IBM Security Directory Server
Wersja 6.3.1.5

# *Podręcznik instalowania i konfigurowania*

SC85-0425-02

IBM Security Directory Server
Wersja 6.3.1.5

# *Podręcznik instalowania i konfigurowania*

SC85-0425-02

**Uwaga**

Przed korzystaniem z tych informacji oraz z produktu, którego dotyczą, należy przeczytać informacje ogólne znajdujące się w sekcji “Uwagi” na stronie 259.

**Uwagi do edycji**

**Uwaga: Niniejsze wydanie dotyczy wersji 6.3.1.5 produktu** *IBM Security Directory Server* **(numer produktu 5724-J39) i wszystkich jego późniejszych wersji oraz modyfikacji, o ile nie zostanie inaczej zaznaczone w nowych wydaniach.**

# Spis treści

# Informacje o tej publikacji

Produkt IBM® Security Directory Server, poprzednio zwany IBM Tivoli Directory Server, to implementacja firmy IBM serwera katalogów LDAP (Lightweight Directory Access Protocol) przeznaczona dla następujących systemów operacyjnych:

- Microsoft Windows
- AIX
- Linux (System x, System z, System p i System i)
- Solaris
- Hewlett-Packard UNIX (HP-UX) (Itanium)

Publikacja *IBM Security Directory Server - Podręcznik instalowania i konfigurowania* zawiera informacje na temat instalowania, konfigurowania i deinstalowania produktu IBM Security Directory Server. Zawiera również informacje na temat aktualizowania ze starszej wersji.

## Dostęp do publikacji i terminologii

Ta sekcja zawiera:

- Listę publikacji w "Biblioteka produktu IBM Security Directory Server".
- Odsyłacze do "Publikacje elektroniczne" na stronie viii.
- Odsyłacz do "Serwis WWW IBM Terminology" na stronie viii.

### Biblioteka produktu IBM Security Directory Server

Następujące dokumenty są dostępne w bibliotece produktu IBM Security Directory Server:

- *IBM Security Directory Server, Version 6.3.1.5 Product Overview*, GC27-6212-01

  Zawiera informacje na temat produktu IBM Security Directory Server, nowych funkcji w bieżącym wydaniu oraz informacje o wymaganiach systemowych.
- *IBM Security Directory Server, Version 6.3.1.5 Quick Start Guide*, GI11-9351-02

  Ułatwia rozpoczęcie pracy z produktem IBM Security Directory Server. Zawiera krótki opis i diagram architektury produktu, jak również odsyłacz do serwisu z dokumentacją oraz instrukcje instalacyjne.
- *IBM Security Directory Server, wersja 6.3.1.5 - Podręcznik instalowania i konfigurowania*, SC85-0425-02

  Zawiera kompletne informacje na temat instalowania, konfigurowania i deinstalowania produktu IBM Security Directory Server. Obejmuje informacje na temat aktualizowania z poprzedniej wersji produktu IBM Security Directory Server.
- *IBM Security Directory Server, Version 6.3.1.5 Administration Guide*, SC27-2749-02

  Zawiera instrukcje wykonywania zadań administracyjnych za pomocą programu Web Administration Tool oraz programów narzędziowych wiersza komend.
- *IBM Security Directory Server, Version 6.3.1.5 Reporting Guide*, SC27-6531-00

  Opisuje narzędzia i oprogramowanie służące do tworzenia raportów dla produktu IBM Security Directory Server.
- *IBM Security Directory Server, Version 6.3.1.5 Command Reference*, SC27-2753-02

  Opisuje składnię oraz sposób użytkowania programów narzędziowych uruchamianych z wiersza komend dostarczanych z produktem IBM Security Directory Server.

- *IBM Security Directory Server, Version 6.3.1.5 Server Plug-ins Reference* , SC27-2750-02

  Zawiera informacje na temat pisania wtyczek serwera.
- *IBM Security Directory Server, Version 6.3.1.5 Programming Reference*, SC27-2754-02

  Zawiera informacje na temat pisania aplikacji klienckich LDAP (Lightweight Directory Access Protocol) w językach C oraz Java™.
- *IBM Security Directory Server, Version 6.3.1.5 Performance Tuning and Capacity Planning Guide*, SC27-2748-02

  Zawiera informacje na temat strojenia serwera katalogów w celu uzyskania lepszej wydajności. Opisuje wymagania dotyczące dysku oraz inne wymagania sprzętowe dla katalogów o różnych wielkościach oraz o rozmaitych prędkościach odczytu i zapisu. Opisuje znane scenariusze działania dla każdego z tych poziomów katalogu oraz wykorzystanie pamięci wewnętrznej i dyskowej; sugeruje również reguły postępowania.
- *IBM Security Directory Server, Version 6.3.1.5 Troubleshooting Guide*, GC27-2752-02

  Zawiera informacje na temat możliwych problemów oraz działań naprawczych, które należy przeprowadzić przed zgłoszeniem problemu do działu wsparcia IBM dla oprogramowania.
- *IBM Security Directory Server, Version 6.3.1.5 Error Message Reference*, GC27-2751-02

  Zawiera listę wszystkich komunikatów ostrzegawczych oraz komunikatów o błędach zawiązanych z produktem IBM Security Directory Server.

### Publikacje elektroniczne

IBM umieszcza publikacje produktu oraz ich aktualizacje w następujących lokalizacjach:

**Serwis WWW z dokumentacją produktu IBM Security Directory Server**
Pod adresem http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.IBMDS.doc/welcome.htm wyświetlana jest strona powitalna dla tego produktu.

**IBM Security Systems Documentation Central i strona powitalna**
Serwis IBM Security Systems Documentation Central zawiera alfabetyczną listę wszystkich publikacji dla produktu IBM Security Systems. Znajdują się tam również odsyłacze do dokumentacji związanej z konkretną wersją danego produktu.

W serwisie Welcome to IBM Security Systems documentation znajduje się wprowadzenie, odsyłacze i ogólne informacje na temat dokumentacji produktu IBM Security Systems.

**Centrum publikacji IBM**
W serwisie http://www-05.ibm.com/e-business/linkweb/publications/servlet/pbi.wss można skorzystać z niestandardowych funkcji wyszukiwania w celu odnalezienia wszystkich szukanych publikacji IBM.

### Serwis WWW IBM Terminology

Serwis WWW terminologii IBM zawiera w jednym miejscu terminologię dla całej biblioteki produktów. Jest on dostępny pod adresem http://www.ibm.com/software/globalization/terminology.

## Ułatwienia dostępu

Ułatwienia dostępu to opcje, których zadaniem jest pomoc użytkownikom niepełnosprawnym fizycznie (na przykład mającym trudności z poruszaniem się lub niedowidzącym) w korzystaniu z produktów oprogramowania. W pracy z niniejszym produktem pomagają technologie pozwalające posługiwać się słuchem podczas korzystania z interfejsu

użytkownika. Wykorzystując wszystkie opcje graficznego interfejsu użytkownika, można także posługiwać się klawiaturą zamiast myszy.

Więcej informacji znajduje się w dodatku Ułatwienia dostępu w publikacji *IBM Security Directory Server - przegląd produktu*.

## Szkolenia techniczne

Aby uzyskać informacje na temat szkoleń technicznych, przejdź do serwisu WWW IBM Education pod adresem: http://www.ibm.com/software/tivoli/education.

## Informacje o wsparciu

Wsparcie firmy IBM pomaga podczas rozwiązywania problemów związanych z kodem i procedurami, instalowaniem i korzystaniem. Serwis WWW działu wsparcia dla oprogramowania IBM jest dostępny pod adresem http://www.ibm.com/software/support/probsub.html.

Publikacja *IBM Security Directory Server - Podręcznik rozwiązywania problemów* zawiera następujące informacje:

- Jakie informacje należy zgromadzić przed skontaktowaniem się z działem wsparcia IBM.
- Różne metody kontaktowania się z działem wsparcia IBM.
- Sposób korzystania z programu IBM Support Assistant.
- Instrukcje oraz zasoby służące do samodzielnego określenia i rozwiązania problemu.

**Uwaga:** Na karcie **Społeczność i wsparcie** w Centrum informacyjnym produktu znajdują się dodatkowe zasoby dotyczące wsparcia.

## Sprawdzone procedury w zakresie bezpieczeństwa

Bezpieczeństwo systemu IT wymaga ochrony systemów i informacji poprzez zapobieganie, wykrywanie i reagowanie na niewłaściwy dostęp z wewnątrz i z zewnątrz organizacji. Niewłaściwy dostęp może spowodować, że informacje zostaną zmienione, zniszczone, przywłaszczone lub niewłaściwie wykorzystane albo systemy mogą zostać uszkodzone lub niewłaściwe wykorzystane, w tym również do ataków na inne systemy. Żaden system ani produkt informatyczny nie jest całkowicie bezpieczny. Żaden pojedynczy produkt, usługa czy zabezpieczenie nie gwarantują pełnej skuteczności ochrony przed niewłaściwym użyciem lub dostępem. Systemy, produkty i usługi IBM zostały zaprojektowane jako część kompleksowego rozwiązania w zakresie zabezpieczeń, obejmującego niezbędne dodatkowe procedury operacyjne i mogącego wymagać większej skuteczności innych systemów, produktów czy usług. IBM NIE GWARANTUJE, ŻE SYSTEMY, PRODUKTY CZY USŁUGI SĄ ODPORNE NA DZIAŁANIA PODEJMOWANE PRZEZ OSOBY TRZECIE W ZŁEJ WIERZE LUB BEZPRAWNIE ANI ŻE TAKIE SYSTEMY, PRODUKTY CZY USŁUGI ZABEZPIECZĄ PRZEDSIĘBIORSTWO PRZED TAKIMI DZIAŁANIAMI OSÓB TRZECICH.

# Rozdział 1. Planowanie instalacji

Przed zainstalowaniem produktu IBM Security Directory Server należy podjąć szereg decyzji na temat sprzętu, oprogramowania, ról użytkowników, bezpieczeństwa itp.

## Przewodnik przejścia

Aby zainstalować serwer, należy skorzystać z listy kontrolnej znajdującej się w tej sekcji.

W przypadku aktualizacji wcześniejszej wersji nie należy korzystać z tej listy kontrolnej. Odpowiednie instrukcje zawiera Rozdział 14, “Aktualizowanie instancji starszej wersji”, na stronie 89.

Aby zainstalować serwer:

1. Przeczytaj krótki przegląd, aby zaznajomić się z komponentami produktu IBM Security Directory Server, które zainstalujesz:
2. Upewnij się, że spełnione są minimalne wymagania dotyczące sprzętu i oprogramowania. Informacje o wymaganiach zawiera sekcja “Wymagania dotyczące miejsca na dysku” na stronie 3.
3. Zainstaluj produkt IBM Security Directory Server za pomocą programu IBM Installation Manager.
4. W czasie restartu systemu na platformie Windows zaloguj się jako użytkownik, który był zalogowany podczas instalacji.
5. Użyj programu Instance Administration Tool, aby zarządzać instancjami serwera katalogów.
6. Opcjonalnie sprawdź instalację i konfigurację, ładując przykładowy plik LDIF do bazy danych. Aby uzyskać więcej informacji, patrz Dodatek B, “Ładowanie przykładowej bazy danych i uruchamianie serwera”, na stronie 245.
7. Uruchom instancję serwera katalogów oraz program Web Administration Tool, jeśli został zainstalowany.
8. Więcej informacji na temat konfigurowania i używania serwera oraz programu Web Administration Tool znajduje się w sekcji Administrowanie dokumentacji produktu IBM Security Directory Server.

Jeśli został zainstalowany pełny serwer katalogów i chcesz zaplanować organizację bazy danych, patrz “Planowanie konfiguracji” na stronie 124.

# Rozdział 2. Przegląd instalacji

Należy przygotować komputer i wybrać tryb instalowania produktu IBM Security Directory Server odpowiedni dla danego środowiska.

Program instalacyjny wykorzystujący program IBM Installation Manager jest dostępny w systemach Windows, Linux64 i AIX. Odpowiednie opakowujące programy instalacyjne są dostępne dla produktu IBM Security Directory Server w systemach UNIX (oprócz systemów Linux 64 i AIX). Za pomocą programu instalacyjnego wykorzystującego program Installation Manager można zainstalować produkt IBM Security Directory Server 6.3.1 z interfejsu GUI lub w trybie instalacji cichej.

## Wymagania dotyczące miejsca na dysku

W celu pomyślnego zainstalowania produktu IBM Security Directory Server i innego wymaganego oprogramowania, na komputerze musi być dostępna odpowiednia ilość miejsca na dysku. Wymagania dotyczące miejsca na dysku zmieniają się w zależności od systemu operacyjnego oraz wybranych do zainstalowania funkcji produktu IBM Security Directory Server i innego oprogramowania.

### Wymagania dotyczące miejsca na dysku w systemie Windows

**Uwaga:** Jeśli zostaną wybrane do zainstalowania funkcje pełnego serwera i serwera proxy, należy dodać wielkość pakietów Client SDK, IBM Java Development Kit i Java Client.

*Tabela 1. Wymagania dotyczące miejsca na dysku dla funkcji produktu IBM Security Directory Server i innego wymaganego oprogramowania w systemie Windows*

| **Funkcja do zainstalowania** | **Miejsce na dysku wymagane do instalacji (w MB)** |
|---|---|
| Pakiet Software Development Kit klienta | 25 MB |
| IBM Java Development Kit | 200 MB |
| Klient Java | 124 MB |
| Wdrożony program Web Administration Tool (zawiera wbudowaną wersję WebSphere Application Server i program Web Administration Tool wdrożony we wbudowanej wersji WebSphere Application Server) | 440 MB |
| Wdrożenie narzędzia Web Administration Tool w istniejącym wbudowanym serwerze WebSphere Application Server lub serwerze WebSphere Application Server | 260 MB |
| Serwer podstawowy | 23 MB |
| Serwer proxy (należy dodać wielkości dla pakietu SDK klienta, klienta Java i serwera podstawowego) | 40 MB |
| Serwer pełny (należy dodać wielkości dla pakietu SDK klienta, klienta Java i serwera podstawowego) | 8 MB |
| IBM DB2 | 763 MB |
| IBM Global Security Kit | 11 MB |

## Wymagania dotyczące miejsca na dysku w systemie AIX

**Uwaga:** Jeśli zostaną wybrane do zainstalowania funkcje pełnego serwera i serwera proxy, należy dodać wielkość pakietów Client SDK, IBM Java Development Kit i Java Client.

*Tabela 2. Wymagania dotyczące miejsca na dysku dla funkcji produktu IBM Security Directory Server i innego wymaganego oprogramowania w systemie AIX*

| **Funkcja do zainstalowania** | **Miejsce na dysku wymagane do instalacji (w MB)** |
|---|---|
| Pakiet Software Development Kit klienta | 8 MB |
| IBM Java Development Kit | 200 MB |
| Klient Java | 91 MB |
| Wdrożony program Web Administration Tool (zawiera wbudowaną wersję WebSphere Application Server i program Web Administration Tool wdrożony we wbudowanej wersji WebSphere Application Server) | 443 MB |
| Wdrożenie narzędzia Web Administration Tool w istniejącym wbudowanym serwerze WebSphere Application Server lub serwerze WebSphere Application Server | 500 MB |
| SSL dla narzędzia Web Administration | 51 MB |
| Serwer podstawowy | 39 MB |
| Serwer proxy (należy dodać wielkości dla pakietu SDK klienta, klienta Java i serwera podstawowego) | 4 MB |
| Serwer pełny (należy dodać wielkości dla pakietu SDK klienta, klienta Java i serwera podstawowego) | 12 MB |
| IBM DB2 | 1250 MB |
| IBM Global Security Kit | 16 MB |

## Wymagania dotyczące miejsca na dysku w systemie Linux

**Uwaga:** Jeśli zostaną wybrane do zainstalowania funkcje pełnego serwera i serwera proxy, należy dodać wielkość pakietów Client SDK, IBM Java Development Kit i Java Client.

*Tabela 3. Wymagania dotyczące miejsca na dysku dla funkcji produktu IBM Security Directory Server i innego wymaganego oprogramowania w systemie Linux*

| **Funkcja do zainstalowania** | **Miejsce na dysku wymagane do instalacji (w MB)** |
|---|---|
| Pakiet Software Development Kit klienta | 9 MB |
| IBM Java Development Kit | 200 MB |
| Klient Java | 166 MB |
| Wdrożony program Web Administration Tool (zawiera wbudowaną wersję WebSphere Application Server i program Web Administration Tool wdrożony we wbudowanej wersji WebSphere Application Server) | 443 MB |

*Tabela 3. Wymagania dotyczące miejsca na dysku dla funkcji produktu IBM Security Directory Server i innego wymaganego oprogramowania w systemie Linux (kontynuacja)*

| **Funkcja do zainstalowania** | **Miejsce na dysku wymagane do instalacji (w MB)** |
|---|---|
| Wdrożenie narzędzia Web Administration Tool w istniejącym wbudowanym serwerze WebSphere Application Server lub serwerze WebSphere Application Server | 375 MB |
| Serwer podstawowy | 32 MB |
| Serwer proxy (należy dodać wielkości dla pakietu SDK klienta, klienta Java i serwera podstawowego) | 40 MB |
| Serwer pełny (należy dodać wielkości dla pakietu SDK klienta, klienta Java i serwera podstawowego) | 8 MB |
| IBM DB2 (System x Linux) | 460 MB |
| IBM DB2 (System zLinux) | 670 MB |
| IBM DB2 (System i i System p Linux) | 520 MB |
| IBM DB2 (AMD64/EM64T Linux) | 1300 MB |
| IBM Global Security Kit | 40 MB |

**Uwaga:** (dotyczy programu instalacyjnego wykorzystującego program Installation Manager) W katalogu z zasobami współużytkowanym wymagane jest 200 MB miejsca na dysku. W katalogu instalacyjnym produktu IBM Security Directory Server wymagane jest dodatkowe 200 MB miejsca na dysku.

Wymagania dotyczące miejsca na dysku dla systemowego katalogu temp: jeśli wybrano zainstalowanie bazy danych DB2, wymagane jest 2048 MB + 500 MB wolnego miejsca w katalogu temp. Jeśli baza danych DB2 nie jest instalowana, w katalogu temp wymagane jest 500 MB wolnego miejsca.

## Wymagania dotyczące miejsca na dysku w systemie Solaris

**Uwaga:** Jeśli zostaną wybrane do zainstalowania funkcje serwera i serwera proxy, należy dodać wielkość pakietów klienta C, IBM Java Development Kit i klienta Java.

*Tabela 4. Wymagania dotyczące miejsca na dysku dla funkcji produktu IBM Security Directory Server i innego wymaganego oprogramowania w systemie Solaris*

| **Funkcja do zainstalowania** | **Miejsce na dysku wymagane do instalacji (w MB)** | **Uwagi** |
|---|---|---|
| Klient C | 11 MB | |
| IBM Java Development Kit | | |
| Klient Java | 145 MB | |
| Serwer | 47 MB | Dodaj wielkość pakietów klienta C i klienta Java |
| Serwer proxy | 40 MB | Dodaj wielkość pakietów klienta C i klienta Java |

*Tabela 4. Wymagania dotyczące miejsca na dysku dla funkcji produktu IBM Security Directory Server i innego wymaganego oprogramowania w systemie Solaris (kontynuacja)*

| Funkcja do zainstalowania | Miejsce na dysku wymagane do instalacji (w MB) | Uwagi |
|---|---|---|
| Web Administration Tool | 470 MB | Zawiera wbudowany serwer aplikacji WebSphere Application Server, oraz narzędzie Web Administration Tool wdrożone we wbudowanym serwerze WebSphere Application Server |
| IBM DB2 | 1155 MB | |
| IBM Global Security Kit | 34 MB | |

### Wymagania dotyczące miejsca na dysku w systemie HP-UX

*Tabela 5. Wymagania dotyczące miejsca na dysku dla funkcji produktu IBM Security Directory Server i innego wymaganego oprogramowania w systemie HP-UX*

| Funkcja do zainstalowania | Miejsce na dysku wymagane do instalacji (w MB) |
|---|---|
| Klient C | 26 MB |
| IBM Java Development Kit | |
| Klient Java | 172 MB |
| IBM Global Security Kit | 41 MB |

## Przygotowanie nośnika instalacyjnego

Pakiet produktu IBM Security Directory Server zawiera produkt IBM Security Directory Server, oprogramowanie wspólne wymaganie oraz program instalacyjny. Nośnik instalacyjny można skopiować z instalacyjnych dysków DVD lub z serwisu Passport Advantage.

Produkt IBM Security Directory Server dostępny jest w postaci pliku .zip, .tar i .iso. Plik .iso zawiera wiele plików odpowiadających plikom .zip lub .tar.

*Tabela 6. Produkt IBM Security Directory Server jest dostępny w następujących formatach w zależności od systemu operacyjnego*

| AIX, Linux, Solaris i Windows | AIX, Linux, Solaris i HP-UX | Windows |
|---|---|---|
| Obraz ISO (plik .iso) | Pliki archiwów taśmowych (pliki .tar) | Pliki skompresowane (pliki .zip) |

Aby użyć dysku DVD jako nośnika instalacyjnego, należy wykonać jedną z następujących czynności:

- Utwórz obraz dysku DVD z obrazu produktu IBM Security Directory Server dla danego systemu operacyjnego.
- Zapisz obraz produktu IBM Security Directory Server na dysku twardym komputera i podłącz go.

Podczas pobierania plików archiwów produktu należy spełnić następujące wymagania:

1. Pobierz wszystkie wymagane pliki archiwów do tego samego katalogu. Nie należy pobierać plików do katalogu, którego ścieżka zawiera spacje.

2. Zdekompresuj wszystkie pliki w tym samym katalogu (ścieżka tego katalogu nie może zawierać spacji). Ścieżka katalogu, w którym znajduje się program instalacyjny, nie może zawierać spacji.

Aby pobrać produkt IBM Security Directory Server z serwisu Passport Advantage, patrz sekcja “Pobieranie oprogramowania z serwisu Passport Advantage”.

Po przygotowaniu nośnika instalacyjnego należy spełnić wymagania programowe dla systemu operacyjnego. Patrz sekcja “Wymagania wstępne dotyczące instalacji” na stronie 15.

# Pobieranie oprogramowania z serwisu Passport Advantage

W celu zainstalowania produktu IBM Security Directory Server należy pobrać oprogramowanie z programu IBM Passport Advantage.

## Zanim rozpoczniesz

Należy zarejestrować się, aby uzyskać numer konta klienta i hasło dostępu do serwisu Passport Advantage IBM.

## Procedura

1. Przejdź do serwisu WWW IBM Passport Advantage pod adresem http://www.ibm.com/software/howtobuy/passportadvantage/pao_customers.htm.
2. Kliknij przycisk **Customer sign in** (Logowanie klienta).
3. W polu **IBM ID** (Identyfikator IBM) wpisz swój identyfikator IBM.
4. W polu **Password** (Hasło) wprowadź hasło.
5. Kliknij przycisk **Sign in** (Zaloguj się).
6. Postępuj zgodnie z instrukcjami, aby pobrać oprogramowanie IBM Security Directory Server.

# Struktura katalogów w pobranych plikach

Po pobraniu plików instalacyjnych produktu IBM Security Directory Server należy sprawdzić strukturę katalogów.

## Struktura katalogów dla pakietów systemu Windows

Nazwy plików pakietów produktu Security Directory Server 6.3.1 dla systemu Windows:

Obraz DVD: sds631-win.iso
Pliki .zip:
– sds631-win-base.zip (klient i serwer Security Directory Server 6.3.1)
– sds631-win-db2.zip (DB2 9.7)
– sds631-win-ewas.zip (wbudowana wersja serwera WebSphere Application Server 7.0.0.29)
– sds631-win-gskit.zip (GSKit 8.0)
– sds631-win-jdk.zip (IBM Java Development Kit)
– sds631-win-IM.zip (IBM Installation Manager)

Po utworzeniu dysku DVD lub rozpakowaniu plików .zip powstaje podana poniżej struktura katalogów:

\sdsV6.3.1 (katalog najwyższego poziomu dla rozpakowanych plików)
– ibm_gskit\ (GSKit)
– license\ (licencje serwera Security Directory Server i innych produktów)

– quickstart\ (podręczniki Szybki start w języku angielskim i innych językach)
– entitlement\ (pliki upoważnień dla serwera proxy)
– entitlement.txt
– tools\ (narzędzia, między innymi migbkup)
– migbkup.bat
– ibm_db2_32bit\ (DB2)
– ibm_db2_64bit\ (DB2)
– ibm_ewas_32bit\ (wbudowana wersja serwera WebSphere Application Server)
– ibm_ewas_64bit\ (wbudowana wersja serwera WebSphere Application Server)
– ibm_im_32bit\ (IBM Installation Manager)
– ibm_im_64bit\ (IBM Installation Manager)
– ibm_jdk\ (IBM Java Development Kit)
– ibm_sds\ (pliki instalatora)
– atoc
– files
– native
– Offerings
– plugins
– ShareableEntities
– build.properties
– repository.config
– repository.xml
– launchpad\
– SilentInstallScripts\ (pliki odpowiedzi używane w instalacji cichej)
– autorun.inf
– imLauncherWindows.bat
– launchpad.exe
– launchpad.ini
– launchpad64.exe
– launchpad64.ini
– sds_install.xml
– write_sds_path.bat

## Pakiet tylko klienta dla systemu Windows

Plik .zip:
– sds631-win-client.zip (klient Security Directory Server 6.3.1)

Po rozpakowaniu pliku .zip powstaje podana poniżej struktura katalogów:

\sdsV6.3.1 (katalog najwyższego poziomu dla rozpakowanych plików)
– ibm_gskit\ (GSKit 8)
– jdk\ (IBM Java Development Kit)
– ibm_im_32bit (IBM Installation Manager)
– ibm_im_64bit (IBM Installation Manager)
– ibm_sds\ (pliki instalatora)
– launchpad\
– SilentInstallScripts\
– autorun.inf
– license\ (licencje serwera Security Directory Server i innych produktów)
– quickstart\ (podręczniki Szybki start w języku angielskim i innych językach)
– ibm_im_32bit\ (IBM Installation Manager)
– ibm_im_64bit\ (IBM Installation Manager)
– imLauncherWindows.bat
– launchpad.exe
– launchpad.ini

– launchpad64.exe
– launchpad64.ini
– sds_install.xml
– write_sds_path.bat

## Struktura katalogów dla pakietów serwera AIX

Nazwy plików pakietów produktu Security Directory Server 6.3.1 dla systemu AIX:

Obraz DVD: sds631-aix-ppc64.iso
Pliki .tar:
– tds63-aix-ppc64-base.tar (klient i serwer Security Directory Server 6.3.1)
– sds631-aix-ppc64-db2.tar (DB2 9.7)
– sds631-aix-ppc64-ewas.tar (wbudowana wersja serwera WebSphere Application Server 7.0.0.29)
– sds631-aix-ppc64-gskit.tar (GSKit 8.0)
– sds631-aix-ppc64-jdk.tar (IBM Java Development Kit)
– sds631-aix-ppc64-IM.tar (IBM Installation Manager)

Po utworzeniu dysku DVD lub rozpakowaniu plików .tar powstaje podana poniżej struktura katalogów:

/sdsV6.3.1 (katalog najwyższego poziomu dla rozpakowanych plików)
– license/ (licencje serwera Security Directory Server i innych produktów)
– quickstart/ (podręczniki Szybki start w języku angielskim i innych językach)
– ibm_im (IBM Installation Manager)
– ibm_db2/ (DB2)
– ibm_ewas/ (wbudowana wersja serwera WebSphere Application Server)
– ibm_gskit/ (GSKit 8)
– ibm_jdk/ (IBM Java Development Kit)
– ibm_sds/ (pliki instalatora)
– atoc/
– files/
– native/
– Offerings/
– plugins/
– ShareableEntities
– build.properties
– repository.config
– repository.xml

– tools/ (narzędzia, między innymi migbkup)
– launchpad/
– SilentInstallScripts/
– launchpad.sh
– sds_install.xml
– write_sds_path.sh
– entitlement/ (pliki upoważnień dla serwera proxy)
– native / (pakiety rodzime)

## Pakiet tylko klienta dla systemu AIX

Plik .zip:
– sds631-aix-ppc64-client.tar (klient Security Directory Server 6.3.1)

Po rozpakowaniu pliku .zip powstaje podana poniżej struktura katalogów:

\sdsV6.3.1 (katalog najwyższego poziomu dla rozpakowanych plików)
– ibm_gskit\ (GSKit 8)
– ibm_jdk\ (IBM Java Development Kit)
– ibm_im\ (IBM Installation Manager)
– ibm_sds\ (pliki instalatora)
– launchpad\
– SilentInstallScripts\
– autorun.inf
– license\ (licencje serwera Security Directory Server i innych produktów)
– quickstart\ (podręczniki Szybki start w języku angielskim i innych językach)
– ibm_im\ (IBM Installation Manager)
– imLauncherWindows.bat
– launchpad.exe
– launchpad.ini
– sds_install.xml
– write_sds_path.bat

## Struktura katalogów dla pakietów serwera Linux x86_64

Nazwy plików pakietów serwera Security Directory Server 6.3.1 dla systemu Linux x86_64:

Obraz DVD: sds631-linux-x86-64.iso
Pliki .tar:
– sds631-linux-x86-64-base.tar (klient i serwer IBM Security Directory Server 6.3.1)
– sds631-linux-x86-64-IM.tar (IBM Installation Manager)
– sds631-linux-x86-64-gskit.tar (GSKit 8)
– sds631-linux-x86-64-db2.tar (DB2 9.7)
– sds631-linux-x86-64-ewas.tar (wbudowana wersja serwera WebSphere Application Server 7.0.0.29)
– sds631-linux-x86-64-jdk.tar (IBM Java Development Kit)

Po utworzeniu dysku DVD lub rozpakowaniu plików .tar powstaje podana poniżej struktura katalogów:

/sdsV6.3.1 (katalog najwyższego poziomu dla rozpakowanych plików)
– license/ (licencje serwera Security Directory Server i innych produktów)
– quickstart/ (podręczniki Szybki start w języku angielskim i innych językach)
– ibm_im (IBM Installation Manager)
– ibm_db2/ (DB2)
– ibm_ewas/ (wbudowana wersja serwera WebSphere Application Server)
– ibm_gskit/ (GSKit 8)
– ibm_jdk/ (IBM Java Development Kit)
– ibm_sds/ (pliki instalatora)
– atoc/
– files/
– native/
– Offerings/
– plugins/
– ShareableEntities
– build.properties
– repository.config
– repository.xml

– tools/ (narzędzia, między innymi migbkup)
– launchpad/
– SilentInstallScripts/

– launchpad.sh
– sds_install.xml
– write_sds_path.sh
– entitlement/ (pliki upoważnień dla serwera proxy)
– native / (pakiet rodzimy)

## Pakiet tylko klienta dla systemu Linux x86_64

Plik .zip:
– sds631-linux-x86-64-client.tar (klient Security Directory Server 6.3.1)

Po rozpakowaniu pliku .zip powstaje podana poniżej struktura katalogów:

\sdsV6.3.1 (katalog najwyższego poziomu dla rozpakowanych plików)
– ibm_jdk\ (IBM Java Development Kit)
– ibm_im (IBM Installation Manager)
– ibm_sds\ (pliki instalatora)
– launchpad\
– SilentInstallScripts\
– autorun.inf
– license\ (licencje serwera Security Directory Server i innych produktów)
– quickstart\ (podręczniki Szybki start w języku angielskim i innych językach)
– ibm_im\ (IBM Installation Manager)
– imLauncherWindows.bat
– launchpad.exe
– launchpad.ini
– sds_install.xml
– write_sds_path.bat

## Struktura katalogów dla pakietów serwera Linux x86

Nazwy plików pakietów serwera Security Directory Server 6.3.1 dla systemu Linux x86:

Obraz DVD: sds631-linux-x86.iso
Pliki .tar:
– sds631-linux-x86-base.tar (klient i serwer IBM Security Directory Server 6.3.1)
– sds631-linux-x86-gskit.tar (GSKit 8)
– sds631-linux-x86-db2.tar (DB2 9.7)
– sds631-linux-x86-ewas.tar (wbudowana wersja serwera WebSphere Application Server 7.0.0.29)
– sds631-linux-x86-jdk.tar (IBM Java Development Kit)

Po utworzeniu dysku DVD lub rozpakowaniu plików .tar powstaje podana poniżej struktura katalogów:

/sdsV6.3.1 (katalog najwyższego poziomu dla rozpakowanych plików)
– appsrv/ (wbudowana wersja serwera WebSphere Application Server)
– db2 (DB2)
– gskit/ (GSKit 8)
– jdk/ (IBM Java Development Kit)
– ids_detectGskitVersion
– idsinstall_i
– idsNativeInstall.sh
– images/ (obrazy rodzime)
– license (licencje serwera Security Directory Server i innych produktów)
– responseFile.txt (plik odpowiedzi)

## Pakiet tylko klienta dla systemu Linux x86

Plik .zip:
– sds631-linux-x86-client.tar (klient Security Directory Server 6.3.1)

Po rozpakowaniu pliku .zip powstaje podana poniżej struktura katalogów:

\sdsV6.3.1 (katalog najwyższego poziomu dla rozpakowanych plików)
– gskit/ (GSKit 8)
– image/
– license/ (licencje serwera Security Directory Server i innych produktów)
– jdk (IBM Java Development Kit)

## Struktura katalogów dla pakietów serwera Linux ppc

Nazwy plików pakietów serwera Security Directory Server 6.3.1 dla systemu Linux ppc:

Obraz DVD: sds631-linux-ppc64.iso
Pliki .tar:
– sds631-linux-ppc64-base.tar (klient i serwer IBM Security Directory Server 6.3.1)
– sds631-linux-ppc64-gskit.tar (GSKit 8)
– sds631-linux-ppc64-db2.tar (DB2 9.7)
– sds631-linux-ppc64-ewas.tar (wbudowana wersja serwera WebSphere Application Server 7.0.0.29)
– sds631-linux-ppc64-jdk.tar (IBM Java Development Kit)

Po utworzeniu dysku DVD lub rozpakowaniu plików .tar powstaje podana poniżej struktura katalogów:

/sdsV6.3.1 (katalog najwyższego poziomu dla rozpakowanych plików)
– appsrv/ (wbudowana wersja serwera WebSphere Application Server)
– db2 (DB2)
– gskit/ (GSKit 8)
– jdk/ (IBM Java Development Kit)
– ids_detectGskitVersion
– idsinstall_i
– idsNativeInstall.sh
– images/ (obrazy rodzime)
– license (licencje serwera Security Directory Server i innych produktów)
– responseFile.txt (plik odpowiedzi)

## Pakiet tylko klienta dla systemu Linux ppc

Plik .zip:
– sds631-linux-ppc64-client.tar (klient Security Directory Server 6.3.1)

Po rozpakowaniu pliku .zip powstaje podana poniżej struktura katalogów:

\sdsV6.3.1 (katalog najwyższego poziomu dla rozpakowanych plików)
– gskit/ (GSKit 8)
– image/
– license/ (licencje serwera Security Directory Server i innych produktów)
– jdk (IBM Java Development Kit)

## Struktura katalogów dla pakietów serwera Linux s390

Nazwy plików pakietów serwera Security Directory Server 6.3.1 dla systemu Linux s390:

Obraz DVD: sds631-linux-s390x.iso
Pliki .tar:
– sds631-linux-s390x-base.tar (klient i serwer IBM Security Directory Server 6.3.1)
– sds631-linux-s390x-gskit.tar (GSKit 8)
– sds631-linux-s390x-db2.tar (DB2 9.7)
– sds631-linux-s390x-ewas.tar (wbudowana wersja serwera WebSphere Application Server 7.0.0.29)
– sds631-linux-s390x-jdk.tar (IBM Java Development Kit)

Po utworzeniu dysku DVD lub rozpakowaniu plików .tar powstaje podana poniżej struktura katalogów:

/sdsV6.3.1 (katalog najwyższego poziomu dla rozpakowanych plików)
– appsrv/ (wbudowana wersja serwera WebSphere Application Server)
– db2 (DB2)
– gskit/ (GSKit 8)
– jdk/ (IBM Java Development Kit)
– ids_detectGskitVersion
– idsinstall_i
– idsNativeInstall.sh
– images/ (obrazy rodzime)
– license (licencje serwera Security Directory Server i innych produktów)
– responseFile.txt (plik odpowiedzi)

## Pakiet tylko klienta dla systemu Linux s390

Plik .zip:
– sds631-linux-s390x-client.tar (klient Security Directory Server 6.3.1)

Po rozpakowaniu pliku .zip powstaje podana poniżej struktura katalogów:

\sdsV6.3.1 (katalog najwyższego poziomu dla rozpakowanych plików)
– gskit/ (GSKit 8)
– image/
– license/ (licencje serwera Security Directory Server i innych produktów)
– jdk (IBM Java Development Kit)

## Struktura katalogów dla pakietów serwera Solaris x86_64

Nazwy plików pakietów serwera Security Directory Server 6.3.1 dla systemu Solaris x86_64:

Obraz DVD: sds631-solaris-x86-64.iso
Pliki .tar:
– sds631-solaris-x86-64-base.tar (klient i serwer IBM Security Directory Server 6.3.1)
– sds631-solaris-x86-64-gskit.tar (GSKit 8)
– sds631-solaris-x86-64-db2.tar(DB2 9.7)
– sds631-solaris-x86-64-ewas.tar (wbudowana wersja serwera WebSphere Application Server 7.0.0.29)
– sds631-solaris-x86-64-jdk.tar (IBM Java Development Kit)

Po utworzeniu dysku DVD lub rozpakowaniu plików .tar powstaje podana poniżej struktura katalogów:

/sdsV6.3.1 (katalog najwyższego poziomu dla rozpakowanych plików)
– appsrv/ (wbudowana wersja serwera WebSphere Application Server)
– db2 (DB2)
– gskit/ (GSKit 8)
– jdk/ (IBM Java Development Kit)
– ids_detectGskitVersion
– idsinstall_i
– idsNativeInstall.sh
– images/ (obrazy rodzime)
– license (licencje serwera Security Directory Server i innych produktów)
– responseFile.txt (plik odpowiedzi)

## Pakiet tylko klienta dla systemu Solaris x86_64

Plik .zip:
– sds631-solaris-x86-64-client.tar (klient Security Directory Server 6.3.1)

Po rozpakowaniu pliku .zip powstaje podana poniżej struktura katalogów:

\sdsV6.3.1 (katalog najwyższego poziomu dla rozpakowanych plików)
– gskit/ (GSKit 8)
– image/
– license/ (licencje serwera Security Directory Server i innych produktów)
– jdk (IBM Java Development Kit)

## Struktura katalogów dla pakietów serwera Solaris sparc

Nazwy plików pakietów serwera Security Directory Server 6.3.1 dla systemu Solaris sparc:

Obraz DVD:
Pliki .tar:
– sds631-solaris-sparc.iso
– sds631-solaris-sparc-base.tar (klient i serwer IBM Security Directory Server 6.3.1)
– sds631-solaris-sparc-gskit.tar (GSKit 8)
– sds631-solaris-sparc-db2.tar (DB2 9.7)
– sds631-solaris-sparc-ewas.tar (wbudowana wersja serwera WebSphere Application Server 7.0.0.29)
– sds631-solaris-sparc-jdk.tar (IBM Java Development Kit)

Po utworzeniu dysku DVD lub rozpakowaniu plików .tar powstaje podana poniżej struktura katalogów:

/sdsV6.3.1 (katalog najwyższego poziomu dla rozpakowanych plików)
– appsrv/ (wbudowana wersja serwera WebSphere Application Server)
– db2 (DB2)
– gskit/ (GSKit 8)
– jdk/ (IBM Java Development Kit)
– ids_detectGskitVersion
– idsinstall_i
– idsNativeInstall.sh
– images/ (obrazy rodzime)
– license (licencje serwera Security Directory Server i innych produktów)
– responseFile.txt (plik odpowiedzi)

### Pakiet tylko klienta dla systemu Solaris Sparc

Plik .zip:
– sds631-solaris-sparc-client.tar (klient Security Directory Server 6.3.1)

Po rozpakowaniu pliku .zip powstaje podana poniżej struktura katalogów:

\sdsV6.3.1 (katalog najwyższego poziomu dla rozpakowanych plików)
– gskit/ (GSKit 8)
– image/
– license/ (licencje serwera Security Directory Server i innych produktów)
– jdk (IBM Java Development Kit)

## Wymagania wstępne dotyczące instalacji

Instalacja produktu IBM Security Directory Server i jego oprogramowania wymaganego może wymagać instalacji dodatkowych komponentów w używanym systemie operacyjnym. Oprogramowanie wymagane wstępnie musi być zainstalowane przed produktem IBM Security Directory Server.

### Pakiety wymagane wstępnie w różnych systemach operacyjnych

Przed zainstalowaniem produktu IBM Security Directory Server i produktów wymaganych, należy w systemie zainstalować pakiety wymagane wstępnie.

W systemach operacyjnych AIX, Linux, Solaris i HP-UX (Itanium) wymagane jest zainstalowanie powłoki Korna. W systemie SuSE Linux Enterprise Server wymagana jest powłoka PDKSH.

Produkt IBM Security Directory Server do zainstalowania wymaga następujących pakietów w zależności od systemu operacyjnego:

**AIX** Instalowanie pakietów RPM w systemie AIX wymaga pobrania menedżera pakietów rpm dla systemu AIX, który dostępny jest pod adresem ftp://public.dhe.ibm.com/aix/freeSoftware/aixtoolbox/INSTALLP/ppc/rpm.rte.

*Tabela 7. Pakiety wymagane wstępnie w systemie operacyjnym AIX*

| Pakiety | Przyczyna | Adres pobierania |
|---|---|---|
| Przeglądarka WWW Mozilla Firefox dla systemu AIX | Do otwarcia startera w systemie AIX niezbędna jest obsługiwana przeglądarka WWW. | Więcej informacji na temat przeglądarek WWW dla systemu AIX dostępnych jest w serwisie http://www.ibm.com/systems/power/software/aix/browsers/. |
| gtk+ RPM (gtk2-2.10.6-4.aix5.2.ppc.rpm) | System Eclipse zmienił wymagania z motif na gtk w systemach UNIX. W systemie AIX do obsługi interfejsu graficznego (GUI) niezbędne jest zainstalowanie bibliotek gtk. W programie IBM Installation Manager interfejsem graficznym jest kreator. | Więcej informacji na temat instalowania bibliotek gtk zawiera nota techniczna Required gtk libraries for Installation Manager on AIX dostępna w serwisie http://www.ibm.com/support/docview.wss?uid=swg21631478. |

*Tabela 7. Pakiety wymagane wstępnie w systemie operacyjnym AIX (kontynuacja)*

| Pakiety | Przyczyna | Adres pobierania |
|---|---|---|
| GNU tar | Do dekompresowania plików archiwum dostarczanych z produktem IBM Security Directory Server w systemach AIX niezbędny jest program GNU tar. Ścieżka programu GNU tar musi poprzedzać ścieżkę systemowego programu tar. Program GNU tar jest instalowany w katalogu /opt/freeware/bin, systemowy program tar znajduje się w katalogu /usr/bin. Aby ustawić ścieżkę /opt/freeware/bin, uruchom następującą komendę: export PATH=/opt/freeware/bin:$PATH. | Aby pobrać plik programu GNU tar (tar), patrz serwis http://www.ibm.com/systems/power/software/aix/linux/toolbox/alpha.html . |
| Zestaw plików X11.adt.lib | Zestaw plików X11.adt.lib jest wymagany do zainstalowania pakietów idsldap.cltjava631 i idsldap.webadmin631 w systemach AIX. | |
| xlC.rte 8.0.0.6 i xlC.aix50.rte 8.0.0.6 lub nowsze | Komponenty środowiska wykonawczego IBM C++ dla systemu AIX wymagają pakietów xlC.rte 8.0.0.6 i xlC.aix50.rte 8.0.0.6 lub nowszych. | |
| bos.loc.iso.en_US 5.3.0.0 | IBM Security Directory Server 6.3.1 wymaga zestawu plików ustawień narodowych poziomu bazowego bos.loc.iso.en_US 5.3.0.0. | |

## Wymaganie wstępne dla klienta LDAP w systemach PowerPC LE

Aby uruchomić klienta serwera IBM Security Directory Server w systemach PowerPC LE (Little Endian), należy zainstalować program IBM Advance Toolchain 7.1.

Program IBM Advance Toolchain 7.1 należy zainstalować, jeśli planowane jest uruchamianie klienta LDAP albo utworzenie własnego klienta wykorzystującego dostarczone biblioteki.

Aby pobrać i zainstalować program IBM Advanced Toolchain 7.1 dla używanego systemu operacyjnego, patrz serwis IBM Advance Toolchain Documentation.

## Użytkownik i grupa idsldap

Jeśli do zainstalowania wybrano serwer lub serwer proxy, program instalacyjny tworzy użytkownika i grupę idsldap.

Program instalacyjny tworzy użytkownika i grupę idsldap, jeśli jeszcze nie istnieją.

**Uwaga:** W systemach AIX, Linux i Solaris program instalacyjny tworzy użytkownika idsldap, używając narzędzi systemowych, jeśli użytkownik ten jeszcze nie istnieje. Jeśli jednak istnieje katalog /home/idsldap (w systemach Linux i AIX) lub /export/home/idsldap (w systemach Solaris), utworzenie użytkownika idsldap może nie być możliwe. Dlatego należy upewnić się, że katalog osobisty użytkownika idsldap nie istnieje, jeśli użytkownik idsldap nie istnieje.

Jeśli w używanym środowisku konieczna jest większa kontrola nad użytkownikiem i grupą idsldap, można te obiekty utworzyć przed rozpoczęciem instalacji. Użytkownik i grupa idsldap musi spełniać następujące wymagania:

- Użytkownik idsldap musi należeć do grupy idsldap.
- W systemach AIX, Linux i Solaris użytkownik root musi być członkiem grupy idsldap. W systemie Windows użytkownik Administrator musi być członkiem grupy idsldap.
- Użytkownik idsldap musi mieć katalog osobisty.
- W systemach AIX, Linux i Solaris domyślną powłoką użytkownika idsldap musi być powłoka korna.
- Użytkownik idsldap może mieć hasło, ale nie jest to obowiązkowe.
- Użytkownik idsldap może być właścicielem instancji serwera katalogów.

Przed zainstalowaniem produktu IBM Security Directory Server wszystkie te wymagania muszą być spełnione. Jeśli użytkownik idsldap istnieje, ale nie spełnia wymagań, instalacja serwera proxy może się nie powieść.

**Uwaga:** Więcej informacji na temat wymagań instancji, instancji katalogu i właściciela bazy danych odnośnie identyfikatora użytkownika zawiera sekcja “Użytkownicy i grupy powiązane z instancją serwera katalogów” na stronie 121.

Podczas tworzenia instancji serwera katalogów do utworzenia użytkowników i grup można użyć programu Instance Administration Tool. Do utworzenia i poprawnego skonfigurowania użytkownika i grupy idsldap można też użyć programów narzędziowych systemu operacyjnego.

## Przykłady

Uruchom następujące systemowe programy narzędziowe do utworzenia użytkownika i grupy idsldap, hasła oraz do dodania użytkownika root do grupy idsldap.

**W systemach AIX:**

Aby utworzyć grupę idsldap, uruchom następującą komendę:

```
mkgroup idsldap
```

Aby utworzyć użytkownika idsldap jako członka grupy idsldap i ustawić powłokę Korn jako domyślną, uruchom następującą komendę:

```
mkuser pgrp=idsldap home=/home/idsldap shell=/bin/ksh idsldap
```

Aby ustawić hasło dla użytkownika idsldap, uruchom komendę:

```
passwd idsldap
```

Aby dodać użytkownika root do grupy idsldap, uruchom następującą komendę:

```
/usr/bin/chgrpmem -m + root idsldap
```

**W systemach Linux:**

Aby utworzyć grupę idsldap, uruchom następującą komendę:

```
groupadd idsldap
```

Aby utworzyć użytkownika idsldap jako członka grupy idsldap i ustawić powłokę Korn jako domyślną, uruchom następującą komendę:

```
useradd -g idsldap -d /home/idsldap -m -s /bin/ksh idsldap
```

Aby ustawić hasło dla użytkownika idsldap, uruchom komendę:

```
passwd idsldap
```

Aby dodać użytkownika root do grupy idsldap, uruchom następującą komendę:

```
usermod -G idsldap,grupy_użytkownika_root root
```

Wartości parametru *grupy_użytkownika_root* dla komputera można określić za pomocą komendy groups root.

**Systemy Solaris:**

Aby utworzyć grupę idsldap, uruchom następującą komendę:

```
groupadd idsldap
```

Aby utworzyć użytkownika idsldap jako członka grupy idsldap i ustawić powłokę Korn jako domyślną, uruchom następującą komendę:

```
useradd -g idsldap -d /export/home/idsldap -m -s /bin/ksh idsldap
```

Aby ustawić hasło dla użytkownika idsldap, uruchom komendę:

```
passwd idsldap
```

Aby dodać użytkownika root do grupy idsldap, uruchom następującą komendę:

```
usermod -G idsldap,root idsldap
```

Aby zmodyfikować identyfikator użytkownika root, tak aby użytkownik root stał się członkiem grupy idsldap, należy użyć odpowiedniego narzędzia.

Więcej informacji na temat komendy do dodawania użytkownika i grupy można znaleźć w dokumentacji systemu operacyjnego.

## Metody instalowania

Aby zainstalować produkt IBM Security Directory Server i wspólnie wymaganie oprogramowanie, należy wybrać metodę instalacji najlepiej dopasowaną do danego środowiska.

Do zainstalowania produktu IBM Security Directory Server i wspólnie wymaganego oprogramowania można zastosować następujące metody:

- Instalowanie za pomocą programu IBM Installation Manager
- Instalowanie z użyciem programów narzędziowych systemu operacyjnego

**UWAGA:**

- **Nie można stosować różnych trybów instalacji na jednym komputerze. Komponenty produktu IBM Security Directory Server należy zainstalować albo za pomocą programu IBM Installation Manager, albo za pomocą narzędzi systemu operacyjnego. Jeśli zostaną pomieszane oba typy instalacji, mogą nie zostać zainstalowane wszystkie poprawne pakiety komponentu.**
- **Należy unikać ręcznej instalacji bazy danych DB2 i wbudowanego serwera WebSphere Application Server w domyślnych ścieżkach instalacji używanych przez program IBM Installation Manager. Tego typu instalacja ręczna może spowodować niepowodzenie instalacji, modyfikacji lub deinstalacji w programie IBM Installation Manager. Więcej informacji na temat domyślnych ścieżek instalacji zawiera sekcja “Domyślne położenia instalacji” na stronie 27.**

# Rozdział 3. Instalowanie za pomocą programu IBM Installation Manager

Program IBM Installation Manager jest narzędziem, którego można użyć do zainstalowania i konserwowania produktu IBM Security Directory Server i wspólnie wymaganego oprogramowania.

## Przegląd programu IBM Installation Manager

Program IBM Installation Manager jest kreatorem, który przeprowadza użytkownika przez proces instalowania, modyfikowania, aktualizowania, wycofywania i deinstalowania produktów IBM. Do instalacji mogą być wykorzystywane lokalne lub zdalne repozytoria.

Program IBM Installation Manager również jest pomocny podczas zarządzania aplikacjami lub pakietami IBM, które zostały zainstalowane na komputerze z jego użyciem.

- Pamięta, jakie programy zostały zainstalowane
- Określa i wyświetla pakiety dostępne do zainstalowania
- Sprawdza wymagania wstępne i wzajemne zależności

Program IBM Installation Manager zawiera sześć kreatorów ułatwiających obsługę pakietów:

- Kreator **instalowania** przeprowadza użytkownika przez proces instalowania. Jednocześnie można zainstalować jeden lub więcej pakietów. Użytkownik może zaakceptować ustawienia domyślne albo zmodyfikować je w celu utworzenia własnej instalacji, jeśli jest to możliwe. Przed instalacją przedstawiane jest pełne podsumowanie opcji wybranych w kreatorze.
- Kreator **aktualizowania** wyszukuje dostępne aktualizacje pakietów zainstalowanych w systemie. Kreator ten udostępnia szczegóły na temat zawartości aktualizacji. Można wybrać, czy aktualizacja ma zostać zastosowana.
- Kreator **modyfikowania** pomaga w modyfikowaniu określonych elementów instalowanego pakietu. Podczas pierwszej instalacji pakietu użytkownik wybiera komponenty do zainstalowania. Jeśli użytkownik stwierdzi później, że potrzebne są inne komponenty, może użyć kreatora modyfikowania w celu ich dodania do pakietu. Za pomocą tego kreatora można również usuwać określone komponenty.
- Kreator **zarządzania licencjami** pomaga zainstalować licencje dla pakietów. Można go użyć do zmiany licencji próbnej na licencję pełną, skonfigurowania serwera do używania licencji sieciowych, a także do wybrania typu licencji dla poszczególnych pakietów.
- Kreator **wycofywania zmian** pozwala przywrócić poprzednią wersję pakietu.
- Kreator **deinstalacji** usuwa pakiet z komputera. Użytkownik może usunąć więcej niż jeden pakiet jednocześnie.

## Obsługiwane systemy operacyjne

Za pomocą programu IBM Installation Manager można zainstalować produkt IBM Security Directory Server w systemie AIX (ppc64), Linux (architektura AMD64/EM64T) i Microsoft Windows.

W kolejnych sekcjach są wymienione systemy operacyjne, w których można zainstalować produkt IBM Security Directory Server za pomocą programu IBM Installation Manager.

Aby zainstalować produkt IBM Security Directory Server w systemie operacyjnym, który nie jest wymieniony na liście:

1. Sprawdź, czy wersja systemu operacyjnego jest obsługiwana przez produkt IBM Security Directory Server. Lista wszystkich obsługiwanych systemów operacyjnych znajduje się w publikacji *IBM Security Directory Server - Przegląd produktu*.
2. Jeśli system jest obsługiwany, zainstaluj produkt IBM Security Directory Server za pomocą programów narzędziowych wiersza komend systemu operacyjnego.

**AIX (ppc64)**

- AIX wersja 6.1
- AIX wersja 7.1

**Linux (AMD64/EM64T)**

- Red Hat Enterprise Linux 5, Advanced Platform
- Red Hat Enterprise Linux 6
- SUSE Linux Enterprise Server 10
- SUSE Linux Enterprise Server 11

**Microsoft Windows (x64)**

- Microsoft Windows Server 2008 R2, Enterprise Edition
- Microsoft Windows Server 2008 R2, Standard Edition
- Microsoft Windows Server 2008, Enterprise Edition
- Microsoft Windows Server 2008, Standard Edition
- Microsoft Windows Server 2012, Standard Edition

## Typy pakietów instalacyjnych w produkcie IBM Security Directory Server

Aby wybrać poprawny pakiet instalacyjny produktu IBM Security Directory Server, należy znać dostępne typy pakietów instalacyjnych.

Dla produktu IBM Security Directory Server dostępne są następujące pakiety instalacyjne do użycia przez program IBM Installation Manager:

*Tabela 8. Typy pakietów instalacyjnych produktu IBM Security Directory Server oraz dostępne opcje instalacji*

| Wszystkie komponenty | Komponenty w pełnym instalatorze produktu | Komponenty dostępne tylko w instalatorze klienta |
|---|---|---|
| IBM DB2 | Tak | Nie |
| IBM Global Security Kit | Tak | Tak |
| Klient C | Tak | Tak |
| IBM Java Development Kit | Tak | Tak |
| Klient Java | Tak | Tak |
| Serwer | Tak | Nie |
| Serwer proxy | Tak | Nie |
| Web Administration Tool | Tak | Nie |

**Uwaga:** W przypadku instalowania komponentu Web Administration Tool program IBM Installation Manager umożliwia zainstalowanie wbudowanej wersji serwera WebSphere Application Server.

## Wytyczne dotyczące instalacji

Przed rozpoczęciem instalowania produktu IBM Security Directory Server za pomocą programu IBM Installation Manager należy rozważyć istniejące ograniczania.

**Metoda instalowania**

Produkt IBM Security Directory Server można zainstalować za pomocą programu IBM Installation Manager lub programów narzędziowych wiersza komend systemu operacyjnego. W każdej przyszłej instalacji lub deinstalacji pakietów produktu IBM Security Directory Server, komponentów i pakietów poprawek, należy użyć tej samej metody instalacji. Na przykład, jeśli produkt IBM Security Directory Server został zainstalowany za pomocą programu IBM Installation Manager, nie należy używać programów narzędziowych wiersza komend do zainstalowania funkcji lub do odinstalowania produktu. W takim przypadku instalacja programu IBM Security Directory Server może zostać uszkodzona lub stać się bezużyteczna.

**Wersja programu IBM Installation Manager**

Program IBM Installation Manager w wersji 1.7.0 i nowszej obsługuje instalowanie produktu IBM Security Directory Server. W następujących sytuacjach na stronie Pakiety instalacyjne programu IBM Installation Manager wyświetlany jest komunikat o błędzie i instalacja nie może być kontynuowana:

- Użytkownik próbuje uruchomić instalację produktu IBM Security Directory Server z poprzednią wersją programu IBM Installation Manager.
- Poprzednia wersja programu IBM Installation Manager została wykryta podczas uruchamiania instalacji produktu IBM Security Directory Server z Startera.

**Wiele instalacji**

Nie można zainstalować wielu kopii tej samej wersji produktu IBM Security Directory Server w jednym systemie. Po ponownym wybraniu pakietu instalacyjnego dla tej samej wersji program IBM Installation Manager generuje komunikat ostrzegawczy i nie można kontynuować instalacji. W jednym systemie mogą jednak istnieć różne wersje produktu IBM Security Directory Server.

**Położenie instalacji w systemach AIX i Linux:**

Produkt IBM Security Directory Server może być zainstalowany tylko w predefiniowanym położeniu w systemach AIX i Linux. Domyślnie ścieżka jest podawana w polu **Katalog instalacyjny** w programie IBM Installation Manager. Pole to jest dostępne do edycji w programie IBM Installation Manager. Jeśli jednak ścieżka domyślna zostanie zmieniona, przycisk **Dalej** nie będzie dostępny i nie będzie można kontynuować instalacji. Należy wtedy przywrócić domyślną ścieżkę instalacji produktu IBM Security Directory Server.

To ograniczenie nie dotyczy systemów operacyjnych Microsoft Windows. Program IBM Security Directory Server można zainstalować w dowolnym miejscu w systemie operacyjnym Microsoft Windows. Nawet jeśli użytkownik wybierze położenie instalacji niestandardowej dla produktu IBM Security Directory Server, katalog idsinstinfo z plikiem idsinstances.ldif jest zawsze tworzony na partycji, która jest określona przez zmienną %SystemDrive%. Jeśli produkt IBM Security Directory Server jest instalowany na dysku E:, a system operacyjny jest na dysku C:, to:

- katalog idsinstinfo jest tworzony na dysku C: (C:\idsinstinfo) a nie w katalogu E:\Program Files\IBM\ldap.

Aby uzyskać więcej informacji na temat domyślnych lokalizacji instalacji, patrz sekcja “Domyślne położenia instalacji” na stronie 27.

# Komponenty produktu IBM Security Directory Server

Podczas instalowania produktu IBM Security Directory Server za pomocą programu IBM Installation Manager można wybrać komponenty do zainstalowania. Program IBM Installation Manager wyświetla zależności każdego wybranego komponentu.

Dostępne do zainstalowania są następujące komponenty produktu IBM Security Directory Server:

**IBM DB2**

Instalowanie produktu IBM DB2 jest opcjonalne. Jeśli jest już zainstalowana obsługiwana wersja produktu IBM DB2, nie trzeba instalować bazy danych DB2 dostarczanej wraz z pakietem produktu IBM Security Directory Server. Informacje na temat obsługiwanych wersji DB2 w różnych systemach operacyjnych zawiera publikacja *IBM Security Directory Server - przegląd produktu*.

Pełny serwer katalogów wymaga produktu IBM DB2, ponieważ dane katalogowe są zapisywane w bazie danych DB2. Produkt IBM DB2 nie jest wymagany do obsługi serwera proxy.

**IBM Global Security Kit**

Pakiet IBM Global Security Kit (GSKit) można zainstalować z innymi komponentami produktu IBM Security Directory Server. Pakiet GSKit jest opcjonalnym komponentem, który jest wymagany tylko wtedy, gdy do zabezpieczania komunikacji ma być stosowany protokół SSL (Secure Sockets Layer) albo TLS (Transport Layer Security). Pakiet GSKit musi być zainstalowany na serwerze jak i na kliencie, aby połączenia były chronione.

**Klient C**

Klient C produktu może być zainstalowany samodzielnie albo wraz z innymi komponentami produktu IBM Security Directory Server. Klient C nie zależy od innych komponentów. Komponenty serwera i serwera proxy zależą jednak od klienta C. Podczas instalowania serwera lub serwera proxy opcja instalowania klienta C jest automatycznie zaznaczana.

Klient C jest pakietem SDK (Software Development Kit) udostępniającym narzędzia niezbędne do tworzenia aplikacji w języku C obsługujących protokół LDAP. Pakiet klienta C zawiera następujące pliki i aplikacje:

- biblioteki klienckie zawierające zestaw interfejsów API języka C,
- pliki nagłówkowe w języku C służące do budowania i kompilowania aplikacji wykorzystujących protokół LDAP,
- programy narzędziowe serwera i klienta,
- kody źródłowe przykładowych programów.

**IBM Java Development Kit**

Pakiet IBM Java Development Kit może być zainstalowany samodzielnie albo wraz z innymi komponentami produktu IBM Security Directory Server. Zaznaczenie opcji instalowania pakietu IBM Java Development Kit powoduje, że program IBM Installation Manager wyodrębnia skompresowany plik do podkatalogu java w katalogu instalacyjnym produktu IBM Security Directory Server. Pakiet IBM Java Development Kit zawiera komponent IBM Java SDK oraz środowisko Java 1.6 SR 14. Pakiet IBM Java Development Kit jest wymagany do kompilowania przykładowych programów w języku Java oraz do uruchamiania programów napisanych w języku Java, takich jak Instance Administration Tool (**idsxinst**) i Configuration Tool (**idsxcfg**).

**Klient Java**

Klient Java produktu może być zainstalowany samodzielnie albo wraz z innymi

komponentami produktu IBM Security Directory Server. Klient Java nie zależy od innych komponentów. Komponenty serwera i serwera proxy zależą jednak od klienta Java. Podczas instalowania serwera lub serwera proxy opcja instalowania klienta Java jest automatycznie zaznaczana.

Klient Java zawiera bibliotekę narzędziową IBM Security Directory Server JNDI oraz programy narzędziowe klienta Java.

**Serwer** Serwer może być instalowany wraz z innymi komponentami produktu IBM Security Directory Server. Komponent serwera zależy od klienta C i klienta Java. Po wybraniu opcji zainstalowania serwera automatycznie zaznaczane są do zainstalowania komponenty klienta C i Java.

Komponent serwera jest wymagany do utworzenia pełnego serwera katalogów lub serwera LDAP. Pełny serwer katalogów należy skonfigurować do pracy z instancją bazy danych. Przetwarza on żądania klientów wymagających dostępu do pozycji zapisanych w bazie danych. Pełny serwer katalogów wymaga bazy danych DB2.

**Serwer proxy**

Serwer proxy może być instalowany wraz z innymi komponentami produktu IBM Security Directory Server. Komponent serwera proxy zależy od klienta C i klienta Java. Po wybraniu opcji zainstalowania serwera proxy automatycznie zaznaczane są do zainstalowania komponenty klienta C i Java.

Serwer proxy jest serwerem LDAP działającym jako serwer frontowy katalogu. Uwierzytelnia on klienta w katalogu i przekierowuje żądania do rzeczywistych serwerów katalogów. Serwer proxy można też wykorzystywać jako serwer frontowy klastra lub katalogu rozproszonego, dzięki czemu możliwa jest realizacja przełączania awaryjnego oraz równoważenie obciążenia.

**Web Administration Tool**

Komponent Web Administration Tool można zainstalować samodzielnie albo wraz z innymi komponentami produktu IBM Security Directory Server. Komponent Web Administration Tool jest opcjonalnym komponentem, który jest wymagany, jeśli konieczne jest zdalne zarządzanie serwerem katalogów. Komponent Web Administration Tool musi być wdrożony w obsługiwanej wersji wbudowanego serwera WebSphere Application Server lub serwera WebSphere Application Server.

Podczas instalowania narzędzia Web Administration Tool, na komputer są również kopiowane pliki języka DSML (Directory Services Markup Language). Więcej informacji na temat języka DSML zawiera sekcja Dodatek A, “Język DSML”, na stronie 243.

