swój własny atrybut changeLogMaxEntries.

Minimum = 0 (brak ograniczenia)

Maksimum = 2.147.483.647 (32-bitowa liczba całkowita ze znakiem)

**Wartość domyślna**

0

**Składnia**

Liczba całkowita

**Maksymalna długość**

11

**Wartość**

Jednowartościowy

**ibm-slapdCLIErrors**

**Opis** Ścieżka do pliku lub urządzenie maszyny hosta ibmslapd, do którego mają być zapisywane komunikaty o błędach interfejsu CLI.

**Wartość domyślna**

/var/db2cli.log

**Składnia**

Ciąg znaków katalogu (z rozróżnianiem wielkości liter)

**Maksymalna długość**

1024

**Wartość**

Jednowartościowy



## **ibm-slapdConcurrentRW**

**Opis** Ustawienie tej wartości na TRUE umożliwia jednocześnie wyszukiwanie i aktualizację. Umożliwia to 'niepewne odczyty', tzn. rezultaty, które mogą nie być spójne z zatwierdzonym stanem bazy danych.

**Ważne:** Użycie tego atrybutu nie jest zalecane.

**Wartość domyślna**

FALSE

**Składnia**

Boolowski

**Maksymalna długość**

5

**Wartość**

Jednowartościowy

## **ibm-slapdDB2CP**

**Opis** Określa stronę kodową bazy danych katalogu. Stroną kodową baz danych UTF-8 jest 1208.

**Składnia**

Ciąg znaków katalogu (z rozróżnianiem wielkości liter)

**Maksymalna długość**

11

**Wartość**

Jednowartościowy

## **ibm-slapdDBAlias**

**Opis** Alias bazy danych DB2.

**Składnia**

Ciąg znaków katalogu (z rozróżnianiem wielkości liter)

**Maksymalna długość**

8

**Wartość**

Jednowartościowy

## **ibm-slapdDbConnections**

**Opis** Określa liczbę połączeń DB2 które serwer przeznaczona dla danego postprocesora DB2. Wartość musi zawierać się w przedziale 5 - 50 (włącznie).

**Uwaga:** Zmienna środowiskowa ODBCCONS przesłania wartość tej dyrektywy.

Jeśli wartość `ibm-slapdDbConnections` (lub `ODBCCONS`) jest mniejsza od 5 lub większa od 50, serwer będzie używał, odpowiednio, wartości 5 lub 50. Zostanie utworzone jedno dodatkowe połączenie dla replikacji (nawet jeśli żadna replikacja nie została zdefiniowana). Dwa dodatkowe połączenia zostaną utworzone dla protokołu zmian (jeśli zostanie on włączony).

**Wartość domyślna**

15

**Składnia**

Liczba całkowita

**Maksymalna długość**

50

**Wartość**

Jednowartościowy

**ibm-slapdDbInstance**

**Opis** Określa instancję bazy danych DB2 danego postprocesora.

**Wartość domyślna**

ldapdb2

**Składnia**

Ciąg znaków katalogu (z rozróżnianiem wielkości liter)

**Maksymalna długość**

8

**Wartość**

Jednowartościowy

**Uwaga:** Wszystkie obiekty `ibm-slapdRdbmBackend` muszą używać tych samych wartości atrybutów `ibm-slapdDbInstance`, `ibm-slapdDbUserID`, `ibm-slapdDbUserPW` oraz tego samego zestawu znaków DB2.

**ibm-slapdDbLocation**

**Opis** Ścieżka w systemie plików do bazy danych postprocesora.

**Składnia**

Ciąg znaków katalogu (z rozróżnianiem wielkości liter)

**Maksymalna długość**

1024

**Wartość**

Jednowartościowy

**ibm-slapdDbName**

**Opis** Określa nazwę bazy danych DB2 danego postprocesora.

**Wartość domyślna**

ldapdb2

**Składnia**

Ciąg znaków katalogu (z rozróżnianiem wielkości liter)

**Maksymalna długość**

8

**Wartość**

Jednowartościowy

**ibm-slapdDbUserID**

**Opis** Określa nazwę użytkownika, za pomocą której dany postprocesor ma łączyć się z bazą danych DB2.

**Wartość domyślna**

ldapdb2

**Składnia**

Ciąg znaków katalogu (z rozróżnianiem wielkości liter)

**Maksymalna długość**

8

**Wartość**

Jednowartościowy

**Uwaga:** Wszystkie obiekty `ibm-slapdRdbmBackend` muszą używać tych samych wartości atrybutów `ibm-slapdDbInstance`, `ibm-slapdDbUserID` i `ibm-slapdDbUserPW` oraz tego samego zestawu znaków DB2.

**ibm-slapdDerefAliases**

**Opis** Maksymalny poziom wyłuskiwania aliasów dla żądań wyszukiwania, niezależnie od opcji wyłuskiwania aliasów określonych w żądaniach klienta. Dozwolone są wartości **never** (nigdy), **find** (odnajdywanie), **search** (wyszukiwanie) **always** (zawsze).

**Wartość domyślna**

zawsze

**Składnia**

Ciąg znaków katalogu

**Maksymalna długość**

6

**Wartość**

Jednowartościowy

**ibm-slapdDbUserPW**

**Opis** Określa hasło użytkownika, za pomocą którego dany postprocesor ma łączyć się z bazą danych DB2. Hasło może być jawnym tekstem lub zaszyfrowane za pomocą algorytmu `imask`.

**Wartość domyślna**

`ldapdb2`

**Składnia**

Kod binarny

**Maksymalna długość**

128

**Wartość**

Jednowartościowy

**Uwaga:** Wszystkie obiekty `ibm-slapdRdbmBackend` muszą używać tych samych wartości atrybutów `ibm-slapdDbInstance`, `ibm-slapdDbUserID`, `ibm-slapdDbUserPW` oraz tego samego zestawu znaków DB2.

**ibm-slapdDigestAdminUser**

**Opis** Określa nazwę użytkownika Digest MD5 administratora LDAP lub członka grupy administracyjnej. Używane, kiedy do uwierzytelniania administratora wykorzystywane jest MD5 Digest.

**Wartość domyślna**

Brak

**Składnia**

Ciąg znaków katalogu

**Maksymalna długość**

512

**Wartość**

Jednowartościowy

## **ibm-slapdDigestAttr**

**Opis** Przesłania domyślny atrybut nazwy użytkownika DIGEST-MD5. Nazwa atrybutu, z którego korzysta opcja wyszukiwania nazwy użytkownika łączenia SASL DIGEST-MD5. Jeśli wartość nie jest określona, serwer używa identyfikatora uid.

### **Wartość domyślna**

Jeśli wartość nie jest określona, serwer używa uid.

### **Składnia**

Ciąg znaków katalogu.

### **Maksymalna długość**

64

### **Wartość**

Jednowartościowy

## **ibm-slapdDigestRealm**

**Opis** Przesłania domyślną dziedzinę DIGEST-MD5. Jest to łańcuch, dzięki któremu użytkownicy mogą dowiedzieć się, która nazwa użytkownika i które hasło powinny zostać użyte, w przypadku gdy użytkownicy posiadają różne nazwy i hasła dla różnych serwerów. W zamyśle byłaby to nazwa kolekcji kont, która mogłyby zawierać konta użytkowników. Łańcuch ten powinien zawierać co najmniej nazwę hosta realizującego uwierzytelnianie i może dodatkowo wskazywać kolekcję użytkowników mogących posiadać dostęp. Na przykład `uzytkownicy_zarejestrowani@gotham.news.example.com`. Jeśli atrybut nie jest określony, serwer używa pełnej nazwy hosta serwera.

### **Wartość domyślna**

Pełna nazwa hosta serwera

### **Składnia**

Ciąg znaków katalogu.

### **Maksymalna długość**

1024

### **Wartość**

Jednowartościowy

## **ibm-slapdEnableEventNotification**

**Opis** Wskazuje, czy włączać powiadamianie o zdarzeniach. Musi mieć wartość TRUE lub FALSE.

Ustawienie FALSE oznacza, że serwer odrzuca wszystkie żądania klientów dotyczące zarejestrowania powiadomień o zdarzeniach, zwracając rozszerzony wynik LDAP\_UNWILLING\_TO\_PERFORM.

### **Wartość domyślna**

TRUE

### **Składnia**

Boolowski

### **Maksymalna długość**

5

### **Wartość**

Jednowartościowy

## **ibm-slapdEntryCacheSize**

**Opis** Maksymalna liczba pozycji przechowywanych w pamięci podręcznej pozycji.

### **Wartość domyślna**

25000

**Składnia**

Liczba całkowita

**Maksymalna długość**

11

**Wartość**

Jednowartościowy

**ibm-slapdErrorLog**

**Opis** Określa ścieżkę do pliku lub urządzenie na maszynie z serwerem Directory Server, do którego zapisywane są komunikaty o błędach.

**Wartość domyślna**

/var/ibmslapd.log

**Składnia**

Ciąg znaków katalogu (z rozróżnianiem wielkości liter)

**Maksymalna długość**

1024

**Wartość**

Jednowartościowy

**ibm-slapdESizeThreshold**

**Opis** Określa liczbę elementów pracy czekających w kolejce roboczej zanim wątek ratunkowy zostanie aktywowany.

**Wartość domyślna**

50

**Składnia**

Liczba całkowita

**Maksymalna długość**

1024

**Wartość**

Jednowartościowy

**ibm-slapdEThreadActivate**

**Opis** Określa warunki aktywujące wątek ratunkowy. Musi przyjmować jedną z następujących wartości:

**S** Tylko wielkość

**T** Tylko czas

**SOT** Wielkość lub czas

**SAT** Wielkość i czas

**Wartość domyślna**

SAT

**Składnia**

Ciąg znaków

**Maksymalna długość**

1024

**Wartość**

Jednowartościowy

## **ibm-slapdEThreadEnable**

**Opis** Określa, czy wątek ratunkowy jest aktywny.

**Wartość domyślna**

True

**Składnia**

Boolowski

**Maksymalna długość**

1024

**Wartość**

Jednowartościowy

## **ibm-slapdETimeThreshold**

**Opis** Określa w minutach okres czasu między elementami usuniętymi z kolejki roboczej zanim wątek ratunkowy zostanie aktywowany.

**Wartość domyślna**

5

**Składnia**

Liczba całkowita

**Maksymalna długość**

1024

**Wartość**

Jednowartościowy

## **ibm-slapdFilterCacheBypassLimit**

**Opis** Filtry wyszukiwania, które dopasowały większą liczbą pozycji niż określona przez ten atrybut, nie są dodawane do pamięci podręcznej filtru wyszukiwania. Ponieważ w tej pamięci podręcznej zawarta jest lista identyfikatorów pozycji zgodnych z filtrem, ustawienie to pomaga ograniczyć wykorzystanie pamięci. Wartość równa 0 oznacza brak ograniczenia.

**Wartość domyślna**

100

**Składnia**

Liczba całkowita

**Maksymalna długość**

11

**Wartość**

Jednowartościowy

## **ibm-slapdFilterCacheSize**

**Opis** Maksymalna liczba pozycji przechowywanych w filtrze wyszukiwania.

**Wartość domyślna**

25000

**Składnia**

Liczba całkowita

**Maksymalna długość**

11

**Wartość**

Jednowartościowy

**ibm-slapdIdleTimeOut**

**Opis** Maksymalny czas utrzymywania otwartego połączenia LDAP, kiedy połączenie nie jest ono aktywne. Czasem bezczynności połączenia LDAP jest czas (mierzony w sekundach) pomiędzy ostatnią aktywnością na tym połączeniu, a momentem pomiaru. Jeśli połączenie traci ważność, z powodu czasu bezczynności dłuższego od podanego w tym atrybucie, serwer LDAP czyści i kończy połączenie LDAP, udostępniając je innym nadchodzącym żądaniom.

**Wartość domyślna**

300

**Składnia**

Liczba całkowita

**Długość**

11

**Liczność**

Pojedynczy

**Wykorzystanie**

Operacja na katalogu

**Modyfikowany przez użytkownika**

Tak

**Klasa dostępu**

Newralgiczna

**Wymagany**

Nie

**ibm-slapdIncludeSchema**

**Opis** Określa ścieżkę do pliku na serwerze Directory Server zawierającego definicje schematów.

**Wartość domyślna**

- /etc/V3.system.at
- /etc/V3.system.oc
- /etc/V3.config.at
- /etc/V3.config.oc
- /etc/V3.ibm.at
- /etc/V3.ibm.oc
- /etc/V3.user.at
- /etc/V3.user.oc
- /etc/V3.ldapsyntaxes
- /etc/V3.matchingrules

**Składnia**

Ciąg znaków katalogu (z rozróżnianiem wielkości liter)

**Maksymalna długość**

1024

**Wartość**

Wielowartościowy

## **ibm-slapdKrbAdminDN**

**Opis** Określa identyfikator Kerberos administratora LDAP (np. `ibm-kn=admin1@dziedzina1`). Stosowany, gdy do uwierzytelniania administratora podczas logowania się do interfejsu administrowania serwerem używane jest uwierzytelnianie Kerberos. Atrybut ten można określić zamiast atrybutów `adminDN` i `adminPW` lub oprócz nich.

### **Wartość domyślna**

Nie ma żadnej wstępnie zdefiniowanej wartości domyślnej.

### **Składnia**

Ciąg znaków katalogu (z rozróżnianiem wielkości liter)

### **Maksymalna długość**

128

### **Wartość**

Jednowartościowy

## **ibm-slapdKrbEnable**

**Opis** Określa, czy serwer obsługuje protokół Kerberos. Musi mieć wartość `TRUE` lub `FALSE`.

### **Wartość domyślna**

`TRUE`

### **Składnia**

Boolowski

### **Maksymalna długość**

5

### **Wartość**

Jednowartościowy

## **ibm-slapdKrbIdentityMap**

**Opis** Wskazuje, czy należy używać odwzorowywania tożsamości Kerberos. Musi mieć wartość `TRUE` lub `FALSE`. Ustawienie `TRUE`, kiedy klient jest uwierzytelniany identyfikatorem Kerberos, powoduje, że serwer wyszukuje wszystkich lokalnych użytkowników o odpowiadających temu identyfikatorowi referencjach Kerberos i dodaje ich nazwy DN do referencji danego łączenia. Umożliwia korzystanie z list ACL opartych na nazwach DN użytkowników LDAP do uwierzytelniania Kerberos.