Komponent Web Administration Tool może być używany jako konsola do zarządzania serwerami katalogów następujących typów:

- IBM Security Directory Server 6.3.1
- IBM Security Directory Server 6.3
- IBM Security Directory Server 6.2
- IBM Security Directory Server 6.1
- IBM Security Directory Server 6.0
- i5/OS V5 R4
- z/OS V1 R6 Integrated Security Services
- z/OS V1 R8 Integrated Security Services
- z/OS V1 R8 IBM Tivoli Directory Server
- z/OS V1 R9 IBM Tivoli Directory Server
- z/OS V1 R10 IBM Tivoli Directory Server

**Ważne:** W systemie z/OS obsługiwane jest zarządzanie danymi katalogu, bez zarządzania serwerem.

**Wbudowany serwer WebSphere Application Server**
Można zainstalować wbudowaną wersję serwera WebSphere Application Server, jeśli instalowany jest komponent Web Administration Tool. Wbudowany serwer WebSphere Application Server jest wymagany tylko wtedy, gdy ma być zainstalowany i wdrożony komponent Web Administration Tool. Jeśli w systemie jest już zainstalowana obsługiwana wersja serwera WebSphere Application Server, zainstalowanie wbudowanego serwera WebSphere Application Server nie jest konieczne. Komponent Web Administration Tool można wdrożyć w istniejącym serwerze WebSphere Application Server lub wbudowanym serwerze WebSphere Application Server.

## Modyfikowanie instalacji produktu IBM Security Directory Server

Istnieje możliwość dostosowania instalacji produktu IBM Security Directory Server do swoich potrzeb.

W instalacji produktu IBM Security Directory Server można wyróżnić następujące kategorie:

- Pełny produkt
- Pełny serwer katalogów
- Serwer proxy
- Klient
- Zdalne zarządzanie serwerem za pomocą Web Administration Tool

*Tabela 9. Instalowanie komponentów produktu IBM Security Directory Server w zależności od planowanego sposobu jego używania*

| Wszystkie komponenty | Pełny serwer katalogów | Serwer proxy | Klient | Zdalne zarządzanie serwerem za pomocą Web Administration Tool |
|---|---|---|---|---|
| IBM DB2 | Tak | Nie | Nie | Nie |
| IBM Global Security Kit | Tak | Tak | Tak | Nie |
| Klient C | Tak | Tak | Tak | Nie |
| IBM Java Development Kit | Tak | Tak | Tak | Nie |
| Klient Java | Tak | Tak | Tak | Nie |
| Serwer | Tak | Nie | Nie | Nie |
| Serwer proxy | Nie | Tak | Nie | Nie |
| Web Administration Tool | Opcjonalne | Opcjonalne | Nie | Tak |

**Uwaga:** W przypadku instalowania komponentu Web Administration Tool program IBM Installation Manager umożliwia zainstalowanie wbudowanej wersji serwera WebSphere Application Server.

Instalując pełny serwer katalogów lub serwer proxy, opcjonalnie można wybrać do zainstalowania wbudowaną wersję serwera WebSphere Application Server i program narzędziowy Web Administration Tool.

## Domyślne położenia instalacji

Po uruchomieniu programu IBM Installation Manager w celu instalacji, produkt IBM Security Directory Server i jego wymagane oprogramowanie jest instalowane w predefiniowanej lokalizacji instalacji.

*Tabela 10. Domyślne położenie instalacji produktu IBM Security Directory Server, IBM DB2, wbudowanego serwera WebSphere Application Server i IBM Java Development Kit.*

| System | IBM Security Directory Server | IBM DB2 | Wbudowana wersja serwera WebSphere Application Server | IBM Java Development Kit |
|---|---|---|---|---|
| Linux | /opt/ibm/ldap/V6.3.1 | /opt/ibm/sdsV6.3.1db2 | /opt/ibm/ldap/V6.3.1/appsrv | /opt/ibm/ldap/V6.3.1/java |
| AIX | /opt/IBM/ldap/V6.3.1 | /opt/IBM/sdsV6.3.1db2 | /opt/IBM/ldap/V6.3.1/appsrv | /opt/IBM/ldap/V6.3.1/java |
| Microsoft Windows | C:\Program Files\IBM\ldap\V6.3.1 | C:\Program Files\IBM\sdsV6.3.1db2 | C:\Program Files\IBM\ldap\V6.3.1\appsrv | C:\Program Files\IBM\ldap\V6.3.1\java |

Produkt IBM Security Directory Server może być zainstalowany tylko w predefiniowanym położeniu w systemach AIX i Linux. Domyślnie ścieżka jest podawana w polu **Katalog instalacyjny** w programie IBM Installation Manager. Pole to jest dostępne do edycji w programie IBM Installation Manager. Jeśli jednak ścieżka domyślna zostanie zmieniona, przycisk **Dalej** nie będzie dostępny i nie będzie można kontynuować instalacji. Należy wtedy przywrócić domyślną ścieżkę instalacji produktu IBM Security Directory Server.

To ograniczenie nie dotyczy systemów operacyjnych Microsoft Windows. Program IBM Security Directory Server można zainstalować w dowolnym miejscu w systemie operacyjnym Microsoft Windows. Nawet jeśli użytkownik wybierze położenie instalacji niestandardowej dla produktu IBM Security Directory Server, katalog idsinstinfo z plikiem idsinstances.ldif jest zawsze tworzony na partycji, która jest określona przez zmienną %SystemDrive%. Jeśli produkt IBM Security Directory Server jest instalowany na dysku E:, a system operacyjny jest na dysku C:, to:

- katalog idsinstinfo jest tworzony na dysku C: (C:\idsinstinfo) a nie w katalogu E:\Program Files\IBM\ldap.

## Repozytoria instalacji

Repozytorium instalacji jest miejscem, w którym pakiety programu IBM Security Directory Server są dostępne w celu wykonania instalacji.

Program IBM Security Directory Server można zainstalować z jednej z następujących lokalizacji:

- Dysk instalacyjny produktu
- Zdalny współużytkowany napęd lub katalog lokalny, który zawiera obraz elektronicznego pakietu instalacyjnego

Repozytorium można wykorzystać do uruchomienia instalacji na jeden z następujących sposobów:

- Uruchom Starter, aby zainstalować z:
  - dysku instalacyjnego produktu,
  - obrazu elektronicznego pakietu instalacyjnego w katalogu lokalnym lub zdalnym dysku sieciowym.

  Jeśli używany jest Starter, proces instalacji jest już skonfigurowany do używania położenia repozytorium z pakietem instalacyjnym.
- Bezpośrednio uruchom program IBM Installation Manager i ręcznie wskaż repozytorium, używając jednej z podanych metod. Na przykład:
  - Adres URL repozytorium na serwerze WWW
  - Ścieżka do zdalnego współużytkowanego dysku sieciowego, który zawiera pakiet produktu

# Uruchamianie instalacji

Można rozpocząć instalację produktu IBM Security Directory Server za pomocą startera lub za pomocą programu IBM Installation Manager z ustawionymi preferencjami dotyczącymi repozytorium.

## Uruchamianie instalacji za pomocą startera

Starter stanowi pojedyncze miejsce pozwalające na rozpoczęcie procesu instalacji.

### O tym zadaniu

Starter można wykorzystać do uruchomienia instalacji na jeden z następujących sposobów:

- Instalacja z dysku instalacyjnego produktu.
- Instalacja z lokalnego katalogu lub zdalnego współużytkowanego dysku, który zawiera obraz pakietu produktu.

Jeśli do uruchomienia instalacji używany jest starter, program IBM Installation Manager zostanie automatycznie zainstalowany, jeśli w systemie nie ma obsługiwanej wersji.

### Procedura

1. Przejdź do katalogu głównego pakietu instalacji.
   - Jeśli używany jest dysk instalacyjny produktu IBM Security Directory Server, włóż go do napędu dysków.
   - Przy instalacji z obrazu elektronicznego pakietu instalacji produktu, przejdź do katalogu, w którym znajduje się obraz.
2. Uruchom starter.

   **Uwaga:** W systemach operacyjnych Windows kliknij prawym przyciskiem myszy plik .exe startera i wybierz opcję **Uruchom jako administrator**.

| System operacyjny | Komenda do uruchomienia: |
|---|---|
| Windows (wersja 32-bitowa) | launchpad.exe |
| Windows (wersja 64-bitowa) | launchpad64.exe |
| AIX i Linux | ./launchpad.sh |

   Zostanie uruchomiony starter instalacji produktu IBM Security Directory Server i wyświetlona zostanie strona Witamy.

3. Na stronie **Witamy** wybierz język z listy **Wybierz język**, a następnie kliknij przycisk **OK**.
4. W obszarze nawigacyjnym po lewej stronie kliknij opcję **Instalacja serwera IBM Directory Server**.
5. Na stronie **Instalacja** kliknij odsyłacz **Uruchom instalator IBM Security Directory Server**. Zostanie uruchomiony program IBM Installation Manager.
6. Sprawdź, czy następujące pakiety są wybrane do instalacji:
   - IBM Installation Manager (jest on wyświetlany tylko wtedy, jeśli obsługiwana wersja nie jest jeszcze zainstalowana w systemie).
   - IBM Security Directory Server
7. Kontynuuj wykonywanie czynności instalacyjnych programu IBM Security Directory Server. Patrz sekcja “Instalowanie przy użyciu programu IBM Installation Manager” na stronie 31.
8. Po zakończeniu instalacji kliknij przycisk **Wyjdź**.

### Wyniki

Jeśli do rozpoczęcia instalacji produktu IBM Security Directory Server używany jest starter, utworzy on plik tymczasowy, sds631.temp, który zawiera nazwę ścieżki nośnika. Plik sds631.temp jest tworzony w następującej lokalizacji w systemie:

**AIX i Linux**
/tmp

**Microsoft Windows**
Domyślny katalog tymczasowy systemu ustawiony w zmiennej *TEMP*.

Nie można zainstalować wielu kopii tej samej wersji produktu IBM Security Directory Server w jednym systemie. Po ponownym wybraniu pakietu instalacyjnego dla tej samej wersji program IBM Installation Manager generuje komunikat ostrzegawczy i nie można kontynuować instalacji. W jednym systemie mogą jednak istnieć różne wersje produktu IBM Security Directory Server.

### Co dalej

Kontynuuj wykonywanie czynności instalacyjnych programu IBM Security Directory Server. Patrz sekcja “Instalowanie przy użyciu programu IBM Installation Manager” na stronie 31.

## Uruchamianie instalacji przez konfigurację preferencji repozytorium

Jeśli obsługiwana wersja programu IBM Installation Manager jest zainstalowany w systemie, można uruchomić go bezpośrednio i określić preferencje dla repozytorium.

### Zanim rozpoczniesz

Program IBM Installation Manager w wersji 1.7.0 i nowszej obsługuje instalowanie produktu IBM Security Directory Server. W następujących sytuacjach na stronie Pakiety instalacyjne programu IBM Installation Manager wyświetlany jest komunikat o błędzie i instalacja nie może być kontynuowana:

- Użytkownik próbuje uruchomić instalację produktu IBM Security Directory Server z poprzednią wersją programu IBM Installation Manager.
- Poprzednia wersja programu IBM Installation Manager została wykryta podczas uruchamiania instalacji produktu IBM Security Directory Server z Startera.

Jeśli system zawiera program IBM Installation Manager w wersji wcześniejszej niż 1.7.0, należy zaktualizować go do wersji 1.7.0 lub nowszej. Możesz wybrać jeden z następujących sposobów, aby zainstalować program IBM Installation Manager w wymaganej wersji.

- Uruchom instalację programu IBM Installation Manager za pomocą startera. Aby uzyskać więcej informacji, patrz “Uruchamianie instalacji za pomocą startera” na stronie 28.
- Pobierz program IBM Installation Manager w wersji 1.7.0 lub nowszej dla używanego systemu operacyjnego. Więcej informacji na temat instalowania w trybie cichym programu IBM Installation Manager znajduje się w dokumentacji produktu IBM Installation Manager pod adresem http://www-01.ibm.com/support/knowledgecenter/SSDV2W/welcome.

## O tym zadaniu

Instalację można uruchomić, ustawiając preferencje repozytorium w następujących scenariuszach instalacji:

- Instalacja z lokalnego katalogu lub zdalnego współużytkowanego dysku, który zawiera pakiet produktu pobrany z serwisu IBM Passport Advantage.
- Instalacja z adresu URL repozytorium WWW.

## Procedura

1. Uruchom program IBM Installation Manager.

   **Windows**

   W menu **Start** kliknij kolejno opcje **Wszystkie programy > IBM Installation Manager > IBM Installation Manager**.

   **AIX i Linux**

   Wprowadź następującą komendę w wierszu komend. Zmodyfikuj poniższą ścieżkę domyślną, jeśli program IBM Installation Manager jest zainstalowany w innej lokalizacji.

   ```
   /opt/IBM/InstallationManager/eclipse/IBMIM
   ```

2. Na stronie Start programu IBM Installation Manager kliknij kolejno opcje **File > Preferences**.
3. Na stronie Repositories (Repozytoria) kliknij opcję **Add Repository** (Dodaj repozytorium).
4. Na stronie Add Repository wpisz adres URL położenia repozytorium lub wskaż go i ustaw ścieżkę pliku.
5. Kliknij przycisk **OK**. Jeśli podano lokalizację repozytorium HTTPS lub repozytorium wymagającego logowania, a następnie należy wprowadzić ID użytkownika i hasło. Zostanie wyświetlona lokalizacja nowego lub zmienionego repozytorium.
6. Aby sprawdzić poprawność dostępu repozytorium, kliknij przycisk **Test Connections**.
7. Kliknij przycisk **OK**, aby zamknąć stronę Repositories.

## Wyniki

Nie można zainstalować wielu kopii tej samej wersji produktu IBM Security Directory Server w jednym systemie. Po ponownym wybraniu pakietu instalacyjnego dla tej samej wersji program IBM Installation Manager generuje komunikat ostrzegawczy i nie można kontynuować instalacji. W jednym systemie mogą jednak istnieć różne wersje produktu IBM Security Directory Server.

## Co dalej

Kontynuuj wykonywanie czynności instalacyjnych programu IBM Security Directory Server. Patrz sekcja “Instalowanie przy użyciu programu IBM Installation Manager” na stronie 31.

# Instalowanie przy użyciu programu IBM Installation Manager

Wykonaj następujące kroki w celu zainstalowania produktu IBM Security Directory Server za pomocą programu IBM Installation Manager.

## Zanim rozpoczniesz

Uruchom instalację.

## Procedura

1. Na stronie Uruchamianie programu IBM Installation Manager kliknij opcję **Zainstaluj**.
2. Na stronie Pakiety instalacyjne wybierz pakiet produktu IBM Security Directory Server do zainstalowania.
3. Kliknij przycisk **Dalej**. Program IBM Installation Manager sprawdza wstępnie wymagane pakiety na komputerze.
4. Jeśli komputer nie spełnia wymagań wstępnych, na stronie **Wyniki sprawdzania poprawności** zostaną wyświetlone wymagania wstępne.
   a. Aby sprawdzić, czy wymagania wstępne są spełnione po zainstalowaniu pakietów wymagań wstępnych, kliknij przycisk **Sprawdź ponownie status**. Więcej informacji o wymaganiach wstępnych zawiera sekcja “Pakiety wymagane wstępnie w różnych systemach operacyjnych” na stronie 15.
   b. Jeśli spełnione są wszystkie wymagania wstępne, kliknij przycisk **Dalej**.
5. Kliknij przycisk **Akceptuję warunki umowy licencyjnej**, a następnie kliknij przycisk **Dalej**. Zostanie wyświetlone położenie katalogu zasobów współużytkowanych.
6. Opcjonalne: Użyj ścieżki domyślnej lub podaj ścieżkę w polu **Katalog zasobów współużytkowanych**. Katalog zasobów współużytkowanych jest katalogiem, w którym są przechowywane artefakty instalacji, dzięki czemu mogą być używane przez jedną lub więcej grup pakietów produktu. Katalog zasobów współużytkowanych można określić tylko podczas pierwszej instalacji pakietu.
7. Kliknij przycisk **Dalej**. Zostaną wyświetlone nazwa grupy pakietów oraz domyślne miejsce instalacji. Domyślnie wybrana jest opcja **Utwórz nową grupę pakietów** i tylko ta opcja jest obsługiwana przy instalacji produktu IBM Security Directory Server. Grupa pakietów reprezentuje katalog, w którym pakiety współużytkują zasoby z innymi pakietami z tej samej grupy. Nazwa grupy pakietów jest przypisywana automatycznie.

   **Ograniczenie:**

   Produkt IBM Security Directory Server może być zainstalowany tylko w predefiniowanym położeniu w systemach AIX i Linux. Domyślnie ścieżka jest podawana w polu **Katalog instalacyjny** w programie IBM Installation Manager. Pole to jest dostępne do edycji w programie IBM Installation Manager. Jeśli jednak ścieżka domyślna zostanie zmieniona, przycisk **Dalej** nie będzie dostępny i nie będzie można kontynuować instalacji. Należy wtedy przywrócić domyślną ścieżkę instalacji produktu IBM Security Directory Server.

   Listę domyślnych miejsc instalacji w różnych systemach operacyjnych zawiera sekcja “Domyślne położenia instalacji” na stronie 27.

   To ograniczenie nie dotyczy systemów operacyjnych Microsoft Windows. Program IBM Security Directory Server można zainstalować w dowolnym miejscu w systemie operacyjnym Microsoft Windows. Nawet jeśli użytkownik wybierze położenie instalacji niestandardowej dla produktu IBM Security Directory Server, katalog idsinstinfo z plikiem idsinstances.ldif jest zawsze tworzony na partycji, która jest określona przez

zmienną %SystemDrive%. Jeśli produkt IBM Security Directory Server jest instalowany na dysku E:, a system operacyjny jest na dysku C:, to:

- katalog idsinstinfo jest tworzony na dysku C: (C:\idsinstinfo) a nie w katalogu E:\Program Files\IBM\ldap.

8. Kliknij przycisk **Dalej**.
9. Na stronie **Pakiety instalacyjne** wybierz wymagane składniki. Aby wyświetlić zależności wybranego składnika lub zależności składnika od innych składników, zaznacz pole wyboru **Pokaż zależności**.

*Tabela 11. Składniki produktu IBM Security Directory Server dostępne do zainstalowania w pełnym pakiecie produktu lub w pakiecie tylko klienta.*

| Wszystkie komponenty | Zależności instalacji | Składniki w pełnym pakiecie produktu | Składniki w pakiecie tylko klienta |
|---|---|---|---|
| IBM DB2 | Brak | Tak | Nie |
| IBM Global Security Kit | Brak | Tak | Tak |
| Klient C | Brak | Tak | Tak |
| IBM Java Development Kit | Brak | Tak | Tak |
| Klient Java | Brak | Tak | Tak |
| Serwer | Klient C<br>Klient Java | Tak | Nie |
| Serwer proxy | Klient C<br>Klient Java | Tak | Nie |
| Web Administration Tool | Brak | Tak | Nie |

10. Kliknij przycisk **Dalej**.
11. Jeśli wybrano do instalacji składnik IBM DB2, kliknij opcję **IBM DB2**, a następnie wykonaj jedną z następujących czynności:
    - Aby zainstalować produkt IBM DB2, wykonaj następujące czynności:
      a. Kliknij opcję **Zainstaluj bazę danych DB2**.
      b. W polu **Ścieżka instalacyjna DB2** podaj nazwę ścieżki do pliku instalacyjnego DB2. Możesz kliknąć przycisk **Przeglądaj** i podać ścieżkę.
      c. W systemie Windows wprowadź ID użytkownika, który ma należeć do grup DB2ADMNS lub DB2USERS, w polu **Nazwa użytkownika**. Tego identyfikatora użytkownika można użyć do uruchamiania na komputerze aplikacji DB2 oraz narzędzi. Jeśli identyfikator użytkownika nie istnieje, program instalacyjny utworzy konto użytkownika.
      d. W systemie Windows wpisz hasło dla identyfikatora użytkownika w polu **Hasło**. Jeśli hasło nie spełnia strategii haseł ustawionej na komputerze, instalacja może się nie powieść.
      e. W systemie Windows wpisz hasło dla identyfikatora użytkownika w polu **Potwierdź hasło**.
      f. Kliknij przycisk **Dalej**.
    - Jeśli na komputerze jest zainstalowana obsługiwana wersja produktu IBM DB2, wykonaj jedną z następujących czynności:
      a. Aby kontynuować z istniejącą wersją produktu IBM DB2, kliknij opcję **Kontynuuj, używając istniejącej bazy danych DB2**.

**Ważne:** Jeśli podczas instalacji zostanie wybrane kontynuowanie z istniejącą bazą danych DB2, program IBM Installation Manager zaktualizuje rejestr o pozycję składnika DB2.

b. Z listy wybierz obsługiwaną wersję DB2, która ma być używana z produktem IBM Security Directory Server.

c. Kliknij przycisk **Dalej**.

12. Jeśli wybrano do instalacji składnik IBM Global Security Kit, kliknij opcję **IBM Global Security Kit**, a następnie wykonaj jedną z następujących czynności:
    - Jeśli na komputerze nie ma zainstalowanego pakietu GSKit w wersji 8.0 lub nowszego, wykonaj następujące czynności:
      a. Kliknij opcję **Zainstaluj GSKit**.
      b. W polu **Ścieżka instalacyjna GSKit** podaj nazwę ścieżki instalacyjnej GSKit. Możesz kliknąć przycisk **Przeglądaj** i podać ścieżkę.

         **Uwaga:** Podana ścieżka musi zawierać zarówno 64-bitowe, jak i 32-bitowe pliki instalacyjne GSKit.

      c. Kliknij przycisk **Dalej**.
    - Jeśli na komputerze znajduje się zainstalowany pakiet GSKit w wersji 8.0 lub nowszy, wykonaj jedną z następujących czynności:
      a. Aby kontynuować z istniejącą wersją produktu GSKit, kliknij opcję **Kontynuuj, używając istniejącego komponentu GSKit**.

         **Ważne:** Jeśli podczas instalacji zostanie wybrane kontynuowanie z istniejącym komponentem GSKit, program IBM Installation Manager zaktualizuje rejestr o pozycję składnika GSKit.

      b. Kliknij przycisk **Dalej**.
13. Jeśli wybrano do instalacji składnik IBM Java Development Kit, kliknij opcję **IBM Java Development Kit** i wykonaj następujące kroki:
    a. W polu **IBM Java Development Kit** podaj nazwę skompresowanego pliku JDK ze ścieżką. Możesz kliknąć przycisk **Przeglądaj** i podać ścieżkę.
    b. Kliknij przycisk **Dalej**.
14. Jeśli wybrano do instalacji składnik Web Administration Tool, kliknij opcję **Web Administration Tool** i wykonaj następujące kroki:
    a. Aby zainstalować wbudowany serwer WebSphere Application Server, wykonaj następujące czynności:
       1) Wybierz opcję **Zainstaluj wbudowany serwer WebSphere Application Server**.
       2) W polu **Ścieżka instalacyjna wbudowanej wersji serwera WebSphere Application Server** podaj nazwę ścieżki do plików instalacyjnych wbudowanego serwera WebSphere Application Server. Możesz kliknąć przycisk **Przeglądaj** i podać ścieżkę.
    b. Aby wdrożyć program Web Administration Tool, wykonaj jedną z następujących czynności:
       - Aby przeprowadzić wdrożenie na wbudowanym serwerze WebSphere Application Server znajdującym się w domyślnej ścieżce instalacji, kliknij opcję **Wdróż w domyślnej wbudowanej wersji serwera WebSphere Application Server**.

         **Uwaga:** Jeśli istnieje poprzednia wersja programu Web Administration Tool, program instalacyjny przeprowadzi jej wdrożenie do bieżącej wersji, o ile spełnione zostały następujące warunki:

1) Poprzednia wersja programu Web Administration Tool oraz wbudowany serwer WebSphere Application Server są zainstalowane w domyślnej ścieżce instalacji.
2) Poprzednia wersja programu Web Administration Tool jest wdrożona na wbudowanym serwerze WebSphere Application Server, który znajduje się w domyślnej ścieżce instalacji.
3) Obsługiwana jest migracja programu Web Administration Tool udostępnionego z produktem IBM Security Directory Server w wersji 6.1, 6.2 lub 6.3.

- Aby przeprowadzić wdrożenie na serwerze WebSphere Application Server lub wbudowanym serwerze WebSphere Application Server w niestandardowej ścieżce instalacji, kliknij opcję **Wdróż w istniejącym serwerze WebSphere Application Server**.
  1) W polu **Ścieżka instalacyjna serwera WebSphere Application Server lub wbudowanego serwera WebSphere Application Server** podaj ścieżkę instalacji istniejącego serwera aplikacji WWW.
- Aby później wdrożyć program Web Administration Tool na obsługiwanym serwerze aplikacji WWW, kliknij opcję **Wdróż ręcznie w innym terminie**.

15. Kliknij przycisk **Dalej**. Zostaną wyświetlone informacje podsumowania przedinstalacyjnego zawierające miejsce instalacji, listę pakietów oraz informacje o repozytorium.
16. Sprawdź informacje podsumowania i kliknij przycisk **Instaluj**. Zostanie uruchomiona instalacja i wyświetlony zostanie pasek postępu. Po zakończeniu instalacji zostanie wyświetlona strona podsumowania poinstalacyjnego.
17. Kliknij odsyłacz **Wyświetl plik dziennika**, aby sprawdzić, czy instalacja zakończyła się pomyślnie. Aby uzyskać więcej informacji, patrz Rozdział 5, “Pliki dziennika programu IBM Installation Manager”, na stronie 43.
18. Aby uruchomić jeden z następujących programów, wykonaj jedną z następujących czynności:
    - Aby uruchomić program Instance Administration Tool, kliknij opcję **Instance Administration Tool (idsxinst)**.
    - Jeśli nie chcesz uruchomić żadnego programu, kliknij przycisk **Brak**.
19. Kliknij przycisk **Zakończ**.
20. Kliknij kolejno opcje **Plik > Wyjście**.

## Wyniki

Jeśli instalacja zakończy się pomyślnie, produkt IBM Security Directory Server został zainstalowany w miejscu instalacji. Informacje o domyślnym katalogu instalacji zawiera sekcja “Domyślne położenia instalacji” na stronie 27. Jeśli instalacja nie powiedzie się dla jakiegokolwiek z wybranych składników, instalacja pakietów IBM Security Directory Server zostanie wycofana.

## Co dalej

Po zainstalowaniu produktu IBM Security Directory Server należy wykonać następujące działania:

- Aby użyć produktu IBM Security Directory Server jako pełnego serwera katalogów, utwórz instancję serwera katalogów. Aby uzyskać więcej informacji, patrz “Tworzenie instancji serwera katalogów” na stronie 134.

- Aby użyć produktu IBM Security Directory Server jako serwera proxy, utwórz instancję serwera proxy. Aby uzyskać więcej informacji, patrz “Tworzenie instancji serwera proxy z własnymi ustawieniami” na stronie 142.

# Instalacja w trybie cichym

W trybie cichym można zainstalować produkt IBM Security Directory Server na wielu systemach bez konieczności samodzielnych interwencji.

Aby użyć instalacji cichej, należy wykonać następujące działania:

1. Zainstaluj program IBM Installation Manager (jeśli nie jest jeszcze zainstalowany).
2. Użyj domyślnego pliku odpowiedzi lub utwórz niestandardowy plik odpowiedzi.
3. Zainstaluj pakiety.

## Plik odpowiedzi dla instalacji cichej

W trybie instalacji cichej, interfejs użytkownika nie jest dostępny. Plik odpowiedzi zawiera dane wejściowe dla instalacji. Plik odpowiedzi to plik XML, który zawiera dane wymagane do wykonania instalacji cichej.

**Zapisywanie niestandardowego pliku odpowiedzi**

Można utworzyć plik odpowiedzi dla następujących zadań:

- Instalowanie pakietów
- Modyfikowanie pakietów
- Deinstalowanie pakietów

Aby zapisać plik odpowiedzi, należy zapisać preferencje i działania instalacyjne za pomocą programu IBM Installation Manager w trybie interfejsu użytkownika. Podczas pierwszego zapisania pliku odpowiedzi dla instalacji cichej, można wybrać, aby nie instalować pakietów, korzystając z parametru **-skipInstall** *położenie_danych_agenta*.

W lokalizacji *położenie_danych_agenta* znajdują się dane do zainstalowania produktu. Aby zapisać plik odpowiedzi dla modyfikacji lub deinstalacji cichej produktu, z parametrem **-skipInstall** należy użyć tej samej lokalizacji *położenie_danych_agenta*.

Dla scenariusza z wieloma instalacjami należy zapisać różne pliki odpowiedzi z różnymi lokalizacjami *położenie_danych_agenta* dla każdego scenariusza.

Więcej informacji na temat zapisywania pliku odpowiedzi dla instalacji cichej znajduje się w dokumentacji programu IBM Installation Manager pod adresem http://www-01.ibm.com/support/knowledgecenter/SSDV2W/welcome.

## Sprawdzanie poprawności instalacji cichej

Po zakończeniu instalacji należy sprawdzić poprawność instalacji cichej. Można to zrobić w jeden z następujących sposobów:

- Sprawdzanie kodu powrotu
- Sprawdzanie pliku dziennika
- Sprawdzanie pakietów

# Instalacja cicha przy użyciu pliku odpowiedzi

Cicha instalacja produktu IBM Security Directory Server umożliwia zainstalowanie wymaganych pakietów bez udziału użytkownika.

## Zanim rozpoczniesz

Do wykonania cichej instalacji pakietów produktu IBM Security Directory Server wymagany jest program IBM Installation Manager w wersji 1.7.0 lub nowszej.

## O tym zadaniu

Można użyć domyślnego pliku odpowiedzi lub zarejestrować zmodyfikowany plik odpowiedzi i użyć go jako pliku wejściowego dla cichej instalacji.

## Procedura

1. Zaloguj się do systemu jako administrator.
2. Uzyskaj dostęp do komendy **IBMIM** w katalogu instalacyjnym IBM Installation Manager.

| System operacyjny | Domyślne położenie komendy IBMIM: |
|---|---|
| **Microsoft Windows** | C:\Program Files\IBM\InstallationManager\eclipse |
| **AIX i Linux** | /opt/IBM/InstallationManager/eclipse |

3. Opcjonalne: Uruchom komendę **IBMIM**, aby zarejestrować plik odpowiedzi dla instalacji.

   **Wskazówka:** Można użyć przykładowego pliku odpowiedzi dla instalacji. Przykładowy domyślny plik odpowiedzi zawiera sekcja “Instalacja w trybie cichym” na stronie 35.

   a. Aby zarejestrować czynności instalacyjne bez instalowania produktu, uruchom następujące komendy w różnych systemach operacyjnych:

      **Microsoft Windows**

      IBMIM.exe -record *ścieżka\plikOdpowiedzi.xml* -skipInstall *agentDataLocation*

      **AIX i Linux**

      ./IBMIM -record *ścieżka/responseFile.xml* -skipInstall *agentDataLocation*

      Ta komenda uruchamia program IBM Installation Manager.

   b. Ustaw repozytorium IBM Security Directory Server. Więcej informacji na ten temat zawiera sekcja 2 na stronie 30

   c. Wykonaj rejestrowanie operacji instalacji produktu IBM Security Directory Server Więcej informacji na ten temat zawiera sekcja “Instalowanie przy użyciu programu IBM Installation Manager” na stronie 31

4. Uruchom komendę **imcl**, aby uruchomić instalację cichą z plikiem odpowiedzi podanym jako dane wejściowe. Komenda **imcl** powinna znajdować się w katalogu <*kat_inst_IBM_Installation_Manager*>/eclipse/tools.

| System operacyjny | Komenda do uruchomienia: |
|---|---|
| **Microsoft Windows** | imcl.exe input *ścieżka\responseFile.xml* -acceptLicense -showProgess |
| **AIX i Linux** | ./imcl input *ścieżka/responseFile.xml* -acceptLicense -showProgess |

   **Uwaga:** Dostępne jest wiele innych parametrów, które mogą być używane wraz z komendą **imcl**. Więcej informacji zawiera pomoc dla komendy **imcl**.

5. Sprawdź podsumowanie instalacji i pliki dziennika.

| System operacyjny | Domyślna ścieżka dziennika: |
|---|---|
| **Microsoft Windows** | C:\ProgramData\IBM\InstallationManager\logs |
| **AIX i Linux** | /var/ibm/InstallationManager/logs/ |

6. Sprawdź. czy pakiety produktu IBM Security Directory Server są w wymaganej wersji.

| System operacyjny | Weryfikowanie pakietów: |
|---|---|
| **Microsoft Windows** | Patrz sekcja “Weryfikowanie funkcji serwera IBM Security Directory Server przy użyciu programu IBM Installation Manager” na stronie 83. |
| **AIX i Linux** | Patrz sekcja “Weryfikowanie funkcji serwera IBM Security Directory Server przy użyciu programu IBM Installation Manager” na stronie 83. |

## Wyniki

Jeśli instalacja zakończy się pomyślnie, produkt IBM Security Directory Server został zainstalowany w swoim katalogu. Informacje o domyślnym katalogu instalacji zawiera sekcja “Domyślne położenia instalacji” na stronie 27. Jeśli instalacja nie powiedzie się dla jakiegokolwiek z wybranych składników, instalacja pakietów IBM Security Directory Server zostanie wycofana.

## Co dalej

**Uwaga:** Jeśli wybrano uruchomienie programu Instance Administration Tool podczas rejestrowania pliku odpowiedzi w trakcie instalacji, program ten nie będzie uruchamiany po wykonaniu instalacji cichej produktu IBM Security Directory Server.

Jeśli wybrano instalację serwera lub serwera proxy, uruchom program Instance Administration Tool, aby utworzyć instancję serwera katalogów lub instancję serwera proxy. Patrz sekcja “Uruchamianie narzędzia Instance Administration Tool” na stronie 131.

# Rozdział 4. Modyfikowanie za pomocą programu IBM Installation Manager

Używając programu IBM Installation Manager, można zainicjować funkcje produktu IBM Security Directory Server, które nie były zainstalowane wcześniej, oraz odinstalować funkcje już zainstalowane.

Nie można usunąć funkcji, jeśli jest wymagana przez inne zainstalowane funkcje. Zależność tę można usunąć tylko wtedy, gdy do wykonania operacji instalowania lub deinstalowania zostaną wybrane wszystkie zależne funkcje.

**Ważne:** Jeśli podczas instalowania wybrana zostanie opcja użycia istniejącej wersji bazy danych DB2 albo pakietu GSKit, program IBM Installation Manager zaktualizuje odpowiednio swój rejestr. Podczas usuwania funkcji zainstalowanej z użyciem opcji **Kontynuuj z istniejącą**, program Installation Manager wykonuje następujące działania:

- Pozycja funkcji jest usuwana z rejestru programu IBM Installation Manager.
- Funkcja nie jest deinstalowana z komputera.

## Modyfikowanie funkcji za pomocą programu IBM Installation Manager

Wykonaj następujące czynności, aby zmodyfikować opcje serwera IBM Security Directory Server przy użyciu programu IBM Installation Manager.

### Zanim rozpoczniesz

Należy zatrzymać wszystkie procesy klienta i serwera IBM Security Directory Server.

- Serwer katalogów
- Serwer administracyjny
- Śledzenie LDAP
- Niestandardowe aplikacje LDAP

Jeśli którykolwiek proces jest używany, nie można usunąć programów i bibliotek.

### Procedura

1. Uruchom program IBM Installation Manager.
   - W systemach AIX i Linux:
     a. Otwórz okno wiersza komend i przejdź do katalogu, który zawiera program IBM Installation Manager. Następujący katalog jest domyślnym położeniem instalacji programu IBM Installation Manager:
        `opt/IBM/InstallationManager/eclipse`
     b. Uruchom komendę:
        `./IBMIM`
   - Microsoft Windows:
     a. Kliknij kolejno opcje **Start > Wszystkie programy > IBM Installation Manager > IBM Installation Manager**.
2. Kliknij przycisk **Modyfikuj**.
3. Wybierz opcję **IBM Security Directory Server**, a następnie kliknij przycisk **Dalej**.
4. Na stronie **Modyfikuj pakiety** wykonaj następujące czynności:

a. Wybierz opcje, które chcesz zainstalować.
b. Wybierz opcje, które chcesz zdeinstalować.

*Tabela 12. Funkcje serwera IBM Security Directory Server dostępne do zmodyfikowania w pełnym produkcie i pakietach zawierających tylko klienty*

| **Wszystkie komponenty** | **Zależności instalacji** | **Składniki w pełnym pakiecie produktu** | **Składniki w pakiecie tylko klienta** |
|---|---|---|---|
| IBM DB2 | Brak | Tak | Nie |
| IBM Global Security Kit | Brak | Tak | Tak |
| Klient C | Brak | Tak | Tak |
| IBM Java Development Kit | Brak | Tak | Tak |
| Klient Java | Brak | Tak | Tak |
| Serwer | Klient C<br>Klient Java | Tak | Nie |
| Serwer proxy | Klient C<br>Klient Java | Tak | Nie |
| Web Administration Tool | Brak | Tak | Nie |

**Ważne:** Jeśli podczas instalowania wybrana zostanie opcja użycia istniejącej wersji bazy danych DB2 albo pakietu GSKit, program IBM Installation Manager zaktualizuje odpowiednio swój rejestr. Podczas usuwania funkcji zainstalowanej z użyciem opcji **Kontynuuj z istniejącą**, program Installation Manager wykonuje następujące działania:

- Pozycja funkcji jest usuwana z rejestru programu IBM Installation Manager.
- Funkcja nie jest deinstalowana z komputera.

Jeśli istnieją instancje DB2 utworzone za pomocą kopii bazy danych DB2 zainstalowanej przy użyciu programu IBM Installation Manager, nie można usunąć bazy danych IBM DB2. W takiej sytuacji należy samodzielnie usunąć instancje DB2, a następnie spróbować ponownie. Zaleca się wykonanie kopii zapasowej bazy danych przed usunięciem instancji DB2.

c. Kliknij przycisk **Dalej**.

5. Jeśli wybrano do instalacji składnik IBM DB2, kliknij opcję **IBM DB2**, a następnie wykonaj jedną z następujących czynności:
   - Aby zainstalować produkt IBM DB2, wykonaj następujące czynności:
     a. Kliknij opcję **Zainstaluj bazę danych DB2**.
     b. W polu **Ścieżka instalacyjna DB2** podaj nazwę ścieżki do pliku instalacyjnego DB2. Możesz kliknąć przycisk **Przeglądaj** i podać ścieżkę.
     c. W systemie Windows wprowadź ID użytkownika, który ma należeć do grup DB2ADMNS lub DB2USERS, w polu **Nazwa użytkownika**. Tego identyfikatora użytkownika można użyć do uruchamiania na komputerze aplikacji DB2 oraz narzędzi. Jeśli identyfikator użytkownika nie istnieje, program instalacyjny utworzy konto użytkownika.
     d. W systemie Windows wpisz hasło dla identyfikatora użytkownika w polu **Hasło**. Jeśli hasło nie spełnia strategii haseł ustawionej na komputerze, instalacja może się nie powieść.
     e. W systemie Windows wpisz hasło dla identyfikatora użytkownika w polu **Potwierdź hasło**.

f. Kliknij przycisk **Dalej**.

- Jeśli na komputerze jest zainstalowana obsługiwana wersja produktu IBM DB2, wykonaj następujące czynności:
  a. Aby kontynuować z istniejącą wersją produktu IBM DB2, kliknij opcję **Kontynuuj, używając istniejącej bazy danych DB2**.

     **Ważne:** Jeśli podczas instalacji zostanie wybrane kontynuowanie z istniejącą bazą danych DB2, program IBM Installation Manager zaktualizuje rejestr o pozycję składnika DB2.
  b. Z listy wybierz obsługiwaną wersję DB2, która ma być używana z produktem IBM Security Directory Server.
  c. Kliknij przycisk **Dalej**.

6. Jeśli wybrano do instalacji składnik IBM Global Security Kit, kliknij opcję **IBM Global Security Kit**, a następnie wykonaj jedną z następujących czynności:
   - Jeśli na komputerze nie ma zainstalowanego pakietu GSKit w wersji 8.0 lub nowszego, wykonaj następujące czynności:
     a. Kliknij opcję **Zainstaluj GSKit**.
     b. W polu **Ścieżka instalacyjna GSKit** podaj nazwę ścieżki instalacyjnej GSKit. Możesz kliknąć przycisk **Przeglądaj** i podać ścieżkę.

        **Uwaga:** Podana ścieżka musi zawierać zarówno 64-bitowe, jak i 32-bitowe pliki instalacyjne GSKit.
     c. Kliknij przycisk **Dalej**.
   - Jeśli na komputerze jest zainstalowany pakiet GSKit w wersji 8.0 lub nowszej, wykonaj następujące czynności:
     a. Aby kontynuować z istniejącą wersją produktu GSKit, kliknij opcję **Kontynuuj, używając istniejącego komponentu GSKit**.

        **Ważne:** Jeśli podczas instalacji zostanie wybrane kontynuowanie z istniejącym komponentem GSKit, program IBM Installation Manager zaktualizuje rejestr o pozycję składnika GSKit.
     b. Kliknij przycisk **Dalej**.
7. Jeśli wybrano do instalacji składnik IBM Java Development Kit, kliknij opcję **IBM Java Development Kit** i wykonaj następujące kroki:
   a. W polu **IBM Java Development Kit** podaj nazwę skompresowanego pliku JDK ze ścieżką. Możesz kliknąć przycisk **Przeglądaj** i podać ścieżkę.
   b. Kliknij przycisk **Dalej**.
8. Jeśli wybrano do instalacji składnik Web Administration Tool, kliknij opcję **Web Administration Tool** i wykonaj następujące kroki:
   a. Aby zainstalować wbudowany serwer WebSphere Application Server, wykonaj następujące czynności:
      1) Wybierz opcję **Zainstaluj wbudowany serwer WebSphere Application Server**.
      2) W polu **Ścieżka instalacyjna wbudowanej wersji serwera WebSphere Application Server** podaj nazwę ścieżki do plików instalacyjnych wbudowanego serwera WebSphere Application Server. Możesz kliknąć przycisk **Przeglądaj** i podać ścieżkę.
   b. Aby wdrożyć program Web Administration Tool, wykonaj jedną z następujących czynności:

- Aby przeprowadzić wdrożenie na wbudowanym serwerze WebSphere Application Server znajdującym się w domyślnej ścieżce instalacji, kliknij opcję **Wdróż w domyślnej wbudowanej wersji serwera WebSphere Application Server**.

  **Uwaga:** Jeśli istnieje poprzednia wersja programu Web Administration Tool, program instalacyjny przeprowadzi jej wdrożenie do bieżącej wersji, o ile spełnione zostały następujące warunki:

  1) Poprzednia wersja programu Web Administration Tool oraz wbudowany serwer WebSphere Application Server są zainstalowane w domyślnej ścieżce instalacji.
  2) Poprzednia wersja programu Web Administration Tool jest wdrożona na wbudowanym serwerze WebSphere Application Server, który znajduje się w domyślnej ścieżce instalacji.
  3) Obsługiwana jest migracja programu Web Administration Tool udostępnionego z produktem IBM Security Directory Server w wersji 6.1, 6.2 lub 6.3.

- Aby przeprowadzić wdrożenie na serwerze WebSphere Application Server lub wbudowanym serwerze WebSphere Application Server w niestandardowej ścieżce instalacji, kliknij opcję **Wdróż w istniejącym serwerze WebSphere Application Server**.
  1) W polu **Ścieżka instalacyjna serwera WebSphere Application Server lub wbudowanego serwera WebSphere Application Server** podaj ścieżkę instalacji istniejącego serwera aplikacji WWW.
- Aby później wdrożyć program Web Administration Tool na obsługiwanym serwerze aplikacji WWW, kliknij opcję **Wdróż ręcznie w innym terminie**.

9. Kliknij przycisk **Dalej**.

   **Ważne:** Jeśli podczas instalowania wybrana zostanie opcja użycia istniejącej wersji bazy danych DB2 albo pakietu GSKit, program IBM Installation Manager zaktualizuje odpowiednio swój rejestr. Podczas usuwania funkcji zainstalowanej z użyciem opcji **Kontynuuj z istniejącą**, program Installation Manager wykonuje następujące działania:
   - Pozycja funkcji jest usuwana z rejestru programu IBM Installation Manager.
   - Funkcja nie jest deinstalowana z komputera.
10. Zweryfikuj podsumowanie informacji i kliknij przycisk **Modyfikuj**.
11. Opcjonalne: Jeśli podczas modyfikowania wystąpi błąd, kliknij opcję **Wyświetl plik dziennika**, aby zapoznać się ze szczegółami. Aby uzyskać więcej informacji, patrz Rozdział 5, “Pliki dziennika programu IBM Installation Manager”, na stronie 43.
12. Kliknij przycisk **Zakończ**.
13. Kliknij kolejno opcje **Plik > Wyjście**.

## Wyniki

Jeśli modyfikacje powiodą się, można zaobserwować następujące zmiany:

- Wybrane funkcje serwera IBM Security Directory Server zostaną zainstalowane w katalogu instalacyjnym. Informacje o domyślnym katalogu instalacji zawiera sekcja “Domyślne położenia instalacji” na stronie 27.
- Funkcje serwera IBM Security Directory Server, które wybrano do usunięcia, zostaną zdeinstalowane.

# Rozdział 5. Pliki dziennika programu IBM Installation Manager

Sprawdzając pliki dziennika tworzone przez program IBM Installation Manager, można sprawdzać poprawność instalacji, aktualizacji i deinstalacji produktu IBM Security Directory Server i jego komponentów.

Jeśli podczas instalowania, modyfikowania lub deinstalowania produktu IBM Security Directory Server i jego komponentów wystąpi błąd, należy sprawdzić zawartość plików dzienników. Program IBM Installation Manager tworzy pliki dziennika w położeniu domyślnym.

*Tabela 13. Domyślne położenie plików dzienników programu IBM Installation Manager w różnych systemach operacyjnych*

| **System operacyjny** | **Domyślne położenie dziennika programu IBM Installation Manager** |
|---|---|
| AIX i Linux | /var/ibm/InstallationManager/logs |
| Microsoft Windows | C:\ProgramData\IBM\InstallationManager\logs |

Domyślne położenie dotyczy wszystkich obsługiwanych wersji systemów AIX, Linux i Microsoft Windows.

# Rozdział 6. Odpytywanie o pakiety serwera IBM Security Directory Server

Pakiety produktu IBM Security Directory Server można zweryfikować, sprawdzając pakiety tego produktu zainstalowane na obsługiwanych platformach.

## O tym zadaniu

Po wykonaniu instalacji produktu IBM Security Directory Server należy sprawdzić, czy wszystkie jego pakiety są w wymaganej wersji. To zadanie pozwala na sprawdzenie numerów wersji pakietów IBM Security Directory Server.

## Procedura

Zaloguj się do systemu, w którym zainstalowano pakiety IBM Security Directory Server uruchom poniższe komendy z uprawnieniami użytkownika root.

- W systemach AIX: uruchom komendę **lslpp**. Na przykład:

  ```
  lslpp -l 'idsldap*'
  ```

- W systemach Linux: uruchom komendę **rpm**. Na przykład:

  ```
  rpm -qa | grep idsldap
  ```

- Systemy Solaris:
  1. Aby wyświetlić listę zainstalowanych pakietów, uruchom komendę **pkginfo**. Na przykład:

     ```
     pkginfo | grep IDSl
     ```

  2. Aby zapytać o wersję konkretnego pakietu IBM Security Directory Server, uruchom komendę **pkgparam**. Na przykład:

     ```
     pkgparam IDSlbc63 VERSION
     ```

- W systemach HP-UX (Itanium) : uruchom komendę **swlist**. Na przykład:

  ```
  swlist | grep idsldap
  ```

# Rozdział 7. Instalowanie i konfigurowanie w trybie rodzimym za pomocą skryptów

Można zainstalować i skonfigurować produkt IBM Security Directory Server za pomocą skryptów.

## Przewodnik przejścia instalacji

W tej sekcji przedstawiono informacje na temat instalowania produktu IBM Security Directory Server w systemach Linux x86, Linux i/pSeries, Linux s390, Solaris i HP-UX.

1. Upewnij się, że spełnione są minimalne wymagania dotyczące sprzętu i oprogramowania. Więcej informacji znajduje się w rozdziale *Wymagania systemowe* w sekcji Przegląd produktu dokumentacji serwera IBM Security Directory Server.
2. Zainstaluj wstępnie wymagane oprogramowanie, takie jak DB2. Jeśli baza danych nie jest jeszcze zainstalowana, sprawdź, czy ścieżka zawierająca pliki instalacyjne DB2 jest dostępna i czy nadane są wszystkie wymagane uprawnienia.
3. Jeśli ma być używana dowolna z poniższych funkcji, należy zainstalować opcjonalne wstępnie wymagane oprogramowanie. Jeśli oprogramowanie to nie jest jeszcze zainstalowane, sprawdź, czy oprogramowanie jest dostępne i czy nadane są wszystkie wymagane uprawnienia.
   - Dla narzędzia Web Administration Tool wymagana jest obsługiwana wersja wbudowanego serwera WebSphere Application Server lub serwera WebSphere Application Server. Również wymagana jest obsługiwana wersja przeglądarki.
   - Aby używać protokołu SSL (Secure Socket Layer) lub TLS (Transport Layer Security), wymagana jest obsługiwana wersja pakietu IBM Global Security Kit (GSKit).
4. W systemach Linux x86, Linux i/pSeries, Linux s390, Solaris i HP-UX należy użyć programu **idsNativeInstall** do zainstalowania pakietów produktu IBM Security Directory Server i innego wymaganego oprogramowania.
5. Po zainstalowaniu produktu IBM Security Directory Server, użyj komendy **idsdefinst**, aby utworzyć i skonfigurować instancję serwera katalogów.
6. Uruchom instancję serwera katalogów.
7. Załaduj do bazy danych przykładowy plik LDIF. Więcej informacji na temat używania instancji serwera katalogów znajduje się w sekcji Administrowanie dokumentacji produktu IBM Security Directory Server.

**Uwaga:** Skrypt instalacji rodzimej (**idsNativeInstall**) nie jest dostępny dla systemów Windows, AIX i Linux x86_64 (wersja 64-bitowa). W tych systemach operacyjnych można użyć programu IBM Installation Manager lub narzędzi systemu operacyjnego.

## Instalowanie pakietów serwera IBM Security Directory Server w systemach Linux, Solaris i HP-UX

W tej sekcji przedstawiono informacje na temat instalowania i aktualizowania pakietów IBM Security Directory Server w systemach Linux x86, Linux i/pSeries, Linux s390, Solaris i HP-UX.

### Zanim rozpoczniesz

Przed rozpoczęciem instalowania pakietów IBM Security Directory Server należy wykonać następujące czynności:

1. Zaloguj się do systemu z uprawnieniami użytkownika root.
2. Wyodrębnij plik archiwum serwera IBM Security Directory Server w wersji 6.3.1 do katalogu, na przykład /sdsV6.3.1, w którym jest odpowiednia ilość wolnego miejsca.
3. Zatrzymaj wszystkie procesy klienta i serwera IBM Security Directory Server, w tym serwer katalogów, serwer administracyjny i niestandardowe aplikacje LDAP. Nie można zastąpić programów i bibliotek w czasie, gdy są one używane. Jeśli włączono śledzenie, wykonaj komendę ldtrc off, aby je wyłączyć. Instrukcje dotyczące zatrzymywania instancji serwera katalogów i serwerów administracyjnych znajdują się w rozdziałach "Podstawowe zadania administracyjne serwera" i "Administracja serwerem katalogów" w sekcji *Administrowanie* dokumentacji produktu IBM Security Directory Server.

## O tym zadaniu

Możesz użyć komendy **idsNativeInstall**, aby zainstalować lub zaktualizować pakiety serwera IBM Security Directory Server w systemach Linux x86, Linux i/pSeries, Linux s390, Solaris i HP-UX. Możesz również użyć komendy **idsNativeInstall**, aby opcjonalnie zainstalować pakiety DB2, GSKit i wbudowany serwer WebSphere Application Server, jeśli nie są one jeszcze zainstalowane w systemie.

**Uwaga:**

- Skrypt instalacji rodzimej (**idsNativeInstall**) nie jest dostępny dla systemów Windows, AIX i Linux x86_64 (wersja 64-bitowa). W tych systemach operacyjnych można użyć programu IBM Installation Manager lub narzędzi systemu operacyjnego.
- W systemach HP-UX są dostępne tylko pakiety klienta IBM Security Directory Server dla instalacji lub aktualizacji.

## Procedura

1. Przejdź do katalogu zawierającego program instalacyjny **idsNativeInstall** i plik responseFile.txt. Pliki idsNativeInstall i responseFile.txt muszą się znajdować w tym samym katalogu.
2. Zaktualizuj następujące pozycje w pliku responseFile.txt. Domyślnie zmienne instalacyjne składników mają ustawioną wartość false, a odpowiadające im zmienne ścieżek nie są ustawione.
   - Aby zainstalować bazę danych DB2, ustaw dla zmiennej *db2FeatureInstall* wartość true i podaj w zmiennej *db2InstallimagePath* pełną ścieżkę pakietu instalacyjnego DB2. Na przykład:

     ```
     db2FeatureInstall=true
     db2InstallimagePath=/sdsV6.3.1/db2
     ```

     **Ważne:** Dla pełnego serwera katalogów baza danych DB2 musi być zainstalowana w systemie. Jeśli ustawiono zmienne DB2, *db2FeatureInstall* i *db2InstallimagePath*, baza danych DB2 zostanie zainstalowana w katalogu /opt/ibm/sdsV6.3.1db2 w systemie Linux lub /opt/IBM/sdsV6.3.1db2 w systemie Solaris. Jeśli wersja bazy danych DB2 jest już zainstalowana w podanym położeniu, instalacja nadpisze istniejące pliki.
   - Aby zainstalować pakiet GSKit, ustaw dla zmiennej *gskitFeatureInstall* wartość true i podaj w zmiennej *gskitInstallimagePath* pełną ścieżkę pakietu instalacyjnego GSKit. Na przykład:

     ```
     gskitFeatureInstall=true
     gskitInstallimagePath=/sdsV6.3.1/gskit
     ```

     **Ważne:** Aby skonfigurować instancję serwera katalogów do komunikacji z wykorzystaniem protokołu SSL lub TLS, w systemie musi być zainstalowana wymagana wersja pakietu GSKit.

- Aby zainstalować pakiet IBM Java Development Kit, ustaw dla zmiennej *JDKFeatureInstall* wartość true i podaj w zmiennej *JDKInstallimagePath* pełną ścieżkę pakietu instalacyjnego IBM Java Development Kit. Na przykład:

  ```
  JDKFeatureInstall=true
  JDKInstallimagePath=/sdsV6.3.1/java/ibm-java-16sr14-linux-i386.tar
  ```

  Pakiet Java Development Kit jest instalowany w katalogu /opt/ibm/ldap/V6.3.1/java w systemach Linux i Solaris.
- Aby zainstalować wbudowaną wersję serwera WebSphere Application Server, ustaw dla zmiennej *eWasFeatureInstall* wartość true i podaj w zmiennej *eWasInstallimagePath* pełną ścieżkę do pakietu instalacyjnego wbudowanej wersji serwera WebSphere Application Server. Na przykład:

  ```
  eWasFeatureInstall=true
  eWasInstallimagePath=/sdsV6.3.1/appsrv
  ```

  Wbudowana wersja serwera WebSphere Application Server jest instalowana w katalogu /opt/ibm/ldap/V6.3/appsrv w systemach Linux i Solaris.
- Aby zainstalować serwer IBM Security Directory Server w wersji 6.3.1 GA (General Availability), podaj w zmiennej *tdsInstallimagePath* pełną ścieżkę pakietu instalacyjnego serwera IBM Security Directory Server 6.3.1 GA. Na przykład:

  ```
  tdsInstallimagePath=/sdsV6.3.1
  ```

  Po podaniu katalogu /sdsV6.3.1 zawierającego wersję instalacyjną serwera IBM Security Directory Server 6.3.1, sprawdź, czy w katalogu tym znajdują się następujące pliki.

  ```
  idsinstall
  idsinstall_i
  ids_detectGskitVersion
  ```

  Pakiety serwera IBM Security Directory Server wersja 6.3.1 muszą znajdować się w katalogu /sdsV6.3.1/tdsfiles.

3. Uruchom komendę **idsNativeInstall** w wierszu komend.

### Wyniki

Po zakończeniu działania komendy **idsNativeInstall** będą zainstalowane pakiety serwera IBM Security Directory Server w wersji 6.3.1. Komenda **idsNativeInstall** może zainstalować także pakiety DB2, GSKit, IBM Java Development Kit lub wbudowany serwer WebSphere Application Server na podstawie wartości podanych w pliku odpowiedzi.

**Uwaga:** Jeśli w systemie nie jest zainstalowany serwer IBM Security Directory Server w wersji 6.3.1, zostaną zainstalowane wszystkie jego komponenty. Serwer IBM Security Directory Server 6.3.1 jest instalowany w katalogu /opt/ibm/ldap/V6.3.1/ w systemach Linux, Solaris i HP-UX.

### Co dalej

Po zainstalowaniu serwera IBM Security Directory Server należy sprawdzić, czy wszystkie jego pakiety zostały zainstalowane. Informacje na temat weryfikowania dzienników zawiera sekcja “Sprawdzanie dziennika instalacji”.

## Sprawdzanie dziennika instalacji

Znajdź plik dziennika, w którym można sprawdzić status instalacji w systemach Linux x86, Linux i/pSeries, Linux s390, Solaris i HP-UX.

Po zakończeniu instalacji, komenda **idsNativeInstall** wyświetli komunikaty z informacją o pomyślnym lub niepomyślnym zakończeniu instalacji. Aby sprawdzić, czy pakiety produktu IBM Security Directory Server zostały zainstalowane, przejrzyj następujący plik dziennika.

Plik dziennika to /var/idsldap/V6.3/idsNativeInstall_*datownik*.log.

Po zapoznaniu się z dziennikiem instalacji sprawdź, czy wszystkie pakiety zostały pomyślnie zainstalowane oraz czy są w wymaganej wersji. Więcej informacji na temat sprawdzania wersji zainstalowanych pakietów znajduje się w sekcji Rozdział 6, “Odpytywanie o pakiety serwera IBM Security Directory Server”, na stronie 45.

# Rozdział 8. Instalowanie IBM DB2

Aby utworzyć instancję produktu IBM Security Directory Server ze skonfigurowaną bazą danych DB2, na komputerze musi być zainstalowana obsługiwana wersja produktu IBM DB2.

Nośnik instalacyjny produktu IBM Security Directory Server zawiera obsługiwaną wersję IBM DB2. Jeśli do zainstalowania produktu IBM Security Directory Server użyte zostały narzędzia systemu operacyjnego, należy zainstalować IBM DB2. Po uruchomieniu instalacji produktu IBM Security Directory Server aktualizowane są pliki właściwości informacjami na temat obsługiwanej wersji IBM DB2. Jeśli na komputerze jest zainstalowana obsługiwana wersja produktu IBM DB2, można jej użyć do skonfigurowania instancji serwera katalogów. Więcej informacji na temat aktualizowania pliku ldapdb.properties zawiera sekcja Dodatek C, “Samodzielne aktualizowanie pliku ldapdb.properties”, na stronie 247.

Aby zainstalować produkt IBM DB2, przejdź do katalogu na nośniku instalacyjnym produktu IBM Security Directory Server, który zawiera program instalacyjny produktu IBM DB2.

Przed uruchomieniem instancji IBM DB2 należy spełnić wymagania wstępne DB2. Aby sprawdzić, czy komputer spełnia wymagania wstępne bazy danych DB2, należy uruchomić komendę **db2prereqcheck**. Jeśli na komputerze brakuje wymaganych pakietów, należy zaktualizować komputer.

W systemach AIX, Linux i Solaris do zainstalowania produktu IBM DB2 można użyć komendy **db2_install**. W systemach Windows do zainstalowania produktu IBM DB2 można użyć komendy **setup.exe**.

W systemie System x Linux na 32-bitowej platformie Intel należy wybrać wersję Workspace Server Edition, wprowadzając WSE. Dla pozostałych obsługiwanych systemów operacyjnych należy wybrać wersję Enterprise Server Edition, wprowadzając ESE.

Po zainstalowaniu produktu IBM DB2 należy sprawdzić plik /tmp/db2_install_log.*XXXXX*, aby upewnić się, że instalacja zakończyła się pomyślnie. Znaki *XXXXX* reprezentują liczbę losową powiązaną z instalacją.

Więcej informacji na temat wymagań wstępnych i instancji bazy danych IBM DB2 znajduje się w dokumentacji tego produktu pod adresem http://www-01.ibm.com/support/knowledgecenter/SSEPGG/welcome.

## Parametry jądra w systemach Solaris

W systemach Solaris przed rozpoczęciem instalacji produktu IBM DB2 może być wymagane zaktualizowanie parametrów jądra w pliku /etc/system. Do określenia poprawnych parametrów jądra dla danego komputera można użyć komendy **db2osconf**. Komenda **projmod** pozwala skonfigurować parametry jądra systemu Solaris przed zainstalowaniem produktu DB2.

W systemie Solaris ze skonfigurowanymi strefami komenda **db2osconf** może być uruchamiana tylko w strefie globalnej.

Aby uzyskać więcej informacji na temat komendy **db2osconf**, wyszukaj frazę db2osconf w dokumentacji produktu IBM DB2 dostępnej pod adresem http://www-01.ibm.com/support/knowledgecenter/SSEPGG/welcome.

# Rozdział 9. Pakiet IBM Java Development Kit dla IBM Security Directory Server

Aby można było kompilować przykładowe programy napisane w języku Java oraz aby można było uruchamiać programy napisane w tym języku, takie jak Instance Administration Tool i Configuration Tool, należy wyodrębnić pakiet IBM Java Development Kit w katalogu instalacyjnym produktu IBM Security Directory Server.

Nośnik instalacyjny produktu IBM Security Directory Server zawiera obsługiwaną wersję pakietu IBM Java Development Kit, IBM Java 1.6 SR 14. Jeśli do zainstalowania produktu IBM Security Directory Server użyte zostały narzędzia systemu operacyjnego, należy zainstalować również pakiet IBM Java Development Kit.

Aby zainstalować pakiet IBM Java Development Kit, przejdź do katalogu na nośniku instalacyjnym produktu IBM Security Directory Server, który zawiera skompresowany plik IBM Java Development Kit.

Plik archiwum pakietu IBM Java Development Kit należy wyodrębnić w katalogu instalacyjnym produktu IBM Security Directory Server. Plik archiwum pakietu IBM Java Development Kit dekompresuje się w katalogu java. Więcej informacji na temat katalogu instalacyjnego produktu IBM Security Directory Server zawiera sekcja “Domyślne położenia instalacji” na stronie 27.

W systemie AIX plik archiwum pakietu IBM Java Development Kit należy wyodrębnić w katalogu instalacyjnym produktu IBM Security Directory Server, używając narzędzia GNU tar. W przeciwnym razie może być konieczne przeniesienie wyodrębnionego katalogu java do katalogu instalacyjnego produktu IBM Security Directory Server. Więcej informacji na temat pakietów wymaganych wstępnie zawiera sekcja “Pakiety wymagane wstępnie w różnych systemach operacyjnych” na stronie 15.

*Tabela 14. Pakiety IBM Java Development Kit, które są dostępne dla różnych systemów operacyjnych*

| System operacyjny | Nazwa pakietu |
|---|---|
| AIX | ibm-java-16sr14-aix-ppc-64.tar |
| System x Linux (wersja 32-bitowa) | ibm-java-16sr14-linux-i386.tar |
| Linux na platformie System i oraz System p | ibm-java-16sr14-linux-ppc-64.tar |
| Linux na platformie System z | ibm-java-16sr14-linux-s390-64.tar |
| Linux on AMD64/EM64T | ibm-java-16sr14-linux-64.tar |
| HP-UX (Itanium) | ibm-java-16sr14-hp-itanium-64.tar |
| Solaris na platformie AMD64/EM64T | ibm-java-16sr14-solaris-amd-64.tar |
| Solaris SPARC | ibm-java-16sr14-solaris-sparc-64.tar |
| Windows (wersja 32-bitowa) | ibm-java-16sr14-win-i386.zip |
| Windows na platformie AMD64/EM64T | ibm-java-16sr14-win-x86_64.zip |

## Przykłady

**Przykład 1:**

Aby wyodrębnić plik archiwum pakietu IBM Java Development Kit w katalogu instalacyjnym produktu IBM Security Directory Server, wydaj następującą komendę:

```
tar -xf ibm-java-16sr14-linux-64.tar -C /opt/ibm/ldap/V6.3.1/
```

# Rozdział 10. Instalowanie pakietu IBM Global Security Kit

Aby w produkcie IBM Security Directory Server możliwe było używanie protokołów SSL (Secure Sockets Layer) i TLS (Transaction Layer Security), należy zainstalować pakiet IBM Global Security Kit (GSKit).

Jeśli dany system operacyjny nie obsługuje instalowania z użyciem programu IBM Installation Manager, można użyć narzędzi systemowych do zainstalowania pakietu IBM Global Security Kit. Pakiet GSKit należy zainstalować zarówno na serwerze, jak i na klientach, aby można było skonfigurować i używać bezpiecznych połączeń.

Pakiet GSKit crypt jest wymagany do obsługi szyfrowania na niskim poziomie. Pakiet GSKit SSL jest wymagany w operacjach uzgadniania bezpiecznej komunikacji. Pakiet GSKit crypt jest wymaganiem wstępnym dla pakietu GSKit SSL.

Nośnik instalacyjny produktu IBM Security Directory Server zawiera następujące pakiety GSKit dla różnych systemów operacyjnych:

**Uwaga:** Nazwy pakietów GSKit dla architektur Solaris x64 i SPARC są takie same.

**AIX**

**Nazwy pakietów GSKit (wersja 64-bitowa)**
GSKit8.gskcrypt64.ppc.rte

GSKit8.gskssl64.ppc.rte

**Nazwy pakietów GSKit (wersja 32-bitowa)**
GSKit8.gskcrypt32.ppc.rte

GSKit8.gskssl32.ppc.rte

**System x Linux**

**Nazwy pakietów GSKit (wersja 32-bitowa)**
gskcrypt32-8.0.14.26.linux.x86.rpm

gskssl32-8.0.14.26.linux.x86.rpm

**Linux na platformie System z**

**Nazwy pakietów GSKit (wersja 64-bitowa)**
gskcrypt64-8.0.14.26.linux.s390x.rpm

gskssl64-8.0.14.26.linux.s390x.rpm

**Nazwy pakietów GSKit (wersja 32-bitowa)**
gskcrypt31-8.0.14.26.linux.s390.rpm

gskssl31-8.0.14.26.linux.s390.rpm

**Linux na platformie System i oraz System p**

**Nazwy pakietów GSKit (wersja 64-bitowa)**
gskcrypt64-8.0.14.26.linux.ppc.rpm

gskssl64-8.0.14.26.linux.ppc.rpm

**Nazwy pakietów GSKit (wersja 32-bitowa)**
gskcrypt32-8.0.14.26.linux.ppc.rpm

gskssl32-8.0.14.26.linux.ppc.rpm

**Linux IA64 (Itanium) i AMD64/EM64T Linux**

**Nazwy pakietów GSKit (wersja 64-bitowa)**
gskcrypt64-8.0.14.26.linux.x86_64.rpm

gskssl64-8.0.14.26.linux.x86_64.rpm

**Nazwy pakietów GSKit (wersja 32-bitowa)**
gskcrypt32-8.0.14.26.linux.x86.rpm

gskssl32-8.0.14.26.linux.x86.rpm

**Solaris**

**Nazwy pakietów GSKit (wersja 64-bitowa)**
gsk8cry64.pkg

gsk8ssl64.pkg

**Nazwy pakietów GSKit (wersja 32-bitowa)**
gsk8cry32.pkg

gsk8ssl32.pkg

**HP-UX (Itanium)**

**Nazwy pakietów GSKit (wersja 64-bitowa)**
gskcrypt64

gskssl64

**Nazwy pakietów GSKit (wersja 32-bitowa)**
gskcrypt32

gskssl32

**Microsoft Windows**

**Nazwy pakietów GSKit (wersja 64-bitowa)**
gsk8crypt64.exe

gsk8ssl64.exe

**Nazwy pakietów GSKit (wersja 32-bitowa)**
gsk8crypt32.exe

gsk8ssl32.exe

# Instalowanie pakietu IBM Global Security Kit komendą installp

Za pomocą komendy **installp** można wykonać instalację pakietu IBM Global Security Kit w systemie AIX.

## Zanim rozpoczniesz

Pliki instalacyjne pakietu IBM Global Security Kit są dostępne na nośniku instalacyjnym produktu IBM Security Directory Server. Informacje na ten temat zawiera sekcja “Przygotowanie nośnika instalacyjnego” na stronie 6.

## O tym zadaniu

W systemie AIX do zainstalowania pakietu IBM Global Security Kit (GSKit) jest używany program instalacyjny **installp**.

### Procedura

1. Zaloguj się do systemu jako użytkownik root.
2. Otwórz wiersz komend.
3. Zmień bieżący katalog roboczy na katalog gskit, w którym znajdują się pliki instalacyjne pakietu IBM Global Security Kit.
4. Uruchom komendę **installp**, aby zainstalować pakiety IBM Global Security Kit.
   a. Aby zainstalować 64-bitowe pakiety GSKit, uruchom następujące komendy:
      ```
      installp -acgXd . GSKit8.gskcrypt64.ppc.rte
      installp -acgXd . GSKit8.gskssl64.ppc.rte
      ```
   b. Aby zainstalować 32-bitowe pakiety GSKit, uruchom następujące komendy:
      ```
      installp -acgXd . GSKit8.gskcrypt32.ppc.rte
      installp -acgXd . GSKit8.gskssl32.ppc.rte
      ```
5. Uruchom następującą komendę, aby sprawdzić, czy instalacja pakietu IBM Global Security Kit powiodła się:
   ```
   lslpp -aL GSKit8*
   ```

### Wyniki

Program instalacyjny instaluje pakiet IBM Global Security Kit w następującym miejscu w systemie AIX:

**64-bitowy pakiet GSKit**
/usr/opt/ibm/gsk8_64/

**32-bitowy pakiet GSKit**
/usr/opt/ibm/gsk8/

## Instalowanie pakietu IBM Global Security Kit z użyciem programów narzędziowych w systemie Linux

Za pomocą komendy **rpm** można wykonać instalację pakietu IBM Global Security Kit w systemie Linux.

### Zanim rozpoczniesz

Pliki instalacyjne pakietu IBM Global Security Kit są dostępne na nośniku instalacyjnym produktu IBM Security Directory Server. Informacje na ten temat zawiera sekcja “Przygotowanie nośnika instalacyjnego” na stronie 6.

### O tym zadaniu

W systemie Linux do zainstalowania pakietu IBM Global Security Kit (GSKit) jest używana komenda **rpm**. W przykładzie przedstawiono instalację pakietu IBM Global Security Kit w systemie Linux AMD64 Opteron/EM64T. W przypadku systemów Linux dla System z, System i lub System p lub System x należy podstawić odpowiednie nazwy pakietów.

### Procedura

1. Zaloguj się do systemu jako użytkownik root.
2. Otwórz wiersz komend.
3. Zmień bieżący katalog roboczy na katalog gskit, w którym znajdują się pliki instalacyjne pakietu IBM Global Security Kit.
4. Uruchom komendę **rpm**, aby zainstalować pakiety IBM Global Security Kit.
   a. Aby zainstalować 64-bitowe pakiety GSKit, uruchom następujące komendy:

```
rpm -ivh gskcrypt64-8.0.14.26.linux.x86_64.rpm
rpm -ivh gskssl64-8.0.14.26.linux.x86_64.rpm
```

b. Aby zainstalować 32-bitowe pakiety GSKit, uruchom następujące komendy:

```
rpm -ivh gskcrypt32-8.0.14.26.linux.x86.rpm
rpm -ivh gskssl32-8.0.14.26.linux.x86.rpm
```

5. Uruchom następującą komendę, aby sprawdzić, czy instalacja pakietu IBM Global Security Kit powiodła się:

```
rpm -qa | grep -i gsk
```

### Wyniki

Program instalacyjny instaluje pakiet IBM Global Security Kit w następujących miejscach w systemie Linux:

**64-bitowy pakiet GSKit**
/usr/local/ibm/gsk8_64/

**32-bitowy pakiet GSKit**
/usr/local/ibm/gsk8/

## Instalowanie pakietu IBM Global Security Kit z użyciem programów narzędziowych w systemie Solaris

Za pomocą komendy **pkgadd** można wykonać instalację pakietu IBM Global Security Kit w systemie Solaris.

### Zanim rozpoczniesz

Otwórz nośnik instalacyjny produktu IBM Security Directory Server. Informacje na ten temat zawiera sekcja “Przygotowanie nośnika instalacyjnego” na stronie 6.

### O tym zadaniu

W systemie Solaris do zainstalowania pakietu IBM Global Security Kit (GSKit) jest używana komenda **pkgadd**. Nazwy pakietów i plików są takie same w systemach operacyjnych Solaris SPARC i Solaris X64.

### Procedura

1. Zaloguj się do systemu jako użytkownik root.
2. Otwórz wiersz komend.
3. Zmień bieżący katalog roboczy na katalog gskit, w którym znajdują się pliki instalacyjne pakietu IBM Global Security Kit.
4. Uruchom komendę **pkgadd**, aby zainstalować pakiety IBM Global Security Kit.
   a. Aby zainstalować 64-bitowe pakiety GSKit, uruchom następujące komendy:

```
pkgadd -d gsk8cry64.pkg
pkgadd -d gsk8ssl64.pkg
```

   b. Aby zainstalować 32-bitowe pakiety GSKit, uruchom następujące komendy:

```
pkgadd -d gsk8cry32.pkg
pkgadd -d gsk8ssl32.pkg
```

5. Uruchom następującą komendę, aby sprawdzić, czy instalacja pakietu IBM Global Security Kit powiodła się:

```
pkginfo | grep -i gsk
pkgparam nazwa_pakietu VERSION
```

Zastąp wartość nazwa_pakietu nazwą pakietu GSKit, aby sprawdzić wersję.

# Instalowanie pakietu IBM Global Security Kit z użyciem programów narzędziowych w systemie HP-UX

Za pomocą komendy **swinstall** można wykonać instalację pakietu IBM Global Security Kit w systemie HP-UX.

## Zanim rozpoczniesz

Pliki instalacyjne pakietu IBM Global Security Kit są dostępne na nośniku instalacyjnym produktu IBM Security Directory Server. Informacje na ten temat zawiera sekcja “Przygotowanie nośnika instalacyjnego” na stronie 6.

## Procedura

1. Zaloguj się do systemu jako użytkownik root.
2. Otwórz wiersz komend.
3. Zmień bieżący katalog roboczy na katalog gskit, w którym znajdują się pliki instalacyjne pakietu IBM Global Security Kit.
4. Uruchom komendę **swinstall**, aby zainstalować pakiety IBM Global Security Kit.
   a. Aby zainstalować 64-bitowe pakiety GSKit, uruchom następujące komendy:

      ```
      swinstall -s
      ścieżka_do_plików_instalacyjnych_gskit/gskcrypt64
      gskcrypt64
      swinstall -s ścieżka_do_plików_instalacyjnych_gskit/gskssl64 gskssl64
      ```

      Należy podać pełną ścieżkę pliku instalacyjnego GSKit w parametrze **-s**.
   b. Aby zainstalować 32-bitowe pakiety GSKit, uruchom następujące komendy:

      ```
      swinstall -s ścieżka_do_plików_instalacyjnych_gskit/gskcrypt32 gskcrypt32
      swinstall -s ścieżka_do_plików_instalacyjnych_gskit/gskssl32 gskssl32
      ```
5. Uruchom następującą komendę, aby sprawdzić, czy instalacja pakietu IBM Global Security Kit powiodła się:

   ```
   swlist | grep -i gsk
   ```

# Instalowanie pakietu IBM Global Security Kit w systemie Windows

Aby przeprowadzić instalację pakietu IBM Global Security Kit w systemie Windows, należy uruchomić program instalacyjny pakietu IBM Global Security Kit.

## Zanim rozpoczniesz

Pliki instalacyjne pakietu IBM Global Security Kit są dostępne na nośniku instalacyjnym produktu IBM Security Directory Server. Informacje na ten temat zawiera sekcja “Przygotowanie nośnika instalacyjnego” na stronie 6.

## O tym zadaniu

W przykładzie przedstawiono instalację 64-bitowego pakietu GSKit crypt oraz 64-bitowego pakietu GSKit SSL. W celu zainstalowania 32-bitowego pakietu GSKit należy użyć odpowiednich pakietów. W 64-bitowym systemie operacyjnym Windows można zainstalować zarówno 64-bitowe, jak i 32-bitowe pakiety GSKit.

## Procedura

1. Zaloguj się do systemu jako członek grupy administratorów.

2. Zmień bieżący katalog roboczy na katalog gskit, w którym znajdują się pliki instalacyjne pakietu IBM Global Security Kit.
3. Aby zainstalować 64-bitowe pakiety GSKit, należy uruchomić program instalacyjny GSKit.
   a. Uruchom pakiet instalacyjny GSKit8 crypt, gsk8crypt64.exe.
   b. W oknie instalacji pakietu GSKit8 wykonaj następujące kroki:
      1) Podaj ścieżkę instalacji dla pakietu GSKit8 crypt.
      2) Kliknij przycisk **Dalej**.
      3) Kliknij opcję **Instaluj**.
      4) Kliknij przycisk **Zakończ**.
   c. Uruchom pakiet instalacyjny GSKit8 SSL, gsk8ssl64.exe.
   d. W oknie instalacji pakietu GSKit8 SSL wykonaj następujące kroki:
      1) Podaj ścieżkę instalacji dla pakietu GSKit8 SSL.
      2) Kliknij przycisk **Dalej**.
      3) Kliknij opcję **Instaluj**.
      4) Kliknij przycisk **Zakończ**.
4. Aby można było uruchamiać komendy GSKit z wiersza komend, ustaw w zmiennej *PATH* katalogi bin oraz lib64 w systemie Windows x86_64.

   **Uwaga:** W 32-bitowym systemie Windows ustaw w zmiennej *PATH* katalogi bin oraz lib.
   Jeśli miejsce instalacji pakietu GSKit to C:\Program Files\IBM\gsk8, ustaw w zmiennej *PATH* następujące wartości:

   ```
   set PATH="C:\Program Files\IBM\gsk8\bin";%PATH%
   set PATH="C:\Program Files\IBM\gsk8\lib64";%PATH%
   ```

## Instalowanie pakietu IBM Global Security Kit w trybie cichym w systemie Windows

Aby przeprowadzić instalację pakietu IBM Global Security Kit w trybie cichym w systemie Windows, należy uruchomić program instalacyjny pakietu IBM Global Security Kit z wiersza komend.

### Zanim rozpoczniesz

Pliki instalacyjne pakietu IBM Global Security Kit są dostępne na nośniku instalacyjnym produktu IBM Security Directory Server. Informacje na ten temat zawiera sekcja “Przygotowanie nośnika instalacyjnego” na stronie 6.

### O tym zadaniu

W przykładzie przedstawiono instalację 64-bitowego pakietu GSKit crypt oraz 64-bitowego pakietu GSKit SSL. W celu zainstalowania 32-bitowego pakietu GSKit należy użyć odpowiednich pakietów. W 64-bitowym systemie operacyjnym Windows można zainstalować zarówno 64-bitowe, jak i 32-bitowe pakiety GSKit.

### Procedura

1. Zaloguj się do systemu jako członek grupy administratorów.
2. Otwórz wiersz komend.
3. Zmień bieżący katalog roboczy na katalog gskit, w którym znajdują się pliki instalacyjne pakietu IBM Global Security Kit.

4. Aby zainstalować 64-bitowe pakiety GSKit w trybie cichym, uruchom następujące komendy:

   ```
   gsk8crypt64.exe /s /v"/quiet"
   gsk8ssl64.exe /s /v"/quiet"
   ```

5. Aby można było uruchamiać komendy GSKit z wiersza komend, ustaw w zmiennej *PATH* katalogi bin oraz lib64 w systemie Windows x86_64.

   **Uwaga:** W 32-bitowym systemie Windows ustaw w zmiennej *PATH* katalogi bin oraz lib.
   Jeśli miejsce instalacji pakietu GSKit to C:\Program Files\IBM\gsk8, ustaw w zmiennej *PATH* następujące wartości:

   ```
   set PATH="C:\Program Files\IBM\gsk8\bin";%PATH%
   set PATH="C:\Program Files\IBM\gsk8\lib64";%PATH%
   ```

# Rozdział 11. Instalowanie pakietów językowych

Chcąc używać serwera w językach innych niż angielski, należy zainstalować odpowiednie pakiety językowe.

Program IBM Installation Manager może zainstalować wszystkie pakiety językowe, które są dostępne dla systemu operacyjnego, jeśli wybrano opcję instalacji w pełnym programie instalacyjnym. Pakiety językowe są instalowane w podkatalogu nls katalogu instalacyjnego produktu IBM Security Directory Server.

**Uwaga:** Nie trzeba instalować pakietów językowych dla klienta. Można zainstalować pakiety językowe dla klienta, jeśli komendy **idslink** i **idsrmlink** mają wyświetlać komunikaty w języku innym niż angielski. Informacje na temat komend **idslink** i **idsrmlink** zawiera *Skorowidz komend*.

Pakiety językowe można zainstalować, używając programu IBM Installation Manager albo używając programów narzędziowych systemu operacyjnego AIX lub Linux. Instalacja pakietu językowego za pomocą programu IBM Installation Manager jest możliwa w pełnym instalatorze produktu IBM Security Directory Server.

**Zapamiętaj:** Instalowanie pakietu językowego za pomocą programu IBM Installation Manager jest obsługiwana tylko w systemach AIX, Linux AMD64/EM64T i Microsoft Windows. W systemach operacyjnych, w których instalowanie produktu IBM Security Directory Server jest obsługiwane przez program IBM Installation Manager, nie można ręcznie instalować pakietów językowych za pomocą programów narzędziowych systemu operacyjnego. Jeśli w używanym systemie operacyjnym nie jest obsługiwane instalowanie pakietów językowych za pomocą programu IBM Installation Manager, do ich zainstalowania można użyć programów narzędziowych systemu operacyjnego.

*Tabela 15. Lista obsługiwanych wersji językowych w systemach AIX, Linux, Solaris i Windows*

| Języki | AIX | Linux | Solaris | Microsoft Windows |
|---|---|---|---|---|
| czeski | ✓ | | | |
| francuski | ✓ | ✓ | ✓ | ✓ |
| niemiecki | ✓ | ✓ | ✓ | ✓ |
| węgierski | ✓ | | | |
| włoski | ✓ | ✓ | ✓ | ✓ |
| japoński | ✓ | ✓ | ✓ | ✓ |
| koreański | ✓ | ✓ | ✓ | ✓ |
| polski | ✓ | | | |
| portugalski (Brazylia) | ✓ | ✓ | ✓ | ✓ |
| rosyjski | ✓ | | | |
| słowacki | ✓ | | | |
| hiszpański | ✓ | ✓ | ✓ | ✓ |
| chiński uproszczony | ✓ | ✓ | ✓ | ✓ |
| chiński tradycyjny | ✓ | ✓ | ✓ | ✓ |

# Pakiety językowe do zainstalowania

Przed zainstalowaniem pakietu językowego należy sprawdzić nazwę pakietu wybranego języka dla obsługiwanego systemu operacyjnego.

## Języki i nazwy pakietów językowych

**Zapamiętaj:** Pakiety językowe dla systemu Linux są obsługiwane w następujących architekturach:

- System x Linux
- Linux na platformie System z
- AMD64 Opteron / Intel EM64T Linux
- Linux na platformie System i oraz System p

**Zapamiętaj:** Pakiety językowe dla systemu Solaris są obsługiwane w następujących architekturach:

- Solaris SPARC
- Solaris X64

*Tabela 16. Lista obsługiwanych języków oraz nazwy pakietów językowych w systemach AIX, Linux i Solaris*

| Języki | AIX | Linux | Solaris |
|---|---|---|---|
| czeski | idsldap.msg631.cs_CZ | | |
| francuski | idsldap.msg631.fr_FR | idsldap-msg631-fr-6.3.1-0.noarch.rpm | idsldap.msg631.fr.pkg |
| niemiecki | idsldap.msg631.de_DE | idsldap-msg631-de-6.3.1-0.noarch.rpm | idsldap.msg631.de.pkg |
| węgierski | idsldap.msg631.hu_HU | | |
| włoski | idsldap.msg631.it_IT | idsldap-msg631-it-6.3.1-0.noarch.rpm | idsldap.msg631.it.pkg |
| japoński | idsldap.msg631.ja_JP | idsldap-msg631-ja-6.3.1-0.noarch.rpm | idsldap.msg631.ja.pkg |
| koreański | idsldap.msg631.ko_KO | idsldap-msg631-ko-6.3.1-0.noarch.rpm | idsldap.msg631.ko.pkg |
| polski | idsldap.msg631.pl_PL | | |
| portugalski (Brazylia) | idsldap.msg631.pt_BR | idsldap-msg631-pt_BR-6.3.1-0.noarch.rpm | idsldap.msg631.pt_BR .pkg |
| rosyjski | idsldap.msg631.ru_RU | | |
| słowacki | idsldap.msg631.sk_SK | | |
| hiszpański | idsldap.msg631.es_ES | idsldap-msg631-es-6.3.1-0.noarch.rpm | idsldap.msg631.es.pkg |
| chiński uproszczony | idsldap.msg631.zh_CN | idsldap-msg631-zh_CN-6.3.1-0.noarch.rpm | idsldap.msg631.zh_CN .pkg |
| chiński tradycyjny | idsldap.msg631.zh_TW | idsldap-msg631-zh_TW-6.3.1-0.noarch.rpm | idsldap.msg631.zh_TW .pkg |

# Instalowanie pakietów językowych za pomocą programów narzędziowych systemu operacyjnego

Jeśli system operacyjny nie obsługuje instalacji z użyciem programu IBM Installation Manager, do zainstalowania pakietów językowych należy użyć programów narzędziowych systemu operacyjnego.

## Zanim rozpoczniesz

Należy przygotować nośniki instalacyjne produktu IBM Security Directory Server. Informacje na ten temat zawiera sekcja “Przygotowanie nośnika instalacyjnego” na stronie 6.

## O tym zadaniu

Chcąc używać serwera w językach innych niż angielski, należy zainstalować odpowiednie pakiety językowe.

## Procedura

1. Zaloguj się do systemu jako użytkownik root.
2. Otwórz wiersz komend.
3. Zmień bieżący katalog roboczy na katalog, w którym znajdują się pliki instalacyjne produktu IBM Security Directory Server.
4. Przejdź do podkatalogu tdsLangpack.
5. Aby zainstalować pakiet językowy dla języka, uruchom komendy instalacji pakietu. W poniższym przykładzie przedstawiona została instalacja pakietu językowego dla języka francuskiego. Zastępując odpowiednią nazwę pakietu dla systemu operacyjnego, można zainstalować dowolny pakiet językowy.

| **System operacyjny** | **Komenda do uruchomienia:** |
|---|---|
| **AIX** | installp -acgXd . idsldap.msg631.fr_FR |
| **Linux** | rpm -ivh idsldap-msg631-fr-6.3.1-0.noarch.rpm |
| **Solaris** | pkgadd -d idsldap.msg631.fr.pkg |

6. Sprawdź, czy instalacja pakietu językowego zakończyła się pomyślnie. Aby uzyskać więcej informacji, patrz sekcja “Weryfikowanie pakietów serwera katalogów IBM Security” na stronie 85.

## Wyniki

Program instalacyjny instaluje pakiety językowe w następujących katalogach:

*Tabela 17. Domyślne miejsce instalacji pakietów językowych produktu IBM Security Directory Server*

| **System operacyjny** | **Miejsce instalacji pakietu językowego** |
|---|---|
| Linux | /opt/ibm/ldap/V6.3.1/nls/msg |
| AIX i Solaris | /opt/IBM/ldap/V6.3.1/nls/msg |

# Rozdział 12. Instalowanie z użyciem programów narzędziowych systemu operacyjnego

Instalację produktu IBM Security Directory Server można przeprowadzić z użyciem komend systemowych, jeśli środowisko graficzne (X11) nie jest dostępne.

**UWAGA:**

- **Nie można stosować różnych trybów instalacji na jednym komputerze. Komponenty produktu IBM Security Directory Server należy zainstalować albo za pomocą programu IBM Installation Manager, albo za pomocą narzędzi systemu operacyjnego. Jeśli zostaną pomieszane oba typy instalacji, mogą nie zostać zainstalowane wszystkie poprawne pakiety komponentu.**
- **Należy unikać ręcznej instalacji bazy danych DB2 i wbudowanego serwera WebSphere Application Server w domyślnych ścieżkach instalacji używanych przez program IBM Installation Manager. Tego typu instalacja ręczna może spowodować niepowodzenie instalacji, modyfikacji lub deinstalacji w programie IBM Installation Manager. Więcej informacji na temat domyślnych ścieżek instalacji zawiera sekcja "Domyślne położenia instalacji" na stronie 27.**

Przed zainstalowaniem produktu IBM Security Directory Server należy uzyskać odpowiednie źródło instalacyjne. Produkt IBM Security Directory Server dostępny jest w postaci plików archiwum i jako obraz instalacyjny. Z obrazu instalacyjnego można utworzyć instalacyjne dyski DVD.

Należy przygotować nośnik instalacyjny. Aby uzyskać więcej informacji, patrz "Przygotowanie nośnika instalacyjnego" na stronie 6.

**Ważne:** Aby użyć produktu IBM Security Directory Server jako pełnego serwera katalogów, zainstaluj obsługiwaną wersję produktu IBM DB2 na komputerze, jeśli nie jest jeszcze zainstalowany. W pliku ldapdb.properties należy podać ścieżkę i wersję produktu IBM DB2.

## Instalowanie z użyciem programów narzędziowych w systemie AIX

Do zainstalowania produktu IBM Security Directory Server w systemie AIX można użyć narzędzi wiersza komend.

Do zainstalowania produktu IBM Security Directory Server można użyć jednego z następujących narzędzi:

**SMIT** Jest to preferowana metoda instalacji. Aby uzyskać więcej informacji, patrz "Instalacja za pomocą programu SMIT" na stronie 70.

**installp**
Aby uzyskać więcej informacji, patrz "Instalowanie za pomocą komendy **installp**" na stronie 71.

### Pakiety przeznaczone do instalacji w systemie AIX

Aby użyć produktu IBM Security Directory Server jako pełnego serwera katalogów, serwera proxy lub klienta w systemie AIX, należy zainstalować odpowiednie pakiety.

## Pakiety i zestawy plików

Produkt IBM Security Directory Server zawiera pakiety dla systemu AIX. Każdy pakiet zawiera jeden lub kilka zestawów plików.

*Tabela 18. Pakiety i zestawy plików znajdujące się w pakietach*

| Pakiety | Zestawy plików powiązanych z pakietem |
|---|---|
| idsldap.license631 | idsldap.license631.rte - licencja |
| idsldap.cltbase631 | • idsldap.cltbase631.rte - pliki wykonawcze klienta podstawowego<br>• idsldap.cltbase631.adt - pakiet SDK klienta podstawowego |
| idsldap.clt32bit631 | • idsldap.clt32bit631.rte - 32-bitowy pakiet klienta C (bez protokołów SSL i TLS) |
| idsldap.clt64bit631 | • idsldap.clt64bit631.rte - 64-bitowy pakiet klienta C (bez protokołów SSL i TLS) |
| idsldap.clt_max_crypto32bit631 | • idsldap.clt_max_crypto32bit631.rte - 32-bitowy pakiet klienta C (z protokołami SSL i TLS) |
| idsldap.clt_max_crypto64bit631 | • idsldap.clt_max_crypto64bit631.rte - 64-bitowy pakiet klienta C (z protokołami SSL i TLS) |
| idsldap.cltjava631 | • idsldap.cltjava631.rte - Java Client |
| idsldap.srvbase64bit631 | • idsldap.srvbase64bit631.rte - serwer podstawowy |
| idsldap.srv_max_cryptobase64bit631 | • idsldap.srv_max_cryptobase64bit631.rte - serwer podstawowy (SSL) |
| idsldap.srvproxy64bit631 | • idsldap.srvproxy64bit631.rte - serwer proxy (64-bitowy) |
| idsldap.srv64bit631 | • idsldap.srv64bit631.rte - serwer katalogów (64-bitowy) |
| idsldap.webadmin631 | • idsldap.webadmin631.rte - narzędzie Web Administration Tool (bez protokołów SSL i TLS) |
| idsldap.webadmin_max_crypto631 | • idsldap.webadmin_max_crypto631.rte - narzędzie Web Administration Tool (z protokołami SSL i TLS) |
| idsldap.msg631.en_US | Niedostępne |
| idsldap.ent631 | • idsldap.ent631.rte - IBM Directory Server Entitlement (dostępne tylko w serwisie Passport Advantage) |

## Kolejność instalowania

Wszystkie funkcje można zainstalować jednocześnie. Jeśli będą one instalowane oddzielnie, należy instalować je w określonej kolejności.

**Ważne:**

- Aby używać protokołu SSL (Secure Socket Layer) lub TLS (Transport Layer Security), należy zainstalować obsługiwaną wersję pakietu IBM Global Security Kit.
- Aby w systemie AIX używać protokołu Kerberos, wymagana jest obsługiwana wersja usługi Network Authentication Service.

**Uwaga:** Jeśli komputer nie obsługuje systemu X11, można pominąć instalowanie komponentu JDK dostępnego w pakiecie IBM JDK. Jeśli komponent JDK nie jest zainstalowany, może nie być możliwe zainstalowanie narzędzi Instance Administration Tool i Configuration Tool.

*Tabela 19. Kolejność instalacji funkcji klienta*

| Klient 32-bitowy (bez protokołów SSL i TLS) | Klient 32-bitowy (z protokołami SSL i TLS) | Klient 64-bitowy (bez protokołów SSL i TLS) | Klient 64-bitowy (z protokołami SSL i TLS) |
|---|---|---|---|
| 1. idsldap.cltbase631<br>2. idsldap.clt32bit631<br>3. idsldap.cltjava631 | 1. idsldap.cltbase631<br>2. idsldap.clt32bit631<br>3. idsldap.clt_max_crypto32bit631<br>4. idsldap.cltjava631 | 1. idsldap.cltbase631<br>2. idsldap.clt64bit631<br>3. idsldap.cltjava631 | 1. idsldap.cltbase631<br>2. idsldap.clt64bit631<br>3. idsldap.clt_max_crypto32bit631<br>4. idsldap.cltjava631 |

**Uwaga:** Jeśli używane jest środowisko klient-serwer z upoważnieniami w pliku archiwum lub obraz ISO z upoważnieniami do instalacji produktu IBM Security Directory Server, należy najpierw zaakceptować warunki licencji i zainstalować pakiet idsldap.license631.

*Tabela 20. Kolejność instalacji funkcji pełnego serwera katalogów*

| 64-bitowy pełny serwer katalogów (bez protokołów SSL i TLS) | 64-bitowy pełny serwer katalogów (z protokołami SSL i TLS) |
|---|---|
| 1. idsldap.license631<br>2. idsldap.cltbase631<br>3. idsldap.clt64bit631<br>4. idsldap.cltjava631<br>5. idsldap.srvbase64bit631<br>6. idsldap.srv64bit631<br>7. idsldap.msg631.en_US<br>8. idsldap.ent631 | 1. idsldap.license631<br>2. idsldap.cltbase631<br>3. idsldap.clt64bit631<br>4. idsldap.clt_max_crypto64bit631<br>5. idsldap.cltjava631<br>6. idsldap.srvbase64bit631<br>7. idsldap.srv_max_cryptobase64bit631<br>8. idsldap.srv64bit631<br>9. idsldap.msg631.en_US<br>10. idsldap.ent631 |

*Tabela 21. Kolejność instalacji funkcji serwera proxy*

| 64-bitowy serwer proxy (bez protokołów SSL i TLS) | 64-bitowy serwer proxy (z protokołami SSL i TLS) |
|---|---|
| 1. idsldap.license631<br>2. idsldap.cltbase631<br>3. idsldap.clt64bit631<br>4. idsldap.cltjava631<br>5. idsldap.srvbase64bit631<br>6. idsldap.srvproxy64bit631<br>7. idsldap.msg631.en_US<br>8. idsldap.ent631 | 1. idsldap.license631<br>2. idsldap.cltbase631<br>3. idsldap.clt64bit631<br>4. idsldap.clt_max_crypto64bit631<br>5. idsldap.cltjava631<br>6. idsldap.srvbase64bit631<br>7. idsldap.srv_max_cryptobase64bit631<br>8. idsldap.srvproxy64bit631<br>9. idsldap.msg631.en_US<br>10. idsldap.ent631 |

**Uwaga:** Aby użyć narzędzia Web Administration Tool, należy je wdrożyć w serwerze aplikacji WWW. Więcej informacji na temat instalowania wbudowanego serwera WebSphere Application Server, znajduje się w sekcji “Samodzielne instalowanie wbudowanego serwera WebSphere Application Server” na stronie 109.

*Tabela 22. Pakiet instalacyjny Web Administration Tool*

| Web Administration Tool (bez protokołów SSL i TLS) | Web Administration Tool (z protokołami SSL i TLS) |
|---|---|
| 1. idsldap.license631<br>2. idsldap.webadmin631 | 1. idsldap.license631<br>2. idsldap.webadmin_max_crypto631 |

Podczas instalowania narzędzia Web Administration Tool, na komputer są również kopiowane pliki języka DSML (Directory Services Markup Language). Więcej informacji na temat języka DSML zawiera sekcja Dodatek A, “Język DSML”, na stronie 243.

# Instalacja za pomocą programu SMIT

Za pomocą komendy **smit** można wykonać instalację produktu IBM Security Directory Server w systemie AIX.

## Zanim rozpoczniesz

Należy przygotować nośnik instalacyjny produktu IBM Security Directory Server. Informacje na ten temat zawiera sekcja “Przygotowanie nośnika instalacyjnego” na stronie 6.

## O tym zadaniu

Program instalacyjny **smit** instaluje produkt IBM Security Directory Server w systemie AIX. Jeśli w systemie jest zainstalowana obsługiwana wersja bazy danych IBM DB2, proces instalacji zaktualizuje w pliku ldapdb.properties nazwę ścieżki i wersję bazy DB2.

## Procedura

1. Zaloguj się do systemu jako użytkownik root.
2. Otwórz wiersz komend.
3. Uruchom komendę **idsLicense**.

   ```
   ./idsLicense
   ```
4. Jeśli akceptujesz warunki umowy licencyjnej, wpisz 1. Dostępne są następujące opcje:
   - 1: zaakceptowanie umowy licencyjnej.
   - 2: odrzucenie umowy licencyjnej i zakończenie instalacji.
   - 3: wydrukowanie umowy licencyjnej.
   - 4: wyświetlenie warunków firm innych niż IBM znajdujących się w umowie licencyjnej.
   - 99: powrót do poprzedniego ekranu.

   Po zaakceptowaniu warunków umowy licencyjnej w katalogu instalacyjnym produktu IBM Security Directory Server zostanie utworzony plik LAPID i folder license. Folder license zawiera pliki licencji produktu IBM Security Directory Server we wszystkich obsługiwanych językach.

   **Ważne:** Nie modyfikuj i nie usuwaj pliku LAPID oraz plików licencji w folderze license.
5. Uruchom komendę **smit install**. Zostanie otwarte okno **Instalacja i konserwacja oprogramowania**.
6. Kliknij kolejno opcje **Instalacja i aktualizacja oprogramowania** > **Instalacja i aktualizacja z całego dostępnego oprogramowania**.
7. Wybierz nośnik instalacyjny.
   - W przypadku instalowania z dysku DVD, wykonaj następujące czynności:
     a. Kliknij opcję **Lista**, aby uzyskać dostęp do urządzenia, które zawiera obrazy programu IBM Security Directory Server.
   - Przy instalowaniu z nieskompresowanego pliku archiwum, wpisz . w polu **Wejściowe urządzenie/katalog oprogramowania**.
8. Kliknij przycisk **Wykonaj**.
9. Przesuń kursor do sekcji **Oprogramowanie do zainstalowania** i wykonaj następujące czynności:

a. Aby zainstalować zestaw plików idsldap, wpisz idsldap.
b. Kliknij przycisk **Lista**, aby wyświetlić wszystkie zestawy plików i wybierz plik zestawów, które chcesz zainstalować.
c. Kliknij przycisk **OK**.

10. Aby rozpocząć instalację, kliknij przycisk **OK**.
11. Sprawdź podsumowanie instalacji na końcu danych wyjściowych, aby zweryfikować pomyślną instalację zestawów plików.
12. Po zakończeniu instalacji kliknij przycisk **Gotowe**.
13. Aby zakończyć działanie programu **SMIT**, naciśnij klawisz F12.
14. Sprawdź, czy instalacja produktu IBM Security Directory Server powiodła się. Aby uzyskać więcej informacji, patrz sekcja “Weryfikowanie pakietów serwera katalogów IBM Security” na stronie 85.

### Wyniki

Program instalacyjny zainstalował produkt IBM Security Directory Server w katalogu /opt/IBM/ldap/V6.3.1 w systemie AIX. Jeśli w systemie jest zainstalowana obsługiwana wersja bazy danych IBM DB2, proces instalacji zaktualizuje w pliku ldapdb.properties nazwę ścieżki i wersję bazy DB2.

### Co dalej

Po zainstalowaniu produktu IBM Security Directory Server należy wykonać następujące działanie:

- Aby użyć produktu IBM Security Directory Server jako pełnego serwera katalogów, utwórz instancję serwera katalogów. Patrz sekcja “Tworzenie instancji serwera katalogów” na stronie 134.
- Aby użyć produktu IBM Security Directory Server jako serwera proxy, utwórz instancję serwera proxy. Patrz sekcja “Tworzenie instancji serwera proxy z własnymi ustawieniami” na stronie 142.

## Instalowanie za pomocą komendy installp

Za pomocą komendy **installp** wykonaj instalację produktu IBM Security Directory Server w systemie AIX.

### Zanim rozpoczniesz

Należy przygotować nośniki instalacyjne produktu IBM Security Directory Server. Informacje na ten temat zawiera sekcja “Przygotowanie nośnika instalacyjnego” na stronie 6.

### O tym zadaniu

Program instalacyjny **installp** instaluje produkt IBM Security Directory Server w systemie AIX. Jeśli w systemie jest zainstalowana obsługiwana wersja bazy danych IBM DB2, proces instalacji zaktualizuje w pliku ldapdb.properties nazwę ścieżki i wersję bazy DB2.

### Procedura

1. Zaloguj się do systemu jako użytkownik root.
2. Otwórz wiersz komend.
3. Zmień bieżący katalog roboczy na katalog, w którym znajdują się pliki instalacyjne produktu IBM Security Directory Server.
4. Uruchom komendę **idsLicense**.

```
./idsLicense
```

5. Jeśli akceptujesz warunki umowy licencyjnej, wpisz 1. Dostępne są następujące opcje:
   - 1: zaakceptowanie umowy licencyjnej.
   - 2: odrzucenie umowy licencyjnej i zakończenie instalacji.
   - 3: wydrukowanie umowy licencyjnej.
   - 4: wyświetlenie warunków firm innych niż IBM znajdujących się w umowie licencyjnej.
   - 99: powrót do poprzedniego ekranu.

   Po zaakceptowaniu warunków umowy licencyjnej w katalogu instalacyjnym produktu IBM Security Directory Server zostanie utworzony plik LAPID i folder license. Folder license zawiera pliki licencji produktu IBM Security Directory Server we wszystkich obsługiwanych językach.

   **Ważne:** Nie modyfikuj i nie usuwaj pliku LAPID oraz plików licencji w folderze license.
6. Określ, które pakiety produktu IBM Security Directory Server mają zostać zainstalowane.
   ```
   installp -ld . | grep idsldap
   ```

   Zostanie wyświetlona lista wszystkich pakietów IBM Security Directory Server możliwych do zainstalowania.
7. Aby zainstalować pakiety, wykonaj następującą komendę:
   ```
   installp -acgXd . nazwy_pakietów
   ```

   Aby zainstalować wszystkie pakiety IBM Security Directory Server znajdujące się w bieżącej ścieżce, wykonaj następującą komendę:
   ```
   installp -acgXd . idsldap
   ```
8. Po zakończeniu instalacji system utworzy podsumowanie instalacji.
9. Sprawdź, czy instalacja produktu IBM Security Directory Server powiodła się. Aby uzyskać więcej informacji, patrz sekcja “Weryfikowanie pakietów serwera katalogów IBM Security” na stronie 85.

### Wyniki

Program instalacyjny zainstalował produkt IBM Security Directory Server w katalogu /opt/IBM/ldap/V6.3.1 w systemie AIX. Jeśli w systemie jest zainstalowana obsługiwana wersja bazy danych IBM DB2, proces instalacji zaktualizuje w pliku ldapdb.properties nazwę ścieżki i wersję bazy DB2.

### Co dalej

Po zainstalowaniu produktu IBM Security Directory Server należy wykonać następujące działania:

- Aby użyć produktu IBM Security Directory Server jako pełnego serwera katalogów, utwórz instancję serwera katalogów. Aby uzyskać więcej informacji, patrz “Tworzenie instancji serwera katalogów” na stronie 134.
- Aby użyć produktu IBM Security Directory Server jako serwera proxy, utwórz instancję serwera proxy. Aby uzyskać więcej informacji, patrz “Tworzenie instancji serwera proxy z własnymi ustawieniami” na stronie 142.

## Instalowanie z użyciem programów narzędziowych w systemie Linux

Do zainstalowania produktu IBM Security Directory Server w systemie Linux można użyć narzędzi wiersza komend.

Produkt IBM Security Directory Server składa się z różnych pakietów dla komputerów z różnymi systemami operacyjnymi i architekturami. Do instalacji na danym komputerze należy wybrać odpowiednie pakiety. Więcej informacji na temat nazw pakietów zawiera sekcja “Pakiety przeznaczone do instalacji w systemie Linux”.

# Pakiety przeznaczone do instalacji w systemie Linux

Aby użyć produktu IBM Security Directory Server jako pełnego serwera katalogów, serwera proxy lub klienta w systemie Linux, należy zainstalować odpowiednie pakiety.

## Pakiety przeznaczone dla różnych wersji systemów Linux

*Tabela 23. Pakiety dostarczane z produktem IBM Security Directory Server dla różnych systemów Linux*

| Pakiety produktu IBM Security Directory Server | AMD64 Opteron/EM64T Linux | System i lub System p | System x | System z |
|---|---|---|---|---|
| IBM Directory Server - licencja | idsldap-license631-6.3.1-0.x86_64.rpm | idsldap-license631-6.3.1-0.ppc.rpm | idsldap-license631-6.3.1-0.i386.rpm | idsldap-license631-6.3.1-0.s390.rpm |
| IBM Directory Server - klient podstawowy | idsldap-cltbase631-6.3.1-0.x86_64.rpm | idsldap-cltbase631-6.3.1-0.ppc.rpm | idsldap-cltbase631-6.3.1-0.i386.rpm | idsldap-cltbase631-6.3.1-0.s390.rpm |
| IBM Directory Server - klient 32-bitowy | idsldap-clt32bit631-6.3.1-0.x86_64.rpm | idsldap-clt32bit631-6.3.1-0.ppc.rpm | idsldap-clt32bit631-6.3.1-0.i386.rpm | idsldap-clt32bit631-6.3.1-0.s390.rpm |
| IBM Directory Server - klient 64-bitowy | idsldap-clt64bit631-6.3.1-0.x86_64.rpm | idsldap-clt64bit631-6.3.1-0.ppc64.rpm | Niedostępne | idsldap-clt64bit631-6.3.1-0.s390x.rpm |
| IBM Directory Server - klient Java | idsldap-cltjava631-6.3.1-0.x86_64.rpm | idsldap-cltjava631-6.3.1-0.ppc.rpm | idsldap-cltjava631-6.3.1-0.i386.rpm | idsldap-cltjava631-6.3.1-0.s390.rpm |
| IBM Directory Server - serwer podstawowy | idsldap-srvbase64bit631-6.3.1-0.x86_64.rpm | idsldap-srvbase64bit631-6.3.1-0.ppc64.rpm | idsldap-srvbase32bit631-6.3.1-0.i386.rpm | idsldap-srvbase64bit631-6.3.1-0.s390x.rpm |
| IBM Directory Server - serwer proxy | idsldap-srvproxy64bit631-6.3.1-0.x86_64.rpm | idsldap-srvproxy64bit631-6.3.1-0.ppc64.rpm | idsldap-srvproxy32bit631-6.3.1-0.i386.rpm | idsldap-srvproxy64bit631-6.3.1-0.s390x.rpm |
| IBM Directory Server - serwer 32-bitowy | Niedostępne | Niedostępne | idsldap-srv32bit631-6.3.1-0.i386.rpm | Niedostępne |
| IBM Directory Server - serwer 64-bitowy | idsldap-srv64bit631-6.3.1-0.x86_64.rpm | idsldap-srv64bit631-6.3.1-0.ppc64.rpm | Niedostępne | idsldap-srv64bit631-6.3.1-0.s390x.rpm |
| IBM Directory Server - Web Administration Tool | idsldap-webadmin631-6.3.1-0.x86_64.rpm | idsldap-webadmin631-6.3.1-0.ppc.rpm | idsldap-webadmin631-6.3.1-0.i386.rpm | idsldap-webadmin631-6.3.1-0.s390.rpm |
| IBM Directory Server - komunikaty w języku angielskim | idsldap-msg631-en-6.3.1-0.x86_64.rpm | idsldap-msg631-en-6.3.1-0.ppc.rpm | idsldap-msg631-en-6.3.1-0.i386.rpm | idsldap-msg631-en-6.3.1-0.s390.rpm |
| IBM Directory Server Entitlement (dostępne tylko w serwisie Passport Advantage) | idsldap-ent631-6.3.1-0.x86_64.rpm | idsldap-ent631-6.3.1-0.ppc.rpm | idsldap-ent631-6.3.1-0.i386.rpm | idsldap-ent631-6.3.1-0.s390.rpm |

## Zależności pakietów

Aby zainstalować niektóre pakiety, należy najpierw zainstalować zależności.

**Uwaga:** Jeśli używane jest środowisko klient-serwer z upoważnieniami w pliku archiwum lub obraz ISO z upoważnieniami do instalacji produktu IBM Security Directory Server, należy najpierw zaakceptować warunki licencji i zainstalować pakiet idsldap-license631-6.3.1-0.*arch*.rpm.

W tabeli przedstawione są zależności AMD64 Opteron/EM64T Linux. W systemach System z, System i, System p oraz System x Linux należy podstawić odpowiednie nazwy pakietów.

*Tabela 24. Pakiet i jego pakiety zależne*

| Nazwa pakietu | Zależy od |
|---|---|
| idsldap-clt32bit631-6.3.1-0.x86_64.rpm | idsldap-cltbase631-6.3.1-0.x86_64.rpm |
| idsldap-clt64bit631-6.3.1-0.x86_64.rpm | idsldap-cltbase631-6.3.1-0.x86_64.rpm |
| idsldap-srvbase64bit631-6.3.1-0.x86_64.rpm | 1. idsldap-license631-6.3.1-0.x86_64.rpm<br>2. idsldap-cltbase631-6.3.1-0.x86_64.rpm<br>3. idsldap-clt64bit631-6.3.1-0.x86_64.rpm |
| idsldap-srv64bit631-6.3.1-0.x86_64.rpm | 1. idsldap-license631-6.3.1-0.x86_64.rpm<br>2. idsldap-cltbase631-6.3.1-0.x86_64.rpm<br>3. idsldap-clt64bit631-6.3.1-0.x86_64.rpm<br>4. idsldap-srvbase64bit631-6.3.1-0.x86_64.rpm |
| idsldap-srvproxy64bit631-6.3.1-0.x86_64.rpm | 1. idsldap-license631-6.3.1-0.x86_64.rpm<br>2. idsldap-cltbase631-6.3.1-0.x86_64.rpm<br>3. idsldap-clt64bit631-6.3.1-0.x86_64.rpm<br>4. idsldap-srvbase64bit631-6.3.1-0.x86_64.rpm |

## Kolejność instalowania

Wszystkie funkcje można zainstalować jednocześnie. Jeśli będą one instalowane oddzielnie, należy instalować je w określonej kolejności.

**Ważne:** Aby używać protokołu SSL (Secure Socket Layer) lub TLS (Transport Layer Security), należy zainstalować obsługiwaną wersję pakietu IBM Global Security Kit.

W przykładowej kolejności instalowania użyto pakietów dla systemu AMD64 Opteron/EM64T Linux. W systemach System z, System i, System p oraz System x Linux należy podstawić odpowiednie nazwy pakietów.

*Tabela 25. Kolejność instalacji funkcji klienta*

| Klient 32-bitowy | Klient 64-bitowy |
|---|---|
| 1. idsldap-cltbase631-6.3.1-0.x86_64.rpm<br>2. idsldap-clt32bit631-6.3.1-0.x86_64.rpm<br>3. idsldap-cltjava631-6.3.1-0.x86_64.rpm | 1. idsldap-cltbase631-6.3.1-0.x86_64.rpm<br>2. idsldap-clt64bit631-6.3.1-0.x86_64.rpm<br>3. idsldap-cltjava631-6.3.1-0.x86_64.rpm |

*Tabela 26. Kolejność instalacji funkcji pełnego serwera katalogów i serwera proxy*

| Pełny 64-bitowy serwer katalogów | 64-bitowy serwer proxy |
|---|---|
| 1. idsldap-license631-6.3.1-0.x86_64.rpm<br>2. idsldap-cltbase631-6.3.1-0.x86_64.rpm<br>3. idsldap-clt64bit631-6.3.1-0.x86_64.rpm<br>4. idsldap-cltjava631-6.3.1-0.x86_64.rpm<br>5. idsldap-srvbase64bit631-6.3.1-0.x86_64.rpm<br>6. idsldap-srv64bit631-6.3.1-0.x86_64.rpm<br>7. idsldap-msg631-en-6.3.1-0.x86_64.rpm<br>8. idsldap-ent631-6.3.1-0.x86_64.rpm | 1. idsldap-license631-6.3.1-0.x86_64.rpm<br>2. idsldap-cltbase631-6.3.1-0.x86_64.rpm<br>3. idsldap-clt64bit631-6.3.1-0.x86_64.rpm<br>4. idsldap-cltjava631-6.3.1-0.x86_64.rpm<br>5. idsldap-srvbase64bit631-6.3.1-0.x86_64.rpm<br>6. idsldap-srvproxy64bit631-6.3.1-0.x86_64.rpm<br>7. idsldap-msg631-en-6.3.1-0.x86_64.rpm<br>8. idsldap-ent631-6.3.1-0.x86_64.rpm |

**Uwaga:** Aby użyć narzędzia Web Administration Tool, należy je wdrożyć w serwerze aplikacji WWW. Więcej informacji na temat instalowania wbudowanego serwera WebSphere

Application Server, znajduje się w sekcji “Samodzielne instalowanie wbudowanego serwera WebSphere Application Server” na stronie 109.

*Tabela 27. Pakiet instalacyjny Web Administration Tool*

| **Web Administration Tool** |
| --- |
| 1. idsldap-license631-6.3.1-0.x86_64.rpm<br>2. idsldap-webadmin631-6.3.1-0.x86_64.rpm |

Podczas instalowania narzędzia Web Administration Tool, na komputer są również kopiowane pliki języka DSML (Directory Services Markup Language). Więcej informacji na temat języka DSML zawiera sekcja Dodatek A, “Język DSML”, na stronie 243.

# Instalowanie z użyciem programów narzędziowych w systemie Linux

Za pomocą komendy **rpm** wykonaj instalację produktu IBM Security Directory Server w systemie Linux.

## Zanim rozpoczniesz

Należy przygotować nośniki instalacyjne produktu IBM Security Directory Server. Informacje na ten temat zawiera sekcja “Przygotowanie nośnika instalacyjnego” na stronie 6.

## O tym zadaniu

Program instalacyjny **rpm** instaluje produkt IBM Security Directory Server w systemie Linux. Jeśli w systemie jest zainstalowana obsługiwana wersja bazy danych IBM DB2, proces instalacji zaktualizuje w pliku ldapdb.properties nazwę ścieżki i wersję bazy DB2.

## Procedura

1. Zaloguj się do systemu jako użytkownik root.
2. Otwórz wiersz komend.
3. Zmień bieżący katalog roboczy na katalog, w którym znajdują się pliki instalacyjne produktu IBM Security Directory Server.
4. Uruchom komendę **idsLicense**.

   ```
   ./idsLicense
   ```
5. Jeśli akceptujesz warunki umowy licencyjnej, wpisz 1. Dostępne są następujące opcje:
   - 1: zaakceptowanie umowy licencyjnej.
   - 2: odrzucenie umowy licencyjnej i zakończenie instalacji.
   - 3: wydrukowanie umowy licencyjnej.
   - 4: wyświetlenie warunków firm innych niż IBM znajdujących się w umowie licencyjnej.
   - 99: powrót do poprzedniego ekranu.

   Po zaakceptowaniu warunków umowy licencyjnej w katalogu instalacyjnym produktu IBM Security Directory Server zostanie utworzony plik LAPID i folder license. Folder license zawiera pliki licencji produktu IBM Security Directory Server we wszystkich obsługiwanych językach.

   **Ważne:** Nie modyfikuj i nie usuwaj pliku LAPID oraz plików licencji w folderze license.
6. Aby zainstalować pakiet, wykonaj następującą komendę:

   ```
   rpm -ivh nazwa_pakietu
   ```

Aby zainstalować wszystkie pakiety IBM Security Directory Server, wykonaj następującą komendę:

```
rpm -ivh idsldap*
```

7. Sprawdź, czy instalacja produktu IBM Security Directory Server powiodła się. Aby uzyskać więcej informacji, patrz sekcja “Weryfikowanie pakietów serwera katalogów IBM Security” na stronie 85.

### Wyniki

Program instalacyjny zainstalował produkt IBM Security Directory Server w katalogu /opt/ibm/ldap/V6.3.1 w systemie Linux. Jeśli w systemie jest zainstalowana obsługiwana wersja bazy danych IBM DB2, proces instalacji zaktualizuje w pliku ldapdb.properties nazwę ścieżki i wersję bazy DB2.

### Co dalej

Po zainstalowaniu produktu IBM Security Directory Server należy wykonać następujące działania:

- Aby użyć produktu IBM Security Directory Server jako pełnego serwera katalogów, utwórz instancję serwera katalogów. Aby uzyskać więcej informacji, patrz “Tworzenie instancji serwera katalogów” na stronie 134.
- Aby użyć produktu IBM Security Directory Server jako serwera proxy, utwórz instancję serwera proxy. Aby uzyskać więcej informacji, patrz “Tworzenie instancji serwera proxy z własnymi ustawieniami” na stronie 142.

## Instalowanie z użyciem programów narzędziowych w systemie Solaris

Do zainstalowania produktu IBM Security Directory Server w systemie Solaris można użyć narzędzi wiersza komend.

Produkt IBM Security Directory Server składa się z tych samych pakietów dla komputerów o różnej architekturze. Dostępne są pakiety dla systemów operacyjnych Sun SPARC Solaris i Solaris z procesorami AMD64 Opteron/EM64T. Nazwy pakietów i plików są takie same dla obu systemów. Więcej informacji na temat nazw pakietów zawiera sekcja “Pakiety przeznaczone do instalacji w systemie Solaris”.

Podczas instalowania pakietów produktu IBM Security Directory Server nie można używać systemowej wartości domyślnej ALL. Wybranie wszystkich (ALL) pakietów spowoduje, że pakiety będą instalowane w niepoprawnej kolejności i instalacja się nie powiedzie.

## Pakiety przeznaczone do instalacji w systemie Solaris

Aby użyć produktu IBM Security Directory Server jako pełnego serwera katalogów, serwera proxy lub klienta w systemie Solaris, należy zainstalować odpowiednie pakiety.

### Pakiety przeznaczone dla systemu Solaris

**Ważne:** Nazwy pakietów i plików są takie same dla obu systemów operacyjnych Solaris SPARC i AMD64 Opteron/EM64T Solaris.

*Tabela 28. Pakiety dostarczane z produktem IBM Security Directory Server dla systemów Solaris.*

| Pakiety produktu IBM Security Directory Server | Nazwy pakietów | Nazwa pliku |
|---|---|---|
| IBM Directory Server - licencja | IDSllicense631 | idsldap-license631.pkg |

*Tabela 28. Pakiety dostarczane z produktem IBM Security Directory Server dla systemów Solaris. (kontynuacja)*

| Pakiety produktu IBM Security Directory Server | Nazwy pakietów | Nazwa pliku |
|---|---|---|
| IBM Directory Server - klient podstawowy | IDSlbc631 | idsldap.cltbase631.pkg |
| IBM Directory Server - klient 32-bitowy | IDSl32c631 | idsldap.clt32bit631.pkg |
| IBM Directory Server - klient 64-bitowy | IDSl64c631 | idsldap.clt64bit631.pkg |
| IBM Directory Server - klient Java | IDSljc631 | idsldap.cltjava631.pkg |
| IBM Directory Server - serwer podstawowy | IDSlbs631 | idsldap.srvbase64bit631.pkg |
| IBM Directory Server - serwer proxy | IDSl64p631 | idsldap.srvproxy64bit631.pkg |
| IBM Directory Server - serwer 64-bitowy | IDSl64s631 | idsldap.srv64bit631.pkg |
| IBM Directory Server - Web Administration Tool | IDSlweb631 | idsldap.webadmin631.pkg |
| IBM Directory Server - komunikaty w języku angielskim | IDSlen631 | idsldap.msg631.en.pkg |
| IBM Directory Server Entitlement (dostępne tylko w serwisie Passport Advantage) | IDSlent631 | idsldap.ent631.pkg |

## Zależności pakietów

Aby zainstalować niektóre pakiety, należy najpierw zainstalować zależności.

*Tabela 29. Pakiet i jego pakiety zależne*

| Nazwa pakietu | Zależy od |
|---|---|
| idsldap.clt32bit631.pkg | idsldap.cltbase631.pkg |
| idsldap.clt64bit631.pkg | idsldap.cltbase631.pkg |
| idsldap.srvbase64bit631.pkg | 1. idsldap-license631.pkg<br>2. idsldap.cltbase631.pkg<br>3. idsldap.clt64bit631.pkg |
| idsldap.srv64bit631.pkg | 1. idsldap-license631.pkg<br>2. idsldap.cltbase631.pkg<br>3. idsldap.clt64bit631.pkg<br>4. idsldap.srvbase64bit631.pkg |
| idsldap.srvproxy64bit631.pkg | 1. idsldap-license631.pkg<br>2. idsldap.cltbase631.pkg<br>3. idsldap.clt64bit631.pkg<br>4. idsldap.srvbase64bit631.pkg |

## Kolejność instalowania

Jeśli pakiety są instalowane w systemie Solaris, należy zainstalować je w określonej kolejności.

**Ważne:** Aby używać protokołu SSL (Secure Socket Layer) lub TLS (Transport Layer Security), należy zainstalować obsługiwaną wersję pakietu IBM Global Security Kit.

*Tabela 30. Kolejność instalacji funkcji klienta*

| Klient 32-bitowy | Klient 64-bitowy |
|---|---|
| 1. idsldap.cltbase631.pkg<br>2. idsldap.clt32bit631.pkg<br>3. idsldap.cltjava631.pkg | 1. idsldap.cltbase631.pkg<br>2. idsldap.clt64bit631.pkg<br>3. idsldap.cltjava631.pkg |

**Uwaga:** Jeśli używane jest środowisko klient-serwer z upoważnieniami w pliku archiwum lub obraz ISO z upoważnieniami do instalacji produktu IBM Security Directory Server, należy najpierw zaakceptować warunki licencji i zainstalować pakiet idsldap-license631.pkg.

*Tabela 31. Kolejność instalacji funkcji pełnego serwera katalogów i serwera proxy*

| Pełny 64-bitowy serwer katalogów | 64-bitowy serwer proxy |
|---|---|
| 1. idsldap-license631.pkg<br>2. idsldap.cltbase631.pkg<br>3. idsldap.clt64bit631.pkg<br>4. idsldap.cltjava631.pkg<br>5. idsldap.srvbase64bit631.pkg<br>6. idsldap.srv64bit631.pkg<br>7. idsldap.msg631.en.pkg<br>8. idsldap.ent631.pkg | 1. idsldap-license631.pkg<br>2. idsldap.cltbase631.pkg<br>3. idsldap.clt64bit631.pkg<br>4. idsldap.cltjava631.pkg<br>5. idsldap.srvbase64bit631.pkg<br>6. idsldap.srvproxy64bit631.pkg<br>7. idsldap.msg631.en.pkg<br>8. idsldap.ent631.pkg |

**Uwaga:** Aby użyć narzędzia Web Administration Tool, należy je wdrożyć w serwerze aplikacji WWW. Więcej informacji na temat instalowania wbudowanego serwera WebSphere Application Server, znajduje się w sekcji “Samodzielne instalowanie wbudowanego serwera WebSphere Application Server” na stronie 109.

*Tabela 32. Pakiet instalacyjny Web Administration Tool*

| Web Administration Tool |
|---|
| 1. idsldap-license631.pkg<br>2. idsldap.webadmin631.pkg |

Podczas instalowania narzędzia Web Administration Tool, na komputer są również kopiowane pliki języka DSML (Directory Services Markup Language). Więcej informacji na temat języka DSML zawiera sekcja Dodatek A, “Język DSML”, na stronie 243.

# Instalowanie z użyciem programów narzędziowych w systemie Solaris

Za pomocą komendy **pkgadd** można wykonać instalację produktu IBM Security Directory Server w systemie Solaris.

## Zanim rozpoczniesz

Otwórz nośnik instalacyjny produktu IBM Security Directory Server. Informacje na ten temat zawiera sekcja “Przygotowanie nośnika instalacyjnego” na stronie 6.

## O tym zadaniu

Program instalacyjny **pkgadd** instaluje produkt IBM Security Directory Server w systemie Solaris. Jeśli w systemie jest zainstalowana obsługiwana wersja bazy danych IBM DB2, proces instalacji zaktualizuje w pliku ldapdb.properties nazwę ścieżki i wersję bazy DB2.

## Procedura

1. Zaloguj się do systemu jako użytkownik root.
2. Otwórz wiersz komend.
3. Zmień bieżący katalog roboczy na katalog, w którym znajdują się pliki instalacyjne produktu IBM Security Directory Server.
4. Uruchom komendę **idsLicense**.

   ```
   ./idsLicense
   ```
5. Jeśli akceptujesz warunki umowy licencyjnej, wpisz 1. Dostępne są następujące opcje:
   - 1: zaakceptowanie umowy licencyjnej.
   - 2: odrzucenie umowy licencyjnej i zakończenie instalacji.
   - 3: wydrukowanie umowy licencyjnej.
   - 4: wyświetlenie warunków firm innych niż IBM znajdujących się w umowie licencyjnej.
   - 99: powrót do poprzedniego ekranu.

   Po zaakceptowaniu warunków umowy licencyjnej w katalogu instalacyjnym produktu IBM Security Directory Server zostanie utworzony plik LAPID i folder license. Folder license zawiera pliki licencji produktu IBM Security Directory Server we wszystkich obsługiwanych językach.

   **Ważne:** Nie modyfikuj i nie usuwaj pliku LAPID oraz plików licencji w folderze license.
6. Aby zainstalować pakiet, wykonaj następującą komendę:

   **Uwaga:** Pakiety produktu IBM Security Directory Server należy instalować w systemie Solaris w określonej kolejności. Aby uzyskać więcej informacji, patrz “Pakiety przeznaczone do instalacji w systemie Solaris” na stronie 76.

   ```
   pkgadd -d nazwa_pakietu
   ```
7. Sprawdź, czy instalacja produktu IBM Security Directory Server powiodła się. Aby uzyskać więcej informacji, patrz sekcja “Weryfikowanie pakietów serwera katalogów IBM Security” na stronie 85.

## Wyniki

Program instalacyjny zainstalował produkt IBM Security Directory Server w katalogu /opt/IBM/ldap/V6.3.1 w systemie Solaris. Jeśli w systemie jest zainstalowana obsługiwana wersja bazy danych IBM DB2, proces instalacji zaktualizuje w pliku ldapdb.properties nazwę ścieżki i wersję bazy DB2.

## Co dalej

Po zainstalowaniu produktu IBM Security Directory Server należy wykonać następujące działanie:

- Aby użyć produktu IBM Security Directory Server jako pełnego serwera katalogów, utwórz instancję serwera katalogów. Aby uzyskać więcej informacji, patrz “Tworzenie instancji serwera katalogów” na stronie 134.

- Aby użyć produktu IBM Security Directory Server jako serwera proxy, utwórz instancję serwera proxy. Aby uzyskać więcej informacji, patrz “Tworzenie instancji serwera proxy z własnymi ustawieniami” na stronie 142.