### **Wartość domyślna**

`FALSE`

### **Składnia**

Boolowski

### **Maksymalna długość**

5

### **Wartość**

Jednowartościowy

## **ibm-slapdKrbKeyTab**

**Opis** Określa plik tablicy kluczy Kerberos serwera LDAP. Plik ten zawiera klucz prywatny serwera LDAP, który związany jest z jego kontem Kerberos. Plik ten należy chronić (tak jak plik bazy danych kluczy SSL serwera).

### **Wartość domyślna**

Nie ma żadnej wstępnie zdefiniowanej wartości domyślnej.

### **Składnia**

Ciąg znaków katalogu (z rozróżnianiem wielkości liter)



**Maksymalna długość**

1024

**Wartość**

Jednowartościowy

**ibm-slapdKrbRealm**

**Opis** Określa dziedzinę Kerberos serwera LDAP. Jest używany do publikowania atrybutu ldapservicename w katalogu głównym DSE. Należy zauważyć, że serwer LDAP może służyć jako repozytorium informacji o koncie dla wielu KDC (i dziedzin), ale serwer LDAP, jako serwer obsługujący protokół Kerberos, może być przypisany tylko do jednej dziedziny.

**Wartość domyślna**

Nie ma żadnej wstępnie zdefiniowanej wartości domyślnej.

**Składnia**

Ciąg znaków katalogu (bez rozróżniania wielkości liter)

**Maksymalna długość**

256

**Wartość**

Jednowartościowy

**ibm-slapdLanguageTagsEnabled**

**Opis** Określa, czy serwer powinien zezwalać na znaczniki języka. Wartością tego atrybutu odczytaną z pliku ibmslapd.conf jest FALSE, ale można ją zmienić na TRUE.

**Wartość domyślna**

FALSE

**Składnia**

Boolowski

**Maksymalna długość**

5

**Wartość**

Jednowartościowy

**ibm-slapdLdapCrlHost**

**Opis** Określa nazwę hosta serwera LDAP, który zawiera listy odwołań certyfikatów (CRL) służące do sprawdzania poprawności certyfikatów x.509v3 klientów. Parametr ten jest potrzebny, kiedy atrybut ibm-slapdSslAuth=serverclientauth, a certyfikaty klienta zostały wysłane do sprawdzenia w CRL.

**Wartość domyślna**

Nie ma żadnej wstępnie zdefiniowanej wartości domyślnej.

**Składnia**

Ciąg znaków katalogu (bez rozróżniania wielkości liter)

**Maksymalna długość**

256

**Wartość**

Jednowartościowy

**ibm-slapdLdapCrlPassword**

**Opis** Określa hasło do łączenia z serwerem LDAP, który zawiera listy odwołań certyfikatów (CRL) służące do

sprawdzania poprawności certyfikatów x.509v3 klientów. Parametr ten może być potrzebny, kiedy atrybut `ibm-slapdSslAuth=serverclientauth`, a certyfikaty klienta zostały wysłane do sprawdzenia w CRL.

**Uwaga:** Jeśli serwer LDAP przechowujący listy CRL zezwala na niewierzytelny dostęp do tych list (tzn. dostęp anonimowy), to `ibm-slapdLdapCrIPassword` nie jest wymagane.

**Wartość domyślna**

Nie ma żadnej wstępnie zdefiniowanej wartości domyślnej.

**Składnia**

Kod binarny

**Maksymalna długość**

128

**Wartość**

Jednowartościowy

**ibm-slapdLdapCrIPort**

**Opis** Określa port używany do łączenia się z serwerem LDAP zawierającym listy odwołań certyfikatów (CRL) służące do sprawdzania poprawności certyfikatów x.509v3 klientów. Parametr ten jest potrzebny, kiedy atrybut `ibm-slapdSslAuth=serverclientauth`, a certyfikaty klienta zostały wysłane do sprawdzenia w CRL. (Porty IP to 16-bitowe liczby całkowite bez znaku z zakresu 1 - 65535).

**Wartość domyślna**

Nie ma żadnej wstępnie zdefiniowanej wartości domyślnej.

**Składnia**

Liczba całkowita

**Maksymalna długość**

11

**Wartość**

Jednowartościowy

**ibm-slapdLdapCrIUser**

**Opis** Określa nazwę rozróżniającą do łączenia z serwerem LDAP, który zawiera listy odwołań certyfikatów (CRL) służące do sprawdzania poprawności certyfikatów x.509v3 klientów. Parametr ten może być potrzebny, kiedy atrybut `ibm-slapdSslAuth=serverclientauth`, a certyfikaty klienta zostały wysłane do sprawdzenia w CRL.

**Uwaga:** Jeśli serwer LDAP przechowujący listy CRL zezwala na niewierzytelny dostęp do tych list (tzn. dostęp anonimowy), to `ibm-slapdLdapCrIUser` nie jest wymagane.

**Wartość domyślna**

Nie ma żadnej wstępnie zdefiniowanej wartości domyślnej.

**Składnia**

Nazwa wyróżniająca

**Maksymalna długość**

1000

**Wartość**

Jednowartościowy

**ibm-slapdMasterDN**

**Opis** Określa nazwę DN łączenia serwera głównego. Wartość ta musi być zgodna z nazwą `replicaBindDN` w obiekcie `replicaObject` zdefiniowanym dla serwera głównego. Kiedy do uwierzytelnienia repliki używa się

protokołu Kerberos, `ibm-slapdMasterDN` musi określać nazwę DN reprezentującą identyfikator Kerberos (np. `ibm-kn=freddy@dziedzina1`). Jeśli używany jest protokół Kerberos, atrybut `MasterServerPW` jest ignorowany.

**Wartość domyślna**

Nie ma żadnej wstępnie zdefiniowanej wartości domyślnej.

**Składnia**

Nazwa wyróżniająca

**Maksymalna długość**

1000

**Wartość**

Jednowartościowy

**ibm-slapdMasterPW**

**Opis** Określa hasło łączenia serwera głównego repliki. Wartość ta musi być zgodna z nazwą `replicaBindDN` w obiekcie `replicaObject` zdefiniowanym dla serwera głównego. Kiedy do uwierzytelnienia repliki używa się protokołu Kerberos, `ibm-slapdMasterDN` musi określać nazwę DN reprezentującą identyfikator Kerberos (np. `ibm-kn=freddy@dziedzina1`). Jeśli używany jest protokół Kerberos, atrybut `MasterServerPW` jest ignorowany.

**Wartość domyślna**

Nie ma żadnej wstępnie zdefiniowanej wartości domyślnej.

**Składnia**

Kod binarny

**Maksymalna długość**

128

**Wartość**

Jednowartościowy

**ibm-slapdMasterReferral**

**Opis** Określa adres URL serwera głównego repliki. Na przykład:

`ldap://master.us.ibm.com`

W przypadku ochrony ustawionej wyłącznie na SSL:

`ldaps://master.us.ibm.com:636`

W przypadku ustawienia ochrony na `none` i wykorzystaniu portu niestandardowego:

`ldap://master.us.ibm.com:1389`

**Wartość domyślna**

brak

**Składnia**

Ciąg znaków katalogu (bez rozróżniania wielkości liter)

**Maksymalna długość**

256

**Wartość**

Jednowartościowy

**ibm-slapdMaxEventsPerConnection**

**Opis** Określa maksymalną liczbę powiadomień o zdarzeniach, które można zarejestrować dla każdego połączenia.

Minimum = 0 (brak ograniczenia)

Maksimum = 2147483647

**Wartość domyślna**

100

**Składnia**

Liczba całkowita

**Maksymalna długość**

11

**Wartość**

Jednowartościowy

**ibm-slapdMaxEventsTotal**

**Opis** Określa maksymalną łączną liczbę powiadomień o zdarzeniu, które można zarejestrować dla wszystkich połączeń.

Minimum = 0 (brak ograniczenia)

Maksimum = 2147483647

**Wartość domyślna**

0

**Składnia**

Liczba całkowita

**Maksymalna długość**

11

**Wartość**

Jednowartościowy

**ibm-slapdMaxNumOfTransactions**

**Opis** Określa maksymalną liczbę transakcji na serwer.

Minimum = 0 (brak ograniczenia)

Maksimum = 2147483647

**Wartość domyślna**

20

**Składnia**

Liczba całkowita

**Maksymalna długość**

11

**Wartość**

Jednowartościowy

**ibm-slapdMaxOpPerTransaction**

**Opis** Określa maksymalną liczbę operacji w jednej transakcji.

Minimum = 0 (brak ograniczenia)

Maksimum = 2147483647

**Wartość domyślna**

5

**Składnia**

Liczba całkowita

**Maksymalna długość**

11

**Wartość**  
Jednowartościowy

### **ibm-slapdMaxPendingChangesDisplayed**

**Opis** Maksymalna liczba wyświetlanych oczekujących zmian.

**Wartość domyślna**  
200

**Składnia**  
Liczba całkowita

**Maksymalna długość**  
11

**Wartość**  
Jednowartościowy

### **ibm-slapdMaxTimeLimitOfTransactions**

**Opis** Określa w sekundach maksymalny czas oczekiwania na zakończenie transakcji.  
Minimum = 0 (brak ograniczenia)  
Maksimum = 2147483647

**Wartość domyślna**  
300

**Składnia**  
Liczba całkowita

**Maksymalna długość**  
11

**Wartość**  
Jednowartościowy

### **ibm-slapdPagedResAllowNonAdmin**

**Opis** Określa, czy serwer powinien zezwalać użytkownikom innym niż administrator na określenie w żądaniu wyszukiwania, że wyniki mają być dzielone na strony. Jeśli wartością odczytaną z pliku ibmslapd.conf jest FALSE, serwer będzie przetwarzać tylko żądania klientów wysłane przez użytkowników z uprawnieniami administratora. Jeśli klient żąda wyszukiwania z podziałem rezultatów na strony i nie ma uprawnień administratora, a wartość tego atrybutu odczytana z pliku ibmslapd.conf jest równa FALSE, serwer zwraca klientowi kod powrotu insufficientAccessRights i nie wykonuje wyszukiwania ani stronicowania.

**Wartość domyślna**  
FALSE

**Składnia**  
Boolowski

**Długość**  
5

**Liczność**  
Pojedynczy

**Wykorzystanie**  
Operacje na katalogu

**Modyfikowany przez użytkownika**  
Tak

**Klasa dostępu**  
Newralgiczna

**Klasa obiektu**  
ibm-slapdRdbmBackend

**Wymagany**  
Nie

### **ibm-slapdPagedResLmt**

**Opis** Określa maksymalną liczbę jednocześnie aktywnych nieprzetworzonych stronicowanych rezultatów wyszukiwania. Zakres = 0.... Jeśli klient żąda operacji stronicującej rezultaty, a w danej chwili aktywna jest maksymalna liczba nieprzetworzonych stronicowanych rezultatów, serwer zwraca klientowi kod powrotu oznaczający zajętość; nie zostanie wykonane wyszukiwanie ani stronicowanie.

**Wartość domyślna**  
3

**Składnia**  
Liczba całkowita

**Długość**  
11

**Liczność**  
Pojedynczy

**Wykorzystanie**  
Operacje na katalogu

**Modyfikowany przez użytkownika**  
Tak

**Klasa dostępu**  
Newralgiczna

**Wymagany**  
Nie

**Klasa obiektu**  
ibm-slapdRdbmBackend

### **ibm-slapdPageSizeLmt**

**Opis** Maksymalna liczba pozycji zwracanych przez wyszukiwanie na jednej stronie, kiedy zażądano stronicowania rezultatów, niezależnie od wielkości strony, która mogła zostać określona w żądaniu wyszukiwania przez klienta. Zakres = 0.... Jeśli klient przekazał wielkość strony, używana jest mniejsza z dwóch następujących wartości: przekazanej przez klienta i odczytanej z pliku ibmslapd.conf.

**Wartość domyślna**  
50

**Składnia**  
Liczba całkowita

**Długość**  
11

**Liczność**  
Pojedynczy

**Wykorzystanie**  
Operacje na katalogu

**Modyfikowany przez użytkownika**

Tak

**Klasa dostępu**

Newralgiczna

**Wymagany**

Nie

**Klasa obiektu**

ibm-slapdRdbmBackend

**ibm-slapdPlugin**

**Opis** Moduł dodatkowy jest biblioteką DLL, która rozszerza możliwości serwera. Atrybut `ibm-slapdPlugin` informuje serwer, jak załadować i zainicjować bibliotekę modułu dodatkowego. Składnia jest następująca:  
*słowo\_kluczowe nazwa\_pliku init\_function [argumenty...]*

Składnia ta jest nieco inna dla każdej platformy ze względu na konwencje nazewnictwa bibliotek.

Większość modułów dodatkowych jest opcjonalna, jedynie moduł dodatkowy postprocesora RDBM jest wymagany dla wszystkich postprocesorów RDBM.

**Wartość domyślna**

*baza\_danych /bin/libback-rdbm.dll rdbm\_backend\_init*

**Składnia**

Ciąg znaków katalogu (z rozróżnieniem wielkości liter)

**Maksymalna długość**

2000

**Wartość**

Wielowartościowy

**ibm-slapdPort**

**Opis** Określa port TCP/IP używany do połączeń nie wykorzystujących SSL. Nie może mieć tej samej wartości co `ibm-slapdSecurePort`. (Porty IP to 16-bitowe liczby całkowite bez znaku z zakresu 1 - 65535).

**Wartość domyślna**

389

**Składnia**

Liczba całkowita

**Maksymalna długość**

5

**Wartość**

Jednowartościowy

**ibm-slapdPWEncryption**

**Opis** Określa mechanizm kodowania haseł użytkowników, zanim zostaną one zapisane w katalogu. Musi być określony jako: `none`, `imask`, `crypt` lub `sha` (w celu uzyskania kodowania SHA-1 należy użyć słowa kluczowego **sha**). Aby wiązanie SASL `cram-md5` powiodło się, wartość tę trzeba ustawić na `none`.

**Wartość domyślna**

brak

**Składnia**

Ciąg znaków katalogu (bez rozróżniania wielkości liter)

**Maksymalna długość**

5

**Wartość**

Jednowartościowy

**ibm-slapdReadOnly**

**Opis** Atrybut ten jest zwykle stosowany tylko wobec postprocesora katalogu. Wskazuje, czy można zapisywać do postprocesora. Musi mieć wartość TRUE lub FALSE. Domyślną wartością jest FALSE. Jeśli ustawiono TRUE, w odpowiedzi na każde żądanie zmieniające dane w bazie danych readOnly serwer zwraca LDAP\_UNWILLING\_TO\_PERFORM (0x35).

**Wartość domyślna**

FALSE

**Składnia**

Boolowski

**Maksymalna długość**

5

**Wartość**

Jednowartościowy

**ibm-slapdReferral**

**Opis** Określa adres URL odwołania LDAP przekazywanego zwrotnie w przypadku niezgodności lokalnych przyrostków z żądaniem. Jest używany dla odwołań do obiektów nadrzędnych (tzn. gdy przyrostek nie znajduje się w kontekście nazewnictwa serwera).

**Wartość domyślna**

Nie ma żadnej wstępnie zdefiniowanej wartości domyślnej.

**Składnia**

Ciąg znaków katalogu (z rozróżnianiem wielkości liter)

**Maksymalna długość**

32700

**Wartość**

Wielowartościowy

**ibm-slapdRepIDbConns**

**Opis** Maksymalna liczba połączeń z bazą danych używanych przez replikację.

**Wartość domyślna**

4

**Składnia**

Liczba całkowita

**Maksymalna długość**

11

**Wartość**

Jednowartościowy

**ibm-slapdReplicaSubtree**

**Opis** Określa nazwę DN replikowanego poddrzewa.

**Składnia**

Nazwa wyróżniająca



**Maksymalna długość**

1000

**Wartość**

Jednowartościowy

**ibm-slapdSchemaAdditions**

**Opis** Atrybut `ibm-slapdSchemaAdditions` służy do jawnego identyfikowania, który plik przechowuje nowe pozycje schematu. Domyślnie ma wartość `/etc/V3.modifiedschema`. Jeśli atrybut ten nie jest zdefiniowany, serwer zastosuje ostatni plik `ibm-slapdIncludeSchema`, tak jak w poprzednich wersjach.

Przed wersją 3.2 ostatnia pozycja `includeSchema` w pliku **slapd.conf** określała plik, do którego serwer dodawał wszystkie nowe pozycje schematu w odpowiedzi na żądanie dodania pozycji otrzymane od klienta. Zwykle ostatnia pozycja `includeSchema` określa plik `V3.modifiedschema`, który jest pustym plikiem zainstalowanym specjalnie do tego celu.

**Uwaga:** Ciąg znaków "modified" (zmodyfikowany) w nazwie jest mylący, gdyż w pliku zapisywane są jedynie nowe pozycje. Zmiany istniejących pozycji schematu dokonywane są w ich oryginalnych plikach.

**Wartość domyślna**`/etc/V3.modifiedschema`**Składnia**

Ciąg znaków katalogu (z rozróżnieniem wielkości liter)

**Maksymalna długość**

1024

**Wartość**

Jednowartościowy

**ibm-slapdSchemaCheck**

**Opis** Określa mechanizm sprawdzania schematu w operacjach dodawania/modyfikowania/usuwania. Musi mieć wartość `V2`, `V3` lub `V3_lenient`.

- `V2` - sprawdzanie takie, jak w wersjach `v2` i `v2.1`. Zalecane do migracji.
- `V3` - sprawdzanie `v3`.
- `V3_lenient` - nie wszystkie nadrzędne klasy obiektu są potrzebne. Podczas dodawania pozycji potrzebna jest tylko bezpośrednio nadrzędna klasa obiektu.

**Wartość domyślna**`V3_lenient`**Składnia**

Ciąg znaków katalogu (bez rozróżniania wielkości liter)

**Maksymalna długość**

10

**Wartość**

Jednowartościowy

**ibm-slapdSecurePort**

**Opis** Określa port TCP/IP używany do połączeń za pomocą protokołu SSL. Nie może mieć tej samej wartości co `ibm-slapdPort`. (Porty IP to 16-bitowe liczby całkowite bez znaku z zakresu 1 - 65535).

**Wartość domyślna**

636

**Składnia**

Liczba całkowita

**Maksymalna długość**

5

**Wartość**

Jednowartościowy

**ibm-slapdSecurity**

**Opis** Włącza połączenia SSL i TLS. Musi mieć wartość: none, SSL, SSLOnly, TLS, lub SSLTLS.

- none - serwer nasłuchuje tylko na porcie niechronionym.
- SSL - serwer nasłuchuje na portach SSL i innych niż SSL. Port chroniony jako jedyny umożliwia korzystanie z połączenia chronionego.
- SSLOnly - serwer nasłuchuje tylko na porcie SSL.
- TLS - serwer nasłuchuje tylko na porcie niechronionym. Rozszerzona operacja StartTLS jako jedyna umożliwia korzystanie z połączenia chronionego.
- SSLTLS - serwer nasłuchuje na portach domyślnych i chronionych. Rozszerzona operacja StartTLS może być użyta do zapewnienia chronionego połączenia na porcie domyślnym. Klient może także bezpośrednio użyć portu chronionego. Wysłanie StartTLS z portu chronionego zwróci komunikat LDAP\_OPERATIONS\_ERROR.

**Wartość domyślna**

brak

**Składnia**

Ciąg znaków katalogu (bez rozróżniania wielkości liter)

**Maksymalna długość**

7

**Wartość**

Jednowartościowy

**ibm-slapdServerId**

**Opis** Identyfikuje serwer używany w replikacji.

**Składnia**

Ciąg znaków IA5 z rozróżnianiem wielkości liter

**Maksymalna długość**

240

**Wartość**

Jednowartościowy

**ibm-slapdSetenv**

**Opis** Podczas uruchomienia serwer uruchamia działanie **putenv()** dla wszystkich wartości **ibm-slapdSetenv** w celu zmiany środowiska wykonawczego serwera. Zmienne powłoki (takie jak %PATH% lub \$LANG) nie są rozwijane.

**Wartość domyślna**

Nie ma żadnej wstępnie zdefiniowanej wartości domyślnej.

**Składnia**

Ciąg znaków katalogu (z rozróżnianiem wielkości liter)

**Maksymalna długość**

2000

**Wartość**

Wielowartościowy

**ibm-slapdSizeLimit**

**Opis** Określa maksymalną liczbę pozycji zwracanych jako wyniki wyszukiwania, bez względu na limit wielkości, który mógł zostać określony w żądaniu wyszukiwania klienta (Zakres = 0...). Jeśli klient przekazał limit, to użyta zostanie mniejsza z następujących wartości: przekazana przez klienta i odczytana z pliku **ibmslapd.conf**. Jeśli klient nie przekroczył limitu i połączył się za pomocą nazwy DN administratora, uważa się, że limit jest nieograniczony. Jeśli klient nie przekazał limitu i nie połączył się za pomocą nazwy DN administratora, limitem jest wartość odczytana z pliku **ibmslapd.conf**. 0 = brak ograniczenia

**Wartość domyślna**

500

**Składnia**

Liczba całkowita

**Maksymalna długość**

12

**Wartość**

Jednowartościowy

**ibm-slapdSortKeyLimit**

**Opis** Maksymalna liczba warunków sortowania (kluczy), które można określić dla pojedynczego żądania wyszukiwania. Zakres = 0.... Jeśli klient przekazał żądanie wyszukiwania o większej liczbie kluczy sortowania niż dozwolony limit, a wartość newralgiczności wyszukiwania sortowanego jest równa FALSE, serwer honoruje wartość odczytaną z pliku **ibmslapd.conf** i ignoruje wszystkie klucze sortowania napotkane po osiągnięciu limitu; wyszukiwanie i sortowanie jest wykonywane. Jeśli klient przekazał żądanie wyszukiwania o większej liczbie kluczy niż dozwolony limit, a wartość newralgiczności wyszukiwania sortowanego jest równa TRUE, serwer zwraca klientowi kod powrotu **adminLimitExceeded** - wyszukiwanie lub sortowanie nie zostaną wykonane.

**Wartość domyślna**

3

**Składnia**

cis

**Długość**

11

**Liczność**

Pojedynczy

**Wykorzystanie**

Operacje na katalogu

**Modyfikowany przez użytkownika**

Tak

**Klasa dostępu**

Newralgiczna

**Klasa obiektu**

ibm-slapdRdbmBackend

**Wymagany**

Nie

## ibm-slapdSortSrchAllowNonAdmin

**Opis** Określa, czy serwer powinien zezwalać użytkownikom innym niż administrator na określenie w żądaniu wyszukiwania, że wyniki mają być sortowane. Jeśli wartością odczytaną z pliku `ibmslapd.conf` jest `FALSE`, serwer będzie przetwarzać tylko żądania klientów wysłane przez użytkowników z uprawnieniami administratora. Jeśli klient żąda wyszukiwania z sortowaniem rezultatów i nie ma uprawnień administratora, a wartość tego atrybutu odczytana z pliku `ibmslapd.conf` jest równa `FALSE`, serwer zwraca klientowi kod powrotu `insufficientAccessRights` i nie wykonuje wyszukiwania ani sortowania.

### Wartość domyślna

FALSE

### Składnia

Boolowski

### Długość

5

### Liczność

Pojedynczy

### Wykorzystanie

Operacje na katalogu

### Modyfikowany przez użytkownika

Tak

### Klasa dostępu

Newralgiczna

### Klasa obiektu

ibm-slapdRdbmBackend

### Wymagany

Nie

## ibm-slapdSslAuth

**Opis** Określa typ uwierzytelnienia dla połączeń ssl: albo `serverauth`, albo `serverclientauth`.

- `serverauth` - obsługuje uwierzytelnianie serwera na kliencie. Jest to wartość domyślna.
- `serverclientauth` - obsługuje uwierzytelnianie zarówno serwera, jak i klienta.

### Wartość domyślna

serverauth

### Składnia

Ciąg znaków katalogu (bez rozróżniania wielkości liter)

### Maksymalna długość

16

### Wartość

Jednowartościowy

## ibm-slapdSslCertificate

**Opis** Określa etykietę identyfikującą certyfikat osobisty serwera w pliku bazy danych kluczy. Etykieta ta jest określona, gdy klucz prywatny oraz certyfikat serwera utworzone są za pomocą aplikacji **gsk4ikm**. Jeśli atrybut `ibm-slapdSslCertificate` nie jest zdefiniowany, serwer LDAP wykorzystuje do połączeń SSL domyślny klucz prywatny zdefiniowany w pliku bazy danych kluczy.

### Wartość domyślna

Nie ma żadnej wstępnie zdefiniowanej wartości domyślnej.

**Składnia**

Ciąg znaków katalogu (z rozróżnianiem wielkości liter)

**Maksymalna długość**

128

**Wartość**

Jednowartościowy

**ibm-slapdSslCipherSpec**

Określa metodę szyfrowania SSL dla klientów uzyskujących dostęp do serwera. Musi przyjmować jedną z następujących wartości:

*Tabela 6. Metody szyfrowania SSL*

Atrybut	Poziom szyfrowania
TripleDES-168	Szyfrowanie Triple DES z kluczem 168-bitowym oraz SHA-1 MAC
DES-56	Szyfrowanie DES z kluczem 56-bitowym oraz SHA-1 MAC
RC4-128-SHA	Szyfrowanie RC4 z kluczem 128-bitowym oraz SHA-1 MAC
RC4-128-MD5	Szyfrowanie RC4 z kluczem 128-bitowym oraz MD5 MAC
RC2-40-MD5	Szyfrowanie RC4 z kluczem 40-bitowym oraz MD5 MAC
RC4-40-MD5	Szyfrowanie RC4 z kluczem 40-bitowym oraz MD5 MAC
AES	Szyfrowanie AES

**Składnia**

Ciąg znaków IA5

**Maksymalna długość**

30

**ibm-slapdSslKeyDatabase**

**Opis** Określa ścieżkę do pliku bazy danych kluczy SSL serwera LDAP. Ten plik bazy danych kluczy używany jest do obsługi połączeń SSL od klientów LDAP, a także do tworzenia bezpiecznych połączeń SSL z serwerami replik LDAP.

**Wartość domyślna**

/etc/key.kdb

**Składnia**

Ciąg znaków katalogu (z rozróżnianiem wielkości liter)

**Maksymalna długość**

1024

**Wartość**

Jednowartościowy

**ibm-slapdSslKeyDatabasePW**

**Opis** Określa hasło związane z plikiem bazy danych kluczy SSL serwera LDAP podanym w parametrze `ibm-slapdSslKeyDatabase`. Jeśli plik bazy danych kluczy serwera LDAP ma związane z sobą plik ukrytych haseł, parametr `ibm-slapdSslKeyDatabasePW` można pominąć lub nadać mu wartość `none` (brak).

**Uwaga:** Plik haseł musi znajdować się w tym samym katalogu i mieć tę samą nazwę, co plik bazy danych kluczy, ale z rozszerzeniem `.sth` zamiast `.kdb`.

**Wartość domyślna**

brak

**Składnia**

Kod binarny

**Maksymalna długość**

128

**Wartość**

Jednowartościowy

**ibm-slapdSslKeyRingFile**

**Opis** Ścieżka do pliku bazy danych kluczy SSL serwera LDAP. Ten plik bazy danych kluczy używany jest do obsługi połączeń SSL od klientów LDAP, a także do tworzenia bezpiecznych połączeń SSL z serwerami replik LDAP.

**Wartość domyślna**

key.kdb

**Składnia**

Ciąg znaków katalogu z rozróżnianiem wielkości liter

**Maksymalna długość**

1024

**Wartość**

Jednowartościowy

**ibm-slapdSuffix**

**Opis** Określa kontekst nazewnictwa zapisany w danym postprocesorze.

**Uwaga:** Ma tę samą nazwę, co klasa obiektu.

**Wartość domyślna**

Nie ma żadnej wstępnie zdefiniowanej wartości domyślnej.

**Składnia**

Nazwa wyróżniająca

**Maksymalna długość**

1000

**Wartość**

Wielowartościowy

**ibm-slapdSupportedWebAdmVersion**

**Opis** Atrybut ten określa najwcześniejszą wersję narzędzia Web Administration, która obsługuje serwer z przyrostkiem cn=configuration.

**Wartość domyślna****Składnia**

Ciąg znaków katalogu

**Maksymalna długość****Wartość**

Jednowartościowy

## **ibm-slapdSysLogLevel**

**Opis** Określa poziom protokołowania statystyki debugowania i działania w pliku slapd.errors. Musi mieć wartość: l, m lub h.