# Instalowanie z użyciem programów narzędziowych w systemie HP-UX

Do zainstalowania produktu IBM Security Directory Server w systemie HP-UX można użyć narzędzi wiersza komend.

Produkt IBM Security Directory Server zawiera pakiety klienckie tylko dla systemów HP-UX Itanium (Intel IA64). Aby uzyskać więcej informacji, patrz “Pakiety przeznaczone do instalacji w systemie HP-UX Itanium”.

## Pakiety przeznaczone do instalacji w systemie HP-UX Itanium

Aby użyć produktu IBM Security Directory Server jako klienta w systemie HP-UX, należy zainstalować odpowiednie pakiety.

### Pakiety przeznaczone dla systemu HP-UX

Produkt IBM Security Directory Server zawiera tylko pakiet kliencki dla systemów HP-UX Itanium (Intel IA64).

*Tabela 33. Pakiety dostarczane z produktem IBM Security Directory Server dla systemów HP-UX*

| Pakiety produktu IBM Security Directory Server | Nazwy pakietów |
|---|---|
| IBM Directory Server - klient podstawowy | idsldap.cltbase631.depot |
| IBM Directory Server - klient 32-bitowy | idsldap.clt32bit631.depot |
| IBM Directory Server - klient 64-bitowy | idsldap.clt64bit631.depot |
| IBM Directory Server - klient Java | idsldap.cltjava631.depot |
| IBM Directory Server - licencja | idsldap.license631.depot |

### Zależności pakietów

Aby zainstalować niektóre pakiety, należy najpierw zainstalować zależności.

*Tabela 34. Pakiet i jego pakiety zależne*

| Nazwa pakietu | Zależy od |
|---|---|
| idsldap.clt32bit631.depot | idsldap.cltbase631.depot |
| idsldap.clt64bit631.depot | idsldap.cltbase631.depot |

### Kolejność instalowania

Jeśli pakiety są instalowane w systemie HP-UX, należy zainstalować je w określonej kolejności.

**Ważne:** Aby używać protokołu SSL (Secure Socket Layer) lub TLS (Transport Layer Security), należy zainstalować obsługiwaną wersję pakietu IBM Global Security Kit.

*Tabela 35. Kolejność instalacji funkcji klienta*

| Klient 32-bitowy | Klient 64-bitowy |
|---|---|
| 1. idsldap.cltbase631.depot<br>2. idsldap.clt32bit631.depot<br>3. idsldap.cltjava631.depot | 1. idsldap.cltbase631.depot<br>2. idsldap.clt64bit631.depot<br>3. idsldap.cltjava631.depot |

# Instalowanie z użyciem programów narzędziowych w systemie HP-UX

Za pomocą komendy **swinstall** można wykonać instalację produktu IBM Security Directory Server w systemie HP-UX.

## Zanim rozpoczniesz

Należy przygotować nośniki instalacyjne produktu IBM Security Directory Server. Informacje na ten temat zawiera sekcja “Przygotowanie nośnika instalacyjnego” na stronie 6.

## O tym zadaniu

Program instalacyjny **pkgadd** instaluje produkt IBM Security Directory Server w systemie Solaris. Jeśli w systemie jest zainstalowana obsługiwana wersja bazy danych IBM DB2, proces instalacji zaktualizuje w pliku ldapdb.properties nazwę ścieżki i wersję bazy DB2.

## Procedura

1. Zaloguj się do systemu jako użytkownik root.
2. Otwórz wiersz komend.
3. Zmień bieżący katalog roboczy na katalog, w którym znajdują się pliki instalacyjne produktu IBM Security Directory Server.
4. Aby zainstalować pakiety, wykonaj następującą komendę:

```
swinstall -s ścieżka_instalacyjna_sds/idsldap.cltbase631.depot \*
swinstall -s ścieżka_instalacyjna_sds/idsldap.clt32bit631.depot \*
swinstall -s ścieżka_instalacyjna_sds/idsldap.clt64bit631.depot \*
swinstall -s ścieżka_instalacyjna_sds/idsldap.cltjava631.depot \*
```

5. Sprawdź, czy instalacja produktu IBM Security Directory Server powiodła się. Aby uzyskać więcej informacji, patrz sekcja “Weryfikowanie pakietów serwera katalogów IBM Security” na stronie 85.

## Wyniki

Program instalacyjny zainstalował produkt IBM Security Directory Server w katalogu /opt/IBM/ldap/V6.3.1 w systemie HP-UX.

# Rozdział 13. Sprawdzanie funkcji serwera IBM Security Directory Server

Po zainstalowaniu, zmodyfikowaniu lub zdeinstalowaniu produktu IBM Security Directory Server należy sprawdzić, czy funkcje IBM Security Directory Server zostały poprawnie zainstalowane, zmodyfikowane lub zdeinstalowane.

Za pomocą programu IBM Installation Manager lub programów narzędziowych systemu operacyjnego można sprawdzić, czy instalacja, modyfikacja lub deinstalacja powiodła się.

## Weryfikowanie funkcji serwera IBM Security Directory Server przy użyciu programu IBM Installation Manager

Użyj programu IBM Installation Manager do weryfikacji funkcji serwera IBM Security Directory Server i wymaganych produktów, które zainstalowano za pomocą programu IBM Installation Manager.

### Procedura

1. Uruchom program IBM Installation Manager.

   **Windows**
   W menu **Start** kliknij kolejno opcje **Wszystkie programy > IBM Installation Manager > IBM Installation Manager**.

   **AIX i Linux**
   Wprowadź następującą komendę w wierszu komend. Zmodyfikuj poniższą ścieżkę domyślną, jeśli program IBM Installation Manager jest zainstalowany w innej lokalizacji.

   ```
   /opt/IBM/InstallationManager/eclipse/IBMIM
   ```

2. Na stronie **IBM Installation Manager** kliknij kolejno opcje **Plik > Wyświetl zainstalowane pakiety**.
3. Z listy **Zainstalowane pakiety i poprawki** na stronie **Zainstalowane pakiety**, rozwiń opcję **IBM Directory Server zabezpieczeń**.
4. Na liście **Zainstalowane pakiety i poprawki** kliknij wersję programu IBM Security Directory Server, dla której chcesz wyświetlić funkcje.
5. W obszarze **Szczegóły** sprawdź instalację produktów i wymaganych składników.
6. Aby zamknąć stronę **Zainstalowane pakiety**, kliknij przycisk **Zamknij**.
7. Aby zamknąć okno programu **IBM Installation Manager**, kliknij opcje **Plik > Zakończ**.

## Weryfikowanie funkcji serwera IBM Security Directory Server w systemie Windows

Można sprawdzić, czy instalacja programu IBM Security Directory Server, jego modyfikacja lub deinstalacja zakończyła się pomyślnie, sprawdzając Rejestr systemu Microsoft Windows.

### O tym zadaniu

Microsoft Windows przechowuje pozycje Rejestru w celu śledzenia oprogramowania zainstalowanego w tym systemie. Po pomyślnej instalacji, modyfikacji lub deinstalacji opcji produktu IBM Security Directory Server, pozycje rejestru są modyfikowane, aby zarejestrować najnowsze aktualizacje w systemie. Przedstawiono przykład pozycji rejestru po

wykonaniu pomyślnej instalacji funkcji produktu IBM Security Directory Server. Przy modyfikowaniu lub deinstalacji funkcji produktu IBM Security Directory Server pozycje rejestru śledzą modyfikowane funkcje, aby przedstawić ich najnowszy status. Pozycje rejestru są wyświetlane dla systemu Microsoft Windows na platformie AMD64/EM64T.

## Procedura

1. Zaloguj się do systemu Windows z uprawnieniami administratora.
2. Otwórz wiersz komend i uruchom następującą komendę:

   ```
   regedit
   ```
3. W oknie **Edytor rejestru** kliknij kolejno opcje **My Computer > HKEY_LOCAL_MACHINE > SOFTWARE > Wow6432NODE > IBM > IDSLDAP > 6.3.1**

   **Uwaga:** Aby zweryfikować instalację produktu IBM Security Directory Server w systemie Microsoft Windows na platformie Intel x86 (IA32), rozwiń opcje **Mój komputer > HKEY_LOCAL_MACHINE > SOFTWARE > IBM > IDSLDAP > 6.3.1** .
   Gałąź Rejestru Mój komputer\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432NODE\IBM\IDSLDAP\6.3.1 przedstawia główne wersje funkcji produktu IBM Security Directory Server zainstalowanych w systemie.

   ```
   BaseServerMajorVersion      6.3.1
   BitMode   64
   ClientMajorVersion          6.3.1
   JavaClientMajorVersion      6.3.1
   LDAPHome                    katalog_instalacji
   ProxyServerMajorVersion     6.3.1
   ServerMajorVersion          6.3.1
   WebadminMajorVersion        6.3.1
   WebSphereAppSrvMajorVersion 7.0
   ```

   Drugorzędne wersje funkcji programu IBM Security Directory Server zainstalowanych w systemie zawiera gałąź Mój komputer\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432NODE\IBM\IDSLDAP\6.3.1. Na przykład:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432NODE\IBM\IDSLDAP\6.3.1\BaseServer\
             BaseServerMinorVersion 1.0

   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432NODE\IBM\IDSLDAP\6.3.1\Client\
             ClientMinorVersion 1.0

   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432NODE\IBM\IDSLDAP\6.3.1\JavaClient\
             JavaClientMinorVersion 1.0

   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432NODE\IBM\IDSLDAP\6.3.1\ProxyServer\
             ProxyServerMinorVersion 1.0

   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432NODE\IBM\IDSLDAP\6.3.1\Server\
             ServerMinorVersion 1.0

   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432NODE\IBM\IDSLDAP\6.3.1\Webadmin\
             WebadminMinorVersion 1.0

   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432NODE\IBM\IDSLDAP\6.3.1\WebSphereAppSrv\
             WebSphereAppSrvMinorVersion 0.25
   ```
4. Aby zamknąć okno **Edytora rejestru** kliknij opcje **Plik > Zakończ**.

# Weryfikowanie pakietów serwera katalogów IBM Security

Można sprawdzić, czy instalacja produktu IBM Security Directory Server została wykonana poprawnie, sprawdzając pakiety zainstalowane w systemie.

## O tym zadaniu

Po wykonaniu instalacji produktu IBM Security Directory Server należy sprawdzić, czy jego pakiety są w wymaganej wersji. Można sprawdzić numer wersji pakietów IBM Security Directory Server.

## Procedura

1. Zaloguj się do systemu jako użytkownik root.
2. Otwórz wiersz komend i uruchom następującą komendę:

| System operacyjny | Komenda do wysłania zapytania o pakiety: |
|---|---|
| **AIX** | `lslpp -l 'idsldap*'` |
| **Linux** | `rpm -qa \| grep -i idsldap` |
| **Solaris** | `pkginfo \| grep IDSl`<br>`pkgparam` nazwa_pakietu `VERSION` |
| **HP-UX** | `swlist \| grep -i idsldap` |

## Wyniki

Komenda wyświetli listę pakietów IBM Security Directory Server zainstalowanych w systemie.

# Sprawdzanie wersji programu Web Administration Tool

Aby sprawdzić, czy instalacja lub aktualizacja programu Web Administration Tool powiodła się, należy sprawdzić wersję tego programu.

## Procedura

1. Zaloguj się z uprawnieniami administratora.
2. Przejdź do katalogu *miejsce_instalacji_serwera_katalogów*/idstools. Wartość *miejsce_instalacji_serwera_katalogów* jest miejscem instalacji produktu IBM Security Directory Server. Poniżej wymieniono domyślne miejsca instalacji dla różnych systemów operacyjnych:

*Tabela 36. Domyślne położenie instalacji produktu IBM Security Directory Server w różnych systemach operacyjnych*

| Systemy operacyjne | Domyślne miejsca instalacji: |
|---|---|
| Microsoft Windows | c:\Program Files\IBM\ldap\V6.3.1 |
| AIX i Solaris | /opt/IBM/ldap/V6.3.1 |
| Linux | /opt/ibm/ldap/V6.3.1 |

3. Uruchom komendę:

| Systemy operacyjne | Komenda do uruchomienia: |
|---|---|
| **Microsoft Windows** | deploy_IDSWebApp.bat -v |
| **AIX, Linux i Solaris** | deploy_IDSWebApp -v |

Komenda wyświetla następujące informacje:

- Wartości wersji i daty komendy **deploy_IDSWebApp**.
- Wartości wersji i daty zainstalowanego pliku IDSWebApp.war.
- Wartości wersji i daty zainstalowanego pliku IDSWebApp.war.

### Co dalej

Należy sprawdzić następujące wartości:

1. Czy wersja i data zainstalowanego pliki IDSWebApp.war jest inna niż wersja i data obecnie wdrożonego pliku IDSWebApp.war.
2. Jeśli wartości są różne, należy wdrożyć najnowszą wersję programu Web Administration Tool w serwerze aplikacji WWW.

## Weryfikowanie instalacji pakietu IBM Global Security Kit w systemie Windows

Zweryfikuj status instalacji pakietu IBM Global Security Kit (GSKit), aby potwierdzić, czy zakończyła się pomyślnie w systemie Windows.

### Procedura

1. Odszukaj plik gskitinst.log.

| System operacyjny | Domyślna ścieżka: |
|---|---|
| **Windows** | C:\Program Files\IBM\ldap\V6.3.1\var |

2. Sprawdź, czy został utworzony następujący katalog: C:\Program Files\IBM\gsk8
3. Sprawdź, czy plik gskitinst.log zawiera wartość EXIT 0. Jeśli instalacja IBM Global Security Kit zakończyło się pomyślnie, ustawiona jest wartość 0, w przeciwnym razie będzie ustawiona wartość niezerowa.
4. Opcjonalne: Jeśli instalacja pakietu IBM Global Security Kit zakończyła się niepowodzeniem, w pliku C:\Program Files\IBM\ldap\V6.3.1\var\gskitinsterr.log zostaną zapisane szczegółowe informacje o błędach.

## Weryfikowanie instalacji pakietu IBM Global Security Kit w systemach AIX, Linux, Solaris i HP-UX

Zweryfikuj pakiet IBM Global Security Kit (GSKit), aby potwierdzić, czy jego instalacja zakończyła się pomyślnie.

### O tym zadaniu

Po wykonaniu instalacji IBM Global Security Kit należy się upewnić, że jego pakiety są w wymaganej wersji. Można sprawdzić numer wersji pakietu IBM Global Security Kit.

### Procedura

1. Zaloguj się do systemu jako użytkownik root.
2. Otwórz wiersz komend i uruchom następującą komendę:

| System operacyjny | Komenda do uruchomienia: |
|---|---|
| **AIX** | `lslpp -al \| grep -i gsk` |
| **Linux** | `rpm -qa \| grep -i gsk` |

| System operacyjny | Komenda do uruchomienia: |
| --- | --- |
| **Solaris** | `pkginfo \| grep gsk`<br>`pkgparam` nazwa_pakietu `VERSION` |
| **HP-UX** | `swlist \| grep -i gsk` |

# Rozdział 14. Aktualizowanie instancji starszej wersji

Aby zamienić istniejącą instancję na najnowszą wersję i nadal korzystać z istniejących plików konfiguracyjnych, należy zaktualizować instancję.

Proces aktualizacji zachowuje zmiany w definicjach schematów, plikach konfiguracyjnych i danych instancji serwera katalogów.

Aktualizowanie instancji starszej wersji wymaga wykonania następującego procesu:

1. Wykonaj instalację produktu IBM Security Directory Server.
2. Zaktualizuj istniejącą instancję starszej wersji.

Produkt IBM Security Directory Server w wersji 6.3.1 (serwer i klient) może istnieć na jednym komputerze z serwerami i klientami w wersji 6.0, 6.1, 6.2 i 6.3.

Poniższe wersje instancji serwera katalogów można bezpośrednio zaktualizować do produktu IBM Security Directory Server w wersji 6.3.1:

- IBM Security Directory Server 6.3
- IBM Security Directory Server 6.2
- IBM Security Directory Server 6.1

**Ważne:** Bezpośrednia aktualizacja instancji produktu IBM Security Directory Server w wersji 6.0 do produktu IBM Security Directory Server w wersji 6.3.1 nie jest obsługiwana. Należy najpierw zaktualizować wersję 6.0 do wersji 6.1, 6.2 lub 6.3, a następnie wykonać aktualizację do wersji 6.3.1.

Można wykonać aktualizację starszej wersji w jeden z następujących sposobów:

- Aktualizacja istniejącej instancji na komputerze lokalnym za pomocą narzędzia Instance Administration Tool (**idsxinst**) produktu IBM Security Directory Server lub za pomocą komendy **idsimigr**. Nie trzeba usuwać instancji serwera katalogów, która ma zostać zaktualizowana. W przypadku instancji pełnego serwera katalogów nie należy dekonfigurować bazy danych. Aktualizacja nie jest obsługiwana, jeśli instancja serwera katalogów zostanie usunięta lub jego baza danych zostanie zdekonfigurowana.
- Aktualizowanie instancji na komputerze zdalnym za pomocą komend **migbkup** i **idsimigr**. Aby uzyskać więcej informacji, patrz “Aktualizowanie zdalnej instancji z poprzedniej wersji za pomocą komendy **idsimigr**” na stronie 94.

**Ważne:** Należy utworzyć kopię zapasową schematu, plików konfiguracyjnych i bazy danych instancji, aby mieć możliwość naprawy wszystkich błędów aktualizacji.

## Aktualizacja bazy danych

Podczas aktualizowania instancji, powiązana baza danych DB2 jest również aktualizowana, jeśli wersja bazy danych DB2 jest starsza niż wersja obsługiwana przez produkt IBM Security Directory Server w wersji 6.3.1. Komenda **idsdbmigr** jest wykonywana wewnętrznie w celu aktualizacji bazy danych DB2.

**Ważne:** Nie jest obsługiwana bezpośrednia aktualizacja instancji serwera katalogów, który jest skonfigurowany z bazą danych DB2 w wersji 9.1 do instancji z bazą danych DB2 w

wersji 10.1.0.2 lub nowszą. Można wykonać aktualizację instancji, która jest skonfigurowana z bazą DB2 w wersji 9.1 do instancji z DB2 w wersji 10.1.0.2 lub nowszej w jeden z następujących sposobów:

- Wykonaj aktualizację instancji z bazą danych DB2 w wersji 9.1 do instancji z DB2 w wersji 9.5, a następnie do instancji z DB2 w wersji 10.1.0.2 lub nowszej.
- Wykonaj aktualizację instancji z bazą danych DB2 w wersji 9.1 do instancji z DB2 w wersji 9.7, a następnie do instancji z DB2 w wersji 10.1.0.2 lub nowszej.

### Aktualizacja instalacji klienta

Jeśli za pomocą programu instalacyjnego klienta IBM Security Directory Server zainstalowano tylko funkcje klienta, aktualizacja nie jest wymagana. Klienty w wersji 6.0, 6.1, 6.2 i 6.3 mogą istnieć na jednym komputerze z serwerem i klientem w wersji 6.3.1.

## Konfigurowanie środowiska przed aktualizacją instancji

Należy skonfigurować środowisko serwera katalogów przed wykonaniem aktualizacji istniejącej instancji.

### Zanim rozpoczniesz

Wykonaj następujące czynności przed skonfigurowaniem środowiska:

- Otwórz nośnik instalacyjny produktu IBM Security Directory Server.
- Wykonaj instalację produktu IBM Security Directory Server w wersji 6.3.1. Patrz sekcja “Uruchamianie instalacji” na stronie 28.
- Zaloguj się jako użytkownik root w systemie operacyjnym AIX, Linux lub Solaris i jako członek grupy administratorów w systemie operacyjnym Windows.

### Procedura

1. Sprawdź, czy system operacyjny, na którym znajduje się instancja przeznaczona do aktualizacji, jest obsługiwany przez IBM Security Directory Server w wersji 6.3.1.
2. Sprawdź, czy instancja w poprzedniej wersji, którą chcesz zaktualizować, uruchamia się pomyślnie. Aby zaktualizować instancję serwera katalogów, należy skonfigurować bazę danych, jeśli nie jest już skonfigurowana.

   **Ważne:** Aktualizacja serwera proxy lub serwera katalogów nie będzie obsługiwana, jeśli serwer nie uruchomi się pomyślnie.
3. Wykonaj kopię zapasową zamkniętej instancji, którą chcesz zaktualizować. Dla instancji serwera katalogów, utwórz kopię zapasową baz danych DB2 i ustawień DB2. Więcej informacji na ten temat zawiera opis komendy **idsdbback** w publikacji *Skorowidz komend*.
4. Aby utworzyć kopię zapasową plików schematu i plików konfiguracyjnych, uruchom komendę **migbkup**:

| System operacyjny | Komenda do uruchomienia: |
|---|---|
| **Microsoft Windows** | **migbkup.bat** nazwa_dysku\idsslapd-nazwa_instancji katalog_kopii_zapasowej |
| **AIX, Linux i Solaris** | **migbkup** katalog_użytkownika/idsslapd-nazwa_instancji katalog_kopii_zapasowej |

   Komenda **migbkup** znajduje się w podkatalogu tools nośnika instalacyjnego produktu IBM Security Directory Server. Jeśli produkt IBM Security Directory Server został zainstalowany, komenda **migbkup** będzie się znajdować w podkatalogu sbin katalogu instalacyjnego IBM Security Directory Server. Następujący katalog jest domyślnym położeniem instalacji w różnych systemach operacyjnych:

**Microsoft Windows**
C:\Program Files\IBM\ldap\V6.3.1

**AIX i Solaris**
/opt/IBM/ldap/V6.3.1

**Linux** /opt/ibm/ldap/V6.3.1

Komenda **migbkup** tworzy kopię zapasową dla następujących plików:

- ibmslapd.conf
- V3.config.at
- V3.config.oc
- V3.ibm.at
- V3.ibm.oc
- V3.system.at
- V3.system.oc
- V3.user.at
- V3.user.oc
- V3.modifiedschema
- V3.ldapsyntaxes
- V3.matchingrules
- ibmslapdcfg.ksf
- ibmslapddir.ksf
- perftune_stat.log
- perftune_input.conf
- ibmdiradmService.cmd (dla Windows)
- ibmslapdService.cmd (dla Windows)

Komenda **migbkup** tworzy następujące pliki:

- db2info zawiera nazwę ścieżki i informacje o wersji bazy danych DB2, która jest używana przez instancję serwera katalogów. Komenda **idsimigr** lub program Instance Administration Tool korzysta z tego pliku do wykonania aktualizacji instancji bazy danych DB2 i bazy danych przy aktualizacji instancji serwera katalogów. Dla instancji serwera proxy ten plik nie jest dostępny.
- platforminfo zawiera informacje na temat systemu operacyjnego i typu procesu.

5. Jeśli użytkownik samodzielnie zmodyfikował plik V3.modifiedschema dla aktualizowanej instancji, plik ten nie może zawierać żadnych zduplikowanych identyfikatorów obiektów (oid) dla klas obiektów lub atrybutów. Jeśli plik zawiera zduplikowane identyfikatory OID, nie zostaną one zachowane podczas aktualizacji. Jeśli pliki schematu zawierają zduplikowane identyfikatory OID, zostanie zachowany identyfikator OID podany w pliku V3.modifiedschema. Jeśli pliki schematu nie będą zawierać atrybutów lub klas obiektów, serwer administracyjny i proces idsslapd mogą się nie uruchomić. W takich sytuacjach należy samodzielnie dodać brakujące atrybuty lub klasy obiektów do schematu plików przed uruchomieniem serwerów.
6. Jeśli instancję skonfigurowano przy użyciu niestandardowych plików schematów, należy je skopiować samodzielnie do katalogu kopii zapasowej. Podczas tworzenia kopii zapasowej plików schematu i plików konfiguracyjnych, komenda **migbkup** tworzy kopię zapasową niestandardowych plików schematu. Jednak te pliki schematu nie może być używane podczas aktualizacji instancji.

### Co dalej

Po skonfigurowaniu środowiska uruchom komendę **idsimigr** lub program Instance Administration Tool, aby zaktualizować instancję z poprzedniej wersji. Aby zaktualizować instancję, użyj jednej z następujących metod:

- "Aktualizowanie instancji z poprzedniej wersji za pomocą komendy **idsimigr**"
- "Aktualizowanie instancji poprzedniej wersji przy użyciu programu Instance Administration Tool" na stronie 147

## Aktualizowanie instancji z poprzedniej wersji za pomocą komendy idsimigr

Za pomocą komendy **idsimigr** można zaktualizować instancję serwera katalogów lub instancję serwera proxy z wersji wcześniejszej do wersji bieżącej.

### Zanim rozpoczniesz

Należy wykonać następujące czynności przed zaktualizowaniem instancji za pomocą komendy **idsimigr**:

- Wykonaj instalację produktu IBM Security Directory Server. Patrz sekcja "Uruchamianie instalacji" na stronie 28.
- Skonfiguruj środowisko przed aktualizacją instancji. Patrz sekcja "Konfigurowanie środowiska przed aktualizacją instancji" na stronie 90.
- Zaloguj się jako użytkownik root w systemie operacyjnym AIX, Linux lub Solaris i jako członek grupy administratorów w systemie operacyjnym Windows.

Możesz także zaktualizować instancję istniejącą na komputerze przy użyciu programu Instance Administration Tool. Aby uzyskać więcej informacji, patrz "Aktualizowanie instancji poprzedniej wersji przy użyciu programu Instance Administration Tool" na stronie 147.

### O tym zadaniu

Po zaktualizowaniu instancji wcześniejszej wersji jest ona przekształcana do w pełni funkcjonalnej instancji produktu IBM Security Directory Server w bieżącej wersji.

### Procedura

1. Otwórz wiersz komend.
2. Przejdź do katalogu sbin. Domyślnie używane są następujące lokalizacje w różnych systemach operacyjnych:

   **Microsoft Windows**
   C:\Program Files\IBM\ldap\V6.3.1\sbin

   **AIX i Solaris**
   /opt/IBM/ldap/V6.3.1/sbin

   **Linux** /opt/ibm/ldap/V6.3.1/sbin
3. Zatrzymaj proces ibmslapd i serwer administracyjnego instancji przeznaczonej do aktualizacji.

   ```
   ibmslapd -I nazwa_instancji
   ibmdiradm -I nazwa_instancji -k
   ```
4. Nie deinstaluj wersji produktu IBM Security Directory Server, która jest powiązana z instancją przeznaczoną do aktualizacji.

5. Wykonaj komendę **idsimigr**, aby zaktualizować z poprzedniej do bieżącej wersji instancję produktu IBM Security Directory Server.

   ```
   idsimigr -I nazwa_instancji
   ```

6. Uruchom proces ibmslapd i serwer administracyjny instancji.

   ```
   ibmslapd -I nazwa_instancji -n
   ibmdiradm -I nazwa_instancji
   ```

7. Wykonaj kopię zapasową zamkniętej bazy danych instancji. Informacje na ten temat zawiera sekcja “Tworzenie kopii zapasowej serwera katalogów” na stronie 187.

## Aktualizowanie instancji starszej wersji na innym komputerze

Można zaktualizować istniejącą instancję starszej wersji znajdującą się na tym komputerze do nowszej wersji znajdującej się na innym komputerze.

Może być konieczna zdalna aktualizacja istniejącej instancji z następujących powodów:

- System operacyjny na komputerze, na którym znajduje się starsza wersja nie jest obsługiwany przez produkt IBM Security Directory Server w wersji 6.3.1. Użytkownik nie chce zaktualizować lub zmienić systemu operacyjnego na komputerze.
- Użytkownik chce zainstalować produkt IBM Security Directory Server w wersji 6.3.1 na komputerze, którego system operacyjny jest inny niż na komputerze, na którym znajduje się starsza wersja. Jednak użytkownik chce utworzyć instancję zawierającą informacje z istniejącej instancji starszej wersji. Na przykład, istniejąca instancja znajduje się na komputerze z systemem AMD64/EM64T, a użytkownik potrzebuje serwera w wersji 6.3.1 na komputerze z systemem AIX. W takim przypadku oba systemy operacyjne muszą korzystać z tej samej konwencji ustalania kolejności bajtów (endian). Jeśli pierwszy komputer korzysta z konwencji little endian, drugi komputer również musi korzystać z tej samej konwencji. Typ konwencji ustalania kolejności bajtów dotyczy określania kolejności bitów podczas zapisywania danych w pamięci. Jeśli systemy operacyjne używają różnych konwencji ustalania kolejności bajtów, aktualizacja instancji nie jest obsługiwana.

Procedura aktualizacji zdalnej jest podobna do procedury aktualizacji na tym samym komputerze. Jedynym wyjątkiem jest to, że należy skopiować pliki kopii zapasowej z komputera na komputer, na którym jest instalowany produkt IBM Security Directory Server w wersji 6.3.1.

**Uwaga:** Jeśli wykonywana jest aktualizacja instancji zdalnej z komputera, który bierze udział w replikacji, wykonaj następujące działania:

- Włącz replikację, podając system źródłowy jako dostawcę.
- Włącz replikację, podając system docelowy jako odbiorcę.

Dzięki replikacji aktualizacje są umieszczane w kolejce i replikowane, gdy system docelowy zostanie uruchomiony. Replikację należy włączyć przed wykonaniem kopii zapasowej instancji systemu źródłowego.

## Obsługiwane systemy operacyjne w operacji aktualizacji instancji zdalnej

Aby zaktualizować instancję zdalną na odpowiednim docelowym systemie operacyjnym, należy sprawdzić systemy operacyjne, będące źródłem i celem instancji.

*Tabela 37. Obsługiwane źródłowe i docelowe systemy operacyjne w operacji aktualizacji zdalnej*

| | **Docelowy system operacyjny (IBM Security Directory Server wersja 6.3.1)** | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Źródłowy system operacyjny (IBM Security Directory Server wersja 6.3 lub starsza) ↓** | **Windows na 32-bitowej platformie Intel** | **Windows AMD64/ EM64T** | **Linux System x (wersja 32-bitowa)** | **Linux AMD64/ EM64T** | **Linux na platformie System i oraz System p** | **Linux System z** | **AIX** | **Solaris SPA-RC** | **Solaris X64** |
| Windows na 32-bitowej platformie Intel | ✓ | ✓ | ✓ | ✓ | | | | | ✓ |
| Windows na platformie AMD/ EM64T | ✓ | ✓ | ✓ | ✓ | | | | | ✓ |
| System x Linux (32-bitowy) | ✓ | ✓ | ✓ | ✓ | | | | | ✓ |
| AMD/ EM64T Linux | ✓ | ✓ | ✓ | ✓ | | | | | ✓ |
| Linux na platformie System i oraz System p | | | | | ✓ | ✓ | ✓ | ✓ | |
| Linux na platformie System z | | | | | ✓ | ✓ | ✓ | ✓ | |
| AIX | | | | | ✓ | ✓ | ✓ | ✓ | |
| Solaris SPARC | | | | | ✓ | ✓ | ✓ | ✓ | |
| Solaris X64 | ✓ | ✓ | ✓ | ✓ | | | | | ✓ |

# Aktualizowanie zdalnej instancji z poprzedniej wersji za pomocą komendy idsimigr

Komenda **idsimigr** z parametrem **-u** pozwala na zaktualizowanie zdalnej instancji serwera katalogów lub instancji serwera proxy z poprzedniej wersji do wersji 6.3.1.

## Zanim rozpoczniesz

Przed aktualizacją instancji przy użyciu narzędzia **idsimigr** z parametrem **-u** należy wykonać następujące zadania:

- Skonfiguruj środowisko przed aktualizacją instancji. Patrz sekcja “Konfigurowanie środowiska przed aktualizacją instancji” na stronie 90.
- Zaloguj się jako użytkownik root w systemie operacyjnym AIX, Linux lub Solaris i jako członek grupy administratorów w systemie operacyjnym Windows.

Można również zaktualizować zdalną instancję przy użyciu plików kopii zapasowej za pomocą programu narzędziowego Instance Administration Tool. Aby uzyskać więcej informacji, patrz “Aktualizowanie zdalnej instancji poprzedniej wersji przy użyciu programu Instance Administration Tool” na stronie 148.

## O tym zadaniu

Po zakończeniu procesu aktualizacji komenda **idsimigr** utworzy instancję w wersji 6.3.1 na komputerze przy użyciu informacji ze zdalnej instancji.

## Procedura

1. Utwórz kopię zapasową bazy danych instancji serwera katalogów, która jest zainstalowana na zdalnym komputerze, za pomocą komendy **idsdb2ldif**.

   **Ważne:** Jeśli aktualizujesz instancję serwera proxy, nie twórz kopii zapasowej bazy danych. Serwer proxy nie ma powiązanej bazy danych.

   ```
   idsdb2ldif -I nazwa_instancji -o inst_out.ldif
   ```

   Więcej informacji na temat komendy **idsdb2ldif** zawiera *Skorowidz komend*.
2. Wykonaj instalację produktu IBM Security Directory Server na komputerze, na którym chcesz zaktualizować zdalną instancję. Więcej informacji na ten temat zawiera sekcja “Uruchamianie instalacji” na stronie 28.
3. Aby utworzyć kopię zapasową plików schematu i plików konfiguracyjnych zdalnej instancji, uruchom komendę **migbkup** dla wersji, do której chcesz zaktualizować:

| System operacyjny | Komenda do uruchomienia: |
|---|---|
| **Microsoft Windows** | **migbkup.bat** nazwa_dysku\idsslapd-nazwa_instancji katalog_kopii_zapasowej |
| **AIX, Linux i Solaris** | **migbkup** katalog_użytkownika/idsslapd-nazwa_instancji katalog_kopii_zapasowej |

   Komenda **migbkup** znajduje się w podkatalogu tools nośnika instalacyjnego produktu IBM Security Directory Server.
4. Skopiuj katalog kopii zapasowej, katalog_kopii_zapasowej, który został utworzony za pomocą komendy **migbkup**, z komputera zdalnego do komputera z zainstalowanym produktem IBM Security Directory Server.
5. Opcjonalne: Skopiuj plik kopii zapasowej bazy danych, inst_out.ldif, z komputera zdalnego do komputera z zainstalowanym serwerem IBM Security Directory Server.
6. Uruchom komendę **idsimigr** z parametrem -u, aby utworzyć instancję przy użyciu danych kopii zapasowej instancji zdalnej.

   ```
   idsimigr -u katalog_kopii_zapasowej
   ```
7. Skonfiguruj bazę danych, przyrostek i nazwę DN oraz hasło administratora dla instancji serwera katalogów.

   **Ważne:** Przy aktualizowaniu instancji serwera proxy, nie należy uruchamiać komendy **idscfgdb**, aby skonfigurować bazę danych.

   ```
   idscfgdb -I nazwa_instancji -a id_admin_db -w hasło_admin_db -t
   nazwa_bazy_danych -l lokalizacja_db
   idscfgsuf -I nazwa_instancji -s przyrostek
   idsdnpw -I nazwa_instancji –u dn_administratora –p hasło_administratora
   ```
8. Opcjonalne: Uruchom komendę **idsldif2db**, aby zaimportować plik kopii zapasowej bazy danych, inst_out.ldif, do zaktualizowanej instancji serwera katalogów.
9. Uruchom proces ibmslapd i serwer administracyjny instancji.

```
ibmslapd -I nazwa_instancji -n
ibmdiradm -I nazwa_instancji
```

10. Należy utworzyć kopię zapasową instancji. Aby uzyskać więcej informacji, patrz “Tworzenie kopii zapasowej serwera katalogów” na stronie 187.

## Dowiązania do serwerowych i klienckich programów narzędziowych

Do utworzenia dowiązań do katalogu z programami narzędziowymi i bibliotekami serwera katalogów można użyć komendy **idslink**.

Po zainstalowaniu serwera IBM Security Directory Server można utworzyć dowiązania do serwerowych i klienckich programów narzędziowych. Dowiązania te nie są tworzone automatycznie podczas instalacji.

Dowiązania utworzone dla poprzedniej wersji serwera IBM Security Directory Server pozostają bez zmian. Aby usunąć dowiązania utworzone przez komendę idslink, należy użyć komendy **idsrmlink**.

Komenda **idslink** pozwala utworzyć dowiązania do programów narzędziowych, takich jak **idsldapmodify** i **idsldapadd**, oraz do bibliotek, takich jak libibmldap.so. Dowiązania te wskazują miejsca, w których znajdują się programy narzędziowe i biblioteki produktu IBM Security Directory Server.

Więcej informacji na temat komend **idslink** i **idsrmlink** zawiera *Skorowidz komend*.

# Rozdział 15. Migrowanie danych i rozwiązań z instancji poprzedniej wersji

Istnieje możliwość zmigrowania danych katalogu i rozwiązań skonfigurowanych w instancji poprzedniej wersji w celu użycia w instancji w wersji 6.3.1.

**Migrowanie danych DB2 z serwera IBM DB2 Enterprise Server Edition (ESE) do serwera IBM DB2 Workspace Server Edition (WSE)**

W systemach System x Linux (architektura 32-bitowa Intel) baza danych IBM DB2 ESE 9.7 lub nowsza nie jest obsługiwana. W systemach System x Linux, produkt IBM Security Directory Server używa bazy danych IBM DB2 WSE 9.7 z pakietem poprawek 6 lub nowszym.

Podczas aktualizowania instancji w wersji 6.1 lub 6.2 wraz z danymi do wersji 6.3.1 może być konieczne uruchamianie zdalnego aktualizowania instancji. Instancję 6.3 z DB2 WSE 9.7 lub nowszą można zaktualizować do wersji 6.3.1 z DB2 WSE 9.7 lub nowszą. W systemach System x Linux bezpośrednia aktualizacja instancji 6.1 lub 6.2 z DB2 ESE w wersji 9.1 lub nowszej do wersji 6.3.1 z DB2 WSE w wersji 9.7 lub nowszej może się nie powieść. Więcej informacji na temat migrowania bazy danych DB2 ESE do DB2 WSE zawiera sekcja “Migrowanie instancji z bazą danych DB2 ESE do instancji z bazą danych DB2 WSE” na stronie 98.

**Migrowanie rozwiązań serwera katalogów wykorzystujących produkt IBM Security Directory Integrator**

Aby wykorzystać rozwiązania skonfigurowane w poprzedniej wersji instancji do instancji 6.3.1, należy je zmigrować.

Obsługiwane są następujące rozwiązania:

- Narzędzie do zarządzania dziennikami
- Protokół SNMP (Simple Network Management Protocol)
- Synchronizowanie z Active Directory

Więcej informacji na temat rozwiązań serwera katalogów znajduje się w sekcji *Administrowanie* dokumentacji produktu IBM Security Directory Server.

Aby rozwiązanie działało, komputer musi mieć zainstalowany produkt IBM Security Directory Integrator 7.1. Więcej informacji na temat instalowania i administrowania produktem IBM Security Directory Integrator znajduje się w sekcji *Instalowanie i administrowanie* dokumentacji produktu dostępnej pod adresem http://www-01.ibm.com/support/knowledgecenter/SSCQGF/welcome.

Jeśli ścieżka instalacji produktu IBM Security Directory Integrator jest inna od ścieżki domyślnej, należy ustawić zmienną *IDS_LDAP_TDI_HOME*, podając w niej położenie instalacji produktu IBM Security Directory Integrator. Poniżej podano domyślne ścieżki instalacji produktu IBM Security Directory Integrator 7.1 w różnych systemach operacyjnych:

**AIX, Linux i Solaris**
/opt/IBM/TDI/V7.1

**Windows**
C:\Program Files\IBM\TDI\V7.1

# Migrowanie instancji z bazą danych DB2 ESE do instancji z bazą danych DB2 WSE

Aby zaktualizować instancję wersji 6.1 lub 6.2 z bazą danych DB2 ESE do instancji wersji 6.3.1 z bazą danych DB2 WSE, należy przeprowadzić migrację danych z bazy danych DB2 ESE do bazy danych DB2 WSE.

## Zanim rozpoczniesz

Przed zmigrowaniem danych z instancji poprzedniej wersji do instancji wersji 6.3.1 wykonaj następujące czynności:

- Wykonaj instalację produktu IBM Security Directory Server w wersji 6.3.1 z produktem IBM DB2 WSE. Patrz sekcja “Uruchamianie instalacji” na stronie 28.
- Skonfiguruj środowisko przed aktualizacją instancji. Patrz sekcja “Konfigurowanie środowiska przed aktualizacją instancji” na stronie 90.
- Zaloguj się jako użytkownik root w systemie operacyjnym AIX, Linux lub Solaris i jako członek grupy administratorów w systemie operacyjnym Windows.

## Procedura

1. Zatrzymaj instancję serwera katalogów, z której chcesz migrować dane katalogu.
2. Uruchom komendę **migbkup** udostępnioną w produkcie aIBM Security Directory Server w wersji 6.3.1 w celu utworzenia kopii zapasowej instancji. Patrz sekcja “Konfigurowanie środowiska przed aktualizacją instancji” na stronie 90. Więcej informacji na temat komendy **migbkup** zawiera *Skorowidz komend*.
3. Utwórz kopię zapasową bazy danych instancji serwera katalogów, z której chcesz migrować dane. Aby utworzyć kopię zapasową bazy danych instancji dsrdbm01, wykonaj następujące kroki:
   a. Przełącz kontekst użytkownika na właściciela instancji DB2.
      ```
      su - dsrdbm01
      ```
   b. Uruchom komendę db2profile dla użytkownika.
      ```
      sqllib/db2profile
      ```
   c. Utwórz kopię zapasową bazy danych DB2 dla instancji.
      ```
      db2 backup database dsrdbm01 to
      katalog_kopii_zapasowej_bazy_danych
      ```
      Właściciel bazy danych musi mieć uprawnienia odczytu, zapisu i wykonywania w katalogu kopii zapasowej bazy danych katalog_kopii_zapasowej_bazy_danych.
   d. Utwórz kopię zapasową bazy danych dziennika zmian, jeśli jest skonfigurowana dla instancji serwera katalogów.
      ```
      db2 backup db ldapclog to
      katalog_kopii_zapasowej_dziennika_zmian
      ```
      Właściciel bazy danych musi mieć uprawnienia odczytu, zapisu i wykonywania w katalogu kopii dziennika zmian katalog_kopii_zapasowej_dziennika_zmian.
   e. Uruchom komendę exit, aby wyjść z kontekstu użytkownika.
4. Usuń instancję serwera katalogów z bazą danych. Więcej informacji na temat usuwania instancji z bazą danych zawiera sekcja “Usuwanie instancji za pomocą programu narzędziowego dla wiersza komend” na stronie 163.
5. Zmień bieżący katalog roboczy na podkatalog sbin w miejscu instalacji produktu IBM Security Directory Server w wersji 6.3.1.
6. Aby użyć katalogu kopii zapasowej instancji do zdalnej aktualizacji instancji, uruchom komendę **idsimigr** w następującym formacie:

```
idsimigr -I dsrdbm01 -u
miejsce_kopii_zapasowej_instancji -l
katalog_główny_instancji -n
```

7. Aby skonfigurować instancję, uruchom komendę **idscfgdb** w następującym formacie:

```
idscfgdb -I dsrdbm01 -a
właściciel_bazy_danych -w hasło
 -t dsrdbm01 -l katalog_główny_instancji -n
```

8. Jeśli skonfigurowano bazę danych dziennika zmian dla instancji, skonfiguruj bazę danych dziennika zmian dla instancji:

```
idscfgchglg -I dsrdbm01 -n
```

9. Odtwórz bazę danych z kopii zapasowej. Aby odtworzyć bazę danych instancji dsrdbm01, wykonaj następujące kroki:
   a. Przełącz kontekst użytkownika na właściciela instancji DB2.

```
su - dsrdbm01
```

   b. Odtwórz bazę danych DB2 dla instancji.

```
db2 restore database dsrdbm01 from
katalog_kopii_zapasowej_bazy_danych replace existing
```

   c. Odtwórz bazę danych dziennika zmian, jeśli jest skonfigurowana dla instancji serwera katalogów.

```
db2 restore db ldapclog from
katalog_kopii_zapasowej_dziennika_zmian
```

   d. Uruchom komendę exit, aby wyjść z kontekstu użytkownika.

10. Aby wpisać do katalogu odtworzoną bazę danych, uruchom następujące komendy:

```
su - dsrdbm01
db2 uncatalog database dsrdbm01
db2 catalog database dsrdbm01 as dsrdbm01 authentication server
exit
```

11. Aby wpisać do katalogu odtworzoną bazę danych dziennika zmian, uruchom następujące komendy:

```
su - dsrdbm01
db2 uncatalog database ldapclog
db2 catalog database ldapclog as ldapclog authentication server
exit
```

12. Uruchom serwer katalogów i serwer administracyjny.

```
ibmslapd -I dsrdbm01 -n -t
ibmdiradm -I dsrdbm01
```

# Migrowanie rozwiązania zarządzania dziennikami

Istnieje możliwość zmigrowania rozwiązania zarządzania dziennikami skonfigurowanego z instancją w poprzedniej wersji do instancji 6.3.1.

## Zanim rozpoczniesz

Przed migrowaniem rozwiązania zarządzania dziennikami z instancji w poprzedniej wersji do instancji wersji 6.3.1 wykonaj następujące czynności:

- Wykonaj instalację produktu IBM Security Directory Server w wersji 6.3.1. Patrz sekcja “Uruchamianie instalacji” na stronie 28.
- Wykonaj instalację produktu IBM Security Directory Integrator w wersji 7.1, jeśli nie jest zainstalowany na komputerze.
- Zaloguj się jako użytkownik root w systemie operacyjnym AIX, Linux lub Solaris i jako członek grupy administratorów w systemie operacyjnym Windows.

### Procedura

1. Utwórz kopię zapasową pliku solution.properties, który znajduje się w katalogu *katalog_główny_instancji_serwera_katalogów*/idsslapd-*nazwa_instancji*/etc/logmgmt dla istniejącej instancji serwera katalogów.
2. Zaktualizuj poprzednią wersję instancji do instancji wersji 6.3.1. Informacje na ten temat zawiera sekcja Rozdział 14, “Aktualizowanie instancji starszej wersji”, na stronie 89.
3. Usuń wszystkie pliki i podkatalogi z katalogu *katalog_główny_instancji_serwera_katalogów*/idsslapd-*nazwa_instancji*/etc/logmgmt dla zaktualizowanej instancji.
4. Jeśli produkt IBM Security Directory Integrator jest w wersji wcześniejszej niż 7.1, przeprowadź instalację produktu IBM Security Directory Integrator w wersji 7.1.
5. Przełącz kontekst użytkownika na właściciela instancji serwera katalogów.

   ```
   su - właściciel_instancji
   ```
6. Skopiuj następujące pliki:
   a. Skopiuj pliki i katalogi z *miejsce_instalacji_Directory_Integrator_7.1*/etc do *katalog_główny_instancji_serwera_katalogów*/idsslapd-*nazwa_instancji*/etc/logmgmt.
   b. Skopiuj pliki i katalogi z *miejsce_instalacji_Directory_Integrator_7.1*/serverapi do *katalog_główny_instancji_serwera_katalogów*/idsslapd-*nazwa_instancji*/etc/logmgmt.
   c. Skopiuj *miejsce_instalacji_Directory_Integrator_7.1*/idisrv.sth do *katalog_główny_instancji_serwera_katalogów*/idsslapd-*nazwa_instancji*/etc/logmgmt.
   d. Skopiuj *miejsce_instalacji_Directory_Integrator_7.1*/testserver.jks do *katalog_główny_instancji_serwera_katalogów*/idsslapd-*nazwa_instancji*/etc/logmgmt.
7. Utwórz katalog o nazwie logs w *katalog_główny_instancji_serwera_katalogów*/idsslapd-*nazwa_instancji*/etc/logmgmt.
8. Dodaj wpis systemqueue.on=false na końcu pliku *katalog_główny_instancji_serwera_katalogów*/idsslapd-*nazwa_instancji*/etc/logmgmt/solutions.properties.
9. Jeśli ścieżka instalacji produktu IBM Security Directory Integrator w wersji 7.1 różni się od ścieżki domyślnej, ustaw w zmiennej *IDS_LDAP_TDI_HOME* miejsce instalacji.
10. Uruchom rozwiązanie zarządzania dziennikami.

## Migrowanie rozwiązania SNMP

Istnieje możliwość zmigrowania rozwiązania SNMP (Simple Network Management Protocol) skonfigurowanego z instancją w poprzedniej wersji do instancji 6.3.1.

### Zanim rozpoczniesz

Przed migrowaniem rozwiązania SNMP z instancji w poprzedniej wersji do instancji wersji 6.3.1 wykonaj następujące czynności:

- Wykonaj instalację produktu IBM Security Directory Server w wersji 6.3.1. Patrz sekcja “Uruchamianie instalacji” na stronie 28.
- Wykonaj instalację produktu IBM Security Directory Integrator w wersji 7.1, jeśli nie jest zainstalowany na komputerze.
- Zaloguj się jako użytkownik root w systemie operacyjnym AIX, Linux lub Solaris i jako członek grupy administratorów w systemie operacyjnym Windows.

## Procedura

1. Utwórz kopię zapasową katalogu snmp w miejscu instalacji produktu IBM Security Directory Server powiązanym z istniejącą instancją w poprzedniej wersji.
2. Zaktualizuj poprzednią wersję instancji do instancji wersji 6.3.1. Informacje na ten temat zawiera sekcja Rozdział 14, “Aktualizowanie instancji starszej wersji”, na stronie 89.
3. Zastąp plik /idstools/snmp/idssnmp.conf znajdujący się w ścieżce instalacji produktu IBM Security Directory Server w wersji 6.3.1 plikiem /idstools/snmp/idssnmp.conf znajdującym się w ścieżce instalacji poprzedniej wersji produktu IBM Security Directory Server.
4. Zastąp plik /idstools/snmp/idssnmp.properties znajdujący się w ścieżce instalacji produktu IBM Security Directory Server w wersji 6.3.1 plikiem /idstools/snmp/idssnmp.properties znajdującym się w ścieżce instalacji poprzedniej wersji produktu IBM Security Directory Server.
5. Zastąp plik /idstools/snmp/IBM-DIRECTORYSERVER-MIB znajdujący się w ścieżce instalacji produktu IBM Security Directory Server w wersji 6.3.1 plikiem /idstools/snmp/IBM-DIRECTORYSERVER-MIB znajdującym się w ścieżce instalacji poprzedniej wersji produktu IBM Security Directory Server.
6. Zastąp plik /idstools/snmp/INET-ADDRESS-MIB znajdujący się w ścieżce instalacji produktu IBM Security Directory Server w wersji 6.3.1 plikiem /idstools/snmp/INET-ADDRESS-MIB znajdującym się w ścieżce instalacji poprzedniej wersji produktu IBM Security Directory Server.
7. Jeśli ścieżka instalacji produktu IBM Security Directory Integrator w wersji 7.1 różni się od ścieżki domyślnej, ustaw w zmiennej *IDS_LDAP_TDI_HOME* miejsce instalacji.
8. Uruchom rozwiązanie SNMP.

# Migrowanie rozwiązania synchronizacji z Active Directory

Istnieje możliwość zmigrowania rozwiązania synchronizacji z Active Directory skonfigurowanego z instancją w poprzedniej wersji do instancji 6.3.1.

## Zanim rozpoczniesz

Przed migrowaniem rozwiązania synchronizacji z Active Directory z instancji w poprzedniej wersji do instancji wersji 6.3.1 wykonaj następujące czynności:

- Wykonaj instalację produktu IBM Security Directory Server w wersji 6.3.1. Patrz sekcja “Uruchamianie instalacji” na stronie 28.
- Wykonaj instalację produktu IBM Security Directory Integrator w wersji 7.1, jeśli nie jest zainstalowany na komputerze.
- Zaloguj się jako użytkownik root w systemie operacyjnym AIX, Linux lub Solaris i jako członek grupy administratorów w systemie operacyjnym Windows.

W produkcie IBM Security Directory Server od wersji 6.3.1 synchronizacja z Active Directory jest funkcją nieaktualną. Zamiast tego należy użyć rozwiązania LDAPSync.

## Procedura

1. Zaktualizuj poprzednią wersję instancji do instancji wersji 6.3.1. Informacje na ten temat zawiera sekcja Rozdział 14, “Aktualizowanie instancji starszej wersji”, na stronie 89.
2. Utwórz instancję serwera katalogów. Informacje na ten temat zawiera sekcja “Tworzenie instancji za pomocą programu Instance Administration Tool” na stronie 134.
3. Skonfiguruj instancję serwera katalogów dla synchronizacji z Active Directory. Informacje na ten temat zawiera sekcja “Synchronizowanie z Active Directory” na stronie 212.

4. Odtwórz zmiany w pliku *katalog_główny_instancji_serwera_katalogów*/idsslapd-*nazwa_instancji*/etc/tdisoldir/solution.properties sprzed zaktualizowania instancji.

   **Uwaga:** Jeśli nowo utworzony plik solution.properties zostanie zastąpiony wcześniejszym plikiem, synchronizacja Active Directory może się nie powieść. Format pliku solution.properties utworzonego po uruchomieniu komendy **idsadscfg** różni się od wcześniejszego pliku.
5. Uruchom rozwiązanie synchronizacji z Active Directory. Więcej informacji na temat komendy **idsadsrun** zawiera publikacja *Skorowidz komend*.

## Migrowanie konfiguracji poprzedniej wersji programu Web Administration Tool

Migrowanie konfiguracji poprzedniej wersji programu Web Administration Tool pozwala na dalsze korzystanie z tych samych ustawień w nowszej wersji programu Web Administration Tool.

Aby przeprowadzić migrację istniejącej konfiguracji narzędzia Web Administration Tool za pomocą komendy **idswmigr**, muszą być spełnione następujące kryteria:

1. Starsza wersja narzędzia Web Administration Tool jest zainstalowana na komputerze.
2. Starsza wersja wbudowanego serwera WebSphere Application Server jest zainstalowana na komputerze.
3. Starsza wersja narzędzia Web Administration Tool jest wdrożona w starszej wersji wbudowanego serwera WebSphere Application Server.
4. Zainstaluj program Web Administration Tool udostępniony z produktem IBM Security Directory Server w wersji 6.3.1.
5. Zainstaluj wbudowany serwer WebSphere Application Server dostarczany z produktem IBM Security Directory Server w wersji 6.3.1.
6. Nie wdrażaj narzędzia Web Administration Tool, które pochodzi z wersji 6.3.1 wbudowanego serwera WebSphere Application Server.

Obsługiwane jest migrowanie programu Web Administration Tool wdrożonego we wbudowanej wersji serwera WebSphere Application Server dostarczanego z następującymi wersjami produktu IBM Security Directory Server:

- IBM Security Directory Server 6.1 i wbudowany serwer WebSphere Application Server w wersji 6.1.0.7 lub nowszej
- IBM Security Directory Server 6.2 i wbudowany serwer WebSphere Application Server w wersji 6.1.0.13 lub nowszej (UNIX) lub wbudowany serwer WebSphere Application Server w wersji 6.1.0.17 (Windows) lub nowszej
- IBM Security Directory Server 6.3 i wbudowany serwer WebSphere Application Server w wersji 7.0.0.7 lub nowszej

Gdy do migrowania ustawień konfiguracyjnych poprzedniej wersji programu Web Administration Tool używana jest komenda **idswmigr**, wykonuje ona następujące operacje:

1. Zapisuje pliki konfiguracyjne poprzedniej wersji programu Web Administration Tool.
2. Anuluje wdrożenie poprzedniej wersji programu Web Administration Tool w poprzedniej wersji wbudowanego serwera WebSphere Application Server.
3. Tworzy kopię zapasową konfiguracji poprzedniej wersji wbudowanego serwera WebSphere Application Server w położeniu wskazanym przez użytkownika.
4. Odtwarza konfigurację poprzedniej wersji wbudowanego serwera WebSphere Application Server.

5. Wdraża program Web Administration Tool w bieżącej wersji wbudowanego serwera WebSphere Application Server dostarczanego z produktem IBM Security Directory Server, 6.3.1.
6. Migruje pliki konfiguracyjne poprzedniej wersji programu Web Administration Tool i odtwarza je w nowszej wersji wbudowanego serwera WebSphere Application Server.

**Uwaga:** Można wykonać migrację narzędzia Web Administration Tool za pomocą programu IBM Installation Manager, tylko jeśli główna wersja wbudowanego serwera WebSphere Application Server, która ma być migrowana, jest starsza niż główna wersja nowo instalowanego wbudowanego serwera WebSphere Application Server.

# idswmigr

Komenda **idswmigr** służy do migrowania istniejącej konfiguracji narzędzia Web Administration Tool ze starszej do nowszej wersji narzędzia Web Administration Tool.

## Opis

Aby przeprowadzić migrację istniejącej konfiguracji narzędzia Web Administration Tool za pomocą komendy **idswmigr**, muszą być spełnione następujące kryteria:

1. Starsza wersja narzędzia Web Administration Tool jest zainstalowana na komputerze.
2. Starsza wersja wbudowanego serwera WebSphere Application Server jest zainstalowana na komputerze.
3. Starsza wersja narzędzia Web Administration Tool jest wdrożona w starszej wersji wbudowanego serwera WebSphere Application Server.
4. Zainstaluj starszą wersję narzędzia Web Administration Tool.
5. Zainstaluj starszą wersję wbudowanego serwera WebSphere Application Server.
6. Nie wdrażaj narzędzia Web Administration Tool, które pochodzi z nowszej wersji wbudowanego serwera WebSphere Application Server.

## Konspekt

```
idswmigr -l ścieżka_tymczasowa [-s ścieżka_źródłowa -t ścieżka_docelowa
          -r nazwa_profilu -a nazwa_aplikacji -v -o ścieżka_do_portów]
```

## Opcje

Komenda **idswmigr** ma następujące parametry:

**-a** *nazwa_aplikacji*
Określa nazwę aplikacji. Jeśli parametr nie zostanie podany, przyjmowana jest wartość domyślna IDSWebApp.war.

**-l** *ścieżka_tymczasowa*
Określa położenie zapisywania plików tymczasowych.

**-o** *ścieżka_do_portów*
Określa pełną ścieżkę do pliku definicji portów. Jeśli parametr nie zostanie podany, używane są następujące ścieżki domyślne:

**Windows**
C:\Program Files\IBM\ldap\V6.3.1\idstools\TDSWEBPortDef.props

**AIX i Solaris**
/opt/IBM/ldap/V6.3.1/idstools/TDSWEBPortDef.props

**Linux** /opt/ibm/ldap/V6.3.1/idstools/TDSWEBPortDef.props

**-r** *nazwa_profilu*
Określa nazwę profilu powiązanego z aplikacją. Jeśli parametr nie zostanie podany, przyjmowana jest wartość domyślna TDSWebAdminProfile.

**-s** *ścieżka_źródłowa*
Określa położenie źródłowe starszej wersji wbudowanego serwera WebSphere Application Server.

**-t** *ścieżka_docelowa*
Określa położenie instalacyjne nowszej wersji wbudowanego serwera WebSphere Application Server.

**-v** Wyświetla informacje o wersji.

## Przykłady

**Przykład 1**

Aby przeprowadzić migrację istniejącej konfiguracji narzędzia Web Administration Tool z wersji 6.2 do wersji 6.3.1, wykonaj następującą komendę:

```
idswmigr -l /tmp/web_migr -s /opt/ibm/ldap/V6.2/appsrv \
-t /opt/ibm/ldap/V6.3.1/appsrv -r TDSWebAdminProfile \
-a IDSWebApp.war
```

# Ręczne migrowanie narzędzia Web Administration Tool

Narzędzie Web Administration Tool można migrować ręcznie.

## Zanim rozpoczniesz

Aby ręcznie przeprowadzić migrację narzędzia Web Administration Tool, należy najpierw zainstalować to narzędzie. Wykonaj następujące kroki, aby przeprowadzić ręczną migrację narzędzia Web Administration Tool. W przedstawionym przykładzie narzędzie Web Administration Tool w produkcie IBM Security Directory Server 6.3 jest migrowane do produktu IBM Security Directory Server 6.3.1.

W systemie AIX komendy migracji są podobne do komend w systemie Linux, poza ścieżką /opt/ibm/ldap, którą należy zastąpić ścieżką /opt/IBM/ldap.

## Procedura

1. W przypadku systemu Windows, dodaj usługę WebSphere Application Server za pomocą następującej komendy:

   ```
   "C:\Program Files\IBM\ldap\V6.3.1\appsrv\bin\WASService.exe" -add
   TDSWebAdmin-V6.3.1 -serverName server1 -profilePath
   "C:\Program Files\IBM\ldap\V6.3.1\appsrv\profiles\TDSWebAdminProfile"
   -startType automatic
   ```

2. Utwórz kopię zapasową plików narzędzia Web Administration Tool z poprzedniej wersji.
   - W systemie Windows te pliki znajdują się w katalogu:

     ```
     C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\
      installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\
      WEB-INF\classes\
     ```

     lub

     ```
     C:\Program Files\IBM\LDAP\V6.3\appsrv\installedApps\DefaultNode
     \IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\classes
     ```

   - W systemie Linux te pliki znajdują się w następującym katalogu:

     ```
     /opt/ibm/ldap/V6.3/appsrv/profiles/TDSWebAdminProfile/installedApps
     /DefaultNode/IDSWebApp.war.ear/IDSWebApp.war/WEB-INF/classes
     ```

lub

```
/opt/ibm/ldap/V6.3/appsrv/installedApps/DefaultNode
/IDSWebApp.war.ear/IDSWebApp.war/WEB-INF/classes
```

Skopiuj tylko pięć następujących plików z katalogów:

security\console_passwd

IDSConfig\IDSSessionConfig\IDSSessionMgmt.xml

IDSConfig\IDSServersConfig\IDSServersInfo.xml

IDSConfig\IDSAppReg\IDSAppReg.xml

IDSConfig\IDSSearchSettings\IDSSearchMgmt.xml

Na przykład:

```
  copy "C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\
installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\classes\
security\console_passwd" c:\BackUp
  copy "C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\
installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\classes\
IDSConfig\IDSSessionConfig\IDSSessionMgmt.xml" c:\BackUp
  copy "C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\
installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\classes\
IDSConfig\IDSServersConfig\IDSServersInfo.xml" c:\BackUp
  copy "C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\
installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\classes\
IDSConfig\IDSAppReg\IDSAppReg.xml" c:\BackUp
  copy "C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\
installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\classes\
IDSConfig\IDSSearchSettings\IDSSearchMgmt.xml" c:\BackUp
```

3. Zdeinstaluj plik WAR z poprzedniej wersji.
   - W systemie Windows komenda znajduje się w następującym katalogu:

     ```
     C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\bin\wsadmin.bat
     ```

     lub

     ```
     C:\Program Files\IBM\LDAP\V6.3\appsrv\bin\wsadmin.bat
     ```

   - W systemie Linux komenda znajduje się w następującym katalogu:

     ```
     /opt/ibm/ldap/V6.3/appsrv/profiles/TDSWebAdminProfile/bin/wsadmin.sh
     ```

     lub

     ```
     /opt/ibm/ldap/V6.3/appsrv/bin/wsadmin.sh
     ```

   ```
   wsadmin.bat -conntype NONE -c "$AdminApp uninstall IDSWebApp.war"
   ```

   Na przykład:

   ```
   "C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\bin\wsadmin.bat"
    -conntype NONE -c "$AdminApp uninstall IDSWebApp.war"
   ```

4. Jeśli jest uruchomiony serwer poprzedniego wbudowanego serwera WebSphere Application Server, należy zatrzymać serwer aplikacji.
   - W systemie Windows komenda znajduje się w następującym katalogu:

     ```
     C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\bin\
     stopServer.bat
     ```

     lub

     ```
     C:\Program Files\IBM\LDAP\V6.3\appsrv\bin\stopServer.bat
     ```

   - W systemie Linux komenda znajduje się w następującym katalogu:

     ```
     /opt/ibm/ldap/V6.3/appsrv/profiles/TDSWebAdminProfile/bin/stopServer.sh
     ```

     lub

```
/opt/ibm/ldap/V6.3/appsrv/bin/stopServer.sh
```

Na przykład:

```
"C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\bin\
stopServer.bat" server1
```

5. Sprawdź, czy w nowym wbudowanym serwerze WebSphere Application Server istnieje profil. Jeśli profil nie istnieje, utwórz nowy profil.
   - W systemie Windows uruchom następującą komendę, aby utworzyć nowy profil:

     ```
     "C:\Program Files\IBM\LDAP\V6.3.1\appsrv\bin\manageprofiles.bat" -create
      -profileName TDSWebAdminProfile -profilePath "C:\Program Files\IBM\
      LDAP\V6.3.1\appsrv\profiles\TDSWebAdminProfile" -templatePath
      "C:\Program Files\IBM\LDAP\V6.3.1\appsrv\ profileTemplates\default"
      -nodeName DefaultNode -hostName localhost -cellName
      DefaultNode -isDefault -portsFile "C:\Program Files\IBM\LDAP\V6.3.1\idstools
      \TDSWEBPortDef.props"
     ```

   - W systemie Linux uruchom następującą komendę, aby utworzyć nowy profil:

     ```
     /opt/ibm/ldap/V6.3.1/appsrv/bin/manageprofiles.sh -create -profileName
      TDSWebAdminProfile -profilePath "/opt/ibm/ldap/V6.3.1/appsrv/profiles/
      TDSWebAdminProfile" -templatePath "/opt/ibm/ldap/V6.3.1/appsrv/
      profileTemplates/default" -nodeName DefaultNode -hostName localhost
      -cellName DefaultNode -isDefault -portsFile "/opt/ibm/ldap/V6.3.1/idstools
      /TDSWEBPortDef.props"
     ```

6. Skopiuj nowy plik WAR do katalogu nowego serwera WebSphere Application Server.
   - W systemie Windows uruchom następującą komendę:

     ```
     copy "C:\Program Files\IBM\LDAP\V6.3.1\idstools\IDSWebApp.war"
      "C:\Program Files\IBM\LDAP\V6.3.1\appsrv\profiles\TDSWebAdminProfile\
      installableApps"
     ```

   - W systemie Linux uruchom następującą komendę:

     ```
     cp "/opt/ibm/ldap/V6.3.1/idstools/IDSWebApp.war"
      "/opt/ibm/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/installableApps"
     ```

7. Zainstaluj nowy plik WAR w nowym produkcie WebSphere Application Server.
   - W systemie Windows uruchom następującą komendę:

     ```
     "C:\Program Files\IBM\LDAP\V6.3.1\appsrv\profiles\TDSWebAdminProfile\bin
      \wsadmin.bat" -conntype NONE -c "$AdminApp install {C:\Program Files\
      IBM\LDAP\V6.3.1\appsrv\profiles\TDSWebAdminProfile\installableApps\
      IDSWebApp.war} {-configroot \"C:\Program Files\IBM\LDAP\V6.3.1\
      appsrv\config\" -node DefaultNode -usedefaultbindings -nodeployejb
      -appname IDSWebApp.war -contextroot \"IDSWebApp\"}"
     ```

   - W systemie Linux uruchom następującą komendę:

     ```
     "/opt/ibm/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/bin/wsadmin.sh"
      -conntype NONE -c "\$AdminApp install {/opt/ibm/ldap/V6.3.1/appsrv/
      profiles/TDSWebAdminProfile/installableApps/IDSWebApp.war}
      {-configroot \"/opt/ibm/ldap/V6.3.1/appsrv/config\"
      -node DefaultNode -usedefaultbindings -nodeployejb -appname IDSWebApp.war
      -contextroot \"IDSWebApp\"}"
     ```

8. Odtwórz zapisane wcześniej pliki konfiguracyjne narzędzia Web Administration Tool.
   - W systemie Windows zastąp następujące pliki plikami z kopii zapasowej:

     ```
     C:\Program Files\IBM\LDAP\V6.3.1\appsrv\profiles\TDSWebAdminProfile\
      installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\
      classes\security\console_passwd
      C:\Program Files\IBM\LDAP\V6.3.1\appsrv\profiles\TDSWebAdminProfile\
      installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\
      classes\IDSConfig\IDSSessionConfig\IDSSessionMgmt.xml
      C:\Program Files\IBM\LDAP\V6.3.1\appsrv\profiles\TDSWebAdminProfile\
      installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\
      classes\IDSConfig\IDSServersConfig\IDSServersInfo.xml
      C:\Program Files\IBM\LDAP\V6.3.1\appsrv\profiles\TDSWebAdminProfile\
      installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\
     ```

```
classes\IDSConfig\IDSAppReg\IDSAppReg.xml
C:\Program Files\IBM\LDAP\V6.3.1\appsrv\profiles\TDSWebAdminProfile\
installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\
classes\IDSConfig\IDSSearchSettings\IDSSearchMgmt.xml
```

- W systemie Linux zastąp następujące pliki plikami z kopii zapasowej:

```
/opt/ibm/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/installedApps/
 DefaultNode/IDSWebApp.war.ear/IDSWebApp.war/WEB-INF/classes/security/
 console_passwd
 /opt/ibm/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/installedApps/
 DefaultNode/IDSWebApp.war.ear/IDSWebApp.war/WEB-INF/classes/IDSConfig/
 IDSSessionConfig/IDSSessionMgmt.xml
 /opt/ibm/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/installedApps/
 DefaultNode/IDSWebApp.war.ear/IDSWebApp.war/WEB-INF/classes/IDSConfig/
 IDSServersConfig/IDSServersInfo.xml
 /opt/ibm/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/installedApps/
 DefaultNode/IDSWebApp.war.ear/IDSWebApp.war/WEB-INF/classes/IDSConfig/
 IDSAppReg/IDSAppReg.xml
 /opt/ibm/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/installedApps/
 DefaultNode/IDSWebApp.war.ear/IDSWebApp.war/WEB-INF/classes/IDSConfig/
 IDSSearchSettings/IDSSearchMgmt.xml
```

9. W systemie Windows uruchom dodaną usługę.