- h - wysoki (udostępnia najwięcej informacji)
- m - średni (domyślny)
- l - niski (udostępnia najmniej informacji)

### **Wartość domyślna**

m

### **Składnia**

Ciąg znaków katalogu (bez rozróżniania wielkości liter)

### **Maksymalna długość**

1

### **Wartość**

Jednowartościowy

## **ibm-slapdTimeLimit**

**Opis** Określa maksymalną liczbę sekund na realizację żądania wyszukiwania niezależnie od limitu czasu, który może być określony w żądaniu klienta. Jeśli klient przekazał limit, to użyta zostanie mniejsza z następujących wartości: przekazana przez klienta i odczytana z pliku **ibmslapd.conf**. Jeśli klient nie przekroczył limitu i połączył się za pomocą nazwy DN administratora, uważa się, że limit jest nieograniczony. Jeśli klient nie przekazał limitu i nie połączył się za pomocą nazwy DN administratora, limitem jest wartość odczytana z pliku **ibmslapd.conf**. 0 = brak ograniczenia

### **Wartość domyślna**

900

### **Składnia**

Liczba całkowita

### **Maksymalna długość**

### **Wartość**

Jednowartościowy

## **ibm-slapdTransactionEnable**

**Opis** Jeśli moduł dodatkowy transakcji jest załadowany, ale atrybut **ibm-slapdTransactionEnable** ma wartość FALSE, serwer odrzuca wszystkie żądania StartTransaction odpowiedzią LDAP\_UNWILLING\_TO\_PERFORM.

### **Wartość domyślna**

TRUE

### **Składnia**

Boolowski

### **Maksymalna długość**

5

### **Wartość**

Jednowartościowy

## **ibm-slapdUseProcessIdPw**

**Opis** Ustawienie TRUE powoduje, że serwer ignoruje atrybuty **ibm-slapdDbUserID** oraz **ibm-slapdDbUserPW** i używa własnych referencji procesu do uwierzytelniania w DB2.

**Wartość domyślna**

FALSE

**Składnia**

Boolowski

**Maksymalna długość**

5

**Wartość**

Jednowartościowy

**ibm-slapdVersion****Opis** Numer wersji IBM Slapd**Wartość domyślna****Składnia**

Ciąg znaków katalogu z rozróżnianiem wielkości liter

**Maksymalna długość****Wartość**

Jednowartościowy

**ibm-slapdWriteTimeout****Opis** Określa wyrażoną w sekundach wartość limitu czasu dla zablokowanych zapisów. Po osiągnięciu limitu czasu połączenie zostanie zerwane.**Wartość domyślna**

120

**Składnia**

Liczba całkowita

**Maksymalna długość**

1024

**Wartość**

Jednowartościowy

**objectClass****Opis** Wartości atrybutu objectClass opisują rodzaj obiektu, któremu odpowiada dana pozycja.**Składnia**

Ciąg znaków katalogu

**Maksymalna długość**

128

**Wartość**

Wielowartościowy

**Identyfikatory obiektów (OID)**

Informacje w tym temacie zawierają identyfikatory obiektów (object identifier - OID) używane w serwerze Directory Server.

- | Na serwerze Directory Server używane są identyfikatory obiektów przedstawione w poniższych tabelach.
- | Identyfikatory obiektów (OID) znajdują się w katalogu głównym DSE. Pozycja DSE katalogu głównego zawiera informacje o samym serwerze. Więcej informacji na temat identyfikatorów obiektów dla rozszerzonych operacji i



elementów sterujących, w tym kodowanie danych żądania i odpowiedzi powiązanych z następującymi elementami sterującymi i rozszerzonymi operacjami znajduje się w Centrum informacyjnym oprogramowania Tivoli.

## Elementy sterujące

Tabela 7. Obsługiwane elementy sterujące serwera Directory Server

Nazwa	Identyfikator OID	Najwcześniejsza wersja systemu i5/OS lub OS/400	Najstarsza wersja serwera IBM Tivoli Directory Server	Opis
Manage DSAIT (Zarządzanie drzewem informacji agenta katalogów systemu)	2.16.840.1.1137.30.3.4.2	V4R5	V3.2	Traktuje pozycje odwołania tak jak zwykle pozycje.
Transactions (“Transakcje” na stronie 51)	1.3.18.0.2.10.5	V4R5	V3.2	Oznacza operacje jako część transakcji.
os400-dltusrprf-ownobjopt	1.3.18.0.2.10.8	V5R2		Opcja usuwania profilu użytkownika dla właściciela obiektu. Szczegóły zawiera temat “Mechanizm rzutowania systemu operacyjnego” na stronie 84.
os400-dltusrprf-pgpopt	1.3.18.0.2.10.9	V5R2		Opcja usuwania profilu użytkownika dla grupy podstawowej. Szczegóły zawiera temat “Mechanizm rzutowania systemu operacyjnego” na stronie 84.
Sorted search (Wyszukiwanie z sortowaniem)	1.2.840.113556.1.4.473 (żądanie) i 1.2.840.113556.1.4.474 (odpowiedź)	V5R2 z poprawką PTF	V4.1	Sortuje wyniki wyszukiwania przed zwróceniem pozycji do klienta. Więcej informacji zawiera temat “Parametry wyszukiwania” na stronie 47.
Paged search (Wyszukiwanie ze stronicowaniem)	1.2.840.113556.1.4.319	V5R2 z poprawką PTF	V4.1	Zwraca do klienta wyniki wyszukiwania podzielone na strony zamiast wszystkich jednocześnie. Więcej informacji zawiera temat “Parametry wyszukiwania” na stronie 47.

Tabela 7. Obsługiwane elementy sterujące serwera Directory Server (kontynuacja)

Nazwa	Identyfikator OID	Najwcześniejsza wersja systemu i5/OS lub OS/400	Najstarsza wersja serwera IBM Tivoli Directory Server	Opis
Tree Delete (Usuwanie drzewa)	1.2.840.113556.1.4.805	V5R3	V5.1	Ten element sterujący jest podłączony do żądania usunięcia w celu wskazania, że określona pozycja i wszystkie podrzędne pozycje mają być usunięte. Użytkownik musi być administratorem katalogu. Pozycja do usunięcia nie może być kontekstem replikacji.
Password policy ("Strategia haseł" na stronie 77)	1.3.6.1.4.1.42.2.27.8.5.1	V5R3	V5.1	Zwraca do klienta dodatkowe informacje o błędzie strategii haseł.
Server administration (Administrowanie serwerem)	1.3.18.0.2.10.15	V5R3	V5.1	Umożliwia administratorowi wykonywanie napraw, które normalnie zostałyby odrzucone (na przykład: aktualizacja repliki tylko do odczytu, aktualizacja wygaszonego serwera lub ustawienie niektórych atrybutów operacyjnych).
Proxy authorization ("Autoryzacja proxy" na stronie 64)	2.16.840.1.113730.3.4.18	V5R4	V5.2	Aplikacja kliencka może połączyć się z katalogiem, korzystając z własnej tożsamości, ale może wykonywać działania w imieniu innej.
Replication supplier bind (Łączenie serwera wysyłającego replikacji)	1.3.18.0.2.10.18	V5R3	V5.2	Ten element sterujący dodawany jest przez serwer wysyłający, jeśli jest on serwerem-bramą.
Refresh Entry (Odświeżanie pozycji)	1.3.18.0.2.10.24	V6R1	V6.0	Ten element sterujący jest używany wewnątrz przez serwer w celu obsługi rozstrzygnięcia konfliktów replikacji.
No Replication Conflict Resolution (Brak rozstrzygnięcia konfliktów replikacji)	1.3.19.0.2.10.27	V6R1	V6.0	Ten element sterujący jest używany wewnątrz przez serwer w celu obsługi rozstrzygnięcia konfliktów replikacji.

Tabela 7. Obsługiwane elementy sterujące serwera Directory Server (kontynuacja)

Nazwa	Identyfikator OID	Najwcześniejsza wersja systemu i5/OS lub OS/400	Najstarsza wersja serwera IBM Tivoli Directory Server	Opis
Do Not Replicate (Bez replikowania)	1.3.19.0.2.10.23	V6R1	V6.0	Ten element sterujący może zostać określony przez administratora w celu zażądania, aby powiązana operacja nie była replikowana na inne serwery. Ten element sterujący nie ma wartości.
Audit (Kontrola)	1.3.18.0.2.10.22	V6R1	V6.0	Ten element sterujący jest używany przez autoryzowane klienty, w tym przez serwer proxy, w celu identyfikowania klienta przesyłającego żądanie, które mogło przejść przez wiele serwerów.
Group Authorization (Autoryzacja na podstawie grup)	1.3.18.0.2.10.21	V6R1	V6.0	Ten element sterujący służy do zaznaczania, że dany identyfikator autoryzacji klienta jest członkiem podanych grup, a nie do zaznaczania członkostwa w grupach serwera lokalnego. Jest on używany w połączeniu ze elementem sterującym Proxy Authorization.
Modify Groups Only (Modyfikowanie wyłącznie grup)	1.3.18.0.2.10.25	V6R1	V6.0	Czynności związane z tym elementem sterującym (delete lub modrdn/dn) zostaną rozpoznane przez serwery zaplecza jako specjalny rodzaj operacji, w której nazwa wyróżniająca nie jest usuwana i nie ulega zmianie. Zamiast tego grupy, w których się ona znajduje, są modyfikowane tak, aby usunąć odniesienie do nazwy wyróżniającej elementu docelowego w tym członkostwie lub zmienić jego nazwę.

Tabela 7. Obsługiwane elementy sterujące serwera Directory Server (kontynuacja)

Nazwa	Identyfikator OID	Najwcześniejsza wersja systemu i5/OS lub OS/400	Najstarsza wersja serwera IBM Tivoli Directory Server	Opis
Omit group referential integrity (Pominięcie integralności referencji grupy)	1.3.18.0.2.10.26	V6R1	V6.0	Pominięcie przetwarzania integralności referencji grupy w żądaniu delete lub modrdn. ACI i członkostwa w grupach nie są aktualizowane w celu odzwierciedlenia tej zmiany.
AES bind (Łączenie AES)	1.3.18.0.2.10.28	V6R1	V6.0	Ten element sterujący umożliwia serwerowi IBM Tivoli Directory Server wysyłanie aktualizacji do serwera odbierającego z hasłami zaszyfrowanymi za pomocą algorytmu AES.

## Rozszerzone operacje

Tabela 8. Identyfikatory OID dla rozszerzonych operacji

Nazwa	Identyfikator OID	Najwcześniejsza wersja systemu i5/OS lub OS/400	Najstarsza wersja serwera IBM Tivoli Directory Server	Opis
Register for events (Rejestrowanie na zdarzenia)	1.3.18.0.2.12.1	V4R5	V3.2	Żądanie rejestrowania na zdarzenia na serwerze Tivoli Directory Server.
Unregister for events (Wyrejestrowanie ze zdarzeń)	1.3.18.0.2.12.3	V4R5	V3.2	Wyrejestrowanie ze zdarzeń przypisanych za pomocą żądania rejestracji na zdarzenia.
Begin transaction (Rozpoczęcie transakcji)	1.3.18.0.2.12.5	V4R5	V3.2	Rozpoczęcie kontekstu transakcyjnego.
End transaction (Zakończenie transakcji)	1.3.18.0.2.12.6	V4R5	V3.2	Zakończenie kontekstu transakcyjnego (zatwierdzenie/wycofanie).
DN normalize request (Żądanie normalizacji nazwy wyróżniającej)	1.3.18.0.2.12.30	V5R3	V5.1	Żądanie normalizacji nazwy wyróżniającej lub sekwencji nazw wyróżniających.
StartTLS (Rozpoczęcie korzystania z protokołu TLS)	1.3.6.1.4.1.1466.20037	V5R4	V5.2	Żądanie uruchomienia TLS (Transport Layer Security).

Definiowane są dodatkowe rozszerzone operacje, które nie są przeznaczone do uruchamiania przez klienta. Operacje te używane są za pośrednictwem narzędzia ldapexop lub operacji wykonywanych przez narzędzie Web Administration. Operacje te oraz uprawnienia wymagane do ich uruchomienia są wymienione poniżej.

Tabela 9. Dodatkowe rozszerzone operacje

Nazwa	Identyfikator OID	Najwcześniejsza wersja systemu i5/OS	Najstarsza wersja serwera IBM Tivoli Directory Server	Opis
Control replication (Sterowanie replikacją)	1.3.18.0.2.12.16	V5R3	V5.1	Ta operacja wykonuje żądane działanie na wskazanym serwerze i przekazuje wywołanie kaskadowo do wszystkich podrzędnych serwerów odbierających w topologii replikacji. Klient musi być administratorem katalogu lub mieć prawa zapisu do obiektu <code>ibm-replicagroup=default</code> dla powiązanego kontekstu replikacji.
Control replication queue (Sterowanie kolejką replikacji)	1.3.18.0.2.12.17	V5R3	V5.1	Ta operacja zaznacza pozycje jako już replikowana dla określonej umowy. Jest ona dozwolona tylko wtedy, gdy użytkownik ma uprawnienia do zapisu do umowy replikacji.
Quiesce or unquiesce (Wygaszenie lub cofnięcie wygaszenia)	1.3.18.0.2.12.19	V5R3	V5.1	Ta operacja umieszcza poddrzewo w stanie, w którym nie akceptuje ono aktualizacji z klienta (lub przerywa ten stan), z wyjątkiem klientów uwierzytelnionych jako administrator katalogu, w którym znajdował się element sterujący Server Administration. Klient musi być uwierzytelniony jako administrator katalogu lub mieć prawa zapisu do obiektu <code>ibm-replicagroup=default</code> dla powiązanego kontekstu replikacji.
Cascading control replication (Kaskadowe sterowanie replikacją)	1.3.18.0.2.12.15	V5R3	V5.1	Ta operacja wykonuje żądane działanie na wskazanym serwerze i przekazuje wywołanie kaskadowo do wszystkich podrzędnych serwerów odbierających w topologii replikacji. Klient musi być administratorem katalogu lub mieć prawa zapisu do obiektu <code>ibm-replicagroup=default</code> dla powiązanego kontekstu replikacji.
Update configuration (Aktualizowanie konfiguracji)	1.3.18.0.2.12.28	V5R3	V5.1	Ta operacja powoduje, że serwer ponownie odczytuje określone ustawienia ze swojej konfiguracji. Jest ona dozwolona tylko wtedy, gdy klient jest administratorem katalogu.
Kill Connection Request (Żądanie zabicia połączenia)	1.3.18.0.2.12.35	V5R4	V5.2	Żądanie zabicia połączeń na serwerze. Wywołujący musi być administratorem katalogu.
Unique attribute request (Żądanie atrybutu unikalnego)	1.3.18.0.2.12.44	V5R4	V5.2	Żąda od serwera listy zwrotnej wszystkich wartości nie-unikalnych dla danej nazwy atrybutu. Zapoznaj się z sekcją "Idapexop" na stronie 226 -op uniqueattr. Wywołujący musi być administratorem katalogu.