```
"C:\Program Files\IBM\ldap\V6.3.1\appsrv\bin\WASService.exe"
 -start TDSWebAdmin-V6.3.1
```

10. W systemie Linux uruchom serwer.

```
/opt/ibm/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/bin/startServer.sh server1
```

# Rozdział 16. Ręczne wdrażanie programu Web Administration Tool

Aby umożliwić zarządzanie i administrowanie instalacjami serwera katalogów za pomocą programu Web Administration Tool, należy wdrożyć program Web Administration Tool w obsługiwanym serwerze aplikacji.

Do wdrożenia programu Web Administration Tool niezbędne jest zainstalowanie obsługiwanej wersji serwera aplikacji. Nośnik instalacyjny produktu IBM Security Directory Server zawiera wbudowaną wersję serwera WebSphere Application Server 7.0.0.25. Do zainstalowania programu Web Administration Tool i wdrożenia go we wbudowanej wersji serwera WebSphere Application Server można użyć programu IBM Installation Manager.

Jeśli używany system operacyjny nie obsługuje instalowania produktu IBM Security Directory Server za pomocą programu IBM Installation Manager, należy ręcznie zainstalować wbudowany serwer WebSphere Application Server. Po zainstalowaniu wbudowanego serwera WebSphere Application Server należy wdrożyć w nim program Web Administration Tool.

Jeśli w systemie jest już zainstalowana obsługiwana wersja serwera WebSphere Application Server, można w niej wdrożyć program Web Administration Tool.

Serwer WebSphere Application Server jest środowiskiem wykonawczym IBM dla aplikacji Java. Więcej informacji znajduje się w dokumentacji produktu WebSphere Application Server pod adresem http://www-01.ibm.com/support/knowledgecenter/SSEQTP/welcome.

## Samodzielne instalowanie wbudowanego serwera WebSphere Application Server

Aby wdrożyć program Web Administration Tool, należy przeprowadzić instalację wbudowanego serwera WebSphere Application Server na komputerze.

### Zanim rozpoczniesz

Aby zainstalować wbudowany serwer WebSphere Application Server, wykonaj następujące kroki:

1. Znajdź nośnik instalacyjny produktu IBM Security Directory Server z plikami instalacyjnymi wbudowanego serwera WebSphere Application Server. Informacje na ten temat zawiera sekcja “Przygotowanie nośnika instalacyjnego” na stronie 6.

### O tym zadaniu

Aby wdrożyć program Web Administration Tool za pomocą komendy deploy_IDSWebApp bez jakichkolwiek parametrów, należy podać następujące wartości:

1. Podaj katalog appsrv w ścieżce instalacji produktu IBM Security Directory Server jako miejsce instalacji wbudowanego serwera WebSphere Application Server. Więcej informacji na temat domyślnej ścieżki instalacji produktu IBM Security Directory Server zawiera sekcja “Domyślne położenia instalacji” na stronie 27.

Dla wbudowanego serwera WebSphere Application Server można podać dowolne inne miejsce instalacji. W takim przypadku należy w komendzie deploy_IDSWebApp w celu wdrożenia programu Web Administration Tool podać parametry **-w**, **-p**, **-r** oraz **-o** z wartościami.

### Procedura

1. Zaloguj się z uprawnieniami administratora.
2. Otwórz wiersz komend.
3. Zmień bieżący katalog roboczy na katalog zawierający pliki instalacyjne wbudowanego serwera WebSphere Application Server.
4. Aby zainstalować wbudowany serwer WebSphere Application Server w domyślnej ścieżce instalacji produktu IBM Security Directory Server, uruchom następującą komendę:

| Systemy operacyjne | Komenda do uruchomienia: |
|---|---|
| **Microsoft Windows** | install.bat -installRoot c:\Program Files\IBM\ldap\V6.3.1\appsrv |
| **AIX i Solaris** | install.sh -installRoot /opt/IBM/ldap/V6.3.1\ appsrv |
| **Linux** | install.sh -installRoot /opt/ibm/ldap/V6.3.1\ appsrv |

### Co dalej

Jeśli program Web Administration Tool nie jest zainstalowany na komputerze, przeprowadź instalację programu Web Administration Tool. Informacje na ten temat zawiera sekcja Rozdział 12, “Instalowanie z użyciem programów narzędziowych systemu operacyjnego”, na stronie 67.

Jeśli na komputerze jest zainstalowany program Web Administration Tool, przeprowadź wdrożenie programu Web Administration Tool. Patrz sekcja “Wdrażanie programu Web Administration Tool na wbudowanym serwerze WebSphere Application Server” na stronie 111.

## Domyślne porty programu Web Administration Tool

Aby uniknąć konfliktów portów między programem Web Administration Tool i innymi aplikacjami, należy znać domyślne porty używane przez program Web Administration Tool.

Wbudowana wersja serwera aplikacji WebSphere Application Server używa następujących portów domyślnych dla programu Web Administration Tool:

- port transportowy HTTP (port 1): 12100
- port transportowy HTTPS (port 2): 12101
- konsola administratora (do administrowania serwerem WebSphere Application Server), port: 12104
- bezpieczna konsola administratora (do administrowania serwerem WebSphere Application Server), port: 12105

Wbudowana wersja serwera aplikacji WebSphere Application Server używa następujących portów domyślnych dla innych aplikacji:

- port bootstrap/rmi: 12102
- port konektora soap: 12103

Inne porty, które mogą być używane przez wbudowaną wersję serwera WebSphere Application Server: 9405, 9406, 9407, 9375, 9105, 7276, 7286, 5558, 5577, 5075, 5076.

Jeśli występują konflikty portów domyślnych z inną aplikacją, wykonaj jedno z poniższych działań w zależności od stosowanego środowiska:

- Zmień porty domyślne na nieużywane porty i zrestartuj aplikację.
- Jeśli aplikacja, która używa portów domyślnych, nie jest ważną usługą albo serwerem, zmień jej porty, aby uwolnić port domyślny.

Aby zmienić porty domyślne używane przez aplikację wbudowanego serwera WebSphere Application Server, należy ustawić odpowiedni numer w pliku portdef.props. Plik portdef.props znajduje się w podkatalogu \appsrv\profiles\TDSWebAdminProfile\properties\ katalogu instalacyjnego produktu IBM Security Directory Server. Więcej informacji na temat domyślnego katalogu instalacyjnego produktu IBM Security Directory Server zawiera sekcja “Domyślne położenia instalacji” na stronie 27.

**Port transportowy HTTP 1**
Aby zmienić numer portu transportowego HTTP, zmień pozycję z numerem portu 12100 na numer odpowiadający nieużywanemu portowi.

**Port transportowy HTTPS 2**
Aby zmienić numer portu transportowego HTTPS, zmień pozycję z numerem portu 12101 na numer odpowiadający nieużywanemu portowi.

**Port bootstrap/rmi**
Aby zmienić numer portu transportowego bootstrap/rmi, zmień pozycję z numerem portu 12102 na numer odpowiadający nieużywanemu portowi.

**Port konektora soap**
Aby zmienić numer portu transportowego soap, zmień pozycję z numerem portu 12103 na numer odpowiadający nieużywanemu portowi.

**Port konsoli administratora**
Aby zmienić numer portu konsoli administratora, zmień pozycję z numerem portu 12104 na numer odpowiadający nieużywanemu portowi.

**Port bezpiecznej konsoli administratora**
Aby zmienić numer bezpiecznego portu konsoli administratora, zmień pozycję z numerem portu 12105 na numer odpowiadający nieużywanemu portowi.

# Wdrażanie programu Web Administration Tool na wbudowanym serwerze WebSphere Application Server

Aby użyć narzędzia Web Administration Tool, należy je wdrożyć w serwerze aplikacji WWW.

## Zanim rozpoczniesz

Przed wdrożeniem narzędzia Web Administration Tool należy wykonać następujące czynności:

1. Wykonaj instalację pakietu Web Administration Tool dla danego systemu operacyjnego.
2. Wykonaj instalację obsługiwanej wersji serwera aplikacji WWW.
3. Jeśli planowane jest migrowanie istniejącej konfiguracji narzędzia Web Administration Tool z poprzedniej wersji, nie należy wdrażać nowszej wersji narzędzia Web Administration Tool.

## O tym zadaniu

Podczas wdrażania narzędzia Web Administration Tool komenda wykonuje następujące działania:

1. Usuwa wcześniejszą wersję narzędzia Web Administration Tool, jeśli istnieje.
2. Wdraża narzędzie Web Administration Tool w serwerze aplikacji WWW.
3. Uruchamia serwer aplikacji WWW.

### Procedura

1. Zaloguj się z uprawnieniami administratora.
2. Przejdź do katalogu *miejsce_instalacji_serwera_katalogów*/idstools. Wartość *miejsce_instalacji_serwera_katalogów* jest miejscem instalacji produktu IBM Security Directory Server. Poniżej wymieniono domyślne miejsca instalacji dla różnych systemów operacyjnych:

| Systemy operacyjne | Domyślne miejsca instalacji: |
|---|---|
| Microsoft Windows | c:\Program Files\IBM\ldap\V6.3.1 |
| AIX i Solaris | /opt/IBM/ldap/V6.3.1 |
| Linux | /opt/ibm/ldap/V6.3.1 |

3. Uruchom komendę:

   **Uwaga:** Jeśli zainstalowano wbudowany serwer WebSphere Application Server w domyślnym katalogu instalacji produktu IBM Security Directory Server, nie należy podawać żadnych parametrów w komendzie deploy_IDSWebApp. Więcej informacji o komendzie deploy_IDSWebApp zawiera składnia komendy, deploy_IDSWebApp -h.

| Systemy operacyjne | Komenda do uruchomienia: |
|---|---|
| **Microsoft Windows** | deploy_IDSWebApp.bat -w *ścieżka_do_pliku_war* -p *ścieżka_instalacji_was* -r *profil* -o plik_portów |
| **AIX, Linux i Solaris** | deploy_IDSWebApp -w *ścieżka_do_pliku_war* -p *ścieżka_instalacji_was* -r *profil* -o plik_portów |

### Wyniki

Komenda wdraża program Web Administration Tool na serwerze aplikacji WWW podanym w zmiennej *ścieżka_instalacji_was*.

### Co dalej

Aby uzyskać dostęp do narzędzia Web Administration Tool, otwórz okno przeglądarki i wprowadź adres http://*nazwa_hosta*:12100/IDSWebApp. Zmienna *nazwa_hosta* wskazuje nazwę hosta lub adres IP komputera, na którym zainstalowano narzędzie Web Administration Tool.

## Wdrażanie programu Web Administration Tool na serwerze WebSphere Application Server

Aby zarządzać aplikacjami na serwerze za pomocą serwera WebSphere Application Server, można wdrożyć narzędzie Web Administration Tool na serwerze WebSphere Application Server.

## Zanim rozpoczniesz

Aby wdrożyć narzędzie Web Administration Tool na serwerze WebSphere Application Server, należy spełnić następujące wymagania:

1. Wykonaj instalację pakietu Web Administration Tool dla danego systemu operacyjnego. Patrz sekcja “Instalowanie przy użyciu programu IBM Installation Manager” na stronie 31.
2. Komputer musi zawierać obsługiwaną wersję serwera WebSphere Application Server.

## O tym zadaniu

Nośnik instalacyjny produktu IBM Security Directory Server zawiera narzędzie Web Administration Tool i wbudowany serwer WebSphere Application Server. Jeśli na danym komputerze znajduje się serwer WebSphere Application Server, można na nim wdrożyć narzędzie Web Administration Tool. Aby wdrożyć narzędzie Web Administration Tool, należy wdrożyć plik IDSWebApp.war znajdujący się w katalogu idstools w miejscu instalacji produktu IBM Security Directory Server.

## Procedura

1. Użyj adresu URL http://*nazwa_hosta_serwera_WAS*:9060/ibm/console w celu zalogowania się do konsoli administracyjnej WebSphere. Zastąp zmienną *nazwa_hosta_serwera_WAS* nazwą hosta lub adresem IP komputera, na którym jest zainstalowany serwer WebSphere Application Server. Jeśli określono port niestandardowy dostępu do konsoli administracyjnej WebSphere, zastąp port domyślny 9060 tym numerem portu.
2. Podaj ID i hasło użytkownika. Użytkownik musi mieć wymagane uprawnienia do uruchamiania operacji na serwerze WebSphere Application Server.
3. Na lewym panelu nawigacyjnym kliknij opcję **Aplikacja > Nowa aplikacja**.
4. Na stronie **Nowa aplikacja** kliknij opcję **Nowa aplikacja korporacyjna**.
5. Na stronie **Ścieżka do nowej aplikacji** wybierz jedną z następujących opcji w zależności od miejsca, w którym jest dostępna konsola administracyjna WebSphere:
   - W przypadku dostępu do konsoli administracyjnej WebSphere z komputera lokalnego wybierz opcję **Lokalny system plików** i wprowadź ścieżkę do pliku IDSWebApp.war w polu **Pełna ścieżka**. Możesz również kliknąć przycisk **Przeglądaj**, aby określić ścieżkę.
   - W przypadku dostępu do konsoli administracyjnej WebSphere z komputera zdalnego wybierz opcję **Zdalny system plików** i wprowadź ścieżkę do pliku IDSWebApp.war w polu **Pełna ścieżka**. Możesz również kliknąć przycisk **Przeglądaj**, aby określić ścieżkę.
6. Na stronie **W jaki sposób zainstalować aplikację** wybierz opcję **Krótka ścieżka** i kliknij przycisk **Dalej**.
7. Na stronie **Wybierz opcje instalacji** są wybrane opcje domyślne.
8. Kliknij przycisk **Dalej**.
9. Na stronie **Odwzoruj moduły na serwery** można odwzorować moduły na serwery podane w polu **Klastry i serwery**.
   a. Zaznacz pole wyboru wymaganego modułu i kliknij przycisk **Zastosuj**.
   b. Po zakończeniu odwzorowywania kliknij przycisk **Dalej**.
10. Na stronie **Odwzoruj hosty wirtualne dla modułów WWW** można odwzorować aplikację WWW na konkretne serwery wirtualne. Jeśli istnieje więcej hostów wirtualnych, serwer będzie wymagać informacji o środowisku WebSphere w celu wybrania właściwego modułu. W tym przykładzie do wyboru jest dostępna opcja default_host.

11. Kliknij przycisk **Dalej**.
12. Na stronie **Odwzoruj kontekstowe katalogi główne dla modułów WWW** wprowadź w polu kontekstowy katalog główny /IDSWebApp.
13. Zostanie wyświetlone podsumowanie z wybranymi opcjami.
14. Kliknij przycisk **Zakończ**. Spowoduje to zainicjowanie instalowania aplikacji. Zostanie wyświetlone podsumowanie instalacji.
15. Aby zapisać zmiany w konfiguracji głównej, kliknij opcję **Zapisz**.
16. Na lewym panelu nawigacyjnym kliknij opcję **Aplikacje > Typy aplikacji > Aplikacje korporacyjne WebSphere**.
17. Na stronie **Aplikacje korporacyjne** zaznacz pole wyboru obok opcji IDSWebApp_war i kliknij przycisk **Uruchom**.
18. Uruchom program Web Administration Tool.
19. Aby uzyskać dostęp do programu Web Administration Tool, otwórz przeglądarkę i wprowadź następujący adres:
    - Aby uzyskać niezabezpieczony dostęp (HTTP), wprowadź http://nazwa_hosta_serwera_WAS:9080/IDSWebApp.
    - Aby uzyskać bezpieczny dostęp (HTTPS), wprowadź https://nazwa_hosta_serwera_WAS:9443/IDSWebApp

    Port 9080 to domyślny port HTTP dla serwera WebSphere Application Server, a port 9443 jest domyślnym portem HTTPS. Jeśli te porty nie są skonfigurowane dla serwera WebSphere Application Server, należy podać odpowiedni numer portu. Jeśli skonfigurowano zabezpieczenia administracyjne lub globalne dla serwera WebSphere Application Server, należy spełnić następujące wymagania:
    a. Wdróż program Web Administration Tool na serwerze WebSphere Application Server jako nowy profil.
    b. Skonfiguruj protokół SSL dla programu Web Administration Tool.
    c. Jeśli nie jest możliwe wdrożenie programu Web Administration Tool w profilu, dodaj certyfikat serwera katalogów do magazynu zaufanych certyfikatów profilu. W przypadku uwierzytelniania serwer-klient dodaj certyfikat profilu serwera WebSphere Application Server do magazynu zaufanych certyfikatów serwera katalogów.

## Uruchamianie wbudowanego serwera aplikacji WebSphere obsługującego program Web Administration Tool

Uruchom serwer aplikacji WWW, który obsługuje program Web Administration Tool umożliwiający dodawanie, zarządzanie i administrowanie instancjami serwera katalogów.

### Zanim rozpoczniesz

Należy wykonać następujące czynności zanim można będzie uruchomić serwer aplikacji WWW, który obsługuje program narzędziowy Web Administration Tool:

1. Zainstaluj narzędzie Web Administration Tool.
2. Wykonaj wdrożenie narzędzia Web Administration Tool w obsługiwanym serwerze aplikacji WWW.

**Uwaga:** Jeśli używasz programu IBM Installation Manager do zainstalowania i wdrożenia programu Web Administration Tool na wbudowanym serwerze WebSphere Application Server, po uruchomieniu serwera aplikacji wykonaj wdrażanie Web Administration Tool.

## Procedura

1. Aby uruchomić serwer aplikacji WWW, który obsługuje program Web Administration Tool, uruchom następującą komendę:

   **Windows**

   Jeśli serwer aplikacji nie jest uruchomiony, uruchom następującą komendę:

   *ścieżka_instalacji*\idstools\bin\startWebadminApp.bat

   Domyślna ścieżka instalacji to C:\Program Files\IBM\ldap\6.3.1.

   **AIX i Solaris**

   /opt/IBM/ldap/V6.3.1/idstools/bin/startWebadminApp

   **Linux**

   /opt/ibm/ldap/V6.3.1/idstools/bin/startWebadminApp

2. Otwórz przeglądarkę WWW.
3. Wpisz w przeglądarce następujący adres URL:

   **Uwaga:** Jeśli program Web Administration Tool został zainstalowany i wdrożony w zdalnym systemie, zastąp localhost nazwą hosta lub adresem IP tego systemu.

   http://localhost:12100/IDSWebApp

## Co dalej

Aby zarządzać i administrować instancjami serwera katalogów, dodaj te serwery w konsoli programu Web Administration Tool. Patrz sekcja “Dostęp do narzędzia Web Administration Tool”.

# Dostęp do narzędzia Web Administration Tool

Aby zarządzać zdalnie instancjami serwera katalogów, otwórz narzędzie Web Administration Tool i skonfiguruj instancję serwera katalogów dla zdalnego zarządzania.

## Zanim rozpoczniesz

Przed otwarciem narzędzia Web Administration Tool należy wykonać następujące zadania:

1. Zainstaluj narzędzie Web Administration Tool.
2. Wykonaj wdrożenie narzędzia Web Administration Tool w obsługiwanym serwerze aplikacji WWW.
3. Uruchom serwer aplikacji WWW powiązany z narzędziem Web Administration Tool.

## Procedura

1. Aby otworzyć narzędzie Web Administration Tool, użyj jednej z następujących opcji:
   - Otwórz przeglądarkę WWW i wpisz następujący adres URL:
     - Dostęp niezabezpieczony: http://nazwa_hosta:12100/IDSWebApp.
     - Dostęp zabezpieczony: https://nazwa_hosta:12101/IDSWebApp.
   - Otwórz w przeglądarce WWW następujący plik:

     **Windows**

     Dostęp niezabezpieczony: *ścieżka_instalacyjna_ds*\idstools\bin\idswebadmin.html. Można również kliknąć opcje **Start > Wszystkie programy > IBM Security Directory Server 6.3.1 > Web Administration Tool**.

Dostęp zabezpieczony: *ścieżka_instalacyjna_ds*\idstools\bin\idswebadminssl.html. Można również kliknąć opcje **Start > Wszystkie programy > IBM Security Directory Server 6.3.1 > Web Administration Tool (bezpieczne)**.

**AIX, Linux i Solaris**

Dostęp niezabezpieczony: *ścieżka_instalacyjna_ds*/idstools/bin/idswebadmin.html.

Dostęp zabezpieczony: *ścieżka_instalacyjna_ds*/idstools/bin/idswebadminssl.html.

Zmienna *ścieżka_instalacyjna_ds* reprezentuje miejsce zainstalowania produktu IBM Security Directory Server. Więcej informacji na temat położenia domyślnego znajduje się w sekcji “Domyślne położenia instalacji” na stronie 27.

2. Zaloguj się do konsoli Web Administration Tool jako administrator.
   a. W polu **Identyfikator użytkownika** wpisz superadmin.
   b. W polu **Hasło** wpisz **secret**.

      **Uwaga:** Po pierwszym zalogowaniu należy zmienić hasło administratora konsoli.
   c. Kliknij przycisk **Logowanie**.
3. Aby dodać do konsoli serwera katalogów, wykonaj następujące działania:
   a. Na stronie **Wprowadzenie** kliknij opcję **Zarządzaj serwerami konsoli**.
   b. Na stronie **Zarządzaj serwerami konsoli** kliknij przycisk **Dodaj**.
   c. W polu **Nazwa serwera** wpisz unikalną nazwę identyfikującą serwer. Jeśli nie zostanie podana nazwa serwera, aplikacja przypisze wartość nazwa_hosta:port lub adres_IP:port.
   d. W polu **nazwa_hosta** wpisz nazwę hosta lub adres IP serwera katalogów.
   e. W polu **Port** wpisz numer portu serwera.
   f. Aby zdefiniować bezpieczną komunikację konsoli z serwerem, wybierz opcję **Włącz szyfrowanie SSL**.
   g. Aby włączyć sterowanie portem administracyjnym, zaznacz opcję **Obsługa serwera administracyjnego**.
   h. W polu **Port administracyjny** wpisz numer portu serwera administracyjnego.
   i. Aby zastosować zmiany, kliknij przycisk **OK**.
4. Aby wylogować się z konsoli Web Administration Tool, kliknij przycisk **Wyloguj**.

# Zatrzymywanie serwera aplikacji WWW

Przed wykonaniem deinstalacji programu Web Administration Tool, należy wylogować się z tego programu i zatrzymać serwer aplikacji WWW, który go obsługuje.

## Zanim rozpoczniesz

Należy wykonać następujące czynności zanim można zatrzymać serwer aplikacji WWW, który obsługuje program narzędziowy Web Administration Tool:

1. Wykonaj wdrożenie narzędzia Web Administration Tool w obsługiwanym serwerze aplikacji WWW.
2. Uruchom serwer aplikacji WWW powiązany z narzędziem Web Administration Tool.

### Procedura

1. Zaloguj się jako użytkownik root w systemach UNIX lub jako członek grupy administratorów w systemie Windows.
2. Otwórz wiersz komend.
3. Przejdź do podkatalogu bin w profilu programu Web Administration Tool. Poniżej podano domyślne ścieżki instalacji wbudowanego serwera aplikacji WebSphere, w którym jest wdrożony program Web Administration Tool. Jeśli podano niestandardową ścieżkę instalacji dla wbudowanego serwera aplikacji WebSphere, należy wprowadzić odpowiednie zmiany.

| System operacyjny | Ścieżka |
|---|---|
| **Windows** | C:\Program Files\IBM\ldap\V6.3.1\appsrv\profiles\TDSWebAdminProfile\bin |
| **AIX i Solaris** | /opt/IBM/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/bin |
| **Linux** | /opt/ibm/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/bin |

4. Aby zatrzymać serwer aplikacji WWW, który jest powiązany z programem Web Administration Tool, uruchom następującą komendę:

| System operacyjny | Komenda do uruchomienia: |
|---|---|
| **Windows** | stopServer.bat server1 |
| **AIX, Linux i Solaris** | ./stopServer server1 |

**Uwaga:** W systemie Windows można również zatrzymać usługę, która jest powiązana z serwerem aplikacji WWW, przy użyciu okna **Usługi**.

## Tryb HTTPS we wbudowanym serwerze WebSphere Application Server

Aby zabezpieczyć dostęp do aplikacji przez sieć WWW, należy skonfigurować i uruchomić aplikację w trybie HTTPS.

Po wdrożeniu narzędzia Web Administration Tool we wbudowanym serwerze WebSphere Application Server, można uruchomić aplikację. Można bezpiecznie połączyć się z narzędziem Web Administration Tool, podając adres WWW i bezpieczny port HTTPS.

Aby użyć protokołu HTTPS, należy otworzyć narzędzie Web Administration Tool, podając następujący adres:

https://*nazwa_hosta*:12101/IDSWebApp

Aby użyć połączenia bez protokołu HTTPS, należy otworzyć narzędzie Web Administration Tool, podając następujący adres:

http://*nazwa_hosta*:12100/IDSWebApp

Można również zamienić domyślne pliki JKS z certyfikatami dostarczonymi z serwerem aplikacji WWW służącymi do bezpiecznego komunikowania się przez protokoły SSL/TLS. Można utworzyć nowy klucz i pliki bazy danych zaufanych certyfikatów, które będą używane z aplikacją wdrożoną we wbudowanym serwerze WebSphere Application Server. Domyślny klucz i pliki bazy danych zaufanych certyfikatów są oddzielne i znajdują się w katalogu *WAS_HOME*/profiles/TDSWebAdminProfile/etc/. Zmienna *WAS_HOME* określa

położenie instalacji wbudowanego serwera WebSphere Application Server. Domyślny plik bazy danych kluczy to DummyServerKeyFile.jks, a domyślny plik bazy danych zaufanych certyfikatów to DummyServerTrustFile.jks.

Jeśli utworzono własne pliki JKS, można zamienić pliki bazy danych kluczy i bazy danych zaufanych certyfikatów. Aby skonfigurować pliki JKS, hasła i formaty plików, dodaj lub zmodyfikuj następujące pozycje (zaznaczone **pogrubieniem**) w pliku *WAS_HOME*/profiles/TDSWebAdminProfile/config/cells/DefaultNode/security.xml:

```
<keyStores xmi:id="KeyStore_DefaultNode_10"
 name="DummyServerKeyFile"
 password="{xor}CDo9Hgw="
 provider="IBMJCE"
 location="${WAS_HOME}/profiles/TDSWebAdminProfile/etc/DummyServerKeyFile.jks"
 type="JKS"
 fileBased="true"
 hostList=""
 managementScope="ManagementScope_DefaultNode_1"/>
<keyStores xmi:id="KeyStore_DefaultNode_11"
 name="DummyServerTrustFile"
 password="{xor}CDo9Hgw="
 provider="IBMJCE"
 location="${WAS_HOME}/profiles/TDSWebAdminProfile/etc/DummyServerTrustFile.jks"
 type="JKS"
 fileBased="true"
 hostList=""
 managementScope="ManagementScope_DefaultNode_1"/>
```

# Wycofanie wdrożenia programu Web Administration Tool na wbudowanym serwerze WebSphere Application Server

Aby zastąpić istniejący program Web Administration Tool (plik IDSWebApp.war) jego nowszą wersją, należy wycofać wdrożenie istniejącej wersji programu.

## Procedura

1. Uruchom serwer aplikacji WWW, który jest powiązany z programem Web Administration Tool, jeśli jest zatrzymany. Patrz sekcja “Uruchamianie wbudowanego serwera aplikacji WebSphere obsługującego program Web Administration Tool” na stronie 114.
2. Przejdź do katalogu *miejsce_instalacji_serwera_katalogów*/idstools. Wartość *miejsce_instalacji_serwera_katalogów* jest miejscem instalacji produktu IBM Security Directory Server. Poniżej wymieniono domyślne miejsca instalacji dla różnych systemów operacyjnych:

| Systemy operacyjne | Domyślne miejsca instalacji: |
|---|---|
| Microsoft Windows | c:\Program Files\IBM\ldap\V6.3.1 |
| AIX i Solaris | /opt/IBM/ldap/V6.3.1 |
| Linux | /opt/ibm/ldap/V6.3.1 |

3. Uruchom komendę:

   **Uwaga:** Jeśli wbudowany serwer WebSphere Application Server zostanie zainstalowany w niestandardowej lokalizacji, należy także podać parametry **-a**, **-w**, **-p** i **-r** dla komendy deploy_idswebapp. Więcej informacji o komendzie deploy_IDSWebApp zawiera składnia komendy, deploy_IDSWebApp -h.

| Systemy operacyjne | Komenda do uruchomienia: |
|---|---|
| **Microsoft Windows** | deploy_IDSWebApp.bat -u |

| Systemy operacyjne | Komenda do uruchomienia: |
| --- | --- |
| **AIX, Linux i Solaris** | deploy_IDSWebApp -u |

# Rozdział 17. Planowanie konfigurowania instancji

Przed utworzeniem i skonfigurowaniem środowiska LDAP należy podjąć szereg decyzji na temat ustawień konfiguracyjnych komputera.

Aby utworzyć instancję serwera katalogów lub instancję serwera proxy, należy najpierw utworzyć identyfikator użytkownika w systemie będącego właścicielem instancji. Należy zdecydować, jaka strona kodowa będzie używana do przechowywania danych w instancji serwera katalogów.

Instalacja produktu IBM Security Directory Server i oprogramowania wspólnie wymaganego oraz utworzenie instancji serwera katalogów wymaga utworzenia na komputerze użytkownika i grupy. Instalacja wspólnie wymaganego oprogramowania produktu IBM Security Directory Server, na przykład IBM DB2, wymaga utworzenia systemowego identyfikatora dla administratora DB2.

## Użytkownicy i grupy powiązane z instancją serwera katalogów

Aby utworzyć instancję serwera katalogów lub instancję serwera proxy, należy utworzyć użytkownika i grupę z wymaganymi uprawnieniami.

Aby utworzyć instancję na własnym komputerze, należy powiązać instancję z systemowym identyfikatorem użytkownika. Ten użytkownik będzie właścicielem instancji serwera katalogów. Jeśli identyfikator użytkownika nie istnieje dla instancji, należy utworzyć na komputerze identyfikator użytkownika. Aby utworzyć identyfikator użytkownika dla właściciela instancji serwera katalogów, właściciela instancji bazy danych i właściciela bazy danych, należy postępować zgodnie z regułami nazewnictwa. Więcej informacji na temat reguł nazewnictwa znajduje się w sekcji “Reguły nazewnictwa” na stronie 122.

W przypadku pełnego serwera katalogów należy również określić systemowy identyfikator użytkownika jako właściciela instancji bazy danych i bazy danych. Można użyć tego samego identyfikatora użytkownika dla wszystkich trzech ról. Jeśli zostanie użyty ten sam identyfikator użytkownika, instancja serwera katalogów, instancja bazy danych i baza danych będą zawierały tę samą nazwę właściciela.

Jeśli instancja serwera katalogów została utworzona za pomocą narzędzia Instance Administration Tool, można za jego pomocą utworzyć również identyfikator właściciela instancji serwera katalogów. Można również utworzyć ten identyfikator za pomocą komendy **idsadduser**. Komenda tworzy identyfikator użytkownika, który spełnia wszystkie wymagania.

Identyfikator użytkownika powiązany z właścicielem instancji serwera katalogów, właścicielem instancji bazy danych i właścicielem bazy danych zawiera następujące role:

**Właściciel instancji serwera katalogów**

Systemowy identyfikator użytkownika musi istnieć na komputerze działającym jako właściciel instancji serwera katalogów. Identyfikator właściciela instancji serwera katalogów jest także nazwą instancji serwera katalogów. Do użytkownika jest przypisane uprawnienie do zarządzania instancją serwera katalogów.

W systemach Windows uprawnienie do zarządzania instancją serwera katalogów ma także członek grupy Administratorzy. W systemach AIX, Linux i Solaris do zarządzania instancją serwera katalogów uprawniona jest także grupa podstawowa właściciela instancji serwera katalogów.

**Uwaga:** W systemach AIX, Linux i Solaris w nazwach właścicieli instancji rozróżniana jest wielkość liter. Nazwa i właściciel instancji serwera katalogów muszą być zawsze określane dokładnie tak, jak podany identyfikator użytkownika. W poniższym przykładzie znajdują się dwie różne nazwy właścicieli: JoeSmith i joesmith.

**Właściciel instancji bazy danych**
Identyfikator użytkownika, który służy jako właściciel instancji bazy danych jest właścicielem instancji bazy danych, która jest skonfigurowana dla instancji serwera katalogów. Nazwa instancji bazy danych jest taka sama, jak nazwa właściciela instancji bazy danych. Użytkownik ten zarządza instancją bazy danych. Instancją bazy danych może też zarządzać właściciel instancji serwera katalogów. Domyślnie ten identyfikator użytkownika jest taki sam, jak identyfikator właściciela instancji serwera katalogów.

**Właściciel bazy danych**
Użytkownik o tym identyfikatorze jest właścicielem bazy danych używanej przez instancję serwera katalogów do zapisywania danych katalogu. Baza danych znajduje się w instancji bazy danych, której właścicielem jest właściciel instancji bazy danych. Instancja serwera katalogów używa identyfikatora i hasła właściciela bazy danych do łączenia się z bazą danych.

## Reguły nazewnictwa

Identyfikator użytkownika i grupa podstawowa instancji serwera katalogów muszą spełniać reguły nazewnictwa.

Wymagania reguł nazewnictwa dotyczą następujących identyfikatorów użytkowników:

- Nazwa instancji serwera katalogów (identyfikator użytkownika, który jest właścicielem instancji serwera katalogów).
- Nazwa instancji bazy danych (identyfikator użytkownika, który jest właścicielem instancji bazy danych). Ten identyfikator użytkownika jest zwykle taki sam, jak nazwa instancji serwera katalogów.
- W systemach AIX, Linux i Solaris grupy podstawowe właścicieli instancji serwera katalogów i instancji bazy danych.

**Uwaga:** Podczas tworzenia identyfikatora użytkownika i grupy należy przypisać odpowiednie uprawnienia. Patrz sekcja “Wymagania dotyczące tworzenia użytkowników i grup” na stronie 123.

Użytkownik i grupa muszą spełniać następujące wymagania:

- Długość nie może przekraczać 8 znaków.
- Nie mogą być żadną z następujących nazw:
  - USERS
  - ADMINS
  - GUESTS
  - PUBLIC
  - LOCAL
  - idsldap
- Nie mogą rozpoczynać się od żadnego z następujących przedrostków:
  - IBM
  - SQL
  - SYS

- Nie mogą zawierać znaków akcentowanych.
- Mogą zawierać następujące znaki:
  - A - Z
  - a - z
  - 0 - 9
  - _ (podkreślenie)
- Muszą zaczynać się jednym z następujących znaków:
  - A - Z
  - a - z

## Wymagania dotyczące tworzenia użytkowników i grup

Podczas tworzenia użytkowników i grup dla instancji, należy przypisać użytkowników i grupy z odpowiednimi uprawnieniami i dodać je jako element odpowiedniej grupy.

Po utworzeniu wymaganych użytkowników i grup dla instancji należy przypisać odpowiednie uprawnienia i dodać użytkowników do właściwych grup. Użytkownik musi spełniać następujące wymagania dotyczące identyfikatorów użytkowników i grup:

**Windows**

- Dodaj właściciela instancji serwera katalogów i właściciela instancji bazy danych do grupy Administratorzy.
- Ustaw ustawienia narodowe poprawne dla właściciela instancji bazy danych na język, w którym serwer ma wygenerować komunikaty. W razie potrzeby należy się zalogować jako ten użytkownik i zmienić ustawienia narodowe na właściwe.

**AIX, Linux i Solaris**

- Dodaj użytkownika root do grupy podstawowej właściciela instancji serwera katalogów i właściciela instancji bazy danych.
- Dodaj użytkownika root do grupy idsldap.
- Dodaj właściciela instancji serwera katalogów i właściciela instancji bazy danych do grupy idsldap.
- Utwórz katalogi osobiste dla właściciela instancji serwera katalogów i właściciela instancji bazy danych.
- Przypisz odpowiednie uprawnienia do katalogu osobistego właściciela instancji serwera katalogów.
  - Użytkownikiem mającym wobec niego prawo własności jest właściciel instancji serwera katalogów.
  - Grupą mającą wobec niego prawo własności jest podstawowa grupa właściciela instancji serwera katalogów.
  - Należy przypisać uprawnienia do odczytu, zapisu i wykonywania do katalogu osobistego właściciela instancji serwera katalogów i jego grupy podstawowej.
- Przypisz dla właściciela instancji serwera katalogów i jego grupy podstawowej uprawnienia do odczytu, zapisu i wykonywania w miejscu, w którym baza danych jest tworzona.
- Właściciel instancji serwera katalogów i właściciel instancji bazy danych instancji serwera katalogów mogą być różnymi użytkownikami. W takim przypadku właściciel instancji serwera katalogów musi być członkiem grupy podstawowej właściciela instancji bazy danych.
- Jeśli właściciel instancji serwera katalogów, właściciel instancji DB2 i właściciel bazy danych są różni, muszą być członkami tej samej grupy.

- Ustaw dla właściciela instancji serwera katalogów, właściciela instancji bazy danych i właściciela bazy danych jako powłokę główną powłokę Korna (/usr/bin/ksh).

Należy poprawnie ustawić hasło właściciela instancji serwera katalogów, właściciela instancji bazy danych i właściciela bazy danych i musi być ono gotowe do użycia. Hasło nie może być przedawnione ani oczekiwać na początkowe sprawdzenie poprawności. Można sprawdzić, czy hasło jest poprawnie ustawione, logując się z użyciem ID i hasła użytkownika za pomocą programu telnet.

Podczas konfigurowania bazy danych zwyczajowo (choć nie jest to konieczne) jako położenie bazy danych podaje się katalog osobisty właściciela instancji bazy danych. W przypadku określenia innej lokalizacji katalog osobisty właściciela instancji bazy danych musi mieć od 3 do 4 MB wolnego miejsca. Baza danych DB2 tworzy dowiązania i dodaje pliki do katalogu osobistego właściciela instancji bazy danych nawet wtedy, gdy baza danych znajduje się w innym miejscu. Jeśli na komputerze nie ma wymaganej ilości wolnego miejsca w katalogu osobistym właściciela instancji bazy danych, można dodać miejsce lub zmienić katalog osobisty.

### Przykłady

Aby utworzyć właściciela instancji, który spełnia wymagania dotyczące właściciela instancji serwera katalogów, można uruchomić komendę **idsadduser**. Komenda **idsadduser** znajduje się w podkatalogu sbin w miejscu instalacji produktu IBM Security Directory Server.

**Przykład 1:**

Aby utworzyć konto użytkownika w systemie AIX, Linux lub Solaris z poniższymi parametrami, uruchom komendę **idsadduser**:

- Nazwa użytkownika: JanKowalski
- Grupa podstawowa: pracownicy
- Katalog osobisty: /home/jank (w systemie Solaris użyj /export/home/jank)
- Hasło: JanK_haslo

```
idsadduser –u JanKowalski –g pracownicy –l /home/jank –w JanK_haslo
```

**Przykład 2:**

Aby utworzyć konto użytkownika z poniższymi parametrami, jako członek grupy administratorów w systemie Windows uruchom komendę **idsadduser**:

- Nazwa użytkownika: JanKowalski
- Hasło: JanK_haslo

```
idsadduser –u JanKowalski –w JanK_haslo
```

## Planowanie konfiguracji

Należy zdecydować, jaki typ danych będzie przechowywany w serwerze katalogów, jaka będzie jego struktura danych i jakie mają być użyte opcje zabezpieczeń.

Przed skonfigurowaniem i zapełnieniem bazy danych należy zdecydować:

**Jaki typ danych będzie przechowywany w serwerze katalogów**

Należy wybrać schemat używany przez serwer katalogów oraz typ danych przechowywanych w tym serwerze. Standardowy zestaw definicji typów atrybutów oraz definicji klas obiektów został dołączony do serwera katalogu. Aby dostosować dane, przed dodaniem pozycji do serwera katalogów można dodać typ atrybutów niestandardowych i definicje klas obiektów.

Schemat można rozbudować lub zmodyfikować po zapełnianiu serwera katalogów danymi. W niektórych przypadkach zmiana schematu może wymagać ponownego załadowania danych.

**Jaka strona kodowa ma być używana**
Należy podjąć decyzję, czy utworzona zostanie baza danych korzystająca z lokalnej strony kodowej, czy korzystająca z uniwersalnego zestawu znaków (UTF-8). Wybór lokalnej strony kodowej umożliwia aplikacjom i użytkownikom serwera IBM Security Directory Server uzyskiwanie rezultatów wyszukiwania uporządkowanych w sposób właściwy dla języka narodowego. Wybranie lokalnej strony kodowej powoduje, że w katalogu dane będą przechowywane w tej stronie kodowej. Wybór kodowania UTF-8 umożliwi zapamiętywanie w katalogu dowolnych danych znakowych, które określane są tym formatem. "Obsługa standardu UTF-8" zawiera więcej informacji na temat standardu UTF-8.

**Uwaga:** Jeśli chcesz używać znaczników języków, baza danych musi być bazą danych UTF-8.

**Jaką strukturę będą miały dane w katalogu**
Program IBM Security Directory Server przechowuje dane w hierarchicznej strukturze drzewa. Nazwy pozycji w katalogu zależą od ich względnej pozycji w strukturze drzewiastej. Ważne jest zdefiniowanie pewnej logicznej organizacji katalogu. Logiczna organizacja ułatwia klientom określenie, która gałąź drzewa zawiera informacje, które próbują oni odszukać.

**Jakie są wymagania dotyczące bezpieczeństwa danych**
Aby uniemożliwić dostęp do danych katalogu przez niezabezpieczony port, należy skonfigurować używanie bezpiecznej komunikacji. Więcej informacji na temat zabezpieczania danych znajduje się w sekcji Administrowanie dokumentacji serwera IBM Security Directory Server.

**Jakie są wymagane uprawnienia dostępu do danych katalogu**
Więcej informacji na temat korzystania z uprawnień dostępu znajduje się w rozdziale dotyczącym list kontroli dostępu w sekcji Administrowanie dokumentacji serwera IBM Security Directory Server.

**Czy jest potrzebny serwer proxy**
Jeśli danych katalogowych jest dużo, a w środowisku występuje wiele operacji zapisu, należy rozważyć użycie serwera proxy. Duże środowiska katalogowe, w których występuje dużo operacji odczytu, mogą osiągać odpowiednie skalowanie dzięki replikacji. Przed podjęciem decyzji o zastosowaniu serwera proxy należy zapoznać się z listą obsługiwanych funkcji serwera proxy znajdującą się w sekcji Administrowanie dokumentacji serwera IBM Security Directory Server.

## Obsługa standardu UTF-8

Można skonfigurować na serwerze katalogów zapisywanie znaków narodowych w standardzie UTF-8.

Produkt IBM Security Directory Server obsługuje dużą liczbę znaków alfabetów narodowych dzięki wykorzystaniu zestawu znaków UTF-8 (format transformacji UCS). W protokole LDAP wersja 3 wszystkie dane znakowe przesyłane są pomiędzy klientem a serwerem LDAP w formacie UTF-8.

Serwer określa typy znaków, które mogą być przechowywane i przeszukiwane w oparciu o stronę kodową, która jest używana do konfigurowania bazy danych. Można podać zestaw

znaków bazy danych ustawiony jako UTF-8 lub ustawić lokalny zestaw znaków systemu, na którym znajduje się serwer. Lokalny zestaw znaków jest określany na podstawie ustawień narodowych, języka i strony kodowej systemu.

Wybór formatu UTF-8 umożliwia zapamiętywanie w katalogu dowolnych danych znakowych, które określane są tym formatem. Klienty LDAP w systemie obsługującym języki UTF-8 mogą poprawnie kontaktować się i przeszukiwać katalog. Jeśli klient LDAP znajduje się w systemie z lokalnym zestawem znaków, wyniki pobrane z serwera mogą nie być wyświetlane poprawnie w danych zestawie znaków.

Jeśli używana jest baza danych w formacie UTF-8, zwiększa się wydajność bazy danych, ponieważ podczas zapisywania lub pobierania danych nie jest wykonywana konwersja.

**Uwaga:** Aby można było używać znaczników języków, baza danych musi być w formacie UTF-8.

## Korzystanie ze standardu UTF-8 na serwerze katalogów

Aby wybrać stronę kodową, która będzie używana, należy zrozumieć, w jaki sposób serwer katalogów korzysta ze strony kodowej do zapisywania i udostępniania danych katalogów.

Baza danych UTF-8 zawiera sekwencję porównującą określającą binarną kolejność znaków UTF-8. Niemożliwe jest w bazie danych UTF-8 zdefiniowanie porządku sortowania zależnego od języka.

Zestaw znaków UTF-8 może nie być odpowiedni dla bazy danych, ponieważ aplikacje lub użytkownicy LDAP mogą nie uzyskiwać następujących wyników:

- Wyszukiwanie z filtrem porządkującym (na przykład "name >= SMITH"), oczekiwana kolejność zbliżona do kolejności sortowania zgodnej z ustawieniami narodowymi.
- Wyszukiwanie z elementem sterującym sortowaniem wyników, oczekiwana kolejność zbliżona do kolejności sortowania zgodnej z ustawieniami narodowymi.

W takiej sytuacji system serwera LDAP i wszystkie systemy klientów muszą korzystać z tego samego zestawu znaków i ustawień narodowych.

Na przykład baza danych serwera LDAP, w której skonfigurowano hiszpańskie ustawienia narodowe, zwraca wyniki wyszukiwania zgodne z oczekiwaniami hiszpańskojęzycznych klientów. Taka konfiguracja ogranicza społeczność użytkowników katalogów do jednego zestawu znaków dla danych ustawień narodowych i sekwencji porównującej.

## Tworzenie pliku LDIF z wartościami UTF-8 za pomocą narzędzi serwera

W celu utworzenia danych w formacie LDIF z wartościami UTF-8 należy użyć rozszerzenia charset.

Ręczne utworzenie pliku LDIF zawierającego wartości UTF-8 jest trudne. W nagłówku pliku LDIF można określić rozszerzenie, które obsługuje nazwy zestawu znaków IANA (Internet Assigned Numbers Authority) wraz z numerem wersji. Więcej informacji na temat obsługiwanych zestawów znaków IANA zawiera sekcja “Obsługiwane zestawy znaków IANA” na stronie 128.

### Przykłady

**Przykład 1:**

Aby narzędzia serwera automatycznie przetwarzały dane z podanego zestawu znaków do zestawu znaków UTF-8, należy użyć znacznika charset.

```
version: 1
charset: ISO-8859-1

dn: cn=Juan Griego, ou=University of New Mexico, o=sample
cn: Juan Griego
sn: Griego
description:: V2hhdCBhIGNhcmVmdWwgcmVhZGVyIHlvd
title: Associate Dean
title: [stanowisko po hiszpańsku]
jpegPhoto:< file:///usr/local/photos/jgriego.jpg
```

W poniższym przykładzie wszystkie nazwy atrybutów z wartościami, które są rozdzielone pojedynczym dwukropkiem, są tłumaczone z kodowania ISO-8859-1 na UTF-8. Wszystkie nazwy atrybutów z wartościami, które są rozdzielone podwójnym dwukropkiem, na przykład description:: V3JvY8WCYXcgamVzdCBzdG9saWPEhSBEb2xuZWdvIMWabMSFc2thLg==, muszą być zapisane z użyciem kodowania base 64 i muszą być danymi binarnymi lub łańcuchem znaków UTF-8. Jeśli wartości są odczytywane z pliku (tak jak dla atrybutu jpegPhoto), który jest określony przez adres WWW, również i on musi być binarny lub zakodowany z użyciem kodowania UTF-8. Dla wartości takich atrybutów nie jest wykonywana translacja z użyciem kodowania podanego w parametrze charset na UTF-8.

**Przykład 2:**

W poniższym przykładzie plik LDIF nie zawiera znacznika charset, tak więc treść powinna być podana w formacie UTF-8:

```
# IBM Directory - przykładowy plik w formacie LDIF
#
# Przed próbą załadowania tych danych należy zdefiniować
# przyrostek "o=sample".

 version: 1

 dn: o=sample
 objectclass: top
 objectclass: organization
 o: sample

 dn: ou=Austin, o=sample
 ou: Austin
 objectclass: organizationalUnit
 seealso: cn=Mary Smith, ou=Austin, o=sample
```

W programie IBM Security Directory Server, plik LDIF o następującej zawartości może być używany bez nagłówka version: 1:

```
# IBM Directory - przykładowy plik w formacie LDIF
#
# Przed próbą załadowania tych danych należy zdefiniować
# przyrostek "o=sample".