Tabela 9. Dodatkowe rozszerzone operacje (kontynuacja)

Nazwa	Identyfikator OID	Najwcześniejsza wersja systemu i5/OS	Najstarsza wersja serwera IBM Tivoli Directory Server	Opis
Attribute type request (Żądanie typu atrybutu)	1.3.18.0.2.12.46	V5R4	V5.2	Żąda od serwera listy zwrotnej wszystkich nazw atrybutów posiadających określone charakterystyki. Zapoznaj się z sekcją "ldapexop" na stronie 226 -op getattributes
User type request (Żądanie typu użytkownika)	1.3.18.0.2.12.37	V5R3	V5.2	Żądanie pobrania typu użytkownika połączonego użytkownika.
Replication error log (Protokół błędów replikacji)	1.3.18.0.2.12.56	V6R1	V6.0	Rozszerzone żądanie IBM Replication Error Control służy do wyświetlania protokołu błędów replikacji oraz ponawiania pozycji i usuwania pozycji z protokołu. Wywołujący musi być administratorem katalogu lub mieć prawa zapisu do obiektu ibm-replicagroup=default dla odpowiedniego kontekstu replikacji.
Group evaluation (Wartościowanie grupy)	1.3.18.0.2.12.50	V6R1	V6.0	Żądanie zwrócenia wszystkich grup, do których należy dany użytkownik. Wywołujący musi być administratorem katalogu.
Replication topology (Topologia replikacji)	1.3.18.0.2.12.54	V6R1	V6.0	Wyzwała replikowanie pozycji związanych z topologią replikacji w danym kontekście replikacji. Wywołujący musi być administratorem katalogu lub mieć prawa zapisu do obiektu ibm-replicagroup=default dla odpowiedniego kontekstu replikacji.
Account status (Status konta)	1.3.18.0.2.12.58	V6R1	V6.0	Ta rozszerzona operacja wysyła do serwera nazwę wyróżniającą pozycji, która zawiera atrybut userPassword, a serwer odsyła status konta użytkownika, którego dotyczy zapytanie: otwarte, zablokowane lub wygasłe. Wywołujący musi być administratorem katalogu.
Get file (Pobranie pliku)	1.3.18.0.2.12.73	V6R1	V6.0	Zwraca zawartość danego pliku na serwerze. Wywołujący musi być administratorem katalogu. Obsługuje protokół LostAndFound oraz dziennik kontroli serwera Tivoli Directory Server. Dziennik kontroli nie jest związany z funkcjami kontrolowania bezpieczeństwa systemu i5/OS dotyczącymi serwera katalogów.

Tabela 9. Dodatkowe rozszerzone operacje (kontynuacja)

Nazwa	Identyfikator OID	Najwcześniejsza wersja systemu i5/OS	Najstarsza wersja serwera IBM Tivoli Directory Server	Opis
Get lines (Pobranie wierszy)	1.3.18.0.2.12.22	V6R1	V6.0	Żądanie pobrania wierszy z pliku protokołu. Wywołujący musi być administratorem katalogu. Obsługuje protokół LostAndFound oraz dziennik kontroli serwera Tivoli Directory Server. Dziennik kontroli nie jest związany z funkcjami kontrolowania bezpieczeństwa systemu i5/OS dotyczącymi serwera katalogów.
Get number of lines (Pobranie liczby wierszy)	1.3.18.0.2.12.24	V6R1	V6.0	Żądanie pobrania liczby wierszy z pliku protokołu. Wywołujący musi być administratorem katalogu. Obsługuje protokół LostAndFound oraz dziennik kontroli serwera Tivoli Directory Server. Dziennik kontroli nie jest związany z funkcjami kontrolowania bezpieczeństwa systemu i5/OS dotyczącymi serwera katalogów.

## Obsługiwane i aktywowane możliwości

Poniższa tabela przedstawia identyfikatory OID dla obsługiwanych i aktywowanych możliwości. Identyfikatory te mogą zostać użyte w celu określenia, czy dany serwer obsługuje te opcje.

Tabela 10. Identyfikatory OID dla obsługiwanych i aktywowanych możliwości.

Nazwa	Identyfikator OID	Opis
Enhanced Replication Model (Rozszerzony model replikacji)	1.3.18.0.2.32.1	Identyfikuje model replikacji wprowadzony przez serwer IBM Directory Server v5.1, w tym replikację poddrzewa i kaskadową.
Entry Checksum (Suma kontrolna pozycji)	1.3.18.0.2.32.2	Wskazuje, że serwer obsługuje opcje <code>ibm-entrychecksum</code> i <code>ibm-entrychecksumop</code> .
Entry UUID (Identyfikator UUID pozycji)	1.3.18.0.2.32.3	Wskazuje, że serwer obsługuje atrybut wykonawczy <code>ibm-entryuuid</code> .
Filter ACLs (Filtrowanie list ACL)	1.3.18.0.2.32.4	Identyfikuje obsługę modelu IBM ACL Filter przez serwer.
Password Policy (Strategia haseł)	1.3.18.0.2.32.5	Wskazuje, że serwer obsługuje strategię haseł.
Sort by DN (Sortowanie według nazwy wyróżniającej)	1.3.18.0.2.32.6	Wskazuje, że serwer obsługuje sortowanie według nazwy wyróżniającej za pomocą atrybutu <code>ibm-slapdDn</code> .
Administrative Group Delegation (Przeniesienie praw grupy administracyjnej)	1.3.18.0.2.32.8	Serwer obsługuje przeniesienie praw administrowania serwerem na grupę administratorów określonych w mechanizmie konfiguracji.
Denial of Service Prevention (Zapobieganie odmowie usługi)	1.3.18.0.2.32.9	Serwer obsługuje opcję zapobiegania odmowie usługi, w tym limit czasu odczytu/zapisu i wątek ratunkowy.
Entry And Subtree Dynamic Updates (Dynamiczne aktualizowanie pozycji i poddrzew)	1.3.18.0.2.32.15	Serwer obsługuje dynamiczne aktualizacje konfiguracji pozycji i poddrzew.

Tabela 10. Identyfikatory OID dla obsługiwanych i aktywowanych możliwości. (kontynuacja)

Nazwa	Identyfikator OID	Opis
Dereference Alias Option (Opcja wyluskania aliasów)	1.3.18.0.2.32.10	Serwer obsługuje opcję pozwalającą wyłączyć domyślne wyluskiwanie aliasów.
Group-Specific Search Limits (Ograniczenia wyszukiwania dla wybranych grup)	1.3.18.0.2.32.17	Opcja ograniczeń wyszukiwania dla wybranych grup obsługuje rozszerzone ograniczenia wyszukiwania dla wybranych grup ludzi.
Dynamic Tracing (Śledzenie dynamiczne)	1.3.18.0.2.32.14	Serwer obsługuje aktywne śledzenie dla serwera za pomocą rozszerzonej operacji LDAP.
TLS Capabilities (Możliwości TLS)	1.3.18.0.2.32.28	Określa możliwość użycia przez serwer protokołu TLS.
Admin Daemon Auditing (Kontrola demona admin)	1.3.18.0.2.32.11	Serwer obsługuje kontrolę demona admin.
Kerberos Capabilities (Możliwości Kerberos)	1.3.18.0.2.32.30	Określa możliwość użycia protokołu Kerberos przez serwer.
Non-blocking Replication (Replikacja nieblokująca)	1.3.18.0.2.32.29	Jeśli serwer odbierający zwraca błąd, serwer wysyłający nie zawsze ponawia próbę wysłania aktualizacji.
ibm-allMembers and ibm-allGroups operational attributes (Atrybuty wykonawcze ibm-allMembers i ibm-allGroups)	1.3.18.0.2.32.31	System zaplecza obsługuje wyszukiwanie w grupach statycznych, dynamicznych i zagnieżdżonych za pomocą atrybutów wykonawczych ibm-allMembers i ibm-allGroups. Podzbiory grup statycznych, dynamicznych i/lub zagnieżdżonych mogą zostać wyszukane za pomocą atrybutu wykonawczego ibm-allMembers. Grupy statyczne, dynamiczne i/lub zagnieżdżone, do których należy nazwa wyróżniająca podzbioru, mogą zostać wyszukane za pomocą atrybutu operacyjnego ibm-allGroups.
Globally Unique Attributes (Atrybuty unikalne globalnie)	1.3.18.0.2.32.16	Opcja serwera wymuszająca wartości atrybutów unikalnych globalnie.
Monitor Operation Counts (Liczniki monitorowania operacji)	1.3.18.0.2.32.24	Serwer udostępnia liczniki monitorowania operacji dla rozpoczętych i zakończonych typów operacji.
Monitor Logging Counts (Liczniki monitorowania protokołowania)	1.3.18.0.2.32.20	Serwer udostępnia liczniki monitorowania komunikatów dodanych do plików protokołów serwera, CLI oraz kontroli.
Monitor Connection Type Counts (Liczniki monitorowania typów połączeń)	1.3.18.0.2.32.22	Serwer udostępnia liczniki monitora typów połączeń dla połączeń SSL i TLS.
Monitor Active Workers Info (Informacje o monitorowaniu aktywnych procesów roboczych)	1.3.18.0.2.32.21	Serwer udostępnia informację o Monitorze aktywnych procesów roboczych (cn=workers,cn=monitor).
Monitor Connections Info (Informacje o monitorowaniu połączeń)	1.3.18.0.2.32.23	Serwer udostępnia informację o Monitorze dla połączeń według adresu IP zamiast ID połączenia (cn=connections, cn=monitor).
Monitor Tracing Info (Informacje o monitorowaniu śledzenia)	1.3.18.0.2.32.25	Serwer udostępnia informacje pochodzące z monitorowania bieżących opcji śledzenia.
Attribute Caching Search Filter Resolution (Buforowanie atrybutów dla rozstrzygania o filtrze wyszukiwania)	1.3.18.0.2.32.13	Serwer obsługuje buforowanie atrybutów dla rozstrzygania o filtrze wyszukiwania.
Proxy Authorization (Autoryzacja proxy)	1.3.18.0.2.32.27	Serwer obsługuje autoryzację proxy dla grupy użytkowników.
Language tag option support (Obsługa opcji znaczników języka)	1.3.6.1.4.1.4203.1.5.4	Wskazuje, że serwer obsługuje znaczniki języka według definicji podanej w RFC 2596.
Max Age ChangeLog Entries (Maksymalny wiek pozycji protokołu zmian)	1.3.18.0.2.32.19	Określa, czy serwer posiada możliwość zachowania pozycji protokołu zmian w oparciu o wiek.



Tabela 10. Identyfikatory OID dla obsługiwanych i aktywowanych możliwości. (kontynuacja)

Nazwa	Identyfikator OID	Opis
IBMpolicies Replication Subtree (Poddrzewo replikacji IBMpolicies)	1.3.18.0.2.32.18	Serwer obsługuje replikację poddrzewa cn=IBMpolicies.
NULL base subtree search (Wyszukiwanie w poddrzewie bazy zerowej)	1.3.18.0.2.32.26	Serwer zezwala na wyszukiwanie w poddrzewie bazy zerowej obejmujące całe drzewo DIT zdefiniowane na serwerze.
Autonomic attribute cache (Autonomiczna pamięć podręczna atrybutów)	1.3.18.0.2.32.50	Obsługuje autonomiczne buforowanie atrybutów
ibm-entrychecksumop	1.3.18.0.2.32.56	Funkcja ibm-entrychecksumop 6.0 IDS
Filtered referrals server capability (Możliwość filtrowania odwołań na serwerze)	1.3.18.0.2.32.36	Wskazuje obsługę rozszerzonych odwołań filtrowanych. Oznacza to, że filtrowana wartość w odwołaniu zostanie w żądaniu wyszukiwania połączona z pierwotnym filtrem.
Global admin group server capability (Obsługa globalnej grupy administracyjnej na serwerze)	1.3.18.0.2.32.38	Wskazuje obsługę globalnej grupy administracyjnej.
Auditing of compare capability (Kontrolowanie funkcji porównywania)	1.3.18.0.2.32.40	Wskazuje obsługę kontrolowania operacji porównywania.
AES password encryption (Szyfrowanie hasła za pomocą algorytmu AES)	1.3.18.0.2.32.39	Wskazuje obsługę szyfrowania hasła za pomocą algorytmu AES.
Maximum Entry Size (Maksymalna wielkość pozycji)	1.3.18.0.2.32.51	Służy do rozstrzygania konfliktów replikacji. Na podstawie tej liczby serwer wysyłający może zdecydować, czy należy ponownie dodać pozycję do serwera docelowego w celu rozstrzygnięcia konfliktu replikacji.
LostAndFound log file (Plik protokołu LostAndFound)	1.3.18.0.2.32.52	Plik, w którym archiwizowane są zastąpione pozycje w wyniku rozstrzygnięcia konfliktów replikacji.
Log Management (Zarządzanie protokołami)	1.3.18.0.2.32.41	Wskazuje obsługę rozszerzonych operacji dostępu do pliku protokołu oraz dziennika kontroli serwera Tivoli Directory Server.
Multi-threaded replication (Replikacja wielowątkowa)	1.3.18.0.2.32.42	
Server configuration of suppliers for replication (Konfiguracja serwerów wysyłających replikacji)	1.3.18.0.2.32.43	
IBMPolicies replication subtree (Poddrzewo replikacji IBMPolicies)	1.3.18.0.2.32.18	Obsługuje konfigurację replikacji nazw cn=ibmpolicies i cn=schema za pomocą poddrzewa cn=ibmpolicies.

## Identyfikatory OID dla mechanizmów ACL

Poniższa tabela przedstawia identyfikatory OID dla mechanizmów ACL.

Tabela 11. Identyfikatory OID dla mechanizmów ACL

Nazwa	Identyfikator OID	Opis
IBM SecureWay V3.2 ACL Model (Model list ACL IBM SecureWay V3.2)	1.3.18.0.2.26.2	Wskazuje, że serwer LDAP obsługuje model listy ACL IBM SecureWay V3.2
IBM Filter Based ACL Mechanism (Mechanizm list ACL IBM opartych na filtrach)	1.3.18.0.2.26.3	Wskazuje, że serwer LDAP obsługuje oparte na filtrach listy ACL IBM Directory Server v5.1

Tabela 11. Identyfikatory OID dla mechanizmów ACL (kontynuacja)

Nazwa	Identyfikator OID	Opis
System Restricted ACL Support (Obsługa list ACL ograniczonych systemowo)	1.3.18.0.2.26.4	Wskazuje, że serwer obsługuje systemowe i ograniczone klasy dostępu w pozycjach ACL.