 dn: o=sample
 objectclass: top
 objectclass: organization
 o: sample

 dn: ou=Austin, o=sample
 ou: Austin
 objectclass: organizationalUnit
 seealso: cn=Linda Carlesberg, ou=Austin, o=sample
```

# Obsługiwane zestawy znaków IANA

Za pomocą nazw zestawów znaków IANA (Internet Assigned Number Authority) w pliku LDIF lub w interfejsie klienta C można identyfikować zestaw znaków danych katalogu.

Produkt IBM Security Directory Server obsługuje nazwy zestawów znaków IANA (Internet Assigned Number Authority) według systemów operacyjnych.

Więcej informacji na temat zestawów znaków zarejestrowanych przez IANA znajduje się w serwisie Zestawy znaków pod adresem www.iana.org/assignments/character-sets.

*Tabela 38. Zestawy znaków IANA*

| Znak | Ustawienia narodowe | | | | | Strona kodowa DB2 | |
|---|---|---|---|---|---|---|---|
| Nazwa zestawu | HP-UX | Linux, Linux_390 | Windows | AIX | Solaris | UNIX | Windows |
| ISO-8859-1 | X | X | X | X | X | 819 | 1252 |
| ISO-8859-2 | X | X | X | X | X | 912 | 1250 |
| ISO-8859-5 | X | X | X | X | X | 915 | 1251 |
| ISO-8859-6 | X | X | X | X | X | 1089 | 1256 |
| ISO-8859-7 | X | X | X | X | X | 813 | 1253 |
| ISO-8859-8 | X | X | X | X | X | 916 | 1255 |
| ISO-8859-9 | X | X | X | X | X | 920 | 1254 |
| ISO-8859–15 | X | nie dotyczy | X | X | X | | |
| IBM437 | nie dotyczy | nie dotyczy | X | nie dotyczy | nie dotyczy | 437 | 437 |
| IBM850 | nie dotyczy | nie dotyczy | X | X | nie dotyczy | 850 | 850 |
| IBM852 | nie dotyczy | nie dotyczy | X | nie dotyczy | nie dotyczy | 852 | 852 |
| IBM857 | nie dotyczy | nie dotyczy | X | nie dotyczy | nie dotyczy | 857 | 857 |
| IBM862 | nie dotyczy | nie dotyczy | X | nie dotyczy | nie dotyczy | 862 | 862 |
| IBM864 | nie dotyczy | nie dotyczy | X | nie dotyczy | nie dotyczy | 864 | 864 |
| IBM866 | nie dotyczy | nie dotyczy | X | nie dotyczy | nie dotyczy | 866 | 866 |
| IBM869 | nie dotyczy | nie dotyczy | X | nie dotyczy | nie dotyczy | 869 | 869 |
| IBM1250 | nie dotyczy | nie dotyczy | X | nie dotyczy | nie dotyczy | | |
| IBM1251 | nie dotyczy | nie dotyczy | X | nie dotyczy | nie dotyczy | | |
| IBM1253 | nie dotyczy | nie dotyczy | X | nie dotyczy | nie dotyczy | | |
| IBM1254 | nie dotyczy | nie dotyczy | X | nie dotyczy | nie dotyczy | | |
| IBM1255 | nie dotyczy | nie dotyczy | X | nie dotyczy | nie dotyczy | | |

*Tabela 38. Zestawy znaków IANA (kontynuacja)*

| Znak | Ustawienia narodowe | | | | | Strona kodowa DB2 | |
|---|---|---|---|---|---|---|---|
| **Nazwa zestawu** | **HP-UX** | **Linux, Linux_390** | **Windows** | **AIX** | **Solaris** | **UNIX** | **Windows** |
| IBM1256 | nie dotyczy | nie dotyczy | X | nie dotyczy | nie dotyczy | | |
| TIS-620 | nie dotyczy | nie dotyczy | X | X | nie dotyczy | 874 | 874 |
| EUC-JP | X | X | nie dotyczy | X | X | 954 | nie dotyczy |
| EUC-KR | nie dotyczy | nie dotyczy | nie dotyczy | X | X | 970 | nie dotyczy |
| EUC-CN | nie dotyczy | nie dotyczy | nie dotyczy | X | X | 1383 | nie dotyczy |
| EUC-TW | X | nie dotyczy | nie dotyczy | X | X | 964 | nie dotyczy |
| Shift-JIS | nie dotyczy | X | X | X | X | 932 | 943 |
| KSC | nie dotyczy | nie dotyczy | X | nie dotyczy | nie dotyczy | nie dotyczy | 949 |
| GBK | nie dotyczy | nie dotyczy | X | X | nie dotyczy | 1386 | 1386 |
| Big5 | X | nie dotyczy | X | X | X | 950 | 950 |
| GB18030 | nie dotyczy | X | X | X | X | | |
| HP15CN | X (z zestawem innym niż GB18030) | | | | | | |

**Uwaga:**

- Standard chińskiego zestawu znaków (GB18030) jest obsługiwany przez odpowiednie poprawki dostępne na stronach www.oracle.com i www.microsoft.com.
- W systemach Windows należy dla zmiennej środowiskowej *zhCNGB18030* ustawić wartość TRUE.

## Znaki ASCII o kodach od 33 do 126

Za pomocą tabeli znaków ASCII można określić znaki używane przez instancję serwera katalogów jako klucz początkowy i klucz dodatkowy szyfrowania.

W łańcuchach klucza początkowego i klucza dodatkowego szyfrowania można używać znaków ASCII do 33 do 126.

*Tabela 39. Znaki ASCII o kodach od 33 do 126*

| Kod ASCII | Znak | Kod ASCII | Znak | Kod ASCII | Znak |
|---|---|---|---|---|---|
| 33 | ! wykrzyknik | 34 | " podwójny cudzysłów | 35 | # krzyżyk |
| 36 | $ znak dolara | 37 | % znak procentu | 38 | & znak ampersand |
| 39 | ’ apostrof | 40 | ( nawias lewy | 41 | ) nawias prawy |
| 42 | * gwiazdka | 43 | + znak plus | 44 | , przecinek |
| 45 | - łącznik | 46 | . kropka | 47 | / ukośnik |

*Tabela 39. Znaki ASCII o kodach od 33 do 126 (kontynuacja)*

| Kod ASCII | Znak | Kod ASCII | Znak | Kod ASCII | Znak |
|---|---|---|---|---|---|
| 48 | 0 | 49 | 1 | 50 | 2 |
| 51 | 3 | 52 | 4 | 53 | 5 |
| 54 | 6 | 55 | 7 | 56 | 8 |
| 57 | 9 | 58 | : dwukropek | 59 | ; średnik |
| 60 | < znak mniejszości | 61 | = znak równości | 62 | > znak większości |
| 63 | ? znak zapytania | 64 | @ znak at | 65 | A wielkie a |
| 66 | B wielkie b | 67 | C wielkie c | 68 | D wielkie d |
| 69 | E wielkie e | 70 | F wielkie f | 71 | G wielkie g |
| 72 | H wielkie h | 73 | I wielkie i | 74 | J wielkie j |
| 75 | K wielkie k | 76 | L wielkie l | 77 | M wielkie m |
| 78 | N wielkie n | 79 | O wielkie o | 80 | P wielkie p |
| 81 | Q wielkie q | 82 | R wielkie r | 83 | S wielkie s |
| 84 | T wielkie t | 85 | U wielkie u | 86 | V wielkie v |
| 87 | W wielkie w | 88 | X wielkie x | 89 | Y wielkie y |
| 90 | Z wielkie z | 91 | [ nawias kwadratowy lewy | 92 | \ ukośnik odwrotny |
| 93 | ] nawias kwadratowy prawy | 94 | ^ znak karetki | 95 | _ podkreślenie |
| 96 | ` akcent grave | 97 | a małe a | 98 | b małe b |
| 99 | c małe c | 100 | d małe d | 101 | e małe e |
| 102 | f małe f | 103 | g małe g | 104 | h małe h |
| 105 | i małe i | 106 | j małe j | 107 | k małe k |
| 108 | l małe l | 109 | m małe m | 110 | n małe n |
| 111 | o małe o | 112 | p małe p | 113 | q małe q |
| 114 | r małe r | 115 | s małe s | 116 | t małe t |
| 117 | u małe u | 118 | v małe v | 119 | w małe w |
| 120 | x małe x | 121 | y małe y | 122 | z małe z |
| 123 | { nawias klamrowy lewy | 124 | \| kreska pionowa | 125 | } nawias klamrowy prawy |
| 126 | ~ znak tyldy | | | | |

# Rozdział 18. Tworzenie i administrowanie instancją

Aby użyć serwera katalogów w infrastrukturze tożsamości, należy utworzyć instancję serwera katalogów zgodnie z wymaganiami.

Po zakończeniu instalacji serwera IBM Security Directory Server należy utworzyć instancję serwera katalogów, a następnie ustawić nazwę DN i hasło administratora dla instancji. Można utworzyć pełny serwer katalogów lub serwer proxy. Aby utworzyć instancję serwera katalogów lub instancję serwera proxy, należy utworzyć identyfikator użytkownika w systemie. Identyfikator ten będzie właścicielem instancji serwera katalogów lub instancji serwera proxy.

W przypadku pełnego serwera katalogów należy również skonfigurować bazę danych DB2 związaną z instancją serwera katalogów. Aby utworzyć bazę danych DB2, należy zainstalować na komputerze obsługiwaną wersję produktu DB2. Należy sprawdzić, czy w pliku ldapdb.properties jest aktualna ścieżka instalacji i wersja DB2. Aby uzyskać więcej informacji, patrz Dodatek C, “Samodzielne aktualizowanie pliku ldapdb.properties”, na stronie 247.

**Uwaga:** W przypadku używania programu Instance Administration Tool (**idsxinst**) produktu IBM Security Directory Server do utworzenia instancji pełnego serwera katalogów, tworzony jest plik ldapdb.properties w katalogu głównym instancji. W systemie Windows plik ldapdb.properties znajduje się w katalogu *katalog_główny_instancji*\idsslapd-*nazwa_instancji*\etc. W systemie AIX, Linux lub Solaris plik ten jest w katalogu *katalog_główny_instancji*/idsslapd-*nazwa_instancji*/etc.

W przypadku instancji serwera proxy nie trzeba tworzyć ani konfigurować bazy danych DB2.

Program Instance Administration Tool jest wyposażonym w graficzny interfejs użytkownika programem służącym do tworzenia instancji serwera katalogów i do zarządzania nimi. Do używania programu Instance Administration Tool niezbędne jest środowisko IBM Java Development Kit. W programie Instance Administration Tool użytkownik może korzystać z kreatora ułatwiającego wykonanie zadania.

Za pomocą programu Instance Administration Tool można tworzyć, przeglądać, kopiować i usuwać instancje, a także modyfikować informacje na ich temat. Narzędzia tego można także używać do tworzenia lub edycji użytkowników, do których należą instancje serwera katalogów, oraz do aktualizowania poprzednich wersji instancji serwera IBM Security Directory Server. Programu Instance Administration Tool można używać do uruchamiania i zatrzymywania serwera lub serwera administracyjnego dla instancji. Dodatkowo z programu Instance Administration Tool można uruchamiać narzędzie konfiguracyjne.

Do tworzenia i zarządzania instancjami serwera katalogów można użyć interfejsu wiersza komend.

## Uruchamianie narzędzia Instance Administration Tool

Za pomocą narzędzia Instance Administration Tool można usunąć utworzyć i administrować instancją serwera katalogów lub instancją serwera proxy.

## Zanim rozpoczniesz

Aby można było korzystać z narzędzia Instance Administration Tool, należy zainstalować produkt IBM Security Directory Server z opcjami Serwer lub Serwera proxy. Aby uruchomić program Instance Administration Tool, należy zalogować się z następującymi uprawnieniami:

**AIX, Linux i Solaris**
Zaloguj się do systemu jako użytkownik root.

**Windows**
Zaloguj się do systemu jako członek grupy administratorów.

Pakiet IBM Java Development Kit musi być umieszczony w ścieżce instalacji IBM Security Directory Server. Dla domyślnej ścieżki instalacji serwera IBM Security Directory Server, patrz sekcja “Domyślne położenia instalacji” na stronie 27.

## Procedura

Aby uruchomić narzędzie Instance Administration Tool, użyj jednej z następujących opcji:

| **Opcje uruchamiania programu Instance Administration Tool** | **Komenda do uruchomienia:** |
|---|---|
| **Instalacja opcji serwera IBM Security Directory Server** | Na stronie **Podsumowanie** kliknij opcję **Instance Administration Tool (idsxinst)**. Sekcja “Instalowanie przy użyciu programu IBM Installation Manager” na stronie 31 zawiera informacje na temat instalowania za pomocą programu SMIT. |
| **Komenda idsxinst** | **Windows**<br>1. Zmień bieżący katalog roboczy na podkatalog sbin w miejscu instalacji produktu IBM Security Directory Server.<br>2. Uruchom komendę **idsxinst**.<br>**Uwaga:** Można również kliknąć opcje **Start > Wszystkie programy > IBM Security Directory Server 6.3.1 > Web Administration Tool**.<br>**AIX, Linux i Solaris**<br>1. Zmień bieżący katalog roboczy na podkatalog sbin w miejscu instalacji produktu IBM Security Directory Server.<br>2. Uruchom komendę **idsxinst**.<br>Więcej informacji na temat ścieżki instalacji produktu IBM Security Directory Server zawiera sekcja “Domyślne położenia instalacji” na stronie 27. |

# Uruchamianie programu Instance Administration Tool, aby zaktualizować instancję

Uruchom program Instance Administration Tool z parametrami, aby zaktualizować instancję zdalnego zawierającego dane kopii zapasowej.

### Zanim rozpoczniesz

Aby zaktualizować zdalną instancję, należy spełnić następujące wymagania:

- Komputer musi zawierać dane kopii zapasowej instancji utworzonych za pomocą komendy **migbkup**. Należy użyć komendy **migbkup** w wersji, do której chcesz zaktualizować zdalną instancję.
- Zaloguj się jako użytkownik root w systemach AIX, Linux i Solaris. W systemie Windows, zaloguj się jako członek grupy administratorów.

### Procedura

1. Otwórz wiersz komend.
2. Zmień bieżący katalog roboczy na podkatalog sbin w miejscu instalacji produktu IBM Security Directory Server. Więcej informacji na temat domyślnych ścieżek instalacji zawiera sekcja “Domyślne położenia instalacji” na stronie 27.
3. Uruchom komendę **idsxinst** w następującym formacie:

   ```
   idsxinst -migrate katalog_kopii_zapasowej
   ```

   Zastąp zmienną *katalog_kopii_zapasowej* lokalizacją, w której są przechowywane dane kopii zapasowej instancji utworzone za pomocą komendy **migbkup**.

## Tworzenie instancji serwera katalogów

Aby używać instancji serwera katalogów w środowisku LDAP, należy utworzyć instancję, która jest kryptograficznie zsynchronizowana z istniejącą instancją w celu uzyskania optymalnej wydajności

Jeśli tworzona jest instancja serwera katalogów jako kopia istniejącej instancji serwera katalogów, instancje te są kryptograficznie zsynchronizowane i nie trzeba ich synchronizować.

Jeśli tworzona instancja nie jest kopią istniejącej instancji, należy ją kryptograficznie zsynchronizować z istniejącą instancją. Kryptograficzne synchronizowanie instancji serwera pozwala uzyskać najlepszą wydajność w następującym środowisku:

- Replikacja
- Katalog rozproszony
- Importowanie i eksportowanie plików LDIF między instancjami serwera

Instancje serwera należy zsynchronizować przed wykonaniem dowolnej z poniższych czynności:

- Uruchomienie nowej instancji serwera.
- Uruchomienie komendy **idsbulkload** dla instancji serwera.
- Uruchomienie komendy **idsldif2db** dla instancji serwera.

Więcej informacji na temat synchronizowania serwerów katalogów znajduje się w sekcji *Administrowanie* dokumentacji serwera IBM Security Directory Server.

Po utworzeniu instancji serwera katalogów i skonfigurowaniu go do używania bazy danych DB2 należy utworzyć kopię zapasową instancji serwera katalogów. Kopia zapasowa musi obejmować konfigurację, schemat, bazę danych DB2 i pliki ukryte klucza katalogu. Do utworzenia kopii zapasowej instancji serwera katalogów można użyć komendy **idsdbback**. Do odtworzenia plików ukrytych kluczy, jeśli to konieczne, można użyć komendy **idsdbrestore**. Więcej informacji na temat komend operacji tworzenia i odtwarzania kopii zapasowych zawiera *Skorowidz komend*.

# Tworzenie instancji za pomocą programu Instance Administration Tool

Należy oszacować wymagania danego środowiska i utworzyć odpowiednią instancję serwera katalogów.

Programu Instance Administration Tool można użyć do utworzenia instancji na kilka sposobów:

- Utworzenie domyślnej instancji z domyślną nazwą i innymi ustawieniami. Informacje na ten temat zawiera sekcja “Tworzenie instancji serwera katalogów”.
- Tworzenie instancji z własnymi ustawieniami. Informacje na ten temat zawiera sekcja “Tworzenie instancji serwera katalogów z ustawieniami niestandardowymi” na stronie 136.
- Aktualizowanie poprzedniej wersji produktu IBM Security Directory Server. Patrz sekcja “Aktualizowanie instancji z poprzedniej wersji za pomocą komendy **idsimigr**” na stronie 92 lub “Aktualizowanie instancji poprzedniej wersji przy użyciu programu Instance Administration Tool” na stronie 147.
- Utworzenie instancji będącej kopią instancji istniejącej na tym samym lub innym komputerze. Informacje na ten temat zawiera sekcja “Tworzenie kopii istniejącej instancji za pomocą narzędzia Instance Administration Tool” na stronie 153.

## Tworzenie instancji serwera katalogów

Użyj domyślnej opcji tworzenia instancji, aby utworzyć instancję serwera katalogów używając predefiniowanej nazwy instancji i ustawień domyślnych.

### Zanim rozpoczniesz

Aby utworzyć domyślną instancję, należy wykonać następujące czynności:

1. Zainstaluj produkt IBM Security Directory Server z funkcją serwera. Patrz sekcja “Instalowanie przy użyciu programu IBM Installation Manager” na stronie 31.
2. Zainstaluj bazę danych DB2. Patrz sekcja “Instalowanie przy użyciu programu IBM Installation Manager” na stronie 31.
3. Sprawdź, czy plik ldapdb.properties zawiera ścieżkę instalacyjną DB2 i informacje o wersji. Patrz sekcja Dodatek C, “Samodzielne aktualizowanie pliku ldapdb.properties”, na stronie 247.

### O tym zadaniu

Jeśli komputer już zawiera istniejącą instancję serwera katalogów z domyślną nazwą instancji, nie można utworzyć domyślnej instancji serwera katalogów.

Domyślna instancja serwera katalogów zawiera następujące ustawienia, których nie można zmienić:

*Tabela 40. Ustawienia dla domyślnej instancji serwera katalogów*

| Ustawienia | Microsoft Windows | AIX i Linux | Solaris |
|---|---|---|---|
| Nazwa | dsrdbm01 | dsrdbm01 | dsrdbm01 |
| Położenie instancji | c:\idsslapd-dsrdbm01 | /home/dsrdbm01 | /export/home/ dsrdbm01 |
| Nazwa grupy | Administratorzy | grrdbm01 | grrdbm01 |
| Nazwa DN administratora | cn=root | cn=root | cn=root |
| Nazwa bazy danych | dsrdbm01 | dsrdbm01 | dsrdbm01 |

Obszar tabel bazy danych DB2 dla domyślnej instancji serwera katalogów jest obszarem typu DMS (Database Managed Storage).

Dla domyślnej instancji serwera katalogów program Instance Administration Tool tworzy przyrostek o=sample. Można później dodać więcej przyrostków przy użyciu programu Configuration Tool lub komendy **idscfgsuf**. Aby uzyskać więcej informacji, patrz “Konfiguracja przyrostka” na stronie 200.

## Procedura

1. Uruchom program Instance Administration Tool. Patrz sekcja “Uruchamianie narzędzia Instance Administration Tool” na stronie 131.
2. Kliknij opcję **Utwórz instancję**.
3. W oknie **Tworzenie nowej instancji serwera katalogów** wykonaj następujące kroki:
   a. Kliknij przycisk **Utwórz instancję domyślną**.
   b. Kliknij przycisk **Dalej**.
   c. W polu **Hasło użytkownika** wprowadź hasło dla konta użytkownika będącego właścicielem instancji serwera katalogów.
   d. W polu **Potwierdź hasło** wprowadź potwierdzenie hasła dla konta użytkownika będącego właścicielem instancji serwera katalogów.
   e. W polu **Klucz początkowy szyfrowania** wprowadź klucz początkowy szyfrowania dla instancji serwera katalogów.

      **Zapamiętaj:** Należy zapamiętać klucz początkowy szyfrowania instancji, ponieważ może on być wymagany przy innych czynnościach konfiguracyjnych.
      Klucz początkowy szyfrowania musi zawierać jedynie znaki drukowalne ISO-8859-1 ASCII z wartościami w zakresie od 33 do 126. Klucz początkowy szyfrowania musi mieć przynajmniej 12 znaków i co najwyżej 1016 znaków. Informacje o znakach, których można użyć, zawiera sekcja “Znaki ASCII o kodach od 33 do 126” na stronie 129. Serwer katalogów używa klucza początkowego szyfrowania do generowania zestawu wartości kluczy tajnych standardu Advanced Encryption Standard (AES). W pliku ukrytych kluczy instancji serwera katalogów są przechowywane wartości kluczy, które służą do szyfrowania i deszyfrowania hasła i atrybutów.
   f. W polu **Potwierdź klucz początkowy szyfrowania** wprowadź klucz początkowy szyfrowania dla instancji serwera katalogów.
   g. W polu **Hasło DN administratora** wpisz hasło dla administratora instancji serwera katalogów.
   h. W polu **Potwierdź hasło** wpisz ponownie hasło administratora instancji serwera katalogów.
   i. Kliknij przycisk **Dalej**.
   j. Zweryfikuj informacje na temat domyślnej instancji serwera katalogów. oraz
   k. Aby rozpocząć tworzenie domyślnej instancji serwera katalogów, kliknij przycisk **Zakończ**. Zostanie wyświetlone okno Wyniki z informacjami dziennika.
4. Sprawdź informacje dziennika wyświetlane w oknie **Wyniki**.
5. Aby zamknąć okno **Wyniki**, kliknij przycisk **Zamknij**.
6. Aby zamknąć program Instance Administration Tool, kliknij przycisk **Zamknij**.

## Wyniki

Program Instance Administration Tool utworzy w systemie domyślną instancję serwera katalogów, dsrdbm01.

### Co dalej

Należy uruchomić proces ibmslapd oraz serwer administracyjny powiązany z instancją serwera katalogów. Informacje na ten temat zawiera sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego” na stronie 156.

## Tworzenie instancji serwera katalogów z ustawieniami niestandardowymi

Narzędzie Instance Administration Server umożliwia utworzenie instancji serwera katalogów z własnymi wymaganymi wartościami.

### Zanim rozpoczniesz

Aby utworzyć instancję serwera katalogów, należy wykonać następujące czynności:

1. Zainstaluj produkt IBM Security Directory Server z funkcją serwera. Patrz sekcja “Instalowanie przy użyciu programu IBM Installation Manager” na stronie 31.
2. Aby utworzyć pełny serwer katalogów z bazą RDBM zaplecza, zainstaluj IBM DB2. Patrz sekcja “Instalowanie przy użyciu programu IBM Installation Manager” na stronie 31.
3. Sprawdź, czy plik ldapdb.properties zawiera ścieżkę instalacyjną DB2 i informacje o wersji. Patrz sekcja Dodatek C, “Samodzielne aktualizowanie pliku ldapdb.properties”, na stronie 247.

### Procedura

1. Uruchom program Instance Administration Tool. Patrz sekcja “Uruchamianie narzędzia Instance Administration Tool” na stronie 131.
2. Kliknij opcję **Utwórz instancję**.
3. W panelu **Utwórz lub przeprowadź migrację** okna **Tworzenie nowej instancji serwera katalogów** kliknij opcję **Utwórz nową instancję serwera katalogów**.
4. Kliknij przycisk **Dalej**.
5. Na panelu **Szczegóły instancji** okna **Tworzenie nowej instancji serwera katalogów** podaj następujące wartości:
   a. Z listy **Nazwa użytkownika** wybierz nazwę użytkownika, do którego należy instancja serwera katalogów. Do instancji serwera katalogów jest przypisana taka sama nazwa jak nazwa użytkownika.
   b. Aby powiązać nowe konto użytkownika z instancją, kliknij przycisk **Utwórz użytkownika**. W oknie **Tworzenie nowego użytkownika instancji serwera katalogów** wykonaj następujące kroki:
      1) W polu **Nazwa użytkownika** wpisz nazwę użytkownika.
      2) W polu **Hasło** wprowadź hasło dla konta użytkownika.
      3) W polu **Potwierdź hasło** wprowadź hasło dla konta użytkownika.
      4) W polu **Katalog osobisty** wprowadź katalog osobisty do skonfigurowania dla konta użytkownika. Możesz również kliknąć przycisk **Przeglądaj** i określić katalog osobisty.
      5) W polu **Grupa podstawowa** wpisz nazwę grupy podstawowej użytkownika.
      6) Aby utworzyć konto użytkownika, kliknij przycisk **Utwórz**.
   c. Aby zmodyfikować istniejące konto użytkownika, wybierz nazwę użytkownika z listy **Nazwa użytkownika** i kliknij opcję **Edytuj użytkownika**. W oknie **Edycja użytkownika instancji serwera katalogów** wykonaj następujące kroki:
      1) W polu **Nazwa użytkownika** znajduje się nazwa użytkownika.

2) W polu **Hasło** wprowadź hasło dla konta użytkownika.
3) W polu **Potwierdź hasło** wprowadź hasło dla konta użytkownika.
4) W polu **Katalog osobisty** wprowadź katalog osobisty do skonfigurowania dla konta użytkownika. Możesz również kliknąć przycisk **Przeglądaj** i określić katalog osobisty.
5) W polu **Grupa podstawowa** wpisz nazwę grupy podstawowej użytkownika.
6) Aby edytować konto użytkownika, kliknij przycisk **Edytuj**.

6. W polu **Położenie instancji** wpisz położenie instancji serwera katalogów. Możesz również kliknąć przycisk **Przeglądaj** i określić katalog główny instancji. W podanym położeniu musi znajdować się przynajmniej 30 MB wolnego miejsca na dysku. W systemach Windows położeniem jest dysk, na przykład C:. Pliki instancji katalogu są zapisywane w katalogu \idsslapd-*nazwa_instancji* podanego dysku. Zmienna *nazwa_instancji* jest nazwą instancji serwera katalogów. W systemach AIX, Linux i Solaris domyślnym położeniem instancji jest katalog osobisty właściciela instancji serwera katalogów, ale można podać inną ścieżkę.
7. W polu **Klucz początkowy szyfrowania** wprowadź klucz początkowy szyfrowania dla instancji źródłowego serwera katalogów.

   **Zapamiętaj:** Należy zapamiętać klucz początkowy szyfrowania instancji, ponieważ może on być wymagany przy innych czynnościach konfiguracyjnych.
   Klucz początkowy szyfrowania musi zawierać jedynie znaki drukowalne ISO-8859-1 ASCII z wartościami w zakresie od 33 do 126. Klucz początkowy szyfrowania musi mieć przynajmniej 12 znaków i co najwyżej 1016 znaków. Informacje o znakach, których można użyć, zawiera sekcja “Znaki ASCII o kodach od 33 do 126” na stronie 129. Serwer katalogów używa klucza początkowego szyfrowania do generowania zestawu wartości kluczy tajnych standardu Advanced Encryption Standard (AES). W pliku ukrytych kluczy instancji serwera katalogów są przechowywane wartości kluczy, które służą do szyfrowania i deszyfrowania hasła i atrybutów.
8. W polu **Potwierdź klucz początkowy szyfrowania** wprowadź klucz początkowy szyfrowania dla instancji serwera katalogów.
9. Aby podać wartość klucza dodatkowego szyfrowania, kliknij opcję **Użyj wartości dodatkowego klucza szyfrowania**.
   a. W polu **Łańcuch klucza dodatkowego szyfrowania** wprowadź wartość klucza dodatkowego szyfrowania dla instancji serwera katalogów. Klucz dodatkowy szyfrowania musi zawierać jedynie znaki drukowalne ISO-8859-1 ASCII z wartościami w zakresie od 33 do 126. Klucz dodatkowy szyfrowania musi zawierać 12 znaków. Informacje o znakach, których można użyć, zawiera sekcja “Znaki ASCII o kodach od 33 do 126” na stronie 129. Aby zsynchronizować kryptograficznie serwer katalogów z inną instancją serwera katalogów, należy użyć tej samej wartości początkowego i dodatkowego klucza szyfrowania.
   b. W polu **Potwierdź klucz dodatkowy szyfrowania** wprowadź wartość klucza dodatkowego szyfrowania dla instancji serwera katalogów.
10. Opcjonalne: W polu **Opis instancji** wprowadź opis instancji serwera katalogów. Opis pomaga w identyfikowaniu instancji.
11. Kliknij przycisk **Dalej**.
12. W polu **Nazwa instancji DB2** na panelu **Szczegóły instancji DB2**, podaj nazwę instancji bazy danych DB2 dla instancji serwera katalogów.

    **Uwaga:** Instancja bazy danych DB2 dla instancji serwera katalogów nie może być skonfigurowana lub używana przez inne programy lub produkty.

    Domyślnie nazwa instancji bazy danych DB2 jest taka sama, jak nazwa instancji serwera katalogów. Można jednak określić inną nazwę instancji DB2. Jeśli zostanie podana inna

nazwa, w systemie musi istnieć ID użytkownika systemowego o tej samej nazwie. Ta nazwa konta użytkownika nie może być powiązana z inną instancją serwera katalogów.

13. Kliknij przycisk **Dalej**.
14. Na panelu **Ustawienia TCP/IP dla hostów multihomed** wybierz jedną z następujących opcji:
    - Aby instancja serwera katalogów nasłuchiwała na wszystkich adresach IP, wybierz opcję **Nasłuchuj na wszystkich skonfigurowanych adresach IP**.
    - Jeśli instancja ma nasłuchiwać na określonym zbiorze adresów IP skonfigurowanych na komputerze, wykonaj następujące kroki:
      a. Usuń zaznaczenie opcji **Nasłuchuj na wszystkich skonfigurowanych adresach IP**.
      b. Z listy **Wybierz konkretne adresy IP, na których należy nasłuchiwać** wybierz adres lub adresy IP, na których ma nasłuchiwać instancja.
15. Kliknij przycisk **Dalej**.
16. Na panelu **Ustawienia portów TCP/IP** podaj następujące wartości:

    **Uwaga:** Należy przypisać unikalne numery portów do portów serwera katalogów i nie można powodować konfliktów z istniejącymi portami używanymi na komputerze. W systemach AIX, Linux i Solaris numery portów z zakresu od 1 do 1000 mogą być używane tylko przez użytkownika root.

    a. W polu **Port serwera** wprowadź numer portu, którego serwer ma używać jako swojego portu niezabezpieczonego. Numer ten musi się mieścić w zakresie od 1 do 65535.
    b. W polu **Chroniony port serwera** wpisz numer portu, którego serwer ma używać jako swojego portu chronionego. Numer ten musi się mieścić w zakresie od 1 do 65535.
    c. W polu **Port serwera administracyjnego** wpisz numer portu, którego serwer administracyjny ma używać jako swojego portu niezabezpieczonego. Numer ten musi się mieścić w zakresie od 1 do 65535.
    d. W polu **Chroniony port serwera administracyjnego** wpisz numer portu, którego serwer administracyjny ma używać jako swojego portu chronionego. Numer ten musi się mieścić w zakresie od 1 do 65535.
    e. Kliknij przycisk **Dalej**.
17. Na panelu **Etapy opcjonalne** wykonaj następujące kroki:
    a. Aby skonfigurować nazwę DN i hasło administratora dla instancji serwera katalogów, wybierz opcję **Konfiguracja nazwy DN i hasła administratora**. Należy ustawić nazwę DN i hasło administratora dla serwera proxy i pełnego serwera katalogów.
    b. Aby skonfigurować bazę danych dla instancji serwera katalogów, wybierz opcję **Konfigurowanie bazy danych**.
    c. Kliknij przycisk **Dalej**.
18. Na panelu **Konfiguracja nazwy DN i hasła administratora** wykonaj następujące kroki:
    a. W polu **Nazwa DN administratora** wprowadź poprawną nazwę DN lub zaakceptuj domyślną nazwę DN, cn=root. W wartości nazwy DN administratora nie jest rozróżniana wielkość liter. Użytkownik o nazwie DN administratora ma pełne prawa dostępu do wszystkich danych w instancji serwera katalogów.
    b. W polu **Hasło administratora** wpisz hasło dla nazwy DN administratora. W hasłach dokonuje się rozróżnienia wielkich i małych liter. Znaki zestawu znaków dwubajtowych (DBCS) w hasłach nie są poprawne.
    c. W polu **Potwierdź hasło** wpisz hasło dla nazwy DN administratora. Hasło zależy zapamiętać na przyszłość.

d. Kliknij przycisk **Dalej**.

19. W panelu **Konfigurowanie bazy danych**, wykonaj następujące czynności, aby skonfigurować bazę danych dla instancji serwera katalogów: Program Instance Administration Tool dodaje informacje dla bazy danych do pliku konfiguracyjnego ibmslapd.conf instancji serwera katalogów. Jeśli baza danych nie istnieje, program Instance Administration Tool utworzy bazę danych.

    a. W polu **Nazwa użytkownika bazy danych** wpisz poprawny identyfikator administratora DB2. Identyfikator administratora DB2 musi istnieć na komputerze i musi mieć wymagane uprawnienia dostępu przed skonfigurowaniem bazy danych.

    **Uwaga:** Administrator DB2 musi ustawić odpowiednie ustawienia narodowe dla języka, w którym mają być wyświetlane komunikaty serwera przed uruchomieniem serwera.

    b. W polu **Hasło** wpisz hasło administratora DB2. W haśle jest rozróżniana wielkość liter.

    **Uwaga:** Jeśli zostanie zmienione hasło systemowe dla administratora DB2, nie można go będzie zaktualizować przy użyciu programu Instance Administration Tool. Należy użyć programu Configuration Tool lub komendy **idscfgdb** z parametrem **-w**. Aby uzyskać więcej informacji, patrz “Zarządzanie hasłem administratora bazy danych DB2” na stronie 179.

    c. W polu **Nazwa bazy danych** wpisz nazwę bazy danych. Nazwa może zawierać od 2 do 8 znaków.

    d. Opcjonalne: Aby ustawić dowolne z następujących ustawień konfiguracji DB2, wybierz opcję **Pokaż zaawansowane opcje obszaru tabel**.

    **Uwaga:** Baza danych DB2 może przy tworzeniu obszarów tabel używać typu pamięci masowej SMS (System Managed Storage) lub DMS (Database Managed Storage). Wartością domyślną dla produktu IBM Security Directory Server jest typ SMS. Wersje IBM Security Directory Server wcześniejsze od 6.2 używają typu SMS dla wszystkich baz danych. Jeśli anulowano zaznaczenie opcji **Pokaż zaawansowane opcje obszaru tabel**, obszary tabel USERSPACE1 i LDAPSPACE zostaną utworzone przy użyciu typu DMS z domyślnymi wielkościami i położeniami. W systemach AIX, Linux i Solaris domyślna ścieżka i nazwa pliku dla obszaru tabel USERSPACE1 to *lokalizacja_bazy_danych*/*nazwa_instancji*/NODE0000/SQL00001/USPACE. W systemie Windows domyślna ścieżka i nazwa pliku dla obszaru tabel USERSPACE1 to *lokalizacja_bazy_danych**nazwa_instancji*\NODE0000\SQL00001\USPACE. W systemach AIX, Linux i Solaris domyślna ścieżka i nazwa pliku dla obszaru tabel LDAPSPACE to *lokalizacja_bazy_danych*/ldap32kcont_*nazwa_instancji*/ldapspace. W systemie Windows domyślna ścieżka i nazwa pliku dla obszaru tabel LDAPSPACE to *lokalizacja_bazy_danych*\ldap32kcont_*nazwa_instancji*\ldapspace.

    - Baza danych ma używać przechowywania danych SMS (System Managed Storage) dla obszarów tabel DB2. Gdy jest używany typ SMS, menedżer systemu plików systemu operacyjnego przydziela obszar tabel, w którym są przechowywane tabele DB2, oraz zarządza tym obszarem tabel.
    - Baza danych ma używać przechowywania danych DMS (Database Managed Storage) dla obszarów tabel DB2. Ponadto baza danych ma zostać skonfigurowana dla obszarów tabel USERSPACE1 i LDAPSPACE, wielkości i położenia. Gdy używany jest typ DMS, obszarami tabel zarządza menedżer bazy danych. O tym, które urządzenia i pliki będą używane, decyduje administrator bazy danych, a obszarami w tych urządzeniach i plikach zarządza DB2.

    e. Kliknij przycisk **Dalej**.

20. Na panelu **Opcje bazy danych** wykonaj następujące kroki:
    a. W polu **Położenie instalacji bazy danych** wpisz ścieżkę położenia bazy danych. Aby określić katalog, możesz kliknąć przycisk **Przeglądaj**. W systemie Windows należy podać położenie dysku, na przykład C:. W systemach AIX, Linux i Solaris położeniem musi być nazwa katalogu, na przykład /home/ldapdb.

       **Uwaga:** Minimalne wymagane miejsce na dysku dla bazy danych typu DMS wynosi 1 GB. W przypadku bazy danych typu SMS minimalne wymagane miejsce na dysku wynosi 150 MB. Wymagania te dotyczą pustej bazy danych. Gdy w bazie danych przechowywane są dane, wymagana jest większa ilość miejsca na dysku.
    b. Aby skonfigurować serwer katalogów z bazą danych dla tworzenia kopii zapasowej otwartej bazy danych, wykonaj następujące kroki:
       1) Wybierz opcję **Konfiguruj tworzenie kopii zapasowej otwartej bazy danych**.
       2) W polu **Położenie kopii zapasowej bazy danych** wprowadź położenie, w którym ma zostać zapisany obraz kopii zapasowej. Aby określić położenie, możesz kliknąć przycisk **Przeglądaj**.

       **Uwaga:** Nie przerywaj działania narzędzia Instance Administration Tool, jeśli trwa operacja tworzenia kopii zapasowej.
       Jeśli baza danych jest konfigurowana do tworzenia kopii zapasowej otwartej bazy danych po zakończeniu konfiguracji bazy danych, uruchamiane jest tworzenie początkowej kopii zapasowej z zamkniętą bazą danych. Po zakończeniu operacji tworzenia kopii zapasowej z zamkniętą bazą danych serwer administracyjny jest restartowany. Można również skonfigurować utworzenie kopii zapasowej otwartej bazy danych dla instancji serwera katalogów za pomocą komendy **idscfgdb**. Nie można jednak zdekonfigurować tworzenia kopii zapasowej otwartej bazy danych, używając komendy **idscfgdb** i parametru **-c**. Jeśli zostanie skonfigurowane tworzenie kopii zapasowej otwartej bazy danych dla instancji za pomocą narzędzia Instance Administration Tool lub Configuration Tool, dekonfigurację można przeprowadzić za pomocą narzędzia Configuration Tool lub komendy **idscfgdb**.
    c. W obszarze **Opcja zestawu znaków** wybierz jedną z następujących opcji, aby utworzyć typ bazy danych:

       **Uwaga:** Utwórz uniwersalną bazę danych DB2, jeśli masz zamiar zapisywać na serwerze katalogów dane w wielu językach. Poza tym uniwersalna baza danych DB2 jest bardziej wydajna, ponieważ wymagana jest mniejsza liczba operacji tłumaczenia danych. Aby można było używać znaczników języków, baza danych musi być w formacie UTF-8. “Obsługa standardu UTF-8” na stronie 125 zawiera więcej informacji na temat standardu UTF-8.
       - Aby utworzyć bazę danych UTF-8 (UCS Transformation Format), w której klienci LDAP będą mogli przechowywać dane znakowe UTF-8, kliknij opcję **Utwórz uniwersalną bazę danych DB2**.
       - Aby utworzyć bazę danych w lokalnej stronie kodowej, kliknij opcję **Utwórz bazę danych DB2 w lokalnej stronie kodowej**.
    d. Kliknij przycisk **Dalej**.
21. Jeśli wybrano opcję **Pokaż zaawansowane opcje obszaru tabel** w panelu **Konfigurowanie bazy danych**, należy wykonać następujące wartości w panelu **Konfigurowanie tabel bazy danych**:
    a. Z listy **Wybierz typ obszaru tabel bazy danych** wybierz typ bazy danych. Typ DMS obszaru tabel bazy danych jest domyślny. Jeśli zostanie wybrany typ SMS obszaru tabel bazy danych, wszystkie pozostałe pola zostaną wyłączone. Obsługa

obszaru tabel DMS jest używana tylko dla obszarów tabel USERSPACE1 oraz LDAPSPACE. Wszystkie pozostałe obszary tabel, takie jak obszar tabel katalogu i tymczasowy obszar tabel są typu SMS.

a. W obszarze **Szczegóły obszaru tabel USERSPACE1** podaj następujące szczegóły:
   1) Z listy **Kontener obszaru tabel** wybierz typ kontenera. Aby obszar tabel USERSPACE1 znajdował się w systemie plików, wybierz opcję **Plik**. Jeśli położeniem kontenera obszaru tabel bazy danych jest system plików, zostanie utworzony przygotowany obszar tabel DMS. Można podać początkową wielkość obszaru tabel i wielkość jednostki rozszerzania, a obszar tabel zostanie automatycznie rozszerzony w razie potrzeby. Aby utworzyć obszar tabel USERSPACE1 na urządzeniu surowym, wybierz opcję **Urządzenie surowe**. Urządzenie surowe to urządzenie, w którym nie zainstalowano żadnego systemu plików, takie jak dysk twardy bez żadnego systemu plików. Jeśli położeniem kontenera obszaru tabel bazy danych jest urządzenie surowe, zostanie utworzony surowy obszar tabel DMS. W takiej sytuacji wielkość kontenera obszaru tabel bazy danych jest stała i obszaru tego nie można zwiększać. Jeśli zostanie wybrana opcja **Urządzenie surowe**, należy podać wielkość razem z położeniem kontenera, a nie zaakceptować wartości domyślne.
   2) Jeśli wybrano opcję **Plik** na liście **Kontener obszaru tabel**, należy podać następujące szczegóły:
      a) W polu **Ścieżka katalogu** podaj ścieżkę katalogu, w którym ma zostać utworzony obszar tabel USERSPACE1. Aby wybrać katalog, możesz kliknąć przycisk **Przeglądaj**.
      b) W polu **Nazwa pliku** wprowadź nazwę pliku obszaru katalogu do utworzenia lub zaakceptuj domyślną nazwę pliku USPACE.
      c) W polu **Wielkość początkowa** wprowadź wielkość początkową obszaru tabel USERSPACE1 w stronach lub zaakceptuj wartość domyślną. W przypadku kontenera obszaru tabel typu **Plik** kontener obszaru tabel USERSPACE1 ma typ automatycznego przyrostu. W polu **Wielkość początkowa** można podać wielkość początkową, a w polu **Wielkość rozszerzania** wielkość jednostki rozszerzania. Wartość domyślna wielkości początkowej wynosi 16 k, a domyślna wielkość jednostki rozszerzania wynosi 8 k. Wielkość strony dla kontenera obszaru tabel USERSPACE1 wynosi 4 kB na stronę.
   3) Jeśli wybrano opcję **Urządzenie surowe** na liście **Kontener obszaru tabel**, należy podać następujące szczegóły:
      a) W polu **Ścieżka urządzenia** wpisz położenie urządzenia surowego. W systemie Windows ścieżka musi rozpoczynać się od \\.\. Przykładowa ścieżka z nazwą urządzenia \\.*nazwa_urządzenia*. W systemach AIX, Linux i Solaris ścieżką urządzenia musi być poprawna ścieżka.
      b) W polu **Wielkość początkowa** wprowadź wielkość początkową obszaru tabel USERSPACE1 lub zaakceptuj wartość domyślną. Dla kontenera obszaru tabel typu **Urządzenie surowe** wielkość kontenera obszaru tabel USERSPACE1 jest stała. Wielkość domyślna wynosi 16 k. Aby uzyskać lepsze wyniki, należy podać odpowiednią wielkość.

b. W obszarze **Szczegóły obszaru tabel LDAPSPACE** podaj następujące szczegóły:
   1) Z listy **Kontener obszaru tabel** wybierz typ kontenera. Aby obszar tabel LDAPSPACE znajdował się w systemie plików, wybierz opcję **Plik**. Aby utworzyć obszar tabel LDAPSPACE na urządzeniu surowym, wybierz opcję **Urządzenie surowe**. Urządzenie surowe to urządzenie, w którym nie zainstalowano żadnego systemu plików, takie jak dysk twardy bez żadnego systemu plików.

2) Jeśli wybrano opcję **Plik** na liście **Kontener obszaru tabel**, należy podać następujące szczegóły:
   a) W polu **Ścieżka katalogu** podaj ścieżkę katalogu, w którym ma zostać utworzony obszar tabel LDAPSPACE. Aby wybrać katalog, możesz kliknąć przycisk **Przeglądaj**.
   b) W polu **Nazwa pliku** wprowadź nazwę pliku obszaru katalogu do utworzenia lub zaakceptuj domyślną nazwę pliku ldapspace.
   c) W polu **Wielkość początkowa** wprowadź wielkość początkową obszaru tabel LDAPSPACE w stronach lub zaakceptuj wartość domyślną. W przypadku kontenera obszaru tabel typu **Plik** kontener obszaru tabel LDAPSPACE ma typ automatycznego przyrostu. W polu **Wielkość początkowa** można podać wielkość początkową, a w polu **Wielkość rozszerzania** wielkość jednostki rozszerzania. Wartość domyślna wielkości początkowej wynosi 16 k, a domyślna wielkość jednostki rozszerzania wynosi 8 k. Wielkość strony dla kontenera obszaru tabel LDAPSPACE wynosi 32 kB na stronę.
3) Jeśli wybrano opcję **Urządzenie surowe** na liście **Kontener obszaru tabel**, należy podać następujące szczegóły:
   a) W polu **Ścieżka urządzenia** wpisz położenie urządzenia surowego. W systemie Windows ścieżka musi rozpoczynać się od \\.\. Przykładowa ścieżka z nazwą urządzenia \\.*nazwa_urządzenia*. W systemach AIX, Linux i Solaris ścieżką urządzenia musi być poprawna ścieżka.
   b) W polu **Wielkość początkowa** wprowadź wielkość początkową obszaru tabel LDAPSPACE lub zaakceptuj wartość domyślną. Dla kontenera obszaru tabel typu **Urządzenie surowe** wielkość kontenera obszaru tabel LDAPSPACE jest stała. Wielkość domyślna wynosi 16 k. Aby uzyskać lepsze wyniki, należy podać odpowiednią wielkość.

c. Jeśli wybrana została opcja **Plik** w jednym lub obu polach **Kontener obszaru tabel**, podaj liczbę stron, o jaką mają zostać rozszerzone kontenery obszaru tabel, w polu **Wielkość rozszerzania**.

d. Kliknij przycisk **Dalej**.

22. Na panelu **Sprawdź ustawienia** zweryfikuj wygenerowane podsumowanie.
23. Aby rozpocząć tworzenie instancji serwera katalogów, kliknij przycisk **Zakończ**.
24. W oknie **Wyniki** sprawdź komunikaty dziennika wygenerowane dla operacji tworzenia instancji.
25. Aby zamknąć okno **Wyniki**, kliknij przycisk **Zamknij**.
26. Aby zamknąć program Instance Administration Tool, kliknij przycisk **Zamknij**.

### Wyniki

Program Instance Administration Tool utworzy instancję serwera katalogów na komputerze.

### Co dalej

Należy uruchomić proces ibmslapd oraz serwer administracyjny powiązany z instancją serwera katalogów. Informacje na ten temat zawiera sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego” na stronie 156.

## Tworzenie instancji serwera proxy z własnymi ustawieniami

Narzędzie Instance Administration Server umożliwia utworzenie instancji serwera proxy z własnymi wymaganymi wartościami.

## Zanim rozpoczniesz

Aby utworzyć instancję serwera proxy, należy wykonać następujące czynności:

1. Zainstaluj produkt IBM Security Directory Server z funkcją serwera proxy. Patrz sekcja “Instalowanie przy użyciu programu IBM Installation Manager” na stronie 31.

## Procedura

1. Uruchom program Instance Administration Tool. Patrz sekcja “Uruchamianie narzędzia Instance Administration Tool” na stronie 131.
2. Kliknij opcję **Utwórz instancję**.
3. Na panelu **Utwórz lub przeprowadź migrację** okna **Tworzenie nowej instancji serwera katalogów** wykonaj następujące kroki, aby utworzyć instancję serwera proxy:
   a. Kliknij opcję **Utwórz nową instancję serwera katalogów**.
   b. Kliknij opcję **Konfiguruj jako proxy**.
4. Kliknij przycisk **Dalej**.
5. Na panelu **Szczegóły instancji** okna **Tworzenie nowej instancji serwera katalogów** podaj następujące wartości:
   a. Z listy **Nazwa użytkownika** wybierz nazwę użytkownika, do którego należy instancja. Do instancji jest przypisana taka sama nazwa jak nazwa użytkownika.
   b. Aby powiązać nowe konto użytkownika z instancją, kliknij przycisk **Utwórz użytkownika**. W oknie **Tworzenie nowego użytkownika instancji serwera katalogów** wykonaj następujące kroki:
      1) W polu **Nazwa użytkownika** wpisz nazwę użytkownika.
      2) W polu **Hasło** wprowadź hasło dla konta użytkownika.
      3) W polu **Potwierdź hasło** wprowadź hasło dla konta użytkownika.
      4) W polu **Katalog osobisty** wprowadź katalog osobisty do skonfigurowania dla konta użytkownika. Możesz również kliknąć przycisk **Przeglądaj** i określić katalog osobisty.
      5) W polu **Grupa podstawowa** wpisz nazwę grupy podstawowej użytkownika.
      6) Aby utworzyć konto użytkownika, kliknij przycisk **Utwórz**.
   c. Aby zmodyfikować istniejące konto użytkownika, wybierz nazwę użytkownika z listy **Nazwa użytkownika** i kliknij opcję **Edytuj użytkownika**. W oknie **Edycja użytkownika instancji serwera katalogów** wykonaj następujące kroki:
      1) W polu **Nazwa użytkownika** znajduje się nazwa użytkownika.
      2) W polu **Hasło** wprowadź hasło dla konta użytkownika.
      3) W polu **Potwierdź hasło** wprowadź hasło dla konta użytkownika.
      4) W polu **Katalog osobisty** wprowadź katalog osobisty do skonfigurowania dla konta użytkownika. Możesz również kliknąć przycisk **Przeglądaj** i określić katalog osobisty.
      5) W polu **Grupa podstawowa** wpisz nazwę grupy podstawowej użytkownika.
      6) Aby edytować konto użytkownika, kliknij przycisk **Edytuj**.
      7) W oknie potwierdzenia **Edycja użytkownika instancji serwera katalogów** kliknij przycisk **Tak**.
6. W polu **Położenie instancji** wprowadź położenie instancji serwera proxy. Możesz również kliknąć przycisk **Przeglądaj** i określić katalog główny instancji. W podanym położeniu musi znajdować się przynajmniej 30 MB wolnego miejsca na dysku. W systemach Windows położeniem jest dysk, na przykład C:. Pliki instancji katalogu są zapisywane w katalogu \idsslapd-*nazwa_instancji* podanego dysku. Zmienna

*nazwa_instancji* jest nazwą instancji serwera proxy. W systemach AIX, Linux i Solaris domyślnym położeniem instancji jest katalog osobisty właściciela instancji serwera proxy, ale można podać inną ścieżkę.

7. W polu **Łańcuch początkowy szyfrowania** wprowadź klucza początkowy szyfrowania dla instancji.

   **Zapamiętaj:** Należy zapamiętać klucz początkowy szyfrowania instancji, ponieważ może on być wymagany w innych czynnościach konfiguracyjnych.
   Klucz początkowy szyfrowania musi zawierać jedynie znaki drukowalne ISO-8859-1 ASCII z wartościami w zakresie od 33 do 126. Klucz początkowy szyfrowania musi mieć przynajmniej 12 znaków i co najwyżej 1016 znaków. Informacje o znakach, których można użyć, zawiera sekcja “Znaki ASCII o kodach od 33 do 126” na stronie 129. Serwer katalogów używa klucza początkowego szyfrowania do generowania zestawu wartości kluczy tajnych standardu Advanced Encryption Standard (AES). W pliku ukrytych kluczy instancji serwera katalogów są przechowywane wartości kluczy, które służą do szyfrowania i deszyfrowania hasła i atrybutów.
8. W polu **Potwierdź klucz początkowy szyfrowania** wprowadź klucz początkowy szyfrowania dla instancji.
9. Aby podać wartość klucza dodatkowego szyfrowania, kliknij opcję **Użyj wartości dodatkowego klucza szyfrowania**.
   a. W polu **Łańcuch klucza dodatkowego szyfrowania** wprowadź wartość klucza dodatkowego szyfrowania dla instancji. Klucz dodatkowy szyfrowania musi zawierać jedynie znaki drukowalne ISO-8859-1 ASCII z wartościami w zakresie od 33 do 126. Klucz dodatkowy szyfrowania musi zawierać 12 znaków. Informacje o znakach, których można użyć, zawiera sekcja “Znaki ASCII o kodach od 33 do 126” na stronie 129.
   b. W polu **Potwierdź klucz dodatkowy szyfrowania** wprowadź wartość klucza dodatkowego szyfrowania dla instancji.
10. Opcjonalne: W polu **Opis instancji** wprowadź opis instancji. Opis pomaga w identyfikowaniu instancji.
11. Kliknij przycisk **Dalej**.
12. Na panelu **Ustawienia TCP/IP dla hostów multihomed** wybierz jedną z następujących opcji:
    - Aby instancja nasłuchiwała na wszystkich adresach IP, wybierz opcję **Nasłuchuj na wszystkich skonfigurowanych adresach IP**.
    - Jeśli instancja ma nasłuchiwać na określonym zbiorze adresów IP skonfigurowanych na komputerze, wykonaj następujące kroki:
      a. Usuń zaznaczenie opcji **Nasłuchuj na wszystkich skonfigurowanych adresach IP**.
      b. Z listy **Wybierz konkretne adresy IP, na których należy nasłuchiwać** wybierz adres lub adresy IP, na których ma nasłuchiwać instancja.
13. Kliknij przycisk **Dalej**.
14. Na panelu **Ustawienia portów TCP/IP** podaj następujące wartości:

    **Uwaga:** Należy przypisać unikalne numery portów do portów serwera katalogów i nie można powodować konfliktów z istniejącymi portami używanymi na komputerze. W systemach AIX, Linux i Solaris numery portów z zakresu od 1 do 1000 mogą być używane tylko przez użytkownika root.
    a. W polu **Port serwera** wprowadź numer portu, którego serwer ma używać jako swojego portu niezabezpieczonego. Numer ten musi się mieścić w zakresie od 1 do 65535.

b. W polu **Chroniony port serwera** wpisz numer portu, którego serwer ma używać jako swojego portu chronionego. Numer ten musi się mieścić w zakresie od 1 do 65535.

c. W polu **Port serwera administracyjnego** wpisz numer portu, którego serwer administracyjny ma używać jako swojego portu niezabezpieczonego. Numer ten musi się mieścić w zakresie od 1 do 65535.

d. W polu **Chroniony port serwera administracyjnego** wpisz numer portu, którego serwer administracyjny ma używać jako swojego portu chronionego. Numer ten musi się mieścić w zakresie od 1 do 65535.

e. Kliknij przycisk **Dalej**.

15. Na panelu **Etapy opcjonalne** wykonaj następujące kroki:
    a. Aby skonfigurować nazwę DN i hasło administratora dla instancji, wybierz opcję **Konfiguracja nazwy DN i hasła administratora**. Należy ustawić nazwę DN i hasło administratora dla instancji serwera proxy.
    b. Kliknij przycisk **Dalej**.
16. Na panelu **Konfiguracja nazwy DN i hasła administratora** wykonaj następujące kroki:
    a. W polu **Nazwa DN administratora** wprowadź poprawną nazwę DN lub zaakceptuj domyślną nazwę DN, cn=root. W wartości nazwy DN administratora nie jest rozróżniana wielkość liter. Użytkownik o nazwie DN administratora ma pełne prawa dostępu do wszystkich danych w instancji.
    b. W polu **Hasło administratora** wpisz hasło dla nazwy DN administratora. W hasłach dokonuje się rozróżnienia wielkich i małych liter. Znaki zestawu znaków dwubajtowych (DBCS) w hasłach nie są poprawne.
    c. W polu **Potwierdź hasło** wpisz hasło dla nazwy DN administratora. Hasło zaleźy zapamiętać na przyszłość.
    d. Kliknij przycisk **Dalej**.
17. Na panelu **Sprawdź ustawienia** zweryfikuj wygenerowane podsumowanie.
18. Aby rozpocząć tworzenie instancji serwera proxy, kliknij przycisk **Zakończ**.
19. W oknie **Wyniki** sprawdź komunikaty dziennika wygenerowane dla operacji tworzenia instancji.
20. Aby zamknąć okno **Wyniki**, kliknij przycisk **Zamknij**.
21. Aby zamknąć program Instance Administration Tool, kliknij przycisk **Zamknij**.

### Wyniki

Program Instance Administration Tool utworzy instancję serwera proxy na komputerze.

### Co dalej

Należy uruchomić serwer administracyjny i proces ibmslapd w trybie tylko konfiguracji i skonfigurować serwery zaplecza. Więcej informacji znajduje się w sekcji *Administrowanie* dokumentacji produktu IBM Security Directory Server.

## Tworzenie instancji za pomocą programu narzędziowego dla wiersza komend

Do utworzenia instancji można użyć programu narzędziowego dla wiersza komend **idsicrt**.

### Zanim rozpoczniesz

Aby utworzyć instancję za pomocą programu narzędziowego dla wiersza komend, należy spełnić następujące warunki:

1. Zainstaluj produkt IBM Security Directory Server z serwerem, serwerem proxy lub obiema opcjami. Patrz sekcja “Instalowanie przy użyciu programu IBM Installation Manager” na stronie 31.
2. Musi istnieć identyfikator użytkownika systemu, do którego musi należeć instancja. Więcej informacji na temat tworzenia identyfikatora użytkownika systemu zawiera sekcja “Użytkownicy i grupy powiązane z instancją serwera katalogów” na stronie 121.

## O tym zadaniu

Po uruchomieniu komendy **idsicrt** tworzy ona instancję oraz instancję bazy danych DB2 dla instancji pełnego serwera katalogów.

## Procedura

1. Zaloguj się jako użytkownik root w systemach AIX, Linux lub Solaris i jako członek grupy administratorów w systemie Windows.
2. Zmień bieżący katalog roboczy na podkatalog sbin w miejscu instalacji produktu IBM Security Directory Server.
3. Aby utworzyć instancję, uruchom następującą komendę: Zastąp zmienną *nazwa_instancji* nazwą poprawnego ID użytkownika systemu.

| Zadania do wykonania | Komenda do uruchomienia: |
|---|---|
| **Utworzyć instancję serwera katalogów.** | idsicrt -I *nazwa_instancji* -e klucz_tajny! -l katalog_główny_instancji |
| **Utworzyć instancję serwera proxy.** | idsicrt -I *nazwa_instancji* -e klucz_tajny! -l katalog_główny_instancji -x |

Więcej informacji na temat komendy **idsicrt** zawiera *Skorowidz komend*.

## Przykłady

**Przykład 1:**

Aby utworzyć instancję serwera katalogów z następującymi wartościami w systemie AIX, Linux lub Solaris, uruchom następującą komendę:

- Nazwa instancji: moja_instancja
- Niezabezpieczony port: 389
- Zabezpieczony port: 636
- Klucz początkowy szyfrowania: klucz_tajny!
- Klucz dodatkowy szyfrowania: klucz_dodatkowy
- Katalog główny instancji: /home/moja_instancja w systemach AIX i Linux oraz /export/home/moja_instancja w systemie Solaris

```
idsicrt -I
moja_instancja -p 389 -s
636 -e klucz_tajny!\
-g klucz_dodatkowy -l
/home/moja_instancja
```

Aby utworzyć instancję serwera katalogów z następującymi wartościami w systemie Windows, uruchom następującą komendę:

- Nazwa instancji: moja_instancja
- Niezabezpieczony port: 389
- Zabezpieczony port: 636
- Klucz początkowy szyfrowania: klucz_tajny!
- Klucz dodatkowy szyfrowania: klucz_dodatkowy

- Katalog główny instancji: C:

```
idsicrt -I moja_instancja -p 389
-s 636 -e klucz_tajny!
-g klucz_dodatkowy -l C:
```

**Przykład 2:**

Aby utworzyć instancję serwera proxy z następującymi wartościami w systemie AIX, Linux lub Solaris, uruchom następującą komendę:

- Nazwa instancji: moje_proxy
- Niezabezpieczony port: 389
- Zabezpieczony port: 636
- Klucz początkowy szyfrowania: klucz_tajny!
- Klucz dodatkowy szyfrowania: klucz_dodatkowy
- Katalog główny instancji: /home/moje_proxy w systemach AIX i Linux oraz /export/home/moje_proxy w systemie Solaris

```
idsicrt -I
moje_proxy -p 389 -s
636 -e klucz_tajny!\
-g klucz_dodatkowy -l
/home/moje_proxy -x
```

Aby utworzyć instancję serwera proxy z następującymi wartościami w systemie Windows, uruchom następującą komendę:

- Nazwa instancji: moje_proxy
- Niezabezpieczony port: 389
- Zabezpieczony port: 636
- Klucz początkowy szyfrowania: klucz_tajny!
- Klucz dodatkowy szyfrowania: klucz_dodatkowy
- Katalog główny instancji: C:

```
idsicrt -I -s -e -p moje_proxy 389
636 klucz_tajny!
-g
klucz_dodatkowy -l C: -x
```

### Co dalej

Przeprowadź następujące konfiguracje, aby utworzyć działającą instancję:

1. Skonfiguruj instancję bazy danych DB2 dla instancji pełnego serwera katalogów.
2. Skonfiguruj nazwę wyróżniającą (DN) i hasło administratora instancji.
3. Skonfiguruj przyrostki dla instancji.

## Aktualizowanie instancji poprzedniej wersji przy użyciu programu Instance Administration Tool

Za pomocą narzędzia Instance Administration Tool można zaktualizować instancję serwera katalogów lub instancję serwera proxy z wersji wcześniejszej do wersji 6.3.1.

### Zanim rozpoczniesz

Przed aktualizacją instancji przy użyciu narzędzia Instance Administration Tool należy wykonać następujące zadania:

- Wykonaj instalację produktu IBM Security Directory Server w wersji 6.3.1. Więcej informacji na ten temat zawiera sekcja “Uruchamianie instalacji” na stronie 28.
- Skonfiguruj środowisko przed aktualizacją instancji. Patrz sekcja “Konfigurowanie środowiska przed aktualizacją instancji” na stronie 90.

- Zaloguj się jako użytkownik root w systemie operacyjnym AIX, Linux lub Solaris i jako członek grupy administratorów w systemie operacyjnym Windows.

### O tym zadaniu

Po zaktualizowaniu instancji wcześniejszej wersji jest ona przekształcana do w pełni funkcjonalnej instancji produktu IBM Security Directory Server w wersji 6.3.1.

### Procedura

1. Otwórz wiersz komend.
2. Przejdź do katalogu sbin. Domyślnie używana jest następująca lokalizacja w różnych systemach operacyjnych:

   **Microsoft Windows**
   C:\Program Files\IBM\ldap\V6.3.1\sbin

   **AIX i Solaris**
   /opt/IBM/ldap/V6.3.1/sbin

   **Linux** /opt/ibm/ldap/V6.3.1/sbin
3. Aby uruchomić program Instance Administration Tool, uruchom następującą komendę:

   **Uwaga:** W systemie Windows można go uruchomić z menu **Start**. Kliknij kolejno opcje **Start > Wszystkie programy > IBM Security Directory Server 6.3.1 > Instance Administration Tool**.

   ```
   idsxinst
   ```
4. Wybierz poprzednią wersję instancji, którą chcesz zaktualizować.
5. Kliknij opcję **Migruj**.
6. Aby zamknąć okno **Migrowanie instancji serwera katalogów**, kliknij przycisk **Zamknij**.
7. Jeśli program Instance Administration Tool wyświetla zapytanie po zakończeniu operacji aktualizacji, kliknij przycisk **OK**.
8. Zweryfikuj informacje podsumowania.
9. Aby zamknąć okno **Migrowanie instancji serwera katalogów**, kliknij przycisk **Zamknij**.
10. Wykonaj kopię zapasową zamkniętej bazy danych instancji. Aby uzyskać więcej informacji, patrz “Tworzenie kopii zapasowej serwera katalogów” na stronie 187.
11. Aby zamknąć program Instance Administration Tool, kliknij przycisk **Zamknij**.

### Wyniki

Program Instance Administration Tool zaktualizuje poprzednią wersję instancji serwera katalogów do wersji 6.3.1.

### Co dalej

Należy uruchomić proces ibmslapd oraz serwer administracyjny powiązany z instancją serwera katalogów. Informacje na ten temat zawiera sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego” na stronie 156.

## Aktualizowanie zdalnej instancji poprzedniej wersji przy użyciu programu Instance Administration Tool

Za pomocą narzędzia Instance Administration Tool można zaktualizować zdalną instancję serwera katalogów lub instancję serwera proxy z wersji wcześniejszej do wersji 6.3.1.

## Zanim rozpoczniesz

Przed aktualizacją instancji przy użyciu narzędzia Instance Administration Tool należy wykonać następujące zadania:

- Skonfiguruj środowisko przed aktualizacją instancji. Patrz sekcja “Konfigurowanie środowiska przed aktualizacją instancji” na stronie 90.
- Zaloguj się jako użytkownik root w systemie operacyjnym AIX, Linux lub Solaris i jako członek grupy administratorów w systemie operacyjnym Windows.

## O tym zadaniu

Po zakończeniu procesu aktualizacji narzędzie Instance Administration Tool utworzy instancję w wersji 6.3.1 na komputerze przy użyciu informacji o zdalnej instancji.

## Procedura

1. Utwórz kopię zapasową bazy danych instancji serwera katalogów, która jest zainstalowana na zdalnym komputerze, za pomocą komendy **idsdb2ldif**.

   **Ważne:** Jeśli aktualizujesz instancję serwera proxy, nie twórz kopii zapasowej bazy danych. Serwer proxy nie ma powiązanej bazy danych.

   ```
   idsdb2ldif -I nazwa_instancji -o inst_out.ldif
   ```

   Więcej informacji na temat komendy **idsdb2ldif** zawiera *Skorowidz komend*.
2. Wykonaj instalację produktu IBM Security Directory Server w wersji 6.3.1 na komputerze, na którym chcesz zaktualizować zdalną instancję. Więcej informacji na ten temat zawiera sekcja “Uruchamianie instalacji” na stronie 28.
3. Aby utworzyć kopię zapasową plików schematu i plików konfiguracyjnych zdalnej instancji, uruchom komendę **migbkup** dla wersji 6.3.1, do której chcesz zaktualizować:

| System operacyjny | Komenda do uruchomienia: |
|---|---|
| **Microsoft Windows** | **migbkup.bat** nazwa_dysku\idsslapd-nazwa_instancji katalog_kopii_zapasowej |
| **AIX, Linux i Solaris** | **migbkup** katalog_użytkownika/idsslapd-nazwa_instancji katalog_kopii_zapasowej |

   Komenda **migbkup** znajduje się w podkatalogu tools nośnika instalacyjnego produktu IBM Security Directory Server.
4. Skopiuj katalog kopii zapasowej, katalog_kopii_zapasowej, który został utworzony za pomocą komendy **migbkup**, z komputera zdalnego do komputera z zainstalowanym produktem IBM Security Directory Server w wersji 6.3.1.
5. Opcjonalne: Skopiuj plik kopii zapasowej bazy danych, inst_out.ldif, z komputera zdalnego do komputera z zainstalowanym serwerem IBM Security Directory Server w wersji 6.3.1.
6. Uruchom program Instance Administration Tool. Patrz sekcja “Uruchamianie narzędzia Instance Administration Tool” na stronie 131.
7. Kliknij opcję **Utwórz instancję**.
8. Na panelu **Utwórz lub zmigruj** wykonaj następujące zadania:
   a. Kliknij przycisk **Przeprowadź migrację poprzedniej wersji serwera katalogów**.
   b. W polu **Podaj ścieżkę kopii zapasowej plików** wpisz katalog, do którego skopiowano kopię zapasową konfiguracji instancji zdalnej i plików schematu. Możesz również kliknąć przycisk **Przeglądaj** i wybrać katalog.
   c. Kliknij przycisk **Dalej**.

9. Na panelu **Szczegóły instancji** okna **Tworzenie nowej instancji serwera katalogów** podaj następujące wartości:

   **Uwaga:** Przy aktualizowaniu instancji nie można edytować informacji o istniejącym użytkowniku.

   a. Z listy **Nazwa użytkownika** wybierz nazwę użytkownika, do którego należy instancja serwera katalogów. Do instancji serwera katalogów jest przypisana taka sama nazwa jak nazwa użytkownika.
   b. Aby powiązać nowe konto użytkownika z instancją, kliknij przycisk **Utwórz użytkownika**. W oknie **Tworzenie nowego użytkownika instancji serwera katalogów** wykonaj następujące kroki:
      1) W polu **Nazwa użytkownika** wpisz nazwę użytkownika.
      2) W polu **Hasło** wprowadź hasło dla konta użytkownika.
      3) W polu **Potwierdź hasło** wprowadź hasło dla konta użytkownika.
      4) W polu **Katalog osobisty** wprowadź katalog osobisty do skonfigurowania dla konta użytkownika. Możesz również kliknąć przycisk **Przeglądaj** i określić katalog osobisty.
      5) W polu **Grupa podstawowa** wpisz nazwę grupy podstawowej użytkownika.
      6) Aby utworzyć konto użytkownika, kliknij przycisk **Utwórz**.
10. W polu **Położenie instancji** wpisz położenie instancji serwera katalogów. Możesz również kliknąć przycisk **Przeglądaj** i określić katalog główny instancji. W podanym położeniu musi znajdować się przynajmniej 30 MB wolnego miejsca na dysku. W systemach Windows położeniem jest dysk, na przykład C:. Pliki instancji katalogu są zapisywane w katalogu \idsslapd-*nazwa_instancji* podanego dysku. Zmienna *nazwa_instancji* jest nazwą instancji serwera katalogów. W systemach AIX, Linux i Solaris domyślną instancją jest katalog osobisty właściciela instancji serwera katalogów, ale można podać inną ścieżkę.
11. Opcjonalne: W polu **Opis instancji** wprowadź opis instancji serwera katalogów. Opis pomaga w identyfikowaniu instancji.
12. Kliknij przycisk **Dalej**.
13. W przypadku aktualizacji zdalnej instancji serwera katalogów przy użyciu szczegółowych informacji o bazie danych DB2, kliknij opcję **Dalej** na panelu **Szczegóły instancji DB2**. Jeśli pliki kopii zapasowej dotyczą zdalnej instancji serwera proxy, panel **Szczegóły instancji DB2** może nie być wyświetlany.
14. Na panelu **Ustawienia TCP/IP dla hostów multihomed** wybierz jedną z następujących opcji:
    - Aby instancja serwera katalogów nasłuchiwała na wszystkich adresach IP, wybierz opcję **Nasłuchuj na wszystkich skonfigurowanych adresach IP**.
    - Jeśli chcesz, aby instancja serwera katalogów nasłuchiwała na określonym zestawie adresów IP skonfigurowanych w systemie, anuluj zaznaczenie opcji **Nasłuchuj na wszystkich skonfigurowanych adresach IP**. Wybierz z listy adres lub adresy IP, na których ma nasłuchiwać instancja serwera katalogów.
15. Kliknij przycisk **Dalej**.
16. Na panelu **Ustawienia portów TCP/IP** podaj następujące wartości:

    **Uwaga:** Należy przypisać unikalne numery portów do portów serwera katalogów i nie można powodować konfliktów z istniejącymi portami używanymi na komputerze. W systemach AIX, Linux i Solaris numery portów z zakresu od 1 do 1000 mogą być używane tylko przez użytkownika root.

a. W polu **Port serwera** wprowadź numer portu, którego serwer ma używać jako swojego portu niezabezpieczonego. Numer ten musi się mieścić w zakresie od 1 do 65535.
b. W polu **Chroniony port serwera** wpisz numer portu, którego serwer ma używać jako swojego portu chronionego. Numer ten musi się mieścić w zakresie od 1 do 65535.
c. W polu **Port serwera administracyjnego** wpisz numer portu, którego serwer administracyjny ma używać jako swojego portu niezabezpieczonego. Numer ten musi się mieścić w zakresie od 1 do 65535.
d. W polu **Chroniony port serwera administracyjnego** wpisz numer portu, którego serwer administracyjny ma używać jako swojego portu chronionego. Numer ten musi się mieścić w zakresie od 1 do 65535.
e. Kliknij przycisk **Dalej**.

17. Na panelu **Sprawdź ustawienia** zweryfikuj wygenerowane podsumowanie.
18. Aby rozpocząć tworzenie instancji serwera katalogów, kliknij przycisk **Zakończ**.
19. W oknie **Wyniki** sprawdź komunikaty dziennika wygenerowane dla operacji tworzenia instancji.
20. Aby zamknąć okno **Wyniki**, kliknij przycisk **Zamknij**.
21. Aby zamknąć program Instance Administration Tool, kliknij przycisk **Zamknij**.

### Wyniki

Program Instance Administration Tool utworzy instancję serwera katalogów na komputerze.

### Co dalej

Należy uruchomić proces ibmslapd oraz serwer administracyjny powiązany z instancją serwera katalogów. Patrz sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego” na stronie 156.

Należy utworzyć kopię zapasową instancji. Informacje na temat tworzenia kopii zapasowej instancji serwera katalogów zawiera sekcja “Tworzenie kopii zapasowej serwera katalogów” na stronie 187.

## Tworzenie instancji na podstawie istniejącej instancji

Program Instance Administration Tool pozwala utworzyć instancję serwera katalogów na podstawie istniejącej instancji lokalnej lub zdalnej. Źródłowy serwer katalogów działa jak szablon dla docelowej instancji serwera katalogów.

Program Instance Administration Tool produktu IBM Security Directory Server obsługuje kopiowanie katalogu źródłowej instancji serwera, jeśli program i instancja są w tej samej wersji. Docelowy serwer katalogów jest tworzony na komputerze, na którym uruchomiony jest program Instance Administration Tool. Jeśli źródłowy serwer katalogów jest na innym komputerze, systemy operacyjne tych dwóch komputerów mogą być różne. Na przykład można utworzyć instancję serwera katalogów w systemie Windows, która jest kopią instancji w systemie Linux.

Gdy program narzędziowy jest używany do kopiowania instancji źródłowej, mogą być wykonywane następujące operacje w zależności od podanych parametrów:

- Można utworzyć docelowy serwer katalogów z tymi samymi ustawieniami konfiguracyjnymi i plikami schematu, co źródłowa instancja serwera katalogów. Ponadto serwer docelowy synchronizuje z serwerem źródłowym pliki kluczy ukrytych.

- Jeśli instancja serwera źródłowego jest pełnym serwerem katalogów, tworzona instancja serwera docelowego również jest pełnym serwerem katalogów. Istnieje możliwość skopiowania danych z istniejącej instancji serwera katalogów. Jeśli serwer źródłowy jest skonfigurowany do tworzenia kopii zapasowej otwartej bazy danych, można utworzyć funkcjonalny docelowy serwer katalogów zawierający pozycje w swojej bazie danych.
- Jeśli instancja serwera źródłowego jest serwerem proxy, tworzona instancja serwera docelowego również jest serwerem proxy.
- Jeśli instancja źródłowego serwera katalogów działa w środowisku replikacji, można skonfigurować docelową instancję jako serwer repliki lub jako serwer równorzędny serwera źródłowego.
- Jeśli instancja źródłowego serwera katalogów działa w środowisku rozproszonym, można skonfigurować docelową instancję jako serwer proxy.
- Jeśli źródłowa instancja serwera katalogów jest skonfigurowana do obsługi bezpiecznej komunikacji, program Instance Administration Tool skopiuje pliki bazy danych kluczy do docelowego serwera katalogów.

Przed utworzeniem serwera docelowego należy upewnić się, że źródłowy serwer katalogów spełnia następujące warunki:

- Źródłowy serwer katalogów musi być produktem IBM Security Directory Server w wersji 6.3.1. Źródłowy serwer katalogów nie może być instancją poprzedniej wersji.
- Źródłowy serwer katalogów musi działać w trybie normalnym. Kopiowanie instancji działającej w trybie konfiguracji nie jest obsługiwane.
- Źródłowa instancja serwera katalogów musi być dostępna z komputera, na którym działa program Instance Administration Tool.
- Aby utworzyć docelowy serwer katalogów jako replikę lub serwer równorzędny, w instancji źródłowego serwera katalogów musi istnieć kontekst replikacji. Nie można za pomocą programu Instance Administration Tool skonfigurować pierwszej repliki ani serwera równorzędnego w topologii replikacji. Źródłowa instancja serwera katalogów musi mieć zdefiniowany co najmniej jeden kontekst replikacji, grupę replikacji i pozycję podrzędną replikacji. Aby skonfigurować instancję jako replikę, instancja źródłowa musi mieć początkową topologię replikacji, w tym uzgodnienie z przynajmniej jednym serwerem. Jeśli konfigurowana jest instancja równorzędna, serwer źródłowy musi być zdefiniowany jako główny dla jednej lub wielu pozycji podrzędnych w konfiguracji replikacji.
- Tworzona instancja równorzędną lub replika ma nową podpozycję replikacji z nazwą wyróżniającą (DN) ibm-replicaGroup=default,*kontekst_replikacji*. Jeśli nie ma tej nazwy wyróżniającej, nie można skopiować instancji.

Aby skopiować dane z źródłowej do docelowej instancji serwera katalogów, należy spełnić następujące wymagania:

- Wersja bazy danych DB2 może być różna w obydwu instancjach serwerów katalogów. Kopię zapasową bazy danych z jednej rodziny systemów operacyjnych można odtworzyć w dowolnym systemie w obrębie tej samej rodziny systemów operacyjnych. Na przykład można odtworzyć bazę danych utworzoną w DB2 UDB wersji 9 w systemach Windows w systemie z DB2, wersja 10. W systemach AIX, Linux i Solaris można odtworzyć kopie zapasowe utworzone w DB2 UDB 9 w DB2 10, jeśli układ bajtów (big endian lub little endian) tych systemów jest taki sam.
- Instancja źródłowego serwera katalogów musi być skonfigurowana do tworzenia kopii zapasowej otwartej bazy danych. Można to skonfigurować podczas początkowej konfiguracji bazy danych. Do skonfigurowania tworzenia kopii zapasowej otwartej bazy danych można użyć programów Instance Administration Tool lub Configuration Tool.

- Przed użyciem programu Instance Administration Tool do skopiowania instancji serwera katalogów należy utworzyć jego początkową kopię zapasową z zamkniętą bazą danych. W podanej ścieżce musi się znajdować wyłącznie jeden obraz kopii zapasowej.
- Ścieżka zawierająca obraz kopii zapasowej musi być dostępna zarówno ze źródłowej, jak i z docelowej instancji serwera katalogów.

# Tworzenie kopii istniejącej instancji za pomocą narzędzia Instance Administration Tool

Za pomocą narzędzia Instance Administration Tool można utworzyć kopię istniejącej instancji.

## Zanim rozpoczniesz

Aby utworzyć kopię istniejącej instancji, należy spełnić następujące wymagania:

- Uruchom proces ibmslapd i serwer administracyjny instancji w trybie normalnym.
- Upewnij się, że źródłowy serwer katalogów jest dostępny z poziomu narzędzia Instance Administration Tool.

## Procedura

1. Uruchom program Instance Administration Tool. Patrz sekcja “Uruchamianie narzędzia Instance Administration Tool” na stronie 131.
2. Wybierz jedną z następujących opcji, aby utworzyć kopię istniejącej instancji:
   - Aby utworzyć kopię istniejącej instancji, która znajduje się na komputerze lokalnym, kliknij opcję **Kopiuj instancję lokalną**.
   - Aby utworzyć kopię istniejącej instancji, która znajduje się na komputerze zdalnym, kliknij opcję **Kopiuj instancję zdalną**.
3. Na panelu **Kopiowanie instancji serwera katalogów** podaj następujące wartości:
   a. W polu **Host** podaj adres IP lub nazwę hosta, jeśli źródłowy serwer katalogów znajduje się na komputerze zdalnym. Jeśli źródłowy serwer katalogów znajduje się na komputerze lokalnym, w polu zostanie wstawiona wartość localhost i nie będzie ono dostępne do edycji.
   b. W polu **Port** wprowadź numer portu serwera katalogów, jeśli numer portu w tym polu nie jest poprawny. Aby użyć bezpiecznego połączenia, należy podać numer zabezpieczonego portu instancji źródłowego serwera katalogów.
   c. W polu **Nazwa DN administratora** podaj nazwę DN administratora źródłowego serwera katalogów, jeśli instancja znajduje się na komputerze zdalnym. Jeśli źródłowy serwer katalogów znajduje się na komputerze lokalnym, w polu tym jest wstawiona wartość nazwy DN administratora i nie jest ono dostępne do edycji.
   d. W polu **Hasło** wpisz hasło nazwy DN administratora.
   e. W polu **Klucz początkowy szyfrowania** wprowadź klucz początkowy szyfrowania dla instancji źródłowego serwera katalogów.
   f. Jeśli źródłowy serwer katalogów jest skonfigurowany do bezpiecznej komunikacji i docelowy serwer katalogów również ma zostać tak skonfigurowany, kliknij opcję **Stosuj połączenie SSL**.
      1) W polu **Plik kluczy** wprowadź nazwę pliku bazy danych kluczy ze ścieżką. Możesz również kliknąć przycisk **Przeglądaj** i określić położenie.
      2) W polu **Nazwa klucza** wpisz nazwę klucza prywatnego do użycia z pliku kluczy źródłowego serwera katalogów.
      3) W polu **Hasło klucza** wpisz hasło bazy danych kluczy pliku kluczy.
   g. Kliknij przycisk **Dalej**.

4. Na panelu **Konfigurowanie instancji - krok 1** wykonaj następujące kroki:
   a. Sprawdź w polach **Adres URL źródła** i **Typ instancji źródłowej** informacje dotyczące źródłowego serwera katalogów. W polu **Typ instancji źródłowej** może znajdować się pełny serwer katalogów lub instancja serwera proxy.
   b. Aby skonfigurować docelowy serwer katalogów jako instancję równorzędną lub replikę w istniejącej topologii replikacji, wybierz opcję **Konfiguruj jako serwer równorzędny lub serwer replik** i wybierz jedną z następujących opcji:
      - Aby skonfigurować docelowy serwer katalogów jako replikę, kliknij opcję **Replika**.
      - Aby skonfigurować docelowy serwer katalogów jako instancję równorzędną, kliknij opcję **Równorzędny**.
   c. W polu **Nazwa użytkownika** wpisz identyfikator użytkownika systemu, do którego musi należeć instancja docelowego serwera katalogów. Nazwa nie może być dłuższa niż 8 znaków. Taka sama nazwa jest ustawiana również dla nazwy instancji serwera katalogów, ID administratora DB2, nazwy instancji bazy danych i nazwy bazy danych. Identyfikator użytkownika musi istnieć na komputerze i nie może być powiązany z żadną inną instancją serwera katalogów na komputerze. “Użytkownicy i grupy powiązane z instancją serwera katalogów” na stronie 121 zawiera szczegółowe informacje na temat identyfikatora użytkownika.
   d. W polu **Hasło** wpisz hasło dla identyfikatora użytkownika.
   e. W polu **Położenie instancji** wpisz położenie instancji serwera katalogów. Możesz również kliknąć przycisk **Przeglądaj** i określić katalog główny instancji. W podanym położeniu musi znajdować się przynajmniej 30 MB wolnego miejsca na dysku. W systemach Windows położeniem jest dysk, na przykład C:. Pliki instancji katalogu są zapisywane w katalogu \idsslapd-*nazwa_instancji* podanego dysku. Zmienna *nazwa_instancji* jest nazwą instancji serwera katalogów. W systemach AIX, Linux i Solaris domyślną instancją jest katalog osobisty właściciela instancji serwera katalogów, ale można podać inną ścieżkę.
   f. Kliknij przycisk **Dalej**.
5. Na panelu **Konfigurowanie instancji - krok 2** wykonaj następujące kroki:
   a. W polu **Nazwa DN administratora** podaj poprawną nazwę DN dla instancji docelowego serwera katalogów. W wartości nazwy DN administratora nie jest rozróżniana wielkość liter. Użytkownik o nazwie DN administratora ma pełne prawa dostępu do wszystkich danych w instancji serwera katalogów.
   b. W polu **Hasło** wpisz hasło dla nazwy DN administratora. W hasłach dokonuje się rozróżnienia wielkich i małych liter. Znaki zestawu znaków dwubajtowych (DBCS) w hasłach nie są poprawne.
   c. W polu **Potwierdź hasło** wpisz hasło dla nazwy DN administratora. Hasło zależy zapamiętać na przyszłość.
   d. Aby skopiować dane z bazy danych serwera źródłowego na serwer docelowy, wybierz opcję **Kopiuj dane z instancji źródłowej do nowej** i wykonaj następujące kroki:

      **Uwaga:** Jeśli wybrano utworzenie docelowego serwera katalogów jako instancji równorzędnej lub repliki, to pole wyboru jest zaznaczone i nie można usunąć tego zaznaczenia.

      1) W polu **Ścieżka obrazów kopii zapasowej** wpisz nazwę ścieżki obrazu kopii zapasowej serwera źródłowego. Aby określić położenie, możesz kliknąć przycisk **Przeglądaj**. Jeśli instancja źródłowa znajduje się na komputerze zdalnym, ścieżka kopii zapasowej musi być udostępniona do współużytkowania i dostępna zarówno z komputera źródłowego, jak i docelowego. Przykładowa ścieżka współużytkowana to system plików NFS do odczytu/zapisu.

e. Kliknij przycisk **Dalej**.

6. Na panelu **Sprawdź ustawienia** zweryfikuj wygenerowane podsumowanie.
7. Aby uruchomić tworzenie kopii źródłowych serwerów katalogów, kliknij przycisk **Zakończ**.
8. W oknie **Wyniki** sprawdź komunikaty dziennika wygenerowane dla operacji tworzenia instancji.
9. Aby zamknąć okno **Wyniki**, kliknij przycisk **Zamknij**.
10. Aby zamknąć program Instance Administration Tool, kliknij przycisk **Zamknij**.

### Wyniki

Program Instance Administration Tool utworzy kopię instancji źródłowego serwera katalogów na komputerze.

### Co dalej

Należy uruchomić proces ibmslapd oraz serwer administracyjny powiązany z instancją serwera katalogów. Patrz sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego” na stronie 156.

Należy utworzyć kopię zapasową instancji. Informacje na temat tworzenia kopii zapasowej instancji serwera katalogów zawiera sekcja “Tworzenie kopii zapasowej serwera katalogów” na stronie 187.

## Tworzenie kopii istniejącej instancji za pomocą programu narzędziowego dla wiersza komend

Do utworzenia kopii instancji można użyć programu narzędziowego dla wiersza komend **idsideploy**.

### Zanim rozpoczniesz

Aby utworzyć kopię istniejącej instancji, należy spełnić następujące wymagania:

- Uruchom proces ibmslapd i serwer administracyjny instancji źródłowej w trybie normalnym. Patrz sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzi dla wiersza komend” na stronie 157.
- Upewnij się, że źródłowy serwer katalogów jest dostępny z komputera, na którym ma zostać utworzona kopia instancji.

### Procedura

1. Zaloguj się jako użytkownik root w systemach AIX, Linux lub Solaris i jako członek grupy administratorów w systemie Windows.
2. Zmień bieżący katalog roboczy na podkatalog sbin w miejscu instalacji produktu IBM Security Directory Server.
3. Aby utworzyć kopię instancji bez danych na podstawie istniejącej instancji serwera katalogów, uruchom następującą komendę:

```
idsideploy -sU
ldap://host:port -sD
nazwaDN_admin_źródł -sw
hasło_admin_źródł
-e klucz_początkowy_szyfrowania -I
nazwa_instancji
```

```
-a hasło_inst -D
nazwa_DN_admin
-w hasło_admin -l
położenie_inst
```

Więcej informacji na temat komendy **idsideploy** zawiera publikacja *Skorowidz komend*.

# Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego

Aby korzystać z instancji serwera katalogów, należy uruchomić proces ibmslapd oraz serwer administracyjny powiązany z instancją.

Po zmodyfikowaniu konfiguracji serwera katalogów, może być konieczne zatrzymanie i uruchomienie serwera i serwera administracyjnego, aby zastosować zmiany. Można zatrzymać serwer i serwer administracyjny, tylko jeśli działają one w trybie normalnym lub w trybie konfiguracji.

Można uruchomić i zatrzymać serwery za pomocą narzędzia Instance Administration Server lub programów narzędziowych serwera, takich jak **ibmslapd** i **ibmdiradm**. Proces ibmslapd jest powiązany z serwerem katalogów. Za pomocą narzędzia Instance Administration Tool można uruchomić instancję serwera katalogów tylko w trybie normalnym. Aby uruchomić serwer katalogów w trybie tylko konfiguracji, należy użyć opcji w wierszu komend.

Serwer katalogów może przyjąć jeden z następujących stanów:

- Uruchomiony
- Zatrzymany
- Uruchomiony (tylko konfiguracja)

Serwer administracyjny może przyjąć jeden z następujących stanów:

- Uruchomiony
- Zatrzymany

# Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego

Użyj narzędzia Instance Administration Tool, aby uruchomić lub zatrzymać serwer katalogów, serwer administracyjny, lub oba te serwery powiązane z instancją.

## Zanim rozpoczniesz

Aby uruchomić lub zatrzymać serwer katalogów i serwer administracyjny instancji, należy spełnić następujące warunki:

1. Musi istnieć instancja o takiej samej wersji narzędzia Instance Administration Tool.
2. Jeśli instancja nie istnieje, utwórz instancję. Patrz sekcja “Tworzenie instancji serwera katalogów” na stronie 134 lub “Tworzenie instancji serwera katalogów z ustawieniami niestandardowymi” na stronie 136.

## Procedura

1. Uruchom program Instance Administration Tool. Patrz sekcja “Uruchamianie narzędzia Instance Administration Tool” na stronie 131.
2. Z listy **Lista instancji serwera katalogów zainstalowanych w systemie** wybierz instancję o takiej samej wersji narzędzia Instance Administration Tool.

3. Aby uruchomić lub zatrzymać serwer katalogów, serwer administracyjny lub oba, kliknij przycisk **Uruchom/zatrzymaj**.
4. W oknie **Zarządzanie stanem serwera** wykonaj następujące czynności:
   - Aby uruchomić serwer katalogów, serwer administracyjny lub obie instancje, wykonaj następujące kroki:
     – Aby uruchomić serwer katalogów, kliknij opcję **Uruchom serwer**.
     – Aby uruchomić serwer administracyjny, kliknij opcję **Uruchom serwer administracyjny**.
     – Kliknij przycisk **OK**.
   - Aby zatrzymać serwer katalogów, serwer administracyjny lub obie instancje, wykonaj następujące kroki:
     – Aby zatrzymać serwer katalogów, kliknij opcję **Zatrzymaj serwer**.
     – Aby zatrzymać serwer administracyjny, kliknij opcję **Zatrzymaj serwer administracyjny**.
     – Kliknij przycisk **OK**.
5. Aby zamknąć okno **Zarządzaj stanem serwera**, kliknij przycisk **Zamknij**.
6. Aby zamknąć program Instance Administration Tool, kliknij przycisk **Zamknij**.

## Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzi dla wiersza komend

Za pomocą narzędzi dla wiersza komend można uruchomić lub zatrzymać serwer katalogów, serwer administracyjny, lub oba te serwery powiązane z instancją.

### Zanim rozpoczniesz

Aby uruchomić lub zatrzymać serwer katalogów i serwer administracyjny instancji, należy spełnić następujące warunki:

- Musi istnieć instancja o tej samej wersji programów narzędziowych dla wiersza komend. Jeśli instancja nie istnieje, utwórz instancję. Patrz sekcja “Tworzenie instancji serwera katalogów” na stronie 134 lub “Tworzenie instancji serwera katalogów z ustawieniami niestandardowymi” na stronie 136.

### Procedura

1. Zaloguj się do komputera z wymaganymi uprawnieniami. Informacje na ten temat zawiera sekcja Rozdział 20, “Konfigurowanie instancji”, na stronie 167.
2. Otwórz wiersz komend.
3. Zmień bieżący katalog roboczy na podkatalog sbin w miejscu instalacji produktu IBM Security Directory Server.
4. Aby uruchomić serwer i serwer administracyjny instancji o nazwie *nazwa_instancji*, uruchom następujące komendy: Zastąp zmienną nazwa_instancji nazwą instancji.

   ```
   ibmslapd -I nazwa_instancji
   ibmdiradm -I nazwa_instancji
   ```

5. Aby zatrzymać serwer i serwer administracyjny instancji, uruchom następujące komendy: Zastąp zmienną nazwa_instancji nazwą instancji.

   ```
   ibmslapd -I nazwa_instancji
   ibmdiradm -I nazwa_instancji -k
   ```

# Modyfikowanie konfiguracji instancji serwera katalogów

Narzędzie konfiguracyjne służy do sprawdzania statusu, zarządzania i modyfikowania konfiguracji instancji serwera katalogów lub serwera proxy.

Narzędzie konfiguracyjne pozwala zarządzać i zmodyfikować konfigurację instancji serwera katalogów lub serwera proxy w tej samej wersji. Nie można używać narzędzia konfiguracyjnego dostarczanego z wcześniejszą wersją produktu IBM Security Directory Server do zarządzania instancją serwera katalogów lub serwera proxy.

Narzędzie konfiguracyjne można uruchomić w następujący sposób:

- Za pomocą programu Instance Administration tool.
- Za pomocą komendy **idsxcfg** z podaniem jako parametru nazwy instancji.

Więcej informacji na temat narzędzia konfiguracyjnego zawiera sekcja Rozdział 20, “Konfigurowanie instancji”, na stronie 167.

## Otwieranie programu Configuration Tool z programu Instance Administration Tool

Otwórz okno Configuration Tool programu IBM Security Directory Server, aby zarządzać lub zmodyfikować konfigurację instancji serwera katalogów lub instancji serwera proxy.

### Zanim rozpoczniesz

Aby zarządzać instancją przy użyciu programu Configuration Tool, należy spełnić następujące warunki:

- Musi istnieć instancja o takiej samej wersji narzędzia Configuration Tool. Jeśli instancja nie istnieje, utwórz instancję. Patrz sekcja “Tworzenie instancji serwera katalogów” na stronie 134 lub “Tworzenie instancji serwera katalogów z ustawieniami niestandardowymi” na stronie 136.

### Procedura

1. Uruchom program Instance Administration Tool. Patrz sekcja “Uruchamianie narzędzia Instance Administration Tool” na stronie 131.
2. Z listy **Lista instancji serwera katalogów zainstalowanych w systemie** wybierz instancję o takiej samej wersji narzędzia Instance Administration Tool.
3. Aby zarządzać instancją przy użyciu programu Configuration Tool, kliknij opcję **Zarządzaj**. Zostanie otwarte okno programu Configuration Tool produktu IBM Security Directory Server dla instancji.
4. Aby zamknąć okno programu Configuration Tool, kliknij opcję **Plik > Wyjście**.
5. W oknie potwierdzenia narzędzia Configuration Tool kliknij opcję **Tak**.

# Modyfikowanie ustawień TCP/IP instancji

Do zmodyfikowania ustawień TCP/IP instancji serwera katalogów lub serwera proxy można użyć programu Instance Administration Tool lub komendy.

Wersje instancji i programu Instance Administration Tool muszą być takie same, aby można było zmodyfikować ustawienia TCP/IP instancji.

## Modyfikowanie ustawień TCP/IP instancji za pomocą narzędzia Instance Administration Tool

Za pomocą narzędzia Instance Administration Tool można zmodyfikować ustawienia TCP/IP dla istniejącej instancji.

## Zanim rozpoczniesz

Aby zmodyfikować ustawienia TCP/IP instancji za pomocą narzędzia Instance Administration Tool, należy spełnić następujące warunki:

1. Musi istnieć instancja o takiej samej wersji narzędzia Instance Administration Tool.
2. Zatrzymaj serwer katalogów i serwer administracyjny instancji. Patrz sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego” na stronie 156.

## Procedura

1. Uruchom program Instance Administration Tool. Patrz sekcja “Uruchamianie narzędzia Instance Administration Tool” na stronie 131.
2. Z listy **Lista instancji serwera katalogów zainstalowanych w systemie** wybierz instancję o takiej samej wersji narzędzia Instance Administration Tool.
3. Aby zmodyfikować ustawienia TCP/IP instancji, kliknij opcję **Edycja ustawień TCP/IP**. Dla instancji zostanie otwarte okno **Edycja ustawień TCP/IP**.
4. W oknie **Edycja ustawień TCP/IP** wybierz jedną z następujących opcji:
   - Jeśli instancja ma nasłuchiwać na wszystkich skonfigurowanych adresach IP komputera, wybierz opcję **Nasłuchuj na wszystkich skonfigurowanych adresach IP**.
   - Jeśli instancja ma nasłuchiwać na określonym zbiorze adresów IP skonfigurowanych na komputerze, wykonaj następujące kroki:
     a. Usuń zaznaczenie opcji **Nasłuchuj na wszystkich skonfigurowanych adresach IP**.
     b. Z listy **Wybierz konkretne adresy IP, na których należy nasłuchiwać** wybierz adres lub adresy IP, na których ma nasłuchiwać instancja.
5. Kliknij przycisk **Dalej**.
6. Na panelu **Szczegóły dotyczące portu** podaj następujące wartości:

   **Uwaga:** Należy przypisać unikalne numery portów do portów serwera katalogów i nie można powodować konfliktów z istniejącymi portami używanymi na komputerze. W systemach AIX, Linux i Solaris numery portów z zakresu od 1 do 1000 mogą być używane tylko przez użytkownika root.

   a. W polu **Port serwera** wprowadź numer portu, którego serwer ma używać jako swojego portu niezabezpieczonego. Numer ten musi się mieścić w zakresie od 1 do 65535.
   b. W polu **Chroniony port serwera** wpisz numer portu, którego serwer ma używać jako swojego portu chronionego. Numer ten musi się mieścić w zakresie od 1 do 65535.
   c. W polu **Port serwera administracyjnego** wpisz numer portu, którego serwer administracyjny ma używać jako swojego portu niezabezpieczonego. Numer ten musi się mieścić w zakresie od 1 do 65535.
   d. W polu **Chroniony port serwera administracyjnego** wpisz numer portu, którego serwer administracyjny ma używać jako swojego portu chronionego. Numer ten musi się mieścić w zakresie od 1 do 65535.
   e. Kliknij przycisk **Zakończ**.
7. W oknie **Rezultaty edycji TCP/IP** zweryfikuj komunikaty dziennika wygenerowane dla operacji edycji ustawień TCP/IP.
8. Aby zamknąć okno **Rezultaty edycji TCP/IP**, kliknij przycisk **Zamknij**.
9. Aby zamknąć program Instance Administration Tool, kliknij przycisk **Zamknij**.

# Modyfikowanie ustawień TCP/IP instancji za pomocą programów narzędziowych wiersza komend

Za pomocą komend **idssethost** i **idssetport** można zmodyfikować ustawienia TCP/IP oraz portów dla istniejącej instancji.

## Zanim rozpoczniesz

Aby zmodyfikować ustawienia TCP/IP instancji za pomocą programów narzędziowych wiersza komend, należy spełnić następujące warunki:

1. Musi istnieć instancja o tej samej wersji programów narzędziowych dla wiersza komend.
2. Zatrzymaj serwer katalogów i serwer administracyjny instancji. Patrz sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzi dla wiersza komend” na stronie 157.

## Procedura

1. Zaloguj się jako użytkownik root w systemach AIX, Linux lub Solaris i jako członek grupy administratorów w systemie Windows.
2. Zmień bieżący katalog roboczy na podkatalog sbin w miejscu instalacji produktu IBM Security Directory Server.
3. Aby zaktualizować adresy IP serwera katalogów *nazwa_instancji*, wybierz jedną z następujących opcji: Zastąp zmienną *nazwa_instancji* nazwą instancji.

| **Adres IP do powiązania** | **Komenda do uruchomienia:** |
|---|---|
| **Konkretny adres IP (xx.xx.xx.xx) na komputerze** | idssethost -l *nazwa_instancji* -i xx.xx.xx.xx |
| **Wszystkie adresy IP skonfigurowane na komputerze** | idssethost -l *nazwa_instancji* -i all |

4. Aby zaktualizować numery portów serwera katalogów *nazwa_instancji*, uruchom następującą komendę: Zastąp zmienną *nazwa_instancji* nazwą instancji.

   **Uwaga:** Należy przypisać unikalne numery portów do portów serwera katalogów i nie można powodować konfliktów z istniejącymi portami używanymi na komputerze. W systemach AIX, Linux i Solaris numery portów z zakresu od 1 do 1000 mogą być używane tylko przez użytkownika root.

| **Porty do skonfigurowania** | **Komenda do uruchomienia:** |
|---|---|
| **Port serwera** | idssetport -l *nazwa_instancji* -p *numer_portu* |
| **Chroniony port serwera** | idssetport -l *nazwa_instancji* -s *port_chroniony* |
| **Port serwera administracyjnego** | idssetport -l *nazwa_instancji* -a *port_adm* |
| **Chroniony port serwera administracyjnego** | idssetport -l *nazwa_instancji* -c *port_chroniony_adm* |

   Więcej informacji na temat komend **idssethost** i **idssetport** zawiera *Skorowidz komend*.
5. Uruchom serwer katalogów i serwer administracyjny. Patrz sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzi dla wiersza komend” na stronie 157.

# Wyświetlanie informacji o instancji

Za pomocą narzędzia Instance Administration Tool lub programu narzędziowego dla wiersza komend można wyświetlić szczegóły instancji, takie jak katalog główny instancji, adresy IP i porty.

Można wyświetlić informacje na temat wszystkich istniejących instancji na komputerze. Instancja może mieć status zatrzymana lub uruchomiona.

Komenda **idsilist** również podaje podobne informacje dla instancji znajdujących się na komputerze. Więcej informacji na temat komendy **idsilist** zawiera *Skorowidz komend*.

## Wyświetlanie informacji o instancji za pomocą narzędzia Instance Administration Tool

Za pomocą narzędzia Instance Administration Tool można wyświetlić szczegółowe informacje o istniejącej instancji.

### Procedura

1. Uruchom program Instance Administration Tool. Patrz sekcja “Uruchamianie narzędzia Instance Administration Tool” na stronie 131.
2. Z listy **Lista instancji serwera katalogów zainstalowanych w systemie** wybierz instancję, dla której chcesz wyświetlić szczegółowe informacje.
3. Kliknij opcję **Wyświetl**. Okno **Widok szczegółów instancji** zawiera ogólne i szczegółowe informacje na temat protokołu TCP/IP dla wybranej instancji.
4. Aby zamknąć okno **Widok szczegółów instancji**, kliknij przycisk **Zamknij**.
5. Aby zamknąć program Instance Administration Tool, kliknij przycisk **Zamknij**.

## Wyświetlanie informacji o instancji za pomocą programu narzędziowego dla wiersza komend

Komenda **idsilist** służy do wyświetlania informacji na temat istniejącej instancji.

### Procedura

1. Zaloguj się jako użytkownik root w systemach AIX, Linux lub Solaris i jako członek grupy administratorów w systemie Windows.
2. Zmień bieżący katalog roboczy na podkatalog sbin w miejscu instalacji produktu IBM Security Directory Server.
3. Aby wyświetlić informacje na temat instancji zainstalowanej na komputerze, uruchom odpowiednią komendę **idsilist**:

| Zadania do wykonania | Komenda do uruchomienia: |
|---|---|
| **Lista wszystkich instancji** | idsilist |
| **Lista wszystkich instancji z pełnymi informacjami i opisem** | idsilist -a |
| **Lista wszystkich instancji z pełnymi informacjami w formacie surowym** | idsilist -r |
| **Lista dla konkretnej instancji** | idsilist -l *nazwa_instancji* |
| **Lista dla konkretnej instancji z pełnymi informacjami i opisem** | idsilist -l *nazwa_instancji* -a |
| **Lista dla konkretnej instancji z pełnymi informacjami w formacie surowym** | idsilist -l *nazwa_instancji* -r |

Więcej informacji na temat komendy **idsilist** zawiera *Skorowidz komend*.

# Usuwanie instancji serwera katalogów

Do usunięcia instancji serwera proxy lub serwera katalogów można użyć programu Instance Administration Tool albo programu narzędziowego uruchamianego w wierszu komend.

Usunięcie instancji z serwera może być niezbędne, gdy instancja jest migrowana na inny komputer albo gdy nie jest już potrzebna.

W przypadku usuwania serwera katalogów z bazą danych DB2, przed usunięciem instancji zaleca się utworzenie kopii zapasowej. W przypadku usuwania instancji serwera proxy, przed usunięciem instancji zaleca się utworzenie kopii zapasowej.

**Uwaga:** Dla instancji serwera proxy usunięcie instancji jest jedyną poprawną opcją.

W programie Instance Administration Tool dostępne są następujące opcje:

- Usunięcie instancji serwera katalogów z zachowaniem instancji bazy danych
- Usunięcie instancji serwera katalogów wraz z instancją bazy danych

W komendzie **idsidrop** dostępne są następujące opcje:

- Usunięcie instancji serwera katalogów z zachowaniem instancji bazy danych
- Usunięcie instancji serwera katalogów wraz z instancją bazy danych
- Zdekonfigurowanie instancji serwera katalogów w instancji bazy danych DB2 i nieusuwanie instancji serwera katalogów

Więcej informacji na temat komendy **idsidrop** zawiera *Skorowidz komend*.

## Usuwanie instancji za pomocą narzędzia Instance Administration Tool

Za pomocą narzędzia Instance Administration Tool można usunąć instancję serwera katalogów lub instancję serwera proxy.

### Zanim rozpoczniesz

Aby zmodyfikować ustawienia TCP/IP instancji za pomocą narzędzia Instance Administration Tool, należy spełnić następujące warunki:

1. Musi istnieć instancja o takiej samej wersji narzędzia Instance Administration Tool.
2. Zatrzymaj serwer katalogów i serwer administracyjny instancji. Patrz sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego” na stronie 156.

### Procedura

1. Uruchom program Instance Administration Tool. Patrz sekcja “Uruchamianie narzędzia Instance Administration Tool” na stronie 131.
2. Z listy **Lista instancji serwera katalogów zainstalowanych w systemie** wybierz instancję o takiej samej wersji narzędzia Instance Administration Tool.
3. Aby rozpocząć operację usuwania, kliknij przycisk **Usuń**.
4. W oknie **Usuwanie instancji serwera katalogów** wykonaj następujące kroki:
   a. Wybierz jedną z następujących metod usuwania:
      - Aby usunąć instancję serwera katalogów bez usuwania powiązanej instancji bazy danych DB2, kliknij opcję **Usuń tylko instancję serwera katalogów**.

**Uwaga:** W przypadku instancji serwera proxy opcja **Usuń tylko instancję serwera katalogów** jest jedyną dostępną poprawną opcją.

- Aby usunąć instancję serwera katalogów z powiązaną instancją bazy danych DB2, kliknij opcję **Usuń instancję serwera katalogów i zniszcz związaną instancję bazy danych**.

b. Kliknij przycisk **Usuń**.

c. W oknie **Ostrzeżenie** kliknij przycisk **Tak**, aby potwierdzić usunięcie instancji.

d. W oknie **Informacje** kliknij przycisk **OK**.

e. Aby zamknąć okno **Usuwanie instancji serwera katalogów**, kliknij przycisk **Zamknij**.

f. Aby zamknąć program Instance Administration Tool, kliknij przycisk **Zamknij**.

# Usuwanie instancji za pomocą programu narzędziowego dla wiersza komend

Za pomocą komendy **idsidrop** można usunąć istniejącą instancję.

## Zanim rozpoczniesz

Aby usunąć instancję za pomocą programu narzędziowego dla wiersza komend, należy spełnić następujące warunki:

1. Musi istnieć instancja o tej samej wersji programu narzędziowego dla wiersza komend.
2. Zatrzymaj serwer katalogów i serwer administracyjny instancji. Patrz sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzi dla wiersza komend” na stronie 157.

## Procedura

1. Zaloguj się jako użytkownik root w systemach AIX, Linux lub Solaris i jako członek grupy administratorów w systemie Windows.
2. Zmień bieżący katalog roboczy na podkatalog sbin w miejscu instalacji produktu IBM Security Directory Server.
3. Aby usunąć instancję *nazwa_instancji*, wybierz jedną z następujących opcji: Zastąp zmienną *nazwa_instancji* nazwą instancji.

| Zadania do wykonania | Komenda do uruchomienia: |
|---|---|
| **Aby usunąć instancję serwera katalogów i zachować powiązaną instancję bazy danych** | `idsidrop -I nazwa_instancji` |
| **Aby usunąć instancję serwera katalogów i powiązaną instancję bazy danych** | `idsidrop -I nazwa_instancji -r` |
| **Aby zdekonfigurować powiązaną instancję bazy danych bez usuwania instancji serwera katalogów** | `idsidrop -I nazwa_instancji -R` |

Więcej informacji na temat komendy **idsidrop** zawiera publikacja *Skorowidz komend*.

# Rozdział 19. Weryfikowanie struktury katalogów

Po zainstalowaniu serwera IBM Security Directory Server należy sprawdzić strukturę katalogów.

## Systemy Windows w wersjach 32- i 64-bitowych

Po zainstalowaniu serwera IBM Security Directory Server w systemie operacyjnym Windows można wyświetlić następujące katalogi i pliki w miejscu instalacji, na przykład: C:\Program Files\IBM\LDAP\6.3.1 (można zmienić położenie instalacji)

appsrv
etc
java
lib
messages
bin
examples
javalib
lib64
nls
var
codeset
idstools
jre
license
properties
config
include
ldapcfg.ico
logs
sbin

## Systemy Linux w wersji 64-bitowej

Po zainstalowaniu serwera katalogów IBM Security w systemie operacyjnym Linux można wyświetlić następujące katalogi i pliki w miejscu instalacji, na przykład: /opt/ibm/ldap/V6.3.1 (nie można zmienić położenia instalacji)

bin
codeset
config
etc
examples
idstools
include
javalib
LAPID
lib
lib64
nls
properties

sbin
tmp
web

# Rozdział 20. Konfigurowanie instancji

Do skonfigurowania instancji serwera katalogów lub serwera proxy można użyć narzędzia konfiguracyjnego lub interfejsu wiersza komend.

Narzędzie konfiguracyjne (**idsxcfg**) produktu IBM Security Directory Server jest interfejsem graficznym (GUI), który umożliwia skonfigurowanie instancji. Narzędzie konfiguracyjne wymaga pakietu IBM Java Development Kit.

Aby uruchomić narzędzie konfiguracyjne, należy zalogować się z następującymi uprawnieniami:

**AIX, Linux lub Solaris**

- Użytkownik root
- Właściciel instancji serwera katalogów
- Użytkownik, który należy do podstawowej grupy właściciela instancji serwera katalogów

**Windows**

- Użytkownik, który należy do domyślnej grupy administratorów

Narzędzie konfiguracyjne pozwala też zmienić istniejącą konfigurację serwera katalogów.

Narzędzia konfiguracyjnego można użyć do wykonywania następujących zadań na pełnej instancji serwera katalogów:

- Uruchamianie i zatrzymywanie serwera
- Zarządzanie nazwą DN i hasłem podstawowego administratora
- Konfigurowanie i dekonfigurowanie bazy danych DB2 instancji serwera katalogów
- Optymalizowanie bazy danych powiązanej z instancją
- Konserwacja bazy danych DB2 wraz z organizowaniem indeksu lub kompresji wiersza
- Tworzenie i odtwarzanie kopii zapasowej bazy danych
- Strojenie wydajności instancji serwera katalogów
- Włączanie i wyłączanie dziennika zmian
- Dodawanie i usuwanie przyrostków
- Dodawanie i usuwanie plików schematu
- Importowanie lub eksportowanie danych LDIF
- Konfigurowanie synchronizacji z Active Directory

Narzędzia konfiguracyjnego można użyć do wykonywania następujących zadań na instancji serwera proxy:

- Uruchamianie i zatrzymywanie serwera
- Zarządzanie nazwą DN i hasłem podstawowego administratora
- Dodawanie i usuwanie przyrostków
- Dodawanie i usuwanie plików schematu
- Tworzenie i odtwarzanie kopii zapasowej instancji

# Uruchamianie programu Configuration Tool

Uruchom program Configuration Tool dla instancji serwera IBM Security Directory Server, aby skonfigurować ją dla używanego środowiska.

## Zanim rozpoczniesz

Aby zarządzać instancją przy użyciu programu Configuration Tool, należy spełnić następujące warunki:

- Musi istnieć instancja o takiej samej wersji narzędzia Configuration Tool. Jeśli instancja nie istnieje, utwórz instancję. Patrz sekcja “Tworzenie instancji serwera katalogów z ustawieniami niestandardowymi” na stronie 136 lub “Tworzenie instancji serwera proxy z własnymi ustawieniami” na stronie 142.
- Pakiet IBM Java Development Kit musi być umieszczony w ścieżce instalacji IBM Security Directory Server. Dla domyślnej ścieżki instalacji serwera IBM Security Directory Server, patrz sekcja “Domyślne położenia instalacji” na stronie 27.

## Procedura

1. Zaloguj się do systemu z wymaganymi uprawnieniami. Informacje na ten temat zawiera sekcja Rozdział 20, “Konfigurowanie instancji”, na stronie 167.
2. Otwórz wiersz komend.
3. Zmień bieżący katalog roboczy na podkatalog sbin w miejscu instalacji produktu IBM Security Directory Server.
4. Uruchom komendę **idsxcfg** w następującym formacie: Zastąp zmienną *nazwa_instancji* nazwą instancji.

   ```
   idsxcfg -I nazwa_instancji
   ```

   Zostanie otwarte okno programu Configuration Tool produktu IBM Security Directory Server dla podanej instancji.
5. Aby zamknąć okno programu Configuration Tool, kliknij opcje **Plik > Wyjście**.
6. W oknie potwierdzenia narzędzia Configuration Tool kliknij opcję **Tak**.

# Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzia Configuration Tool

Za pomocą narzędzia Configuration Tool można uruchomić proces ibmslapd oraz serwer administracyjny powiązany z instancją.

Po zmodyfikowaniu konfiguracji serwera katalogów, może być konieczne zatrzymanie i uruchomienie serwera i serwera administracyjnego, aby zastosować zmiany. Można zatrzymać serwer i serwer administracyjny, tylko jeśli działają one w trybie normalnym lub w trybie konfiguracji.

Za pomocą narzędzia Configuration Tool lub programów narzędziowych serwera (na przykład **ibmslapd** i **ibmdiradm**) można uruchomić lub zatrzymać serwer i serwer administracyjny. Proces ibmslapd jest powiązany z serwerem katalogów. Za pomocą narzędzia Configuration Tool można uruchomić instancję serwera katalogów tylko w trybie normalnym. Aby uruchomić serwer katalogów w trybie tylko konfiguracji, należy użyć opcji w wierszu komend.

Serwer katalogów może przyjąć jeden z następujących stanów:

- Uruchomiony
- Zatrzymany

- Uruchomiony (tylko konfiguracja)

Serwer administracyjny może przyjąć jeden z następujących stanów:

- Uruchomiony
- Zatrzymany

## Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzia Configuration Tool

Użyj narzędzia Configuration Tool, aby uruchomić lub zatrzymać serwer katalogów, serwer administracyjny, lub oba te serwery powiązane z instancją.

### Procedura

1. Uruchom narzędzie Configuration Tool dla instancji. Patrz sekcja “Uruchamianie programu Configuration Tool” na stronie 168.
2. Na liście zadań znajdującej się w panelu nawigacyjnym po lewej stronie kliknij opcję **Zarządzanie hasłem administratora**.
3. Na stronie **Bieżący stan** sprawdź bieżący stan serwera i serwera administracyjnego.
4. Na stronie **Bieżący stan** wykonaj następujące czynności:
   - Aby uruchomić serwer katalogów, serwer administracyjny lub obie instancje, wykonaj następujące kroki:
     - Aby uruchomić serwer katalogów, kliknij opcję **Uruchom serwer**.
     - Aby uruchomić serwer administracyjny, kliknij opcję **Uruchom serwer administracyjny**.
     - W oknie **Informacje** kliknij przycisk **OK**.
   - Aby zatrzymać serwer katalogów, serwer administracyjny lub obie instancje, wykonaj następujące kroki:
     - Aby zatrzymać serwer katalogów, kliknij opcję **Zatrzymaj serwer**.
     - Aby zatrzymać serwer administracyjny, kliknij opcję **Zatrzymaj serwer administracyjny**.
     - W oknie **Informacje** kliknij przycisk **OK**.
5. Aby zamknąć stronę **Bieżący stan**, kliknij przycisk **Zamknij**.
6. Aby zamknąć okno programu Configuration Tool, kliknij opcje **Plik > Wyjście**.
7. W oknie potwierdzenia narzędzia Configuration Tool kliknij opcję **Tak**.

## Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzi dla wiersza komend

Za pomocą narzędzi dla wiersza komend można uruchomić lub zatrzymać serwer katalogów, serwer administracyjny, lub oba te serwery powiązane z instancją.

### Zanim rozpoczniesz

Aby uruchomić lub zatrzymać serwer katalogów i serwer administracyjny instancji, należy spełnić następujące warunki:

- Musi istnieć instancja o tej samej wersji programów narzędziowych dla wiersza komend. Jeśli instancja nie istnieje, utwórz instancję. Patrz sekcja “Tworzenie instancji serwera katalogów” na stronie 134 lub “Tworzenie instancji serwera katalogów z ustawieniami niestandardowymi” na stronie 136.

### Procedura

1. Zaloguj się do komputera z wymaganymi uprawnieniami. Informacje na ten temat zawiera sekcja Rozdział 20, “Konfigurowanie instancji”, na stronie 167.
2. Otwórz wiersz komend.
3. Zmień bieżący katalog roboczy na podkatalog sbin w miejscu instalacji produktu IBM Security Directory Server.
4. Aby uruchomić serwer i serwer administracyjny instancji o nazwie *nazwa_instancji*, uruchom następujące komendy: Zastąp zmienną nazwa_instancji nazwą instancji.

   ```
   ibmslapd -I nazwa_instancji
   ibmdiradm -I nazwa_instancji
   ```

5. Aby zatrzymać serwer i serwer administracyjny instancji, uruchom następujące komendy: Zastąp zmienną nazwa_instancji nazwą instancji.

   ```
   ibmslapd -I nazwa_instancji
   ibmdiradm -I nazwa_instancji -k
   ```

## Zarządzanie nazwą wyróżniającą podstawowego administratora instancji

Do uzyskania dostępu do konfiguracji i wszystkich danych w instancji katalogu, należy utworzyć i skonfigurować nazwę wyróżniającą (DN) podstawowego administratora instancji.

Nazwa wyróżniająca (DN) administratora jest nazwą wyróżniającą używaną przez podstawowego administratora instancji. W instancji można utworzyć tylko jednego podstawowego administratora.

Domyślną nazwą DN jest cn=root. W wartości nie jest rozróżniana wielkość liter.

Nazwa DN zawiera pary atrybut:wartość oddzielone przecinkami. Poniżej zamieszczono przykład wartości DN.

```
cn=Jan Nowak,ou=kontrola,o=test
```

Do ustawienia lub zmiany nazwy wyróżniającej administratora podstawowego można użyć narzędzia konfiguracyjnego lub komendy **idsdnpw**. Aby ustawić lub zmienić nazwę wyróżniającą podstawowego administratora, należy zatrzymać proces ibmslapd powiązany z instancją.

## Zarządzanie nazwą DN podstawowego administratora za pomocą programu Configuration Tool

Program Configuration Tool umożliwia skonfigurowanie nazwy DN podstawowego administratora instancji.

### Zanim rozpoczniesz

Aby skonfigurować nazwę DN podstawowego administratora dla instancji, należy spełnić następujące wymagania:

- Zatrzymaj serwer katalogów. Patrz sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzia Configuration Tool” na stronie 169.

### Procedura

1. Uruchom narzędzie Configuration Tool dla instancji. Patrz sekcja “Uruchamianie programu Configuration Tool” na stronie 168.

2. Na liście zadań znajdującej się w panelu nawigacyjnym po lewej stronie kliknij opcję **Zarządzanie nazwą DN administratora**.
3. W polu **Nazwa DN administratora** wprowadź nazwę DN podstawowego administratora lub zaakceptuj domyślną nazwę DN, cn=root.
4. Kliknij przycisk **OK**.
5. Aby potwierdzić działanie, kliknij przycisk **OK**.
6. Aby zamknąć okno programu Configuration Tool, kliknij opcje **Plik** > **Wyjście**.
7. Aby potwierdzić działanie, kliknij przycisk **Tak**.

### Co dalej

Uruchom serwer katalogów. Patrz sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzia Configuration Tool” na stronie 169.

## Zarządzanie nazwą DN podstawowego administratora za pomocą programu narzędziowego dla wiersza komend

Za pomocą programu narzędziowego dla wiersza komend **idsdnpw** można zarządzać nazwą DN podstawowego administratora instancji.

### Zanim rozpoczniesz

Aby skonfigurować nazwę DN podstawowego administratora dla instancji, należy spełnić następujące wymagania:

- Zatrzymaj serwer katalogów. Patrz sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzi dla wiersza komend” na stronie 157.

### O tym zadaniu

Jeśli nie zostanie podana wartość DN administratora, w pliku ibmslapd.conf dla instancji serwera katalogów zostanie ustawiona wartość domyślna cn=root. Konieczne jest podanie hasła podstawowego administratora instancji.

Jeśli nie zostanie podane hasło, komenda **idsdnpw** zapyta o hasło. Hasło nie jest wyświetlane w wierszu komend podczas wpisywania.

### Procedura

1. Zaloguj się jako właściciel instancji serwera katalogów.
2. Otwórz wiersz komend.
3. Zmień bieżący katalog roboczy na podkatalog sbin w miejscu instalacji produktu IBM Security Directory Server.
4. Aby ustawić nazwę DN administratora instancji, uruchom następującą komendę: Zastąp wartości nazwa_instancji, DN_administratora oraz hasło_administratora zgodnie z wymaganiami.

   ```
   idsdnpw -I nazwa_instancji -u
   DN_administratora -p
   hasło_administratora
   ```

   Więcej informacji na temat komendy **idsdnpw** zawiera publikacja *Skorowidz komend*.

### Co dalej

Uruchom serwer katalogów. Patrz sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzi dla wiersza komend” na stronie 157.

## Zarządzanie hasłem podstawowego administratora instancji

W celu uwierzytelniania w instancji i uzyskiwania dostępu do konfiguracji i danych katalogu, należy utworzyć i skonfigurować hasło podstawowego administratora instancji.

W haśle jest rozróżniana wielkość liter. Znaki dwubajtowego zestawu znaków (DBCS) nie są obsługiwane w hasłach. Hasło administratora należy zapisać w bezpiecznym miejscu w celu użycia w przyszłości.

Do ustawienia hasła podstawowego administratora można użyć narzędzia konfiguracyjnego lub komendy **idsdnpw**. Aby ustawić hasło administratora, należy zatrzymać proces ibmslapd powiązany z instancją.

Jeśli włączona jest strategia haseł administratora, hasło podstawowego administratora musi spełniać wymagania tej strategii. Więcej informacji na temat strategii haseł znajduje się w sekcji *Administrowanie* dokumentacji serwera IBM Security Directory Server.

### Zarządzanie hasłem podstawowego administratora za pomocą programu Configuration Tool

Program Configuration Tool umożliwia skonfigurowanie hasła dla podstawowego administratora instancji.

#### Zanim rozpoczniesz

Aby skonfigurować hasło dla podstawowego administratora instancji, należy spełnić następujące wymagania:

- Zatrzymaj serwer katalogów. Patrz sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzia Configuration Tool” na stronie 169.

#### Procedura

1. Uruchom narzędzie Configuration Tool dla instancji. Patrz sekcja “Uruchamianie programu Configuration Tool” na stronie 168.
2. Na liście zadań znajdującej się w panelu nawigacyjnym po lewej stronie kliknij opcję **Zarządzanie hasłem administratora**.
3. W polu **Hasło administratora** wpisz hasło podstawowego administratora.
4. W polu **Potwierdź hasło** wpisz hasło podstawowego administratora.
5. Kliknij przycisk **OK**.
6. Aby potwierdzić działanie, kliknij przycisk **OK**.
7. Aby zamknąć stronę **Zarządzanie hasłem administratora**, kliknij przycisk **OK**.
8. Aby zamknąć okno programu Configuration Tool, kliknij opcje **Plik > Wyjście**.
9. Aby potwierdzić działanie, kliknij przycisk **Tak**.

#### Co dalej

Uruchom serwer katalogów. Patrz sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzia Configuration Tool” na stronie 169.

## Zarządzanie hasłem podstawowego administratora za pomocą programu narzędziowego dla wiersza komend

Za pomocą programu narzędziowego dla wiersza komend **idsdnpw** można zarządzać hasłem podstawowego administratora instancji.

### Zanim rozpoczniesz

Aby skonfigurować hasło podstawowego administratora dla instancji, należy spełnić następujące wymagania:

- Zatrzymaj serwer katalogów. Patrz sekcja "Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzi dla wiersza komend" na stronie 157.

### Procedura

1. Zaloguj się jako właściciel instancji serwera katalogów.
2. Otwórz wiersz komend.
3. Zmień bieżący katalog roboczy na podkatalog sbin w miejscu instalacji produktu IBM Security Directory Server.
4. Aby ustawić hasło administratora instancji, uruchom następującą komendę: Zastąp wartości nazwa_instancji, DN_administratora oraz hasło_administratora zgodnie z wymaganiami.

   ```
   idsdnpw -I nazwa_instancji -u
   DN_administratora -p
   hasło_administratora
   ```

   Więcej informacji na temat komendy **idsdnpw** zawiera publikacja *Skorowidz komend*.

### Co dalej

Uruchom serwer katalogów. Patrz sekcja "Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzi dla wiersza komend" na stronie 157.

## Konfiguracja bazy danych dla instancji serwera katalogów

Aby użyć instancji do przechowywania danych serwera katalogów, należy skonfigurować bazę danych DB2 dla instancji.

Do utworzenia i skonfigurowania bazy danych DB2 można użyć narzędzia do administrowania instancją, narzędzia konfiguracyjnego lub komendy **idscfgdb**. Przed rozpoczęciem konfigurowania lub dekonfigurowania bazy danych należy zatrzymać serwer katalogów. Więcej informacji na temat komendy **idscfgdb** zawiera *Skorowidz komend*.

Jeśli wybrano opcję utworzenia domyślnej instancji za pomocą narzędzia do administrowania instancją, dodatkowo tworzona jest i konfigurowana instancja bazy danych DB2. Dla instancji serwera proxy nie jest wymagane skonfigurowanie bazy danych DB2.

Podczas konfigurowania bazy danych DB2 dla instancji plik konfiguracyjny instancji jest aktualizowany z użyciem informacji na temat bazy danych DB2. Program narzędziowy tworzy również bazę danych i lokalne ustawienia pętli zwrotnej.

Ustawienia dotyczące bazy danych i lokalnej pętli zwrotnej są tworzone, jeśli jeszcze nie istnieją. Można określić, czy baza danych ma zostać utworzona w lokalnej stronie kodowej, czy w stronie kodowej UTF-8 (jest to opcja domyślna).

# Konfigurowanie bazy danych dla instancji za pomocą narzędzia Configuration Tool

Narzędzie Configuration Tool umożliwia skonfigurowanie bazy danych DB2 dla instancji serwera katalogów.

## Zanim rozpoczniesz

Aby skonfigurować bazę danych DB2 dla instancji serwera katalogów, wykonaj następujące czynności:

- Zatrzymaj serwer katalogów. Patrz sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzia Configuration Tool” na stronie 169.
- Musi istnieć identyfikator użytkownika systemu będący właścicielem instancji bazy danych DB2. Więcej informacji na temat wymagań dotyczących identyfikatora użytkownika systemu zawiera sekcja “Użytkownicy i grupy powiązane z instancją serwera katalogów” na stronie 121.

## Procedura

1. Uruchom narzędzie Configuration Tool dla instancji. Patrz sekcja “Uruchamianie programu Configuration Tool” na stronie 168.
2. Na liście zadań znajdującej się na lewym panelu nawigacyjnym kliknij opcję **Zadania bazy danych > Konfigurowanie bazy danych**.
3. Na stronie **Konfigurowanie bazy danych** wybierz jedną z następujących opcji:
   - Aby skonfigurować bazę danych dla instancji, wykonaj następujące kroki:
     a. W polu **Nazwa użytkownika bazy danych** wpisz identyfikator użytkownika systemu, do którego musi należeć baza danych. Instancja serwera katalogów używa tego identyfikatora użytkownika systemu do łączenia się z bazą danych.
     b. W polu **Hasło** wpisz hasło administratora bazy danych.
     c. W polu **Nazwa bazy danych** wpisz nazwę bazy danych.
     d. Aby ustawić dowolne z następujących ustawień konfiguracji DB2, wybierz opcję **Pokaż zaawansowane opcje obszaru tabel**.
        – Baza danych ma używać przechowywania danych SMS (System Managed Storage) dla obszarów tabel DB2. Gdy jest używany typ SMS, menedżer systemu plików systemu operacyjnego przydziela obszar tabel, w którym są przechowywane tabele DB2, oraz zarządza tym obszarem tabel.
        – Baza danych ma używać przechowywania danych DMS (Database Managed Storage) dla obszarów tabel DB2. Ponadto baza danych ma zostać skonfigurowana dla obszarów tabel USERSPACE1 i LDAPSPACE, wielkości i położenia. Gdy używany jest typ DMS, obszarami tabel zarządza menedżer bazy danych. O tym, które urządzenia i pliki będą używane, decyduje administrator bazy danych, a obszarami w tych urządzeniach i plikach zarządza DB2.

        Jeśli nie wybrano opcji **Pokaż zaawansowane opcje obszaru tabel**, baza danych DB2 z obszarami tabel USERSPACE1 i LDAPSPACE jest tworzona z użyciem typu DMS z domyślnymi wielkościami i położeniami. Jeśli instancja jest konfigurowana z istniejącą bazą danych, opcja **Pokaż zaawansowane opcje obszaru tabel** zostaje wyłączona po wprowadzeniu nazwy istniejącej bazy danych w polu **Nazwa bazy danych**.
     e. Kliknij przycisk **Dalej**.
   - Aby ponownie skonfigurować hasło administratora bazy danych, wykonaj następujące kroki:

a. Kliknij przycisk **Resetuj hasło**.
b. W polu **Hasło** wpisz hasło administratora bazy danych.
c. W polu **Potwierdź hasło** wpisz hasło administratora bazy danych.
d. Kliknij przycisk **Dalej**.

4. Aby utworzyć i skonfigurować bazę danych DB2, wykonaj następujące kroki:
   a. W polu **Położenie instalacji bazy danych** wpisz ścieżkę położenia bazy danych. Aby określić katalog, możesz kliknąć przycisk **Przeglądaj**. W systemie Windows należy podać położenie dysku, na przykład C:. W systemach AIX, Linux i Solaris położeniem musi być nazwa katalogu, na przykład /home/ldapdb.

      **Uwaga:** Minimalne wymagane miejsce na dysku dla bazy danych typu DMS wynosi 1 GB. W przypadku bazy danych typu SMS minimalne wymagane miejsce na dysku wynosi 150 MB. Wymagania te dotyczą pustej bazy danych. Gdy w bazie danych przechowywane są dane, wymagana jest większa ilość miejsca na dysku.
   b. Aby skonfigurować serwer katalogów z bazą danych dla tworzenia kopii zapasowej otwartej bazy danych, wykonaj następujące kroki:
      1) Wybierz opcję **Konfiguruj tworzenie kopii zapasowej otwartej bazy danych**.
      2) W polu **Położenie kopii zapasowej bazy danych** wprowadź położenie, w którym ma zostać zapisany obraz kopii zapasowej. Aby określić położenie, możesz kliknąć przycisk **Przeglądaj**.

      **Uwaga:** Nie należy wychodzić z narzędzia Configuration Tool ani anulować uruchomionej operacji tworzenia kopii zapasowej.
      Jeśli baza danych jest konfigurowana do tworzenia kopii zapasowej otwartej bazy danych po zakończeniu konfiguracji bazy danych, uruchamiane jest tworzenie początkowej kopii zapasowej z zamkniętą bazą danych. Po zakończeniu operacji tworzenia kopii zapasowej z zamkniętą bazą danych serwer administracyjny jest restartowany. Można również skonfigurować utworzenie kopii zapasowej otwartej bazy danych dla instancji serwera katalogów za pomocą komendy **idscfgdb**. Nie można jednak zdekonfigurować tworzenia kopii zapasowej otwartej bazy danych, używając komendy **idscfgdb** i parametru **-c**. Jeśli zostanie skonfigurowane tworzenie kopii zapasowej otwartej bazy danych dla instancji za pomocą narzędzia Instance Administration Tool lub Configuration Tool, dekonfigurację można przeprowadzić za pomocą narzędzia Configuration Tool lub komendy **idscfgdb**.
   c. W obszarze **Opcja zestawu znaków** wybierz jedną z następujących opcji, aby utworzyć typ bazy danych:

      **Uwaga:** Utwórz uniwersalną bazę danych DB2, jeśli masz zamiar zapisywać na serwerze katalogów dane w wielu językach. Poza tym uniwersalna baza danych DB2 jest bardziej wydajna, ponieważ wymagana jest mniejsza liczba operacji tłumaczenia danych. Aby można było używać znaczników języków, baza danych musi być w formacie UTF-8. “Obsługa standardu UTF-8” na stronie 125 zawiera więcej informacji na temat standardu UTF-8.
      - Aby utworzyć bazę danych UTF-8 (UCS Transformation Format), w której klienci LDAP będą mogli przechowywać dane znakowe UTF-8, kliknij opcję **Utwórz uniwersalną bazę danych DB2**.
      - Aby utworzyć bazę danych w lokalnej stronie kodowej, kliknij opcję **Utwórz bazę danych DB2 w lokalnej stronie kodowej**.
   d. Kliknij przycisk **Dalej**.

5. Jeśli została wybrana opcja **Pokaż zaawansowane opcje obszaru tabel**, musisz wykonać następujące kroki:

a. Z listy **Wybierz typ obszaru tabel bazy danych** wybierz typ bazy danych. Typ DMS obszaru tabel bazy danych jest domyślny. Jeśli zostanie wybrany typ SMS obszaru tabel bazy danych, wszystkie pozostałe pola zostaną wyłączone. Obsługa obszaru tabel DMS jest używana tylko dla obszarów tabel USERSPACE1 oraz LDAPSPACE. Wszystkie pozostałe obszary tabel, takie jak obszar tabel katalogu i tymczasowy obszar tabel są typu SMS.

a. W obszarze **Szczegóły obszaru tabel USERSPACE1** podaj następujące szczegóły:

1) Z listy **Kontener obszaru tabel** wybierz typ kontenera. Aby obszar tabel USERSPACE1 znajdował się w systemie plików, wybierz opcję **Plik**. Jeśli położeniem kontenera obszaru tabel bazy danych jest system plików, zostanie utworzony przygotowany obszar tabel DMS. Można podać początkową wielkość obszaru tabel i wielkość jednostki rozszerzania, a obszar tabel zostanie automatycznie rozszerzony w razie potrzeby. Aby utworzyć obszar tabel USERSPACE1 na urządzeniu surowym, wybierz opcję **Urządzenie surowe**. Urządzenie surowe to urządzenie, w którym nie zainstalowano żadnego systemu plików, takie jak dysk twardy bez żadnego systemu plików. Jeśli położeniem kontenera obszaru tabel bazy danych jest urządzenie surowe, zostanie utworzony surowy obszar tabel DMS. W takiej sytuacji wielkość kontenera obszaru tabel bazy danych jest stała i obszaru tego nie można zwiększać. Jeśli zostanie wybrana opcja **Urządzenie surowe**, należy podać wielkość razem z położeniem kontenera, a nie zaakceptować wartości domyślne.

2) Jeśli wybrano opcję **Plik** na liście **Kontener obszaru tabel**, należy podać następujące szczegóły:

a) W polu **Ścieżka katalogu** podaj ścieżkę katalogu, w którym ma zostać utworzony obszar tabel USERSPACE1. Aby wybrać katalog, możesz kliknąć przycisk **Przeglądaj**.

b) W polu **Nazwa pliku** wprowadź nazwę pliku obszaru katalogu do utworzenia lub zaakceptuj domyślną nazwę pliku USPACE.

c) W polu **Wielkość początkowa** wprowadź wielkość początkową obszaru tabel USERSPACE1 w stronach lub zaakceptuj wartość domyślną. W przypadku kontenera obszaru tabel typu **Plik** kontener obszaru tabel USERSPACE1 ma typ automatycznego przyrostu. W polu **Wielkość początkowa** można podać wielkość początkową, a w polu **Wielkość rozszerzania** wielkość jednostki rozszerzania. Wartość domyślna wielkości początkowej wynosi 16 k, a domyślna wielkość jednostki rozszerzania wynosi 8 k. Wielkość strony dla kontenera obszaru tabel USERSPACE1 wynosi 4 kB na stronę.

3) Jeśli wybrano opcję **Urządzenie surowe** na liście **Kontener obszaru tabel**, należy podać następujące szczegóły:

a) W polu **Ścieżka urządzenia** wpisz położenie urządzenia surowego. W systemie Windows ścieżka musi rozpoczynać się od \\.\. Przykładowa ścieżka z nazwą urządzenia \\.*nazwa_urządzenia*. W systemach AIX, Linux i Solaris ścieżką urządzenia musi być poprawna ścieżka.

b) W polu **Wielkość początkowa** wprowadź wielkość początkową obszaru tabel USERSPACE1 lub zaakceptuj wartość domyślną. Dla kontenera obszaru tabel typu **Urządzenie surowe** wielkość kontenera obszaru tabel USERSPACE1 jest stała. Wielkość domyślna wynosi 16 k. Aby uzyskać lepsze wyniki, należy podać odpowiednią wielkość.

b. W obszarze **Szczegóły obszaru tabel LDAPSPACE** podaj następujące szczegóły:

1) Z listy **Kontener obszaru tabel** wybierz typ kontenera. Aby obszar tabel LDAPSPACE znajdował się w systemie plików, wybierz opcję **Plik**. Aby utworzyć obszar tabel LDAPSPACE na urządzeniu surowym, wybierz opcję

**Urządzenie surowe**. Urządzenie surowe to urządzenie, w którym nie zainstalowano żadnego systemu plików, takie jak dysk twardy bez żadnego systemu plików.

2) Jeśli wybrano opcję **Plik** na liście **Kontener obszaru tabel**, należy podać następujące szczegóły:
   a) W polu **Ścieżka katalogu** podaj ścieżkę katalogu, w którym ma zostać utworzony obszar tabel LDAPSPACE. Aby wybrać katalog, możesz kliknąć przycisk **Przeglądaj**.
   b) W polu **Nazwa pliku** wprowadź nazwę pliku obszaru katalogu do utworzenia lub zaakceptuj domyślną nazwę pliku ldapspace.
   c) W polu **Wielkość początkowa** wprowadź wielkość początkową obszaru tabel LDAPSPACE w stronach lub zaakceptuj wartość domyślną. W przypadku kontenera obszaru tabel typu **Plik** kontener obszaru tabel LDAPSPACE ma typ automatycznego przyrostu. W polu **Wielkość początkowa** można podać wielkość początkową, a w polu **Wielkość rozszerzania** wielkość jednostki rozszerzania. Wartość domyślna wielkości początkowej wynosi 16 k, a domyślna wielkość jednostki rozszerzania wynosi 8 k. Wielkość strony dla kontenera obszaru tabel LDAPSPACE wynosi 32 kB na stronę.
3) Jeśli wybrano opcję **Urządzenie surowe** na liście **Kontener obszaru tabel**, należy podać następujące szczegóły:
   a) W polu **Ścieżka urządzenia** wpisz położenie urządzenia surowego. W systemie Windows ścieżka musi rozpoczynać się od \\.\. Przykładowa ścieżka z nazwą urządzenia \\.*nazwa_urządzenia*. W systemach AIX, Linux i Solaris ścieżką urządzenia musi być poprawna ścieżka.
   b) W polu **Wielkość początkowa** wprowadź wielkość początkową obszaru tabel LDAPSPACE lub zaakceptuj wartość domyślną. Dla kontenera obszaru tabel typu **Urządzenie surowe** wielkość kontenera obszaru tabel LDAPSPACE jest stała. Wielkość domyślna wynosi 16 k. Aby uzyskać lepsze wyniki, należy podać odpowiednią wielkość.

c. Jeśli wybrana została opcja **Plik** w jednym lub obu polach **Kontener obszaru tabel**, podaj liczbę stron, o jaką mają zostać rozszerzone kontenery obszaru tabel, w polu **Wielkość rozszerzania**.

6. Kliknij przycisk **Zakończ**.
7. Aby zaakceptować zakończenie zadania, kliknij przycisk **OK**.
8. Zweryfikuj dzienniki wygenerowane dla operacji konfiguracji bazy danych.
9. Aby zamknąć stronę **Konfigurowanie bazy danych**, kliknij przycisk **Zamknij**.
10. Aby zamknąć okno programu Configuration Tool, kliknij opcje **Plik > Wyjście**.
11. Aby potwierdzić działanie, kliknij przycisk **Tak**.

## Co dalej

Po skonfigurowaniu bazy danych należy wykonać następujące konfiguracje dla instancji:

- Skonfigurowanie nazwy DN i hasła podstawowego administratora. Patrz sekcja “Zarządzanie nazwą DN podstawowego administratora za pomocą programu Configuration Tool” na stronie 170 i “Zarządzanie hasłem podstawowego administratora za pomocą programu Configuration Tool” na stronie 172.
- Skonfigurowanie wymaganych przyrostków. Patrz sekcja “Konfiguracja przyrostka” na stronie 200.

# Konfigurowanie bazy danych dla instancji za pomocą programu narzędziowego dla wiersza komend

Program narzędziowy dla wiersza komend **idscfgdb** umożliwia skonfigurowanie bazy danych DB2 dla instancji serwera katalogów.

## Zanim rozpoczniesz

Aby skonfigurować bazę danych DB2 dla instancji serwera katalogów, wykonaj następujące czynności:

- Nie ustawiaj zmiennej środowiskowej *DB2COMM* podczas konfigurowania bazy danych.
- Zatrzymaj serwer katalogów. Patrz sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzi dla wiersza komend” na stronie 157.
- Musi istnieć identyfikator użytkownika systemu będący właścicielem instancji bazy danych DB2. Więcej informacji na temat wymagań dotyczących identyfikatora użytkownika systemu zawiera sekcja “Użytkownicy i grupy powiązane z instancją serwera katalogów” na stronie 121.

## O tym zadaniu

Można uruchomić komendę **idscfgdb**, aby wykonać następujące operacje:

- Utworzenie i skonfigurowanie bazy danych instancji serwera katalogów. Utworzenie ustawień lokalnej pętli zwrotnej, jeśli nie istnieją.
- Dodanie informacji o bazie danych do pliku ibmslapd.conf instancji serwera katalogów.

Można określić, czy baza danych ma zostać utworzona w lokalnej stronie kodowej, czy w stronie kodowej UTF-8 (jest to opcja domyślna).

## Procedura

1. Zaloguj się jako właściciel instancji serwera katalogów.
2. Otwórz wiersz komend.
3. Zmień bieżący katalog roboczy na podkatalog sbin w miejscu instalacji produktu IBM Security Directory Server.
4. Aby skonfigurować bazę danych DB2 dla instancji serwera katalogów z następującymi wartościami, uruchom następującą komendę:
   - Nazwa instancji: ldapdb
   - Nazwa bazy danych: ldapdb
   - ID administratora bazy danych DB2: ldapdb
   - Hasło administratora bazy danych DB2: ldapdb123
   - Położenie bazy danych: /home/ldapdb

   ```
   idscfgdb -I ldapdb -a ldapdb -w ldapdb123 -t ldapdb
   -l /home/ldapdb
   ```

   W systemie Windows, podaj nazwę dysku dla położenia bazy danych. W systemie Solaris, podaj położenie odpowiedniej bazy danych. Więcej informacji na temat komendy **idscfgdb** zawiera *Skorowidz komend*. Komenda konfiguruje bazę danych z obszarami tabel DMS o domyślnych wielkościach.

## Przykłady

**Przykład 1:**

Aby skonfigurować bazę danych z obszarem tabel DMS w systemie plików i o wielkości podanej dla obszaru tabel, uruchom komendę **idscfgdb** z następującymi wartościami:

- Nazwa instancji: ldapdb
- Nazwa bazy danych: ldapdb
- ID administratora bazy danych DB2: dbadmin
- Hasło administratora bazy danych DB2: ldapdb123
- Położenie bazy danych: c:\dblocation
- Położenie obszaru tabel USERSPACE1: c:\dblocation\ldapinst\tablespaceloc\USPACE
- Wielkość kontenera obszarów tabel USERSPACE1: 10000 stron
- Wielkość rozszerzenia: 16 stron