### Pojęcia pokrewne

“Elementy sterujące i rozszerzone operacje” na stronie 93

Elementy sterujące i rozszerzone operacje umożliwiają zwiększanie możliwości protokołu LDAP bez jego modyfikowania.

## Równoważność produktu IBM Tivoli Directory Server

Serwer Directory Server jest kompatybilny z produktem IBM Tivoli Directory Server na innych platformach. Na poniższej tabeli przedstawiono wersje produktu IBM Tivoli Directory Server odpowiadające poszczególnym wersjom serwera i5/OS Directory Server. Tabela ta może być przydatna podczas ustalania, czy serwer i5/OS Directory Server spełnia wymagania wstępne stawiane serwerowi katalogów w danym zastosowaniu.

Tabela 12. Równoważność produktu IBM Tivoli Directory Server

i5/OS Directory Server	IBM Tivoli Directory Server
Wersja 6 wydanie 1	IBM Tivoli Directory Server wersja 6.0
Wersja 5 wydanie 4	IBM Tivoli Directory Server wersja 5.2
Wersja 5 wydanie 3	IBM Directory Server wersja 5.1
Wersja 5 wydanie 2 (z PTF SI08487)	IBM Directory Server wersja 4.1
Wersja 5 wydanie 2 (GA)	IBM SecureWay Directory Server wersja 3.2.2

## Konfiguracja domyślna serwera Directory Server

Serwer Directory Server jest instalowany automatycznie podczas instalowania systemu operacyjnego i5/OS. Instalacja ta obejmuje konfigurację domyślną.

Serwer Directory Server korzysta z konfiguracji domyślnej, jeśli spełnione są następujące warunki:

- Administratorzy nie uruchomili Kreatora konfiguracji serwera katalogów (Directory Server Configuration Wizard) ani nie zmienili ustawień katalogu na stronach właściwości.
- Publikowanie serwera Directory Server nie jest skonfigurowane.
- Serwer Directory Server nie może odnaleźć żadnych informacji DNS o LDAP.

Jeśli serwer Directory Server korzysta z konfiguracji domyślnej, to:

- Uruchamia się automatycznie w momencie uruchamiania protokołu TCP/IP.
- System tworzy nowe konto administratora, cn=Administrator, oraz generuje używane wewnętrznie hasło. Jeśli później zajdzie potrzeba użycia hasła administratora, można ustawić nowe na stronie właściwości serwera Directory Server.
- 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 Directory Server korzysta z domyślnej biblioteki danych QUSRDIRDB, którą system tworzy w systemowej ASP.
- Serwer korzysta z portu 389 do niechronionej komunikacji. Jeśli dla LDAP skonfigurowano certyfikat cyfrowy, to włączony jest protokół SSL i do chronionej komunikacji używany jest port 636.

### Zadania pokrewne

“Konfigurowanie serwera Directory Server” na stronie 101

Ustawienia serwera Directory Server można dostosować za pomocą Kreatora konfiguracji serwera katalogów.

---

## Rozwiązywanie problemów z serwerem Directory Server

Informacje pomocne w rozwiązywaniu problemów. Obejmują sugestie dotyczące gromadzenia danych o usługach oraz rozwiązywania konkretnych problemów.

Niestety, nawet niezawodne serwery, takie jak Directory Server, czasami powodują problemy. Gdy Directory Server wykaże błąd, w określeniu jego przyczyny i sposobów rozwiązania mogą pomóc następujące informacje:

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

Aby uzyskać dodatkowe informacje o typowych problemach z serwerem Directory Server, zapoznaj się ze stroną główną produktu Directory Server ([www.iseries.ibm.com/ldap](http://www.iseries.ibm.com/ldap)).

Serwer Directory Server korzysta z wielu serwerów SQL (Structured Query Language), które są zadaniami QSQRV. 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 odsyła do protokołów zadań serwera SQL. Jednakże czasami QDIRSRV może nie zawierać tego komunikatu ani odwołania, nawet jeśli przyczyną problemu jest serwer SQL. Wtedy warto dowiedzieć się, które zadania serwera SQL uruchomił serwer, na podstawie czego wiadomo, które protokoły zadania QSQRV zawierają dodatkowe błędy.

Gdy serwer Directory Server jest normalnie uruchamiany normalnie, generuje komunikat podobny do następującego:

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

>> CALL PGM(QSYS/QGLDSVR)
Job 057448/QUSER/QSQRV used for SQL server mode processing.
Job 057340/QUSER/QSQRV used for SQL server mode processing.
Job 057448/QUSER/QSQRV used for SQL server mode processing.
Job 057166/QUSER/QSQRV used for SQL server mode processing.
Job 057279/QUSER/QSQRV used for SQL server mode processing.
Job 057288/QUSER/QSQRV used for SQL server mode processing.
Directory Server started successfully.
```

Komunikaty dotyczą zadań QSQRV uruchomionych dla serwera. Liczba komunikatów może się różnić w zależności od konfiguracji i liczby zadań QSQRV potrzebnych do uruchomienia serwera.

Na stronie właściwości **Baza danych/przyrostki** (Database/Suffixes) serwerów katalogów w programie System i Navigator można określić łączną liczbę serwerów SQL, z których serwer Directory Server korzysta po uruchomieniu do wykonywania operacji na katalogu. Dodatkowe serwery SQL są uruchamiane do obsługi replikacji.

### Informacje pokrewne



Strona główna serwera Directory Server

## Monitorowanie błędów i dostępu za pomocą protokołu zadania serwera Directory Server

Jeśli po wystąpieniu błędu na serwerze Directory Server istnieje potrzeba uzyskania dokładniejszych informacji, można przejrzeć protokół zadania QDIRSRV.

Przeglądanie protokołu zadania serwera Directory Server może pomóc w wykrywaniu błędów i w monitorowaniu dostępu do serwera. Protokół zadania zawiera:

- Komunikaty o działaniu serwera i wszystkich problemach na serwerze, takich jak awarie zadań serwera SQL lub replikacji.
- Komunikaty dotyczące ochrony odzwierciedlające operacje klienta, na przykład wpisanie złego hasła.
- Komunikaty zawierające szczegóły o błędach klienta, takich jak brakujące atrybuty wymagane.

Użytkownik może nie chcieć protokołować błędów klienta, chyba że jest w trakcie ich debugowania. Protokołowaniem błędów klienta można sterować na karcie właściwości **Ogólne** (General) serwera Directory Server w programie System i Navigator.

## Wyświetlanie protokołu zadania QDIRSRV, gdy serwer jest uruchomiony

Jeśli serwer został uruchomiony, to aby przejrzeć protokół zadania QDIRSRV, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń pozycję **Sieć**.
2. Rozwiń pozycję **Serwery**.
3. Kliknij **TCP/IP**.
4. Prawym przyciskiem myszy kliknij element **IBM Directory Server** i wybierz opcję **Zadania serwera** (Server Jobs).
5. Z menu **Plik** wybierz opcję **Protokół zadania**.

## Wyświetlanie protokołu zadania QDIRSRV, gdy serwer jest zatrzymany

Jeśli serwer został zatrzymany, to aby przejrzeć protokół zadania QDIRSRV, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń pozycję **Operacje podstawowe**.
2. Kliknij opcję **Wydruk**.
3. W kolumnie **Użytkownik**, w prawym panelu programu System i Navigator, zostanie wyświetlony QDIRSRV. Aby wyświetlić protokół zadania, kliknij dwukrotnie **Qpjoblog** po lewej stronie pozycji QDIRSRV w tym samym wierszu.

**Uwaga:** Program System i Navigator można skonfigurować tak, aby wyświetlał jedynie pliki buforowe. Jeśli na liście nie ma pozycji QDIRSRV, kliknij pozycję **Zbiór wydruku**, a następnie wybierz opcję **Włącz** z menu **Opcje**. W polu **Użytkownik** podaj wartość **Wszystcy**, a następnie kliknij **OK**.

**Uwaga:** Do wykonywania niektórych zadań serwer Directory Server korzysta z innych zasobów systemu. Jeśli błąd wystąpi w jednym z tych zasobów, protokół zadania wskaże źródło dalszych informacji. W niektórych przypadkach serwer Directory Server może nie móc określić, gdzie należy szukać. Należy wówczas przejrzeć protokół zadania serwerów SQL (Structured Query Language) i sprawdzić, czy błąd nie jest związany z serwerami SQL.

## Odszukiwanie problemów za pomocą komendy TRCTCPAPP

W przypadku powtarzających się błędów można uruchomić śledzenie błędów za pomocą komendy śledzenia aplikacji TCP/IP (TRCTCPAPP APP(\*DIRSRV)).

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 rozumieć całej treści danych śledzenia. Na ich podstawie może jednak sprawdzić, czy między dwoma węzłami nastąpiła faktycznie wymiana danych.

- | Komendy Śledzenie aplikacji TCP/IP (Trace TCP/IP Application - TRCTCPAPP) można użyć na serwerze Directory Server w celu znalezienia problemów z klientami i aplikacjami.
- | Komendy TRCTCPAPP można użyć w celu śledzenia aktywnej instancji serwera. Na przykład:
- | TRCTCPAPP APP(\*DIRSRV) INSTANCE(QUSRDIR)

| Można także uruchomić śledzenie za pomocą komendy STRTCPSVR i dodając wartość '-h dft' podczas uruchamiania instancji. Spowoduje to uruchomienie śledzenia w instancji serwera oraz samej instancji serwera. Na przykład:

| STRTCPSVR SERVER(\*DIRSRV) INSTANCE(QUSRDIR '-h dft')

| Aby zakończyć śledzenie, należy uruchomić następującą komendę:

| TRCTCPAPP APP(\*DIRSRV) SET(\*OFF)

#### **Pojęcia pokrewne**

Śledzenie komunikacji

#### **Informacje pokrewne**

Śledzenie aplikacji TCP/IP (Trace TCP/IP Application - TRCTCPAPP)

## **Używanie opcji LDAP\_OPT\_DEBUG do śledzenia błędów**

Należy śledzić problemy z klientami używającymi funkcji API LDAP C.

Opcji LDAP\_OPT\_DEBUG funkcji API `ldap_set_option()` można użyć w celu śledzenia problemów z klientami używającymi funkcji API języka C dla protokołu LDAP. Opcja debugowania ma wiele ustawień poziomu debugowania, które są pomocne w rozwiązywaniu problemów z tymi aplikacjami.

Poniżej przedstawiono przykład włączania opcji debugowania śledzenia klienta.

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

Kolejnym sposobem ustawienia poziomu debugowania jest skonfigurowanie liczbowej wartości zmiennej środowiskowej LDAP\_DEBUG dla zadania, w którym aplikacja kliencka jest uruchamiana, na tę samą, którą zmienna wartość\_debugowania 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, wpisz w wierszu komend następującą komendę:

```
DMPUSRTRC numer_zadania_klienta
```

gdzie numer\_zadania\_klienta jest numerem zadania klienta.

Aby wyświetlić te informacje interaktywnie, wpisz w wierszu komend następującą komendę:

```
DSPPFM QAP0ZDMP QP0Znnnnn
```

gdzie QAP0ZDMP zawiera zero, a 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. W wierszu komend wpisz wpisz następującą komendę:  
SAVOBJ OBJ(QAP0ZDMP) LIB(QTEMP) DEV(\*SAVF) SAVF(xxx)

gdzie QAP0ZDMP zawiera zero, a xxx jest nazwą pliku SAVF.

#### **Pojęcia pokrewne**

Funkcje API protokołu LDAP

Temat Funkcje API protokołu LDAP zawiera więcej informacji o funkcjach API serwera katalogów.

#### **Informacje pokrewne**

Dodanie zmiennej środowiskowej (Add Environment Variable - ADDENVVAR)

Zrzut śledzenia użytkownika (Dump User Trace - DMPUSRTRC)  
Wyświetlenie podzbioru fizycznego (Display Physical File Member - DSPPFM)  
Tworzenie zbioru składowania (Create Save File - CRTSAVF)  
Składowanie obiektu (Save Object - SAVOBJ)

## Identyfikatory komunikatów GLEnnnn

Ten temat zawiera wykaz identyfikatorów komunikatów GLE wraz z opisami.

Identyfikatory komunikatów przybierają postać GLEnnnn, gdzie nnnn oznacza numer błędu podany w wartościach dziesiętnych. Na przykład, aby wyświetlić opis kodu powrotu 50 (0x32), należy wpisać następującą komendę:

```
DSPMSGD RANGE(GLE0050) MSGF(QGLDMSG)
```

W ten sposób wyświetlony zostanie opis dla LDAP\_INSUFFICIENT\_ACCESS.

Poniższa tabela zawiera identyfikatory komunikatów GLE i ich opisy.

Identyfikator komunikatu	Opis
GLE0000	Żądanie powiodło się (LDAP_SUCCESS)
GLE0001	Błąd operacji (LDAP_OPERATIONS_ERROR)
GLE0002	Błąd protokołu (LDAP_PROTOCOL_ERROR)
GLE0003	Przekroczono limit czasu (LDAP_TIMELIMIT_EXCEEDED)
GLE0004	Przekroczono limit wielkości (LDAP_SIZELIMIT_EXCEEDED)
GLE0005	Porównywany typ i wartość nie istnieją w pozycji (LDAP_COMPARE_FALSE)
GLE0006	Porównywany typ i wartość istnieją w pozycji (LDAP_COMPARE_TRUE)
GLE0007	Nieobsługiwana metoda uwierzytelniania (LDAP_AUTH_METHOD_NOT_SUPPORTED)
GLE0008	Wymagane ściśle uwierzytelnianie (LDAP_STRONG_AUTH_REQUIRED)
GLE0009	Otrzymano częściowe wyniki i odwołanie (LDAP_PARTIAL_RESULTS)
GLE0010	Zwrócono odwołanie (LDAP_REFERRAL)
GLE0011	Przekroczono limit administracyjny (LDAP_ADMIN_LIMIT_EXCEEDED)
GLE0012	Nieobsługiwane rozszerzenie krytyczne (LDAP_UNAVAILABLE_CRITICAL_EXTENSION)
GLE0013	Wymagana poufność (LDAP_CONFIDENTIALITY_REQUIRED)
GLE0014	Łączenie SASL w toku (LDAP_SASLBIND_IN_PROGRESS)
GLE0016	Atrybut nie występuje (LDAP_NO_SUCH_ATTRIBUTE)
GLE0017	Niezdefiniowany typ atrybutu (LDAP_UNDEFINED_TYPE)
GLE0018	Nieodpowiednie dopasowanie (LDAP_INAPPROPRIATE_MATCHING)
GLE0019	Naruszenie ograniczenia (LDAP_CONSTRAINT_VIOLATION)
GLE0020	Typ lub wartość istnieje (LDAP_TYPE_OR_VALUE_EXISTS)

<b>Identyfikator komunikatu</b>	<b>Opis</b>
GLE0021	Niepoprawna składnia (LDAP_INVALID_SYNTAX)
GLE0032	Obiekt nie występuje (LDAP_NO_SUCH_OBJECT)
GLE0033	Błąd aliasu (LDAP_ALIAS_PROBLEM)
GLE0034	Niepoprawna składnia nazwy wyróżniającej (LDAP_INVALID_DN_SYNTAX)
GLE0035	Obiekt jest liściem (LDAP_IS_LEAF)
GLE0036	Błąd wyłuskiwania aliasów (LDAP_ALIAS_DEREF_PROBLEM)
GLE0048	Niepoprawne uwierzytelnienie (LDAP_INAPPROPRIATE_AUTH)
GLE0049	Niepoprawne referencje (LDAP_INVALID_CREDENTIALS)
GLE0050	Niewystarczający poziom dostępu (LDAP_INSUFFICIENT_ACCESS)
GLE0051	Serwer katalogów jest zajęty (LDAP_BUSY)
GLE0052	Agent serwera katalogów jest niedostępny (LDAP_UNAVAILABLE)
GLE0053	Serwer katalogów nie może wykonać żadanego działania (LDAP_UNWILLING_TO_PERFORM)
GLE0054	Wykryto pętlę (LDAP_LOOP_DETECT)
LE0064	Naruszenie nazewnictwa (LDAP_NAMING_VIOLATION)
LE0065	Naruszenie klasy obiektu (LDAP_OBJECT_CLASS_VIOLATION)
GLE0066	Działanie niedozwolone na nie-liściu (LDAP_NOT_ALLOWED_ON_NONLEAF)
GLE0067	Działanie niedozwolone na względnej nazwie wyróżniającej (LDAP_NOT_ALLOWED_ON_RDN)
GLE0068	Już istnieje (LDAP_ALREADY_EXISTS)
GLE0069	Nie można zmienić klasy obiektu (LDAP_NO_OBJECT_CLASS_MODS)
GLE0070	Zbyt duże wyniki (LDAP_RESULTS_TOO_LARGE)
GLE0071	Wpływa na wiele serwerów (LDAP_AFFECTS_MULTIPLE_DSAS)
GLE0080	Nieznany błąd (LDAP_OTHER)
GLE0081	Nie można połączyć z serwerem LDAP (LDAP_SERVER_DOWN)
GLE0082	Błąd lokalny (LDAP_LOCAL_ERROR)
GLE0083	Błąd kodowania (LDAP_ENCODING_ERROR)
GLE0084	Błąd dekodowania (LDAP_DECODING_ERROR)
GLE0085	Przekroczono limit czasu żądania (LDAP_TIMEOUT)
GLE0086	Nieznana metoda uwierzytelniania (LDAP_AUTH_UNKNOWN)
GLE0087	Błędny filtr wyszukiwania (LDAP_FILTER_ERROR)
GLE0088	Działanie anulowane przez użytkownika (LDAP_USER_CANCELLED)
GLE0089	Błędny parametr procedury LDAP (LDAP_PARAM_ERROR)

Identyfikator komunikatu	Opis
GLE0090	Brak pamięci (LDAP_NO_MEMORY)
GLE0091	Błąd połączenia (LDAP_CONNECT_ERROR)
GLE0092	Opcja nieobsługiwana (LDAP_NOT_SUPPORTED)
GLE0093	Nie znaleziono elementu sterującego (LDAP_CONTROL_NOT_FOUND)
GLE0094	Nie zwrócono wyników (LDAP_NO_RESULTS_RETURNED)
GLE0095	Więcej wyników do zwrócenia (LDAP_MORE_RESULTS_TO_RETURN)
GLE0096	Adres URL spoza LDAP (LDAP_URL_ERR_NOTLDAP)
GLE0097	Adres URL nie posiada nazwy wyróżniającej (LDAP_URL_ERR_NODN)
GLE0098	Wartość zasięgu URL jest niepoprawna (LDAP_URL_ERR_BADSCOPE)
GLE0099	Błąd przydzielania pamięci (LDAP_URL_ERR_MEM)
GLE0100	Pętla klienta (LDAP_CLIENT_LOOP)
GLE0101	Przekroczono limit odwołania (LDAP_REFERRAL_LIMIT_EXCEEDED)
GLE0112	Środowisko SSL już zainicjowane (LDAP_SSL_ALREADY_INITIALIZED)
GLE0113	Wywołanie inicjowania nie powiodło się (LDAP_SSL_INITIALIZE_FAILED)
GLE0114	Środowisko SSL nie zostało zainicjowane (LDAP_SSL_CLIENT_INIT_NOT_CALLED)
GLE0115	Określono niedozwoloną wartość parametru SSL (LDAP_SSL_PARAM_ERROR)
GLE0116	Nawiązanie połączenia chronionego nie powiodło się (LDAP_SSL_HANDSHAKE_FAILED)
GLE0118	Nie można znaleźć biblioteki SSL (LDAP_SSL_NOT_AVAILABLE)
GLE0128	Nie znaleziono jawnego właściciela (LDAP_NO_EXPLICIT_OWNER)
GLE0129	Nażalenie blokady na żądany zasób było niemożliwe (LDAP_NO_LOCK)
GLE0133	Nie znaleziono serwerów LDAP w systemie DNS (LDAP_DNS_NO_SERVERS)
GLE0134	Obcięte wyniki DNS (LDAP_DNS_TRUNCATED)
GLE0135	Analiza danych DNS była niemożliwa (LDAP_DNS_INVALID_DATA)
GLE0136	Nie można rozstrzygnąć domeny systemu lub serwera nazw (LDAP_DNS_RESOLVE_ERROR)
GLE0137	Błąd pliku konfiguracyjnego DNS (LDAP_DNS_CONF_FILE_ERROR)
GLE0160	Przepełnienie bufora wyjściowego (LDAP_XLATE_E2BIG)
GLE0161	Obcięty bufor wejściowy (LDAP_XLATE_EINVAL)
GLE0162	Znak wejściowy nie do użycia (LDAP_XLATE_EILSEQ)



Identyfikator komunikatu	Opis
GLE0163	Znak nie odwzorowuje punktu zestawu kodowego (LDAP_XLATE_NO_ENTRY)

### Informacje pokrewne

Wyświetlenie opisu komunikatu (Display Message Description - DSPMSGD)

## Najczęstsze błędy klienta LDAP

Ten temat zawiera informacje o typowych błędach klienta LDAP.

Znajomość przyczyn występowania najczęstszych błędów klienta LDAP może pomóc w rozwiązywaniu problemów z serwerem. Pełną listę warunków błędu klienta LDAP zawiera temat “Funkcje API serwera Directory Server” w kolekcji tematów Programowanie.

Komunikaty o błędach klienta mają następujący format:

[Operacja LDAP wykazująca błąd]:[warunki błędów API klienta LDAP]

**Uwaga:** W wyjaśnieniu tych błędów przyjęto, że klient komunikuje się z serwerem LDAP działającym w systemie operacyjnym i5/OS. Klient komunikujący się z serwerem na innej platformie może powodować podobne błędy, lecz przyczyny i rozwiązania najprawdopodobniej będą inne.

### Pojęcia pokrewne

Funkcje API protokołu LDAP

Temat Funkcje API protokołu LDAP zawiera więcej informacji o funkcjach API serwera katalogów.

### ldap\_search: przekroczono limit czasu

Ten błąd występuje, gdy komenda ldapsearch działa powoli.

Aby naprawić ten błąd, można wykonać jedną z poniższych czynności lub obie:

- Zwiększyć limit czasu wyszukiwania dla serwera Directory Server.
- Zmniejszyć aktywność w systemie. Można także zmniejszyć liczbę aktywnych zadań klientów LDAP.

### Zadania pokrewne

“Dopasowywanie ustawień wyszukiwania” na stronie 127

Ten temat zawiera informacje dotyczące określania możliwości użytkowników w zakresie wyszukiwania.

### [Błędna operacja LDAP]: Błąd podczas działania

([Błędna operacja LDAP]: Błąd podczas działania). Błąd ten może być spowodowany kilkoma przyczynami.

Aby uzyskać informacje o przyczynie tego błędu w konkretnym przypadku, należy zapoznać się z protokołami zadania QDIRSRV i protokołami zadań serwera SQL.

### Pojęcia pokrewne

“Rozwiązywanie problemów z serwerem Directory Server” na stronie 309

Informacje pomocne w rozwiązywaniu problemów. Obejmują sugestie dotyczące gromadzenia danych o usługach oraz rozwiązywania konkretnych problemów.

### Zadania pokrewne

“Monitorowanie błędów i dostępu za pomocą protokołu zadania serwera Directory Server” na stronie 309

Jeśli po wystąpieniu błędu na serwerze Directory Server istnieje potrzeba uzyskania dokładniejszych informacji, można przejrzeć protokół zadania QDIRSRV.

### ldap\_bind: Brak takiego obiektu

(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 poda błędną nazwę wyróżniającą administratora. Na przykład użytkownik może określić QSECOFR lub Administrator, podczas gdy rzeczywista nazwa wyróżniająca administratora może mieć formę cn=Administrator.

Szczegółowe informacje dotyczące tego błędu zawiera protokół zadania QDIRSRV.

#### **Zadania pokrewne**

“Monitorowanie błędów i dostępu za pomocą protokołu zadania serwera Directory Server” na stronie 309

Jeśli po wystąpieniu błędu na serwerze Directory Server istnieje potrzeba uzyskania dokładniejszych informacji, można przejrzeć protokół zadania QDIRSRV.

### **ldap\_bind: Niewłaściwe uwierzytelnienie**

Serwer zwraca niepoprawne referencje, gdy hasło lub nazwa wyróżniająca łączenia 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 i5/OS mającego atrybut UID, ale nie atrybut userpassword (hasło użytkownika). Powoduje to porównanie podanego hasła z hasłem użytkownika systemu i5/OS, które nie są zgodne.
- Z pozycji, która reprezentuje użytkownika rzutowanego i zażądano metody połączenia innej niż prosta.

Błąd ten generowany jest zazwyczaj, gdy klient usiłuje nawiązać połączenie z niepoprawnym hasłem. Aby uzyskać szczegółowe informacje dotyczące tego błędu, należy zapoznać się z protokołem zadania QDIRSRV.

#### **Zadania pokrewne**

“Monitorowanie błędów i dostępu za pomocą protokołu zadania serwera Directory Server” na stronie 309

Jeśli po wystąpieniu błędu na serwerze Directory Server istnieje potrzeba uzyskania dokładniejszych informacji, można przejrzeć protokół zadania QDIRSRV.

### **[Błędna operacja LDAP]: Niewłaściwy dostęp**

([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).

Aby uzyskać informacje dotyczące tego błędu, należy zapoznać się z protokołem zadania QDIRSRV.

#### **Zadania pokrewne**

“Monitorowanie błędów i dostępu za pomocą protokołu zadania serwera Directory Server” na stronie 309

Jeśli po wystąpieniu błędu na serwerze Directory Server istnieje potrzeba uzyskania dokładniejszych informacji, można przejrzeć protokół zadania QDIRSRV.

### **[Błędna operacja LDAP]: Nie można się połączyć z serwerem LDAP**

Najczęstszą przyczyną tego błędu jest przesłanie żądania zanim serwer stanie się gotowy lub podanie niepoprawnego numeru portu.

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

- Klient LDAP wysłał 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 klient usiłuje w żądaniu użyć portu 387.

Aby uzyskać informacje dotyczące tego błędu, należy zapoznać się z protokołem zadania QDIRSRV. Jeśli serwer Directory Server został pomyślnie uruchomiony, w protokole zadania QDIRSRV zostanie zapisany odpowiedni komunikat.

### Zadania pokrewne

“Monitorowanie błędów i dostępu za pomocą protokołu zadania serwera Directory Server” na stronie 309  
Jeśli po wystąpieniu błędu na serwerze Directory Server istnieje potrzeba uzyskania dokładniejszych informacji, można przejrzeć protokół zadania QDIRSRV.

## [Błędna operacja LDAP]: Połączenie z serwerem SSL nie powiodło się

([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).

W przypadku aplikacji dla systemu i5/OS napisanych w języku C dostępne są dodatkowe informacje o błędach protokołu SSL. Szczegółowe informacje zawiera sekcja “Funkcje API serwera Directory Server” w temacie Programowanie.

### Pojęcia pokrewne

Funkcje API protokołu LDAP

Temat Funkcje API protokołu LDAP zawiera więcej informacji o funkcjach API serwera katalogów.

## Błędy związane ze strategią haseł

Aktywacja strategii haseł może czasami powodować nieoczekiwane błędy.

Włączenie niektórych strategii haseł, może powodować awarie, które nie są oczywiste. Aby uzyskać pomoc w rozwiązywaniu problemów związanych ze strategiami haseł, należy zapoznać się z poniższymi informacjami.

**Połączenie przy użyciu poprawnego hasła zwraca błąd “niepoprawne referencje”:** Hasło mogło utracić ważność lub konto mogło zostać zablokowane. Sprawdź atrybuty pwdchangedtime i pwdaccountlockedtime tej pozycji.

**Żądania zwracają komunikat “nie można wykonać” po pomyślnym nawiązaniu połączenia:** hasło mogło zostać wyzerowane, co powoduje, że połączenie powiedzie się, ale jedynym działaniem dozwolonym przez serwer jest zmiana hasła przez użytkownika. Pozostałe żądania nie powiedzą się i zwrócony zostanie komunikat “nie można wykonać” do momentu, kiedy hasło zostanie zmienione.

**Uwierzytelnienie za pomocą zmienionego hasła powoduje nieoczekiwane zachowanie:** Jeśli hasło zostało zmienione, żądanie połączenia powiedzie się zgodnie z opisem powyżej. Oznacza to, że użytkownik może dokonać uwierzytelnienia za pomocą wyzerowanego hasła bezterminowo.

### Odsyłacze pokrewne

“Wskazówki dotyczące strategii haseł” na stronie 80

Strategia haseł nie zawsze działa zgodnie z oczekiwaniami.

## Rozwiązywanie problemów z funkcją API QGLDCPYVL

Użycie narzędzia śledzenia użytkownika może pomóc w zrozumieniu błędu i określeniu, czy konieczna jest pomoc serwisowa.

Ta funkcja API wykorzystuje narzędzie śledzenia użytkownika do zapisywania swego działania. W przypadku wystąpienia błędów lub możliwości ich wystąpienia, śledzenie może pomóc w zrozumieniu błędu i określeniu, czy konieczna jest obsługa. Śledzenie można wywołać w następujący sposób:

```
STRTRC SSNID(COPYVLDL) JOBTRCTYPE(*TRCTYPE) TRCTYPE((*DIRSRV *INFO))
CALL QGLDCPYVL PARM(...)
ENDTRC SSNID(COPYVLDL) DTALIB(QTEMP) PRTRTC(*YES)
```

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

1. Utwórz plik SAVF za pomocą komendy CRTSAVF.
2. W wierszu komend wpisz następującą komendę:  
SAVOBJ OBJ(QAP0ZDMP) LIB(QTEMP) DEV(\*SAVF) SAVF(*xxx*)  
gdzie QAP0ZDMP zawiera zero, a *xxx* jest nazwą pliku SAVF.

#### Pojęcia pokrewne

Funkcje API protokołu LDAP

Temat Funkcje API protokołu LDAP zawiera więcej informacji o funkcjach API serwera katalogów.

#### Informacje pokrewne

Uruchomienie śledzenia (Start Trace - STRTRC)

Tworzenie zbioru składowania (Create Save File - CRTSAVF)




Składowanie obiektu (Save Object - SAVOBJ)

---

## Informacje pokrewne

Poniżej wymieniono dokumentację techniczną IBM Redbooks (w formacie PDF), serwisy WWW oraz tematy Centrum informacyjnego powiązane z tematem dotyczącym serwera Directory Server. Dokumenty te można wyświetlać na ekranie i drukować.

### Dokumentacja techniczna IBM Redbooks ([www.redbooks.ibm.com](http://www.redbooks.ibm.com))

- Understanding LDAP, SG24-4986  .
- Using LDAP for Directory Integration: A Look at IBM SecureWay Directory, Active Directory, and Domino, SG24-6163  .
- Implementation and Practical Use of LDAP on the iSeries Server, SG24-6193  .

### Serwisy WWW

- Serwis WWW IBM Directory Server for iSeries  ([www.ibm.com/servers/eserver/iseres/ldap](http://www.ibm.com/servers/eserver/iseres/ldap))
- Serwis WWW z kursem The Java Naming and Directory Interface (JNDI) Tutorial  ([java.sun.com/products/jndi/tutorial/](http://java.sun.com/products/jndi/tutorial/))

### Inne informacje

“Funkcje API protokołu LDAP” w kategorii Programowanie.

---

## Dodatek. Uwagi

Niniejsza publikacja została przygotowana z myślą o produktach i usługach oferowanych w Stanach Zjednoczonych.

IBM może nie oferować w innych krajach produktów, usług lub opcji, omawianych w tej publikacji. Informacje o produktach i usługach dostępnych w danym kraju można uzyskać od lokalnego przedstawiciela IBM. Odwołanie do produktu, programu lub usługi IBM nie oznacza, że można użyć wyłącznie tego produktu, programu lub usługi. Zamiast nich można zastosować ich odpowiednik funkcjonalny pod warunkiem, że nie narusza to praw własności intelektualnej IBM. Jednakże cała odpowiedzialność za ocenę przydatności i sprawdzenie działania produktu, programu lub usługi pochodzących od producenta innego niż IBM spoczywa na użytkowniku.

IBM może posiadać patenty lub złożone wnioski patentowe na towary i usługi, o których mowa w niniejszej publikacji. Przedstawienie niniejszej publikacji nie daje żadnych uprawnień licencyjnych do tychże patentów. Pisemne zapytania w sprawie licencji można przysyłać na adres:

IBM Director of Licensing  
IBM Corporation  
North Castle Drive  
Armonk, NY 10504-1785  
USA

Zapytania w sprawie licencji na informacje dotyczące zestawów znaków dwubajtowych (DBCS) należy kierować do lokalnych działów własności intelektualnej IBM (IBM Intellectual Property Department) lub zgłaszać na piśmie pod adresem:

IBM World Trade Asia Corporation  
Licensing  
2-31 Roppongi 3-chome, Minato-ku  
Tokio 106-0032, Japonia

**Poniższy akapit nie obowiązuje w Wielkiej Brytanii, a także w innych krajach, w których jego treść pozostaje w sprzeczności z przepisami prawa miejscowego:** INTERNATIONAL BUSINESS MACHINES CORPORATION DOSTARCZA TĘ PUBLIKACJĘ W STANIE, W JAKIM SIĘ ZNAJDUJE "AS IS" BEZ UDZIELANIA JAKICHKOLWIEK GWARANCJI (W TYM TAKŻE RĘKOJMI), WYRAŻNYCH LUB DOMNIEMANYCH, A W SZCZEGÓLNOŚCI DOMNIEMANYCH GWARANCJI PRZYDATNOŚCI HANDLOWEJ, PRZYDATNOŚCI DO OKREŚLONEGO CELU ORAZ GWARANCJI, ŻE PUBLIKACJA NIE NARUSZA PRAW STRON TRZECICH. Ustawodawstwa niektórych krajów nie dopuszczają zastrzeżeń dotyczących gwarancji wyraźnych lub domniemanych w odniesieniu do pewnych transakcji; w takiej sytuacji powyższe zdanie nie ma zastosowania.

Informacje zawarte w niniejszej publikacji mogą zawierać nieścisłości techniczne lub błędy drukarskie. Informacje te są okresowo aktualizowane, a zmiany te zostaną uwzględnione w kolejnych wydaniach tej publikacji. IBM zastrzega sobie prawo do wprowadzania ulepszeń i/lub zmian w produktach i/lub programach opisanych w tej publikacji w dowolnym czasie, bez wcześniejszego powiadomienia.

Wszelkie wzmianki w tej publikacji na temat stron internetowych innych firm zostały wprowadzone wyłącznie dla wygody użytkowników i w żadnym wypadku nie stanowią zachęty do ich odwiedzania. Materiały dostępne na tych stronach nie są częścią materiałów opracowanych dla tego produktu IBM, a użytkownik korzysta z nich na własną odpowiedzialność.

IBM ma prawo do korzystania i rozpowszechniania informacji przysłanych przez użytkownika w dowolny sposób, jaki uzna za właściwy, bez żadnych zobowiązań wobec ich autora.

Licencjobiorcy tego programu, którzy chcieliby uzyskać informacje na temat programu w celu: (i) wdrożenia wymiany informacji między niezależnie utworzonymi programami i innymi programami (łącznie z tym opisywanym) oraz (ii) wspólnego wykorzystywania wymienianych informacji, powinni skontaktować się z:

IBM Corporation  
Software Interoperability Coordinator, Department YBWA  
3605 Highway 52 N  
Rochester, MN 55901  
USA

Informacje takie mogą być udostępnione, o ile spełnione zostaną odpowiednie warunki, w tym, w niektórych przypadkach, uiszczenie odpowiedniej opłaty.

Licencjonowany program opisany w niniejszej publikacji oraz wszystkie inne licencjonowane materiały dostępne dla tego programu są dostarczane przez IBM na warunkach określonych w Umowie IBM z Klientem, Międzynarodowej Umowie Licencyjnej IBM na Program, Umowie Licencyjnej IBM na Kod Maszynowy lub w innych podobnych umowach zawartych między IBM i użytkownikami.

Wszelkie dane dotyczące wydajności zostały zebrane w kontrolowanym środowisku. W związku z tym rezultaty uzyskane w innych środowiskach operacyjnych mogą się znacząco różnić. Niektóre pomiary mogły być dokonywane na systemach będących w fazie rozwoju i nie ma gwarancji, że pomiary te wykonane na ogólnie dostępnych systemach dadzą takie same wyniki. Niektóre z pomiarów mogły być estymowane przez ekstrapolację. Rzeczywiste wyniki mogą być inne. Użytkownicy powinni we własnym zakresie sprawdzić odpowiednie dane dla ich środowiska.

Informacje dotyczące produktów firm innych niż IBM pochodzą od dostawców tych produktów, z opublikowanych przez nich zapowiedzi lub innych powszechnie dostępnych źródeł. Firma IBM nie testowała tych produktów i nie może potwierdzić dokładności pomiarów wydajności, kompatybilności ani żadnych innych danych związanych z tymi produktami. Pytania dotyczące możliwości produktów firm innych niż IBM należy kierować do dostawców tych produktów.

Wszelkie stwierdzenia dotyczące przyszłych kierunków rozwoju i zamierzeń IBM mogą zostać zmienione lub wycofane bez powiadomienia.

Wszelkie ceny podawane przez IBM są propozycjami cen detalicznych; ceny te są aktualne i podlegają zmianom bez wcześniejszego powiadomienia. Ceny podawane przez dealerów mogą być inne.

Niniejsza informacja służy jedynie do celów planowania. Informacja ta podlega zmianom do chwili, gdy produkty, których ona dotyczy, staną się dostępne.

Publikacja ta zawiera przykładowe dane i raporty używane w codziennych operacjach działalności gospodarczej. W celu kompleksowego ich zilustrowania, podane przykłady zawierają nazwiska osób prywatnych, nazwy przedsiębiorstw oraz nazwy produktów. Wszystkie te nazwy/nazwiska są fikcyjne i jakiegokolwiek podobieństwo do istniejących nazw/nazwisk i adresów jest całkowicie przypadkowe.

#### LICENCJA W ZAKRESIE PRAW AUTORSKICH:

Niniejsza publikacja zawiera przykładowe aplikacje w kodzie źródłowym, ilustrujące techniki programowania w różnych systemach operacyjnych. Użytkownik może kopiować, modyfikować i dystrybuować te programy przykładowe w dowolnej formie bez uiszczania opłat na rzecz IBM, w celu projektowania, używania, sprzedaży lub dystrybucji aplikacji zgodnych z aplikacyjnym interfejsem programowym dla tego systemu operacyjnego, dla którego napisane zostały programy przykładowe. Programy przykładowe nie zostały gruntownie przetestowane. IBM nie może zatem gwarantować ani sugerować niezawodności, użyteczności i funkcjonalności tych programów.

W przypadku przeglądania niniejszych informacji w formie elektronicznej, zdjęcia i kolorowe ilustracje mogą nie być wyświetlane.

---

## Znaki towarowe

Następujące nazwy są znakami towarowymi International Business Machines Corporation w Stanach Zjednoczonych i/lub w innych krajach:

Application System/400  
AS/400  
DB2  
Domino  
e(logoserver)  
eServer  
i5/OS  
IBM  
iSeries  
Java  
Lotus  
Lotus Notes  
Operating System/400  
OS/400  
Redbooks  
RDN  
SecureWay  
System i  
Tivoli  
UNIX  
WebSphere  
XT  
400

Adobe, logo Adobe, PostScript oraz logo PostScript są zastrzeżonymi znakami towarowymi lub znakami towarowymi firmy Adobe Systems Incorporated w Stanach Zjednoczonych i/lub w innych krajach.

Microsoft, Windows, Windows NT oraz logo Windows są znakami towarowymi Microsoft Corporation w Stanach Zjednoczonych i/lub w innych krajach.

Java oraz wszystkie znaki towarowe dotyczące języka Java są znakami towarowymi Sun Microsystems, Inc. w Stanach Zjednoczonych i/lub w innych krajach.

UNIX jest zastrzeżonym znakiem towarowym Open Group w Stanach Zjednoczonych i w innych krajach.

Nazwy innych przedsiębiorstw, produktów i usług mogą być znakami towarowymi lub znakami usług innych podmiotów.

---

## Warunki

Zezwolenie na korzystanie z tych publikacji jest przyznawane na poniższych warunkach.

**Użytek osobisty:** Użytkownik ma prawo kopiować te publikacje do własnego, niekomercyjnego użytku pod warunkiem zachowania wszelkich uwag dotyczących praw własności. Użytkownik nie ma prawa dystrybuować ani wyświetlać tych publikacji czy ich części, ani też wykonywać na ich podstawie prac pochodnych bez wyraźnej zgody IBM.

**Użytek służbowy:** Użytkownik ma prawo kopiować te publikacje, dystrybuować je i wyświetlać wyłącznie w ramach przedsiębiorstwa Użytkownika pod warunkiem zachowania wszelkich uwag dotyczących praw własności. Użytkownik nie ma prawa wykonywać na podstawie tych publikacji ani ich fragmentów prac pochodnych, kopiować ich, dystrybuować ani wyświetlać poza przedsiębiorstwem Użytkownika bez wyraźnej zgody IBM.

Z wyjątkiem zezwoleń wyraźnie udzielonych w niniejszym dokumencie, nie udziela się jakichkolwiek innych zezwoleń, licencji ani praw, wyraźnych czy domniemanych, odnoszących się do tych publikacji czy jakichkolwiek informacji, danych, oprogramowania lub innej własności intelektualnej, o których mowa w niniejszym dokumencie.

IBM zastrzega sobie prawo do anulowania zezwolenia przyznanego w niniejszym dokumencie w każdej sytuacji, gdy, według uznania IBM, korzystanie z tych publikacji jest szkodliwe dla IBM lub jeśli IBM uzna, że warunki niniejszego dokumentu nie są przestrzegane.

Użytkownik ma prawo pobierać, eksportować lub reeksportować niniejsze informacje pod warunkiem zachowania bezwzględnej i pełnej zgodności z obowiązującym prawem i przepisami, w tym ze wszelkimi prawami i przepisami eksportowymi Stanów Zjednoczonych.

**IBM NIE UDZIELA JAKICHKOLWIEK GWARANCJI, W TYM TAKŻE RĘKOJMI, DOTYCZĄCYCH TREŚCI TYCH PUBLIKACJI. PUBLIKACJE TE SĄ DOSTARCZANE W STANIE, W JAKIM SIĘ ZNAJDUJĄ ("AS IS") BEZ UDZIELANIA JAKICHKOLWIEK GWARANCJI, W TYM TAKŻE RĘKOJMI, WYRAŹNYCH CZY DOMNIEMANYCH, A W SZCZEGÓLNOŚCI DOMNIEMANYCH GWARANCJI PRZYDATNOŚCI HANDLOWEJ, PRZYDATNOŚCI DO OKREŚLONEGO CELU ORAZ NIENARUSZANIA PRAW STRON TRZECICH.**







Drukowane w USA