```
idscfgdb -I ldapdb -a dbadmin -t ldapdb
-w ldapdb123 -n -l c:\dblocation
-u c:\dblocation\ldapinst\tablespaceloc\USPACE -U 10000 -z 16
```

**Przykład 2:**

Aby skonfigurować tę samą bazę danych z obszarami tabel SMS, uruchom komendę **idscfgdb** z następującymi wartościami:

- Nazwa instancji: ldapdb
- Nazwa bazy danych: ldapdb
- ID administratora bazy danych DB2: dbadmin
- Hasło administratora bazy danych DB2: ldapdb123
- Położenie bazy danych: c:\dblocation

```
idscfgdb -I ldapdb -a dbadmin -t ldapdb
-w ldapdb123 -n -l c:\dblocation
-m SMS
```

## Co dalej

Po skonfigurowaniu bazy danych należy wykonać następujące konfiguracje dla instancji:

- Skonfigurowanie nazwy DN i hasła podstawowego administratora. Patrz sekcja “Zarządzanie nazwą DN podstawowego administratora za pomocą programu narzędziowego dla wiersza komend” na stronie 171 oraz “Zarządzanie hasłem podstawowego administratora za pomocą programu narzędziowego dla wiersza komend” na stronie 173.
- Skonfigurowanie wymaganych przyrostków. Patrz sekcja “Konfiguracja przyrostka” na stronie 200.

# Zarządzanie hasłem administratora bazy danych DB2

Jeśli zostanie zmienione hasło systemowe dla właściciela instancji DB2, należy zaktualizować hasło w pliku konfiguracyjnym instancji serwera katalogów.

Gdy zmieniane jest hasło systemowe właściciela instancji bazy danych DB2, hasło w pliku konfiguracyjnym instancji nie jest aktualizowane. Jeśli hasło administratora bazy danych w pliku konfiguracyjnym instancji nie będzie takie samo, jak hasło systemowe tego użytkownika, instancja może się nie uruchomić w trybie normalnym. Należy wtedy zaktualizować plik konfiguracyjny instancji bazy danych, podając najnowsze hasło właściciela instancji DB2.

Do zaktualizowania hasła administratora bazy danych DB2 można użyć narzędzia konfiguracyjnego, komendy **idscfgdb** lub komendy **idsldapmodify**.

Przed zmianą hasła administratora bazy danych za pomocą narzędzia konfiguracyjnego lub komendy **idscfgdb** należy zatrzymać serwer katalogów. Aby zmienić hasło administratora bazy danych za pomocą komendy **idsldapmodify**, należy uruchomić serwer w trybie konfiguracji. Uruchom komendę **idsldapmodify** jako podstawowy administrator serwera katalogów albo jako członek lokalnej grupy administratorów z przypisaną rolą dirdata.

Więcej informacji na temat komend **idscfgdb** i **idsldapmodify** zawiera *Skorowidz komend*.

# Modyfikowanie hasła administratora bazy danych DB2 przy użyciu programu narzędziowego Configuration Tool

Program Configuration Tool umożliwia zaktualizowanie hasła administratora bazy danych DB2 w pliku konfiguracyjnym instancji serwera katalogów.

## Zanim rozpoczniesz

Aby zaktualizować hasło administratora bazy danych DB2 w pliku konfiguracyjnym instancji, należy wykonać następujące czynności:

- Musi istnieć instancja serwera katalogów, dla której skonfigurowano bazę danych DB2. Patrz sekcja “Konfigurowanie bazy danych dla instancji za pomocą narzędzia Configuration Tool” na stronie 174.
- Zatrzymaj serwer katalogów. Patrz sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzia Configuration Tool” na stronie 169.

## O tym zadaniu

Program Configuration Tool zaktualizuje hasło administratora bazy danych DB2 w pliku konfiguracyjnym instancji serwera katalogów. Jeśli dla instancji jest skonfigurowany dziennik zmian, narzędzie zaktualizuje również w pliku konfiguracyjnym hasło dla właściciela bazy danych dziennika zmiany.

## Procedura

1. Uruchom narzędzie Configuration Tool dla instancji. Patrz sekcja “Uruchamianie programu Configuration Tool” na stronie 168.
2. Na liście zadań znajdującej się na lewym panelu nawigacyjnym kliknij opcję **Zadania bazy danych > Konfigurowanie bazy danych**.
3. Na stronie **Konfiguracja bazy danych** wykonaj następujące kroki:
   a. Kliknij przycisk **Resetuj hasło**.
   b. W polu **Hasło** wpisz hasło administratora bazy danych.
   c. W polu **Potwierdź hasło** wpisz hasło administratora bazy danych.
   d. Kliknij przycisk **Dalej**.
4. Kliknij przycisk **Zakończ**.
5. Aby zaakceptować zakończenie zadania, kliknij przycisk **OK**.
6. Zweryfikuj dzienniki wygenerowane dla operacji konfiguracji hasła bazy danych.
7. Aby zamknąć stronę **Konfigurowanie bazy danych**, kliknij przycisk **Zamknij**.
8. Aby zamknąć okno programu Configuration Tool, kliknij opcje **Plik > Wyjście**.
9. Aby potwierdzić działanie, kliknij przycisk **Tak**.

### Co dalej

Uruchom serwer katalogów. Patrz sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzia Configuration Tool” na stronie 169.

## Modyfikowanie hasła administratora bazy danych DB2 za pomocą programu narzędziowego dla wiersza komend

Użyj komendy **idscfgdb** lub narzędzia **idsldapmodify** dla wiersza komend, aby zaktualizować hasło administratora bazy danych DB2 w pliku konfiguracyjnym instancji serwera katalogów.

### Zanim rozpoczniesz

Aby zaktualizować hasło administratora bazy danych DB2 w pliku konfiguracyjnym instancji, należy wykonać następujące czynności:

- Musi istnieć instancja serwera katalogów, dla której skonfigurowano bazę danych DB2. Patrz sekcja “Konfigurowanie bazy danych dla instancji za pomocą programu narzędziowego dla wiersza komend” na stronie 178.

### O tym zadaniu

Możesz uruchomić komendę **idscfgdb**, aby zaktualizować hasło administratora bazy danych DB2 w pliku konfiguracyjnym instancji. Przed uruchomieniem komendy **idscfgdb** należy zatrzymać serwer katalogów.

Za pomocą komendy **idsldapmodify** można zmienić hasło, gdy instancja serwera katalogów jest uruchomiona. Uruchom komendę **idsldapmodify** jako podstawowy administrator serwera katalogów albo jako członek lokalnej grupy administratorów z przypisaną rolą dirdata.

Więcej informacji na temat komend **idscfgdb** i **idsldapmodify** zawiera *Skorowidz komend*.

### Procedura

1. Zaloguj się jako właściciel instancji serwera katalogów.
2. Otwórz wiersz komend.
3. Aby zmienić hasło administratora bazy danych DB2, wybierz jedną z następujących metod:
   - Aby zmienić hasło administratora bazy danych DB2 za pomocą komendy **idscfgdb**, wykonaj następujące kroki:
     a. Zmień bieżący katalog roboczy na podkatalog sbin w miejscu instalacji produktu IBM Security Directory Server.
     b. Zatrzymaj serwer katalogów. Patrz sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzi dla wiersza komend” na stronie 157.
     c. Uruchom komendę **idscfgdb** w następującym formacie:
        ```
        idscfgdb -I nazwa_instancji -w db2adminPWD
        ```
     d. Uruchom serwer katalogów. Patrz sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzi dla wiersza komend” na stronie 157.
   - Aby zmienić hasło administratora bazy danych DB2 za pomocą komendy **idsldapmodify**, wykonaj następujące kroki:

a. Zmień bieżący katalog roboczy na podkatalog bin w miejscu instalacji produktu IBM Security Directory Server.
b. Uruchom komendę **idsldapmodify** w następującym formacie:

```
idscfgdb -h adres_IP -p
port -D DN_admin -w hasło_admin -i file1.ldif
```

Plik file1.ldif zawiera następujące pozycje:

```
dn: cn=Directory, cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration
changetype: modify
replace: ibm-slapdDbUserPW
ibm-slapdDbUserPW: db2adminPWD
```

c. Zrestartuj serwer katalogów. Patrz sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzi dla wiersza komend” na stronie 157.

# Dekonfiguracja bazy danych z instancji serwera katalogów

Aby użyć istniejącej instancji serwera katalogów z inną bazą danych DB2, należy zdekonfigurować z instancji istniejącą bazę danych.

W instancji serwera katalogów można zdekonfigurować bazę danych, tylko jeśli dla instancji skonfigurowano bazę danych DB2.

Za pomocą narzędzia Configuration Tool lub komendy **idsucfgdb** można uruchomić następujące operacje:

- Usunięcie informacji o bazie danych DB2 z pliku konfiguracyjnego instancji serwera katalogów. W tej operacji narzędzie dekonfiguruje z instancji bazę danych DB2 i nie usuwa bazy danych DB2.
- Usunięcie informacji o bazie danych DB2 z pliku konfiguracyjnego instancji serwera katalogów i usunięcie bazy danych DB2. W tej operacji, baza danych DB2 jest usuwana i wszystkie dane zostaną utracone.

Po zdekonfigurowaniu bazy danych z instancji serwera katalogów, baza danych jest niedostępna dla instancji.

Dla instancji serwera proxy operacja dekonfigurowania bazy danych nie jest obsługiwana.

Więcej informacji na temat komendy **idsucfgdb** zawiera publikacja *Skorowidz komend*.

## Dekonfigurowanie bazy danych dla instancji za pomocą narzędzia Configuration Tool

Narzędzie Configuration Tool umożliwia zdekonfigurowanie bazy danych DB2 dla instancji serwera katalogów.

### Zanim rozpoczniesz

Aby zdekonfigurować bazę danych DB2 dla instancji, instancja ta musi spełniać następujące wymagania:

- Musi istnieć instancja serwera katalogów, dla której skonfigurowano bazę danych DB2. Patrz sekcja “Konfigurowanie bazy danych dla instancji za pomocą narzędzia Configuration Tool” na stronie 174.
- Zatrzymaj serwer katalogów. Patrz sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzia Configuration Tool” na stronie 169.

### Procedura

1. Uruchom narzędzie Configuration Tool dla instancji. Patrz sekcja "Uruchamianie programu Configuration Tool" na stronie 168.
2. Na liście zadań znajdującej się na lewym panelu nawigacyjnym kliknij opcję **Zadania bazy danych > Dekonfigurowanie bazy danych**.
3. Na stronie **Dekonfiguracja bazy danych** wykonaj następujące kroki:
   a. W obszarze Opcje wybierz jedną z następujących opcji:
      - Aby zdekonfigurować bazę danych DB2 dla instancji bez usuwania bazy danych DB2, kliknij opcję **Zdekonfiguruj bazę danych**.
      - Aby zdekonfigurować bazę danych DB2 dla instancji i jednocześnie usunąć bazę danych DB2, kliknij opcję **Zdekonfiguruj i usuń bazę danych**.
   b. Aby usunąć kopię zapasową bazy danych dla instancji, jeśli baza danych ma skonfigurowane tworzenie kopii zapasowej otwartej bazy danych, wybierz opcję **Usuń kopię zapasową bazy danych**.
   c. Aby rozpocząć dekonfigurację, kliknij przycisk **Dekonfiguruj**.
   d. W oknie potwierdzenia kliknij przycisk **Tak**.
4. Aby zaakceptować zakończenie zadania, kliknij przycisk **OK**.
5. Zweryfikuj dzienniki wygenerowane dla operacji dekonfiguracji bazy danych.
6. Aby zamknąć stronę **Dekonfigurowanie bazy danych**, kliknij przycisk **Zamknij**.
7. Aby zamknąć okno programu Configuration Tool, kliknij opcje **Plik > Wyjście**.
8. Aby potwierdzić działanie, kliknij przycisk **Tak**.

## Dekonfigurowanie bazy danych dla instancji za pomocą programu narzędziowego dla wiersza komend

Program narzędziowy dla wiersza komend **idsucfgdb** umożliwia zdekonfigurowanie bazy danych dla instancji serwera katalogów.

### Zanim rozpoczniesz

Aby zdekonfigurować bazę danych DB2 dla instancji, instancja ta musi spełniać następujące wymagania:

- Musi istnieć instancja serwera katalogów, dla której skonfigurowano bazę danych DB2. Patrz sekcja "Konfigurowanie bazy danych dla instancji za pomocą programu narzędziowego dla wiersza komend" na stronie 178.
- Zatrzymaj serwer katalogów. Patrz sekcja "Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzi dla wiersza komend" na stronie 157.

### Procedura

1. Zaloguj się jako właściciel instancji serwera katalogów.
2. Otwórz wiersz komend.
3. Zmień bieżący katalog roboczy na podkatalog sbin w miejscu instalacji produktu IBM Security Directory Server.
4. Aby zdekonfigurować bazę danych DB2 dla instancji, wybierz jedną z następujących opcji:
   - Aby zdekonfigurować bazę danych dla instancji serwera katalogów, uruchom komendę **idsucfgdb**.

     ```
     idsucfgdb -I nazwa_instancji
     ```

- Aby zdekonfigurować i usunąć bazę danych dla instancji serwera katalogów, uruchom komendę **idsucfgdb**.

  ```
  idsucfgdb -I nazwa_instancji -r
  ```

# Optymalizowanie bazy danych

Aby zwiększyć wydajność wyszukiwania w bazie danych DB2 należy ją zoptymalizować i zaktualizować statystyki tabel DB2.

W celu zoptymalizowania bazy danych DB2 można użyć narzędzia konfiguracyjnego lub komendy **idsrunstats**. Optymalizowanie bazy danych DB2 należy przeprowadzać okresowo lub po aktualizowaniu, takim jak importowanie danych.

Po uruchomieniu optymalizacji bazy danych narzędzie gromadzi statystyki dla wszystkich indeksów, które są zdefiniowane w tabelach, następnie aktualizuje je. Optymalizator zapytań DB2 używa tych informacji statystycznych podczas określania najwydajniejszego sposobu uzyskania dostępu do danych.

Nie można uruchomić optymalizacji DB2, jeśli instancja jest serwerem proxy lub jeśli instancja nie jest skonfigurowana do pracy z bazą danych DB2.

Więcej informacji na temat komendy **idsrunstats** zawiera *Skorowidz komend*.

## Optymalizowanie bazy danych za pomocą programu Configuration Tool

Za pomocą programu Configuration Tool można zoptymalizować bazę danych powiązaną z instancją.

### Zanim rozpoczniesz

Aby zoptymalizować bazę danych DB2 instancji, instancja ta musi spełniać następujące wymagania:

- Musi istnieć instancja serwera katalogów, dla której skonfigurowano bazę danych DB2. Patrz sekcja “Konfigurowanie bazy danych dla instancji za pomocą narzędzia Configuration Tool” na stronie 174.

### Procedura

1. Uruchom narzędzie Configuration Tool dla instancji. Patrz sekcja “Uruchamianie programu Configuration Tool” na stronie 168.
2. Na liście zadań znajdującej się na lewym panelu nawigacyjnym kliknij opcję **Zadania bazy danych > Optymalizacja bazy danych**.
3. Na stronie **Optymalizacja bazy danych** wykonaj następujące kroki:
   a. Aby uruchomić operację optymalizacji bazy danych, kliknij opcję **Optymalizuj**.
   b. Aby zaakceptować zakończenie zadania, kliknij przycisk **OK**.
   c. Zweryfikuj dzienniki wygenerowane dla operacji optymalizacji bazy danych.
   d. Aby wyczyścić dzienniki, kliknij przycisk **Wyczyść wyniki**.
4. Aby zamknąć stronę **Optymalizacja bazy danych**, kliknij przycisk **Zamknij**.
5. Aby zamknąć okno programu Configuration Tool, kliknij opcje **Plik > Wyjście**.
6. Aby potwierdzić działanie, kliknij przycisk **Tak**.

## Optymalizowanie bazy danych za pomocą programu narzędziowego dla wiersza komend

Za pomocą programu narzędziowego dla wiersza komend, **idsrunstats** można zoptymalizować bazę danych DB2, która jest powiązana z instancją.

### Zanim rozpoczniesz

Aby zoptymalizować bazę danych DB2 instancji, instancja ta musi spełniać następujące wymagania:

- Musi istnieć instancja serwera katalogów, dla której skonfigurowano bazę danych DB2. Patrz sekcja “Konfigurowanie bazy danych dla instancji za pomocą programu narzędziowego dla wiersza komend” na stronie 178.

### Procedura

1. Zaloguj się jako właściciel instancji serwera katalogów.
2. Otwórz wiersz komend.
3. Zmień bieżący katalog roboczy na podkatalog sbin w miejscu instalacji produktu IBM Security Directory Server.
4. Aby zoptymalizować bazę danych DB2, uruchom komendę **idsrunstats** w następującym formacie:

   ```
   idsrunstats -I nazwa_instancji
   ```

   Więcej informacji na temat komendy **idsrunstats** zawiera *Skorowidz komend*.

# Konserwowanie bazy danych

Aby usprawnić operacje wyszukiwania lub aktualizacji wykonywane w instancji, można uruchomić reorganizację indeksu lub kompresję wierszy DB2.

Aby zreorganizować indeks bazy danych DB2 lub włączyć kompresję wiersza, można użyć narzędzia konfiguracyjnego lub komendy **idsdbmaint**.

Gdy tabele używane w bazie danych DB2 są aktualizowane przez wiele operacji wstawiania i usuwania, przeszukiwanie i aktualizowanie bazy danych zajmuje coraz więcej czasu. Jeśli indeks DB2 zostanie zreorganizowany, wydajność operacji wyszukiwania i aktualizacji się poprawi.

Po włączeniu kompresji wierszy DB2 narzędzie wyszukuje powtarzające się wzorce i zastępuje je krótszymi symbolami. Narzędzie analizuje, a następnie włącza kompresję wierszy tylko wtedy, gdy skuteczność kompresji jest większa od 30 procent.

Można także użyć komendy **idsdbmaint**, aby przekształcić obszar tabel SMS w obszar tabel DMS lub obszar tabel DMS w obszar tabel SMS. Konwertowanie obszaru tabel nie jest obsługiwane przez narzędzie konfiguracyjne. Więcej informacji na temat komendy **idsdbmaint** zawiera *Skorowidz komend*.

## Konserwacja bazy danych za pomocą programu Configuration Tool

Za pomocą programu Configuration Tool można wykonać konserwację bazy danych powiązanej z instancją.

### Zanim rozpoczniesz

Aby wykonać operację konserwacji bazy danych DB2 instancji, instancja ta musi spełniać następujące wymagania:

- Musi istnieć instancja serwera katalogów, dla której skonfigurowano bazę danych DB2. Patrz sekcja "Konfigurowanie bazy danych dla instancji za pomocą narzędzia Configuration Tool" na stronie 174.
- Zatrzymaj serwer katalogów. Patrz sekcja "Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzia Configuration Tool" na stronie 169.

### Procedura

1. Uruchom narzędzie Configuration Tool dla instancji. Patrz sekcja "Uruchamianie programu Configuration Tool" na stronie 168.
2. Na liście zadań znajdującej się na lewym panelu nawigacyjnym kliknij opcję **Zadania bazy danych > Konserwacja bazy danych**.
3. Na stronie **Konserwacja** wykonaj następujące kroki:
   a. Wybierz operację konserwacji bazy danych DB2, które chcesz uruchomić:
      - Aby uruchomić reorganizację indeksu DB2, kliknij opcję **Wykonaj reorganizację indeksu**.
      - Aby uruchomić kompresję wierszy DB2, kliknij opcję **Zbadaj tabele i przeprowadź kompresję wierszy**.

   b. Kliknij przycisk **OK**.
   c. W oknie zakończenia zadania kliknij przycisk **OK**.
   d. Zweryfikuj dzienniki wygenerowane dla operacji konserwacji bazy danych.
   e. Aby wyczyścić dzienniki, kliknij przycisk **Wyczyść wyniki**.
4. Aby zamknąć stronę **Konserwacja bazy danych**, kliknij przycisk **Zamknij**.
5. Aby zamknąć okno programu Configuration Tool, kliknij opcje **Plik > Wyjście**.
6. Aby potwierdzić działanie, kliknij przycisk **Tak**.

### Co dalej

Uruchom serwer katalogów. Patrz sekcja "Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzia Configuration Tool" na stronie 169.

## Konserwacja bazy danych za pomocą programu narzędziowego dla wiersza komend

Za pomocą programu narzędziowego dla wiersza komend **idsdbmaint** można wykonać czynności konserwacyjne dla bazy danych DB2, która jest powiązana z instancją.

### Zanim rozpoczniesz

Aby można było uruchomić operację konserwacji bazy danych DB2 instancji, instancja ta musi spełniać następujące wymagania:

- Musi istnieć instancja serwera katalogów, dla której skonfigurowano bazę danych DB2. Patrz sekcja "Konfigurowanie bazy danych dla instancji za pomocą programu narzędziowego dla wiersza komend" na stronie 178.
- Zatrzymaj serwer katalogów. Patrz sekcja "Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzi dla wiersza komend" na stronie 157.

### Procedura

1. Zaloguj się jako właściciel instancji serwera katalogów.
2. Otwórz wiersz komend.
3. Zmień bieżący katalog roboczy na podkatalog sbin w miejscu instalacji produktu IBM Security Directory Server.
4. Aby uruchomić reorganizację indeksu DB2, uruchom komendę **idsdbmaint** w następującym formacie:

   ```
   idsdbmaint -I nazwa_instancji -i
   ```

   Więcej informacji na temat komendy **idsdbmaint** zawiera *Skorowidz komend*.
5. Aby uruchomić kompresję wierszy DB2, uruchom komendę **idsdbmaint** w następującym formacie:

   ```
   idsdbmaint -I nazwa_instancji -r
   ```

### Co dalej

Uruchom serwer katalogów. Patrz sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzi dla wiersza komend” na stronie 157.

## Tworzenie kopii zapasowej serwera katalogów

Aby mieć możliwość przywrócenia pracy instancji serwera katalogów po awarii, należy często tworzyć kopie zapasowe.

Do utworzenia kopii zapasowej instancji można użyć narzędzia konfiguracyjnego albo komendy **idsdbback**. Do utworzenia kopii zapasowej instancji serwera proxy nie można użyć komendy **idsdbback**, ponieważ z serwerem proxy nie jest powiązana żadna baza danych.

Używając komendy **idscfgdb**, można skonfigurować tworzenie kopii zapasowej otwartej bazy danych, która jest powiązana z instancją. Nie można jednak zdekonfigurować tworzenie kopii zapasowej otwartej bazy danych, używając komendy **idscfgdb** z opcją **-c**. Jeśli kopię zapasową otwartej bazy danych skonfigurowano dla instancji z użyciem narzędzia administracyjnego instancji lub narzędzia konfiguracyjnego, można je zdekonfigurować za pomocą narzędzia konfiguracyjnego lub komendy **idscfgdb**. Aby uzyskać pewny wynik, do skonfigurowania tworzenia kopii zapasowej otwartej bazy danych należy użyć narzędzia administracyjnego instancji lub narzędzia konfiguracyjnego.

Można również użyć komendy **idsdb2ldif**, aby wyeksportować pozycje z serwera katalogów do pliku LDIF. Do tworzenia kopii zapasowej schematu oraz plików konfiguracyjnych instancji serwera katalogów i serwera proxy służy komenda **migbkup**. Więcej informacji na temat komend **idsdbback**, **idsdb2ldif** i **migbkup** zawiera publikacja *Skorowidz komend*. Więcej informacji na temat komend odpowiednich dla danego środowiska znajduje się w sekcji *Strojenie i planowanie wydajności* w dokumentacji serwera IBM Security Directory Server.

W narzędziu konfiguracyjnym można wykonać następujące czynności:

- Tworzenie kopii zapasowej ustawień konfiguracyjnych instancji serwera katalogów lub instancji serwera proxy.
- Tworzenie kopii zapasowej instancji serwera katalogów wraz z jego bazą danych.
- Tworzenie kopii zapasowej instancji serwera katalogów i bazy danych dziennika zmian, jeśli ją skonfigurowano dla tej instancji.

Więcej informacji na temat operacji tworzenia i odtwarzania kopii zapasowych znajduje się w sekcji *Administrowanie* w dokumentacji serwera IBM Security Directory Server.

# Tworzenie kopii zapasowej bazy danych instancji serwera katalogów za pomocą narzędzia Configuration Tool

Za pomocą narzędzia Configuration Tool można utworzyć kopię zapasową instancji serwera katalogów wraz z jej bazą danych, którą będzie można odtworzyć po awarii.

## Zanim rozpoczniesz

Aby utworzyć kopię zapasową instancji serwera katalogów wraz z jej bazą danych, instancja musi spełniać następujące wymagania:

- Musi istnieć instancja serwera katalogów, dla której skonfigurowano bazę danych DB2. Patrz sekcja “Konfigurowanie bazy danych dla instancji za pomocą narzędzia Configuration Tool” na stronie 174.

## Procedura

1. Uruchom narzędzie Configuration Tool dla instancji. Patrz sekcja “Uruchamianie programu Configuration Tool” na stronie 168.
2. Na liście zadań znajdującej się w panelu nawigacyjnym po lewej stronie kliknij opcje **Kopia zapasowa/odtwarzanie > Kopia zapasowa bazy danych**.
3. Na stronie **Kopia zapasowa bazy danych** wykonaj następujące kroki:
   a. W polu **Katalog kopii zapasowych** wpisz ścieżkę katalogu, w którym będą umieszczane kopie zapasowe danych i plików konfiguracyjnych. Można również kliknąć przycisk **Przeglądaj** i wybrać ścieżkę katalogu.
   b. Aby utworzyć kopię zapasową otwartej bazy danych, wybierz jedną z następujących opcji:
      - Aby skonfigurować wykonywanie kopii zapasowej serwera katalogów i jego bazy danych, wybierz opcję **Zaktualizuj konfigurację bazy danych o obsługę tworzenia kopii zapasowej otwartej bazy danych**.
      - Aby uruchomić tworzenie kopii zapasowej instancji serwera katalogów (jeśli na serwerze skonfigurowano tworzenie kopii zapasowej otwartej bazy danych), wybierz opcję **Wykonaj kopię zapasową otwartej bazy danych**.
   c. Aby utworzyć kopię zapasową bazy danych dziennika zmian instancji (jeśli skonfigurowano dziennik zmian), wybierz opcję **Dołącz dane dziennika zmian do kopii zapasowej**.
   d. Aby wykluczyć z kopii zapasowej pliki bazy danych, wybierz opcję **Nie twórz kopii zapasowej plików bazy danych**. Jeśli zostanie wybrana opcja **Nie twórz kopii zapasowej plików bazy danych**, nie zostanie utworzona kopia zapasowa plików bazy danych dziennika zmian dla instancji serwera katalogów. Narzędzie tworzy kopie zapasowe plików instancji serwera katalogów, takich jak pliki ukryte kluczy, pliki schematu i pliki konfiguracyjne.
   e. Aby zdecydować, czy kontynuować tworzenie kopii zapasowej w zależności od tego, czy katalog kopii zapasowych istnieje, wybierz jedną z następujących opcji:
      - Aby utworzyć katalog kopii zapasowych (jeśli on nie istnieje), kliknij opcję **Utwórz katalog kopii zapasowych**.
      - Jeśli katalog kopii zapasowych nie istnieje i nie ma być utworzony, kliknij opcję **Zatrzymaj, jeśli nie znaleziono katalogu kopii zapasowych**. Jeśli katalog kopii zapasowych nie istnieje i wybrano tę opcję, kopia zapasowa bazy danych nie zostanie utworzona.

**Uwaga:** Nie przerywaj działania narzędzia Configuration Tool, jeśli trwa operacja tworzenia kopii zapasowej.

f. Aby uruchomić operację tworzenia kopii zapasowej, kliknij przycisk **Kopia zapasowa**.

g. Jeśli operacja tworzenia kopii zapasowej wymaga zatrzymania serwera katalogów, kliknij przycisk **Tak**.

h. Aby potwierdzić zakończenie zadania, kliknij przycisk **OK**.

i. Zweryfikuj dzienniki wygenerowane dla operacji tworzenia kopii zapasowej.

j. Aby wyczyścić dzienniki, kliknij przycisk **Wyczyść wyniki**.

k. Aby zamknąć stronę **Tworzenie kopii zapasowej bazy danych**, kliknij przycisk **Zamknij**.

4. Aby zamknąć okno programu Configuration Tool, kliknij opcje **Plik > Wyjście**.
5. Aby potwierdzić działanie, kliknij przycisk **Tak**.

# Tworzenie kopii zapasowej instancji serwera proxy za pomocą narzędzia Configuration Tool

Za pomocą narzędzia Configuration Tool można utworzyć kopię zapasową instancji serwera proxy, którą będzie można odtworzyć po awarii.

## Zanim rozpoczniesz

Można utworzyć kopię zapasową tylko istniejącej instancji serwera proxy. Patrz sekcja “Tworzenie instancji serwera proxy z własnymi ustawieniami” na stronie 142.

## Procedura

1. Uruchom narzędzie Configuration Tool dla instancji. Patrz sekcja “Uruchamianie programu Configuration Tool” na stronie 168.
2. Na liście zadań znajdującej się w panelu nawigacyjnym po lewej stronie kliknij opcje **Kopia zapasowa/odtwarzanie > Kopia zapasowa instancji**.
3. Na stronie **Kopia zapasowa instancji** wykonaj następujące kroki:
   a. W polu **Katalog kopii zapasowych** wpisz ścieżkę katalogu, w którym będą umieszczane kopie zapasowe plików schematów i plików konfiguracyjnych. Można również kliknąć przycisk **Przeglądaj** i wybrać ścieżkę katalogu.
   b. Dla instancji serwera proxy jest zaznaczone pole wyboru **Nie twórz kopii zapasowej plików bazy danych**.
   c. Aby zdecydować, czy kontynuować tworzenie kopii zapasowej w zależności od tego, czy katalog kopii zapasowych istnieje, wybierz jedną z następujących opcji:
      - Aby utworzyć katalog kopii zapasowych (jeśli on nie istnieje), kliknij opcję **Utwórz katalog kopii zapasowych**.
      - Jeśli katalog kopii zapasowych nie istnieje i nie ma być utworzony, kliknij opcję **Zatrzymaj, jeśli nie znaleziono katalogu kopii zapasowych**. Jeśli katalog kopii zapasowych nie istnieje i wybrano tę opcję, kopia zapasowa instancji proxy nie zostanie utworzona.

      **Uwaga:** Nie przerywaj działania narzędzia Configuration Tool, jeśli trwa operacja tworzenia kopii zapasowej.

   d. Aby uruchomić operację tworzenia kopii zapasowej, kliknij przycisk **Kopia zapasowa**.
   e. Jeśli operacja wymaga zatrzymania instancji, kliknij przycisk **Tak**.
   f. Aby potwierdzić zakończenie zadania, kliknij przycisk **OK**.

g. Zweryfikuj dzienniki wygenerowane dla operacji tworzenia kopii zapasowej.
h. Aby wyczyścić dzienniki, kliknij przycisk **Wyczyść wyniki**.
i. Aby zamknąć stronę **Tworzenie kopii zapasowej instancji**, kliknij przycisk **Zamknij**.

4. Aby zamknąć okno programu Configuration Tool, kliknij opcje **Plik > Wyjście**.
5. Aby potwierdzić działanie, kliknij przycisk **Tak**.

# Odtwarzanie serwera katalogów

Jeśli instancja serwera katalogów ulegnie awarii, można ją odtworzyć z najnowszego obrazu kopii zapasowej.

Mając wcześniej utworzoną kopię zapasową, można odtworzyć dane katalogu i opcjonalnie ustawienia konfiguracyjne, posługując się narzędziem konfiguracyjnym lub komendą **idsdbestore**. Przed odtworzeniem bazy danych lub ustawień konfiguracyjnych należy zatrzymać serwer katalogów.

Dla serwera proxy możliwe jest odtworzenie ustawień konfiguracyjnych. W tym celu należy uruchomić komendę **idsdbrestore** z opcją **-x**.

Dla instancji z bazą danych DB2 możliwe jest odtworzenie bazy danych do bazy danych oraz instancji bazy danych o takiej samej nazwie, jaka była używana podczas tworzenia kopii zapasowej. Dla serwera katalogów z bazą danych DB2 możliwe jest odtworzenie tylko wtedy, gdy baza danych jest skonfigurowana dla instancji serwera katalogów. Komenda **idsdbestore** odtwarza kopię zapasową bazy danych do bazy danych skonfigurowanej w danej chwili. Działanie komendy kończy się niepowodzeniem, gdy kopie zapasowe instancji bazy danych i bazy danych są niezgodne ze skonfigurowaną instancją bazy danych i bazą danych. Aby odtworzyć bazę danych, położenie bazy danych z kopii zapasowej i odtwarzanej bazy danych musi być takie same.

Więcej informacji na temat komendy **idsdbrestore** zawiera *Skorowidz komend*.

## Odtwarzanie kopii zapasowej bazy danych serwera katalogów za pomocą narzędzia Configuration Tool

Użyj narzędzia Configuration Tool, aby odtworzyć instancję serwera katalogów i jego bazy danych z kopii zapasowej obrazu.

### Zanim rozpoczniesz

Aby odtworzyć instancję serwera katalogów wraz z jej bazą danych, instancja musi spełniać następujące wymagania:

- Musi istnieć instancja serwera katalogów, dla której skonfigurowano bazę danych DB2. Patrz sekcja “Konfigurowanie bazy danych dla instancji za pomocą narzędzia Configuration Tool” na stronie 174.
- Musi istnieć obraz kopii zapasowej instancji serwera katalogów. Patrz sekcja “Tworzenie kopii zapasowej bazy danych instancji serwera katalogów za pomocą narzędzia Configuration Tool” na stronie 188.
- Zatrzymaj serwer katalogów. Patrz sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzia Configuration Tool” na stronie 169.

### Procedura

1. Uruchom narzędzie Configuration Tool dla instancji. Patrz sekcja “Uruchamianie programu Configuration Tool” na stronie 168.

2. Na liście zadań znajdującej się w panelu nawigacyjnym po lewej stronie kliknij opcje **Kopia zapasowa/odtwarzanie > Odtwarzanie bazy danych**.
3. Na stronie **Odtwarzanie bazy danych** wykonaj następujące kroki:
   a. W polu **Odtwarzanie katalogu** wpisz ścieżkę katalogu, który zawiera obraz kopii zapasowej instancji. Możesz również kliknąć przycisk **Przeglądaj** i wybrać ścieżkę katalogu.
   b. Jeśli chcesz odtworzyć z kopii zapasowej tylko dane katalogu, a nie ustawienia konfiguracyjne, wybierz opcję **Zachowaj bieżące ustawienia konfiguracyjne**. Jeśli chcesz odtworzyć z kopii zapasowej dane katalogu oraz ustawienia konfiguracyjne, anuluj zaznaczenie opcji **Zachowaj bieżące ustawienia konfiguracyjne**.
   c. Jeśli dla instancji jest skonfigurowany dziennik zmian i chcesz go odtworzyć, wybierz opcję **Dołącz dane dziennika zmian do odtwarzania**.
   d. Aby uruchomić operację odtwarzania kopii zapasowej, kliknij przycisk **Odtwarzanie**.
   e. Jeśli operacja wymaga zatrzymania serwera katalogów, kliknij przycisk **Tak**.
   f. Aby potwierdzić zakończenie zadania, kliknij przycisk **OK**.
   g. Zweryfikuj dzienniki wygenerowane dla operacji odtwarzania.
   h. Aby wyczyścić dzienniki, kliknij przycisk **Wyczyść wyniki**.
   i. Aby zamknąć stronę **Odtwarzanie bazy danych**, kliknij przycisk **Zamknij**.
4. Aby zamknąć okno programu Configuration Tool, kliknij opcje **Plik > Wyjście**.
5. Aby potwierdzić działanie, kliknij przycisk **Tak**.

# Odtwarzanie instancji serwera proxy z kopii zapasowej za pomocą narzędzia Configuration Tool

Za pomocą narzędzia Configuration Tool można odtworzyć instancję serwera proxy z kopii zapasowej po ewentualnej awarii.

## Zanim rozpoczniesz

Aby odtworzyć instancję serwera proxy, instancja ta musi spełniać następujące wymagania:

- Musi istnieć instancja serwera proxy. Patrz sekcja “Tworzenie instancji serwera proxy z własnymi ustawieniami” na stronie 142.
- Musi istnieć obraz kopii zapasowej instancji serwera proxy. Patrz sekcja “Tworzenie kopii zapasowej instancji serwera proxy za pomocą narzędzia Configuration Tool” na stronie 189.
- Zatrzymaj serwer katalogów. Patrz sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzia Configuration Tool” na stronie 169.

## Procedura

1. Uruchom narzędzie Configuration Tool dla instancji. Patrz sekcja “Uruchamianie programu Configuration Tool” na stronie 168.
2. Na liście zadań znajdującej się w panelu nawigacyjnym po lewej stronie kliknij opcje **Kopia zapasowa/odtwarzanie > Odtwarzanie instancji**.
3. Na stronie **Odtwarzanie instancji** wykonaj następujące kroki:
   a. W polu **Odtwarzanie katalogu** wpisz ścieżkę katalogu, który zawiera obraz kopii zapasowej instancji. Możesz również kliknąć przycisk **Przeglądaj** i wybrać ścieżkę katalogu.
   b. Jeśli nie chcesz odtworzyć ustawień konfiguracyjnych z kopii zapasowej obrazu, wybierz opcję **Zachowaj bieżące ustawienia konfiguracyjne**.
   c. Aby uruchomić operację odtwarzania kopii zapasowej, kliknij przycisk **Odtwarzanie**.

d. Jeśli operacja wymaga zatrzymania serwera katalogów, kliknij przycisk **Tak**.
e. Aby potwierdzić zakończenie zadania, kliknij przycisk **OK**.
f. Zweryfikuj dzienniki wygenerowane dla operacji odtwarzania.
g. Aby wyczyścić dzienniki, kliknij przycisk **Wyczyść wyniki**.
h. Aby zamknąć stronę **Odtwarzanie instancji**, kliknij przycisk **Zamknij**.

4. Aby zamknąć okno programu Configuration Tool, kliknij opcje **Plik** > **Wyjście**.
5. Aby potwierdzić działanie, kliknij przycisk **Tak**.

## Strojenie serwera katalogów w celu poprawienia wydajności

Należy dostroić instancję serwera katalogów, aby zwiększyć wydajność operacji wyszukiwania i aktualizacji.

Można dostroić instancję serwera katalogów za pomocą narzędzia Configuration Tool lub komendy **idsperftune**. Narzędzie generuje wartości ustawień dostrajania wydajności dla pamięci podręcznych serwera katalogów i pul buforów bazy danych DB2. Narzędzie generuje ustawienia na podstawie wartości podanych dla instancji serwera katalogów. Narzędzie może również zaktualizować ustawienia strojenia dla instancji. Narzędzie tworzy kopię zapasową pliku ibmslapd.conf i zapisuje ją w pliku logs/ibmslapd.conf.save w katalogu głównym instancji serwera katalogów.

Narzędzie zapisuje podane informacje w pliku logs/perftune_input.conf w katalogu głównym instancji serwera katalogów.

Narzędzie Configuration Tool lub komenda **idsperftune** wykorzystują podane wartości do obliczenia następujących ustawień strojenia instancji:

- Wielkość pamięci podręcznej pozycji
- Wielkość pamięci podręcznej filtrów
- Wielkość pamięci podręcznej elementów grup
- Limit pomijania pamięci podręcznej elementów grup
- Wielkość puli buforów DB2 LDAPDB
- Wielkość puli buforów DB2 IBMDEFAULTDB

Jeśli instancja serwera katalogów jest uruchomiona, narzędzie monitoruje wydajność instancji i dostarcza do bazy danych informacje o sprawdzeniu poprawności bazy danych. Te informacje zawierają następujące parametry bazy danych DB2:

- DB2 NUM_IOSERVERS
- DB2 NUM_IOCLEANERS
- CATALOGCACHE_SZ
- PCKCACHESZ
- LOGFILSIZ
- LOCKLIST

Jeśli w instancji zostanie wykonane strojenie zaawansowane, narzędzie zgromadzi i przeanalizuje dane na temat instancji serwera katalogów. Instancja musi działać przez pewien czas, aby podczas analiz informacji o poprawności zgromadzić dane strojenia bazy danych DB2. Narzędzie generuje wartości strojenia dla następujących parametrów bazy danych i zapisuje je w pliku logs/perftune_stat.log dla danej instancji.

- SORTHEAP
- MAXFILOP
- DBHEAP

- CHNGPGS_THRESH
- NUM_IOSERVERS
- NUM_IOCLEANERS

Sugestie dotyczące statusu poprawności parametrów DB2 mogą przyjmować jedną z następujących wartości:

- OK
- Zwiększ
- Zmniejsz
- Nie zbierano

Statusowi poprawności parametrów bazy danych DB2, które nie są analizowane jest przypisywana wartość Nie zbierano. Można użyć wartości sugerowanych dla parametrów bazy danych DB2, aby uzyskać większą wydajność.

Aby zwiększyć wydajność, w instancji należy uruchomić narzędzie natychmiast po początkowym załadowaniu danych. Po początkowym dostrojeniu należy okresowo uruchamiać narzędzie, szczególnie po dodaniu wielu pozycji lub po zmianie treści pozycji.Więcej informacji na temat strojenia instancji serwera katalogów znajduje się w sekcji *Strojenie i planowanie wydajności* dokumentacji serwera IBM Security Directory Server.

Za pomocą narzędzia Configuration Tool lub komendy **idsperftune** nie można stroić instancji serwera proxy lub instancji, w której nie skonfigurowano bazy danych.

# Konfigurowanie strojenia wydajności serwera katalogów za pomocą narzędzia Configuration Tool

Za pomocą narzędzia Configuration Tool można dostroić serwer katalogów, aby zwiększyć wydajność operacji wyszukiwania i aktualizowania.

## Zanim rozpoczniesz

Aby dostroić instancję serwera katalogów, instancja musi spełniać następujące wymagania:

- Musi istnieć instancja serwera katalogów, dla której skonfigurowano bazę danych DB2. Patrz sekcja “Konfigurowanie bazy danych dla instancji za pomocą narzędzia Configuration Tool” na stronie 174.

## Procedura

1. Uruchom narzędzie Configuration Tool dla instancji. Patrz sekcja “Uruchamianie programu Configuration Tool” na stronie 168.
2. Na liście zadań znajdującej się w panelu nawigacyjnym po lewej stronie kliknij opcje **Zadania bazy danych > Strojenie wydajności**.
3. Na stronie **Strojenie wydajności** wykonaj następujące działania:
   a. W polu **Procent dostępnej pamięci systemowej, która ma zostać przydzielona do tej instancji katalogu** wpisz procent pamięci systemowej, która ma zostać przydzielona do instancji. Dostępna pamięć systemowa jest dzielona między wiele instancji serwera katalogów lub między instancje i inne serwery, które mają być uruchamiane w systemie. Narzędzie wykorzystuje podaną wartość do obliczenia wielkości pamięci podręcznej pozycji i filtrów.
   b. W polu **Planowana liczba grup** wpisz oczekiwaną liczbę grup, które mają być dodane w instancji. Narzędzie wykorzystuje podaną wartość do obliczenia wielkości pamięci podręcznych serwera katalogu.

c. W polu **Maksymalna liczba elementów grupy, do których będą następować częste odwołania** wpisz średnią liczbę elementów najczęściej wykorzystywanych grup.

d. W obszarze **Liczba pozycji i średnia wielkość pozycji** wybierz jedną z następujących opcji:

- Aby oszacować liczbę pozycji w katalogu i średnią wielkość pozycji, wykonaj następujące czynności:
  1) W polu **Planowana liczba pozycji** wpisz planowaną łączną liczbę pozycji dla instancji. Narzędzie spróbuje określić liczbę pozycji w instancji serwera katalogów. Jeśli oszacowanie nie powiedzie się, zostanie użyta wartość domyślna 10.000 pozycji. Narzędzie wykorzystuje tę wartość do obliczenia wielkości pamięci podręcznych serwera katalogu.
  2) W polu **Średnia wielkość pozycji** wpisz średnią wielkość (w bajtach) pozycji tej instancji. Narzędzie spróbuje obliczyć wielkość pozycji w instancji serwera katalogów. Jeśli okaże się to niemożliwe, przyjmowana jest domyślna wielkość 2650 bajtów. Narzędzie wykorzystuje tę wartość do obliczenia wielkości pamięci podręcznych serwera katalogu.
- Aby narzędzie określiło łączną liczbę pozycji oraz średnią wielkość pozycji, kliknij opcję **Ładuj z bazy danych instancji serwera**. Narzędzie wypełnia pola **Planowana liczba pozycji** i **Średnia wielkość pozycji**.

e. W obszarze **Częstotliwość aktualizacji** wybierz jedną z następujących opcji:

- Jeśli oczekiwana jest częsta aktualizacja instancji, należy kliknąć opcję **Częste aktualizacje**. Jako częstą przyjmuje się więcej niż jedną aktualizację na 500 operacji wyszukiwania.
- Jeśli oczekiwana jest mniejsza liczba aktualizacji lub będą one wykonywane w grupach albo w określonej porze dnia, kliknij opcję **Aktualizacje wsadowe**.

Narzędzie używa tych informacji do ustawienia wielkość pamięci podręcznej filtrów. Pamięć podręczna filtrów jest przydatna tylko dla niezbyt częstych aktualizacji instancji oraz w sytuacji, gdy te same wyszukiwania są wykonywane kilka razy. Gdy spodziewane są częste aktualizacje, wielkość pamięci podręcznej filtrów zostanie ustawiona na wartość 0. Kiedy jednak oczekiwana częstotliwość aktualizacji jest niewielka lub mają być one przeprowadzane wsadowo, wielkość pamięci podręcznej filtrów zostanie ustawiona na 1024 pozycji.

f. Aby narzędzie podawało wartości analizy wydajności, wybierz opcję **Włącz zbieranie dodatkowych danych systemowych na potrzeby strojenia rozszerzonego**.

- Po zaznaczeniu pola wyboru, włączane są przełączniki monitorowania DB2 BUFFERPOOL i SORTHEAP. Wydajność instancji serwera katalogów może się obniżyć, jeśli narzędzie włączy gromadzenie danych przez przełączniki monitorowania DB2.
- Aby uzyskać dokładne dane do optymalnego dostrojenia instancji serwera katalogów, zaznacz pole wyboru, gdy w środowisku wykonywane są typowe działania katalogu. Jeśli sprawdzenie poprawności bazy danych zostanie uruchomione, gdy serwer nie jest obciążony, uzyskane dane nie będą optymalne.

g. Kliknij przycisk **Dalej**. Zostanie otwarta strona **Dostrajanie wydajności: weryfikacja**.

4. Na stronie **Dostrajanie wydajności: weryfikacja** wykonaj następujące działania:

a. Na liście **Status poprawności bazy danych**, sprawdź ustawienia dostrajania wydajności wygenerowane przez narzędzie. Jeśli brak jest działań bazy danych instancji, lista **Status poprawności bazy danych** może być pusta. Na liście znajdują

się dane, jeśli narzędzie zgromadzi informacje o co najmniej jednym parametrze bazy danych DB2. Ustawienia strojenia są również rejestrowane w pliku perftune_stat.log.

b. Aby zmodyfikować wartości parametrów bazy danych, kliknij opcję **Dostrój parametry bazy danych**. Zostanie otwarte okno **Parametry bazy danych**.

c. W oknie **Parametry bazy danych** podaj wartości następujących parametrów bazy danych:

1) W polu **Sterta bazy danych** wpisz maksymalną pamięć (w stronach) dla sterty bazy danych. Sterta bazy danych zawiera informacje bloku sterującego dla tabel, indeksów, obszarów tabel i pul buforów. Zawiera ona także pamięć dla buforu dziennika i pamięci tymczasowej używanej przez programy narzędziowe.

2) W polu **Wielkość pamięci podręcznej pakietu** wpisz wielkość (w stronach) pamięci podręcznej przeznaczonej dla sekcji statycznych i dynamicznych instrukcji SQL i XQuery w bazie danych.

3) W polu **Wielkość buforu dziennika** wpisz wielkość (w stronach) buforu, który musi być przydzielony dla rekordów dziennika. Należy podać wielkość sterty bazy danych, która zostanie użyta jako bufor dla rekordów dziennika.

4) W polu **Maksymalna liczba otwartych plików bazy danych na aplikację** wpisz maksymalną liczbę uchwytów plików, które mogą być otwarte przez jednego agenta bazy danych.

5) W polu **Próg zmienionych stron** wpisz procent zmienionych stron.

6) W polu **Wielkość sterty sortowania** wpisz maksymalną wielkość (w stronach) sterty sortowania. Sterta sortowania może być używana jako strony pamięci prywatnej dla prywatnych operacji sortowania lub jako strony pamięci współużytkowanej dla współużytkowanych operacji sortowania.

7) W polu **Wielkość pliku dziennika** wpisz wielkość plików dzienników (w kB). Ten parametr definiuje wielkość każdego podstawowego i dodatkowego pliku dziennika.

8) W polu **Ścieżka dziennika bazy danych** wpisz położenie, w którym mają być przechowywane pliki dziennika. Aby określić położenie, możesz kliknąć przycisk **Przeglądaj**.

9) Aby zapisać wartości i zaktualizować parametry bazy danych, kliknij przycisk **OK**. Jeśli wartości parametrów nie zostaną podane, zostaną ustawione wartości domyślne.

5. Aby potwierdzić aktualizację ustawień katalogu i bazy danych, wybierz jedną z następujących opcji:
   - Aby zaktualizować ustawienia dostrajania instancji serwera katalogów, kliknij opcję **Tak, zaktualizuj ustawienia konfiguracyjne katalogu i bazy danych zalecanymi wartościami**.
   - Aby nie używać ustawień dostrajania, kliknij opcję **Nie, zachowaj bieżące ustawienia. Ustawienia konfiguracyjne nie zostaną zaktualizowane**.
6. Aby zastosować zmiany, kliknij przycisk **Zakończ**.
7. Aby potwierdzić zakończenie zadania, kliknij przycisk **OK**.
8. Zweryfikuj dzienniki wygenerowane podczas aktualizowania ustawień dostrajania.
9. Aby wyczyścić dzienniki, kliknij przycisk **Wyczyść wyniki**.
10. Aby zamknąć stronę **Strojenie wydajności**, kliknij przycisk **Zamknij**.
11. Aby zamknąć okno programu Configuration Tool, kliknij opcje **Plik > Wyjście**.
12. Aby potwierdzić działanie, kliknij przycisk **Tak**.

## Konfigurowanie strojenia wydajności serwera katalogów za pomocą programu narzędziowego dla wiersza komend

Za pomocą programu narzędziowego dla wiersza komend (**idsperftune**) można dostroić serwer katalogów, aby zwiększyć wydajność operacji wyszukiwania i aktualizowania.

### Zanim rozpoczniesz

Aby dostroić instancję serwera katalogów, instancja musi spełniać następujące wymagania:

- Musi istnieć instancja serwera katalogów, dla której skonfigurowano bazę danych DB2. Patrz sekcja "Konfigurowanie bazy danych dla instancji za pomocą programu narzędziowego dla wiersza komend" na stronie 178.

### Procedura

1. Zaloguj się jako właściciel instancji serwera katalogów.
2. Otwórz wiersz komend.
3. Zmień bieżący katalog roboczy na podkatalog sbin w miejscu instalacji produktu IBM Security Directory Server.
4. Aby dostroić serwer katalogów i jego bazę danych, wykonaj komendę **idsperftune**.
   - Aby wykonać podstawowe strojenie serwera katalogów, wykonaj komendę **idsperftune** w następującym formacie:

     ```
     idsperftune -I nazwa_instancji -i plik_właściwości -B -u
     ```

     Jeśli zostanie podany parametr **-u**, ustawienia pamięci podręcznej LDAP i puli buforów DB2 zostaną zaktualizowane na serwerze i w bazie danych. Jeśli nie zostanie podany parametr **-u**, ustawienia strojenia zostaną zarejestrowane tylko w pliku perftune_stat.log.
   - Aby uzyskać z instancji i jej bazy danych liczbę pozycji i średnią wielkość pozycji, wykonaj komendę **idsperftune** w następującym formacie:

     ```
     idsperftune -I nazwa_instancji -s
     ```
   - Aby wykonać zaawansowane strojenie serwera katalogów, wykonaj komendę **idsperftune** w następującym formacie:

     ```
     idsperftune -I nazwa_instancji -i plik_właściwości -A -m
     ```

     Jeśli zostanie podany parametr **-m**, zostaną włączone przełączniki monitora BUFFERPOOL i SORT. Aby uzyskać dokładne dane do optymalnego dostrojenia instancji, uruchom komendę w czasie, gdy w środowisku wykonywane są typowe działania katalogu.

   Więcej informacji na temat komendy **idsperftune** zawiera publikacja *Skorowidz komend*.

## Zarządzanie dziennikiem zmian instancji serwera katalogów

Istnieje możliwość skonfigurowania bazy danych dziennika zmian w celu rejestrowania zmian schematu lub pozycji katalogu.

Dziennik zmian rejestruje wszystkie operacje aktualizacji, takie jak add (dodawanie), delete (usuwanie), modify (modyfikowanie) i modrdn (modyfikowanie RDN), wykonywane w instancji serwera katalogów. Można użyć narzędzi klienta do pobrania danych dziennika zmian, które są zapisywane podczas modyfikowania bazy danych serwera katalogów.

Można użyć narzędzia konfiguracyjnego lub interfejsu wiersza komend, aby włączyć lub wyłączyć bazę danych dziennika zmian. Przed rozpoczęciem konfigurowania lub dekonfigurowania bazy danych dziennika zmian należy zatrzymać serwer katalogów.

Aby skonfigurować dziennik zmian dla serwera katalogów, użyj komendy **idscfgchglg**. Aby zdekonfigurować dziennik zmian dla serwera katalogów, użyj komendy **idsucfgchglg**. Nie można skonfigurować bazy danych dziennika zmian dla instancji serwera proxy.

Aby skonfigurować dziennik zmian instancji serwera katalogów, użytkownik musi spełniać następujące kryteria:

1. Musi istnieć instancja bazy danych DB2 o takiej samej nazwie, jak instancja serwera katalogów.
2. Należy skonfigurować bazę danych dla instancji serwera katalogów.
3. W systemach AIX, Linux i Solaris w pliku /etc/services musi być zarejestrowana usługa loopback.

Baza danych dziennika zmian zostanie utworzona w tej samej instancji bazy danych, co baza danych instancji serwera katalogów. Baza danych dziennika zmian wymaga dodatkowo 30 MB wolnego miejsca na dysku. Podczas konfigurowania dziennika zmian do pliku konfiguracyjnego instancji serwera katalogów dodawana jest pozycja dziennika zmian.

# Konfigurowanie dziennika zmian za pomocą programu Configuration Tool

Narzędzie Configuration Tool umożliwia skonfigurowanie bazy danych dziennika zmian dla instancji serwera katalogów.

## Zanim rozpoczniesz

Aby skonfigurować dziennik zmian dla instancji, instancja musi spełniać następujące wymagania:

- Musi istnieć instancja serwera katalogów, dla której skonfigurowano bazę danych DB2. Patrz sekcja “Konfigurowanie bazy danych dla instancji za pomocą narzędzia Configuration Tool” na stronie 174.
- Zatrzymaj serwer katalogów. Patrz sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzia Configuration Tool” na stronie 169.

## Procedura

1. Uruchom narzędzie Configuration Tool dla instancji. Patrz sekcja “Uruchamianie programu Configuration Tool” na stronie 168.
2. Na liście zadań znajdującej się w panelu nawigacyjnym po lewej stronie kliknij opcję **Zarządzanie przyrostkami**.
3. Na stronie **Zarządzanie dziennikiem zmian** wykonaj następujące kroki:
   a. Aby skonfigurować dziennik zmian, wybierz opcję **Włącz bazę danych dziennika zmian**.
   b. W obszarze **Maksymalna liczba pozycji dziennika** podaj maksymalną liczbę pozycji, które mają zostać zarejestrowane w bazie danych dziennika zmian.
      - Aby zarejestrować nieograniczoną liczbę pozycji w dzienniku zmian, kliknij przycisk **Bez ograniczenia**.
      - Aby zarejestrować określoną liczbę pozycji, kliknij przycisk **Pozycje** i podaj liczbę pozycji. Wartością domyślną jest 1.000.000 pozycji.

c. W obszarze **Maksymalny wiek** podaj maksymalną liczbę przedziałów czasu, dla których w bazie danych dziennika zmian mają być przechowywane pozycje.
   - Aby pozycje w dzienniku zmian były przechowywane w nieskończoność, kliknij opcję **Bez ograniczenia**.
   - Aby zapisać pozycje przez konkretny przedział czasu, kliknij opcję **Wiek** i wprowadź liczbę dni i godzin.

d. Aby zastosować zmiany, kliknij przycisk **Aktualizuj**.

e. Aby potwierdzić zakończenie zadania, kliknij przycisk **OK**.

f. Zweryfikuj dzienniki wygenerowane dla konfiguracji bazy danych dziennika zmian.

g. Aby wyczyścić dzienniki, kliknij przycisk **Wyczyść wyniki**.

h. Aby zamknąć stronę **Zarządzanie dziennikiem zmian**, kliknij przycisk **Zamknij**.

4. Aby zamknąć okno programu Configuration Tool, kliknij opcje **Plik > Wyjście**.
5. Aby potwierdzić działanie, kliknij przycisk **Tak**.

### Co dalej

Uruchom serwer katalogów. Patrz sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzia Configuration Tool” na stronie 169.

## Konfigurowanie dziennika zmian za pomocą programu narzędziowego dla wiersza komend

Program narzędziowy dla wiersza komend **idscfgchglg** umożliwia konfigurowanie bazy danych dziennika zmian dla instancji serwera katalogów.

### Zanim rozpoczniesz

Aby skonfigurować dziennik zmian dla instancji, instancja musi spełniać następujące wymagania:

- Musi istnieć instancja serwera katalogów, dla której skonfigurowano bazę danych DB2. Patrz sekcja “Konfigurowanie bazy danych dla instancji za pomocą programu narzędziowego dla wiersza komend” na stronie 178.
- Zatrzymaj serwer katalogów. Patrz sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzi dla wiersza komend” na stronie 157.

### Procedura

1. Zaloguj się jako właściciel instancji serwera katalogów.
2. Otwórz wiersz komend.
3. Zmień bieżący katalog roboczy na podkatalog sbin w miejscu instalacji produktu IBM Security Directory Server.
4. Aby skonfigurować dziennik zmian dla instancji serwera katalogów, uruchom komendę **idscfgchglg**.
   - Aby skonfigurować dziennik zmian dla instancji bez limitu wieku i limitu wielkości, uruchom komendę **idscfgchglg**:

     ```
     idscfgchglg
     -I nazwa_instancji -m 0
     ```

   - Aby skonfigurować dziennik zmian dla instancji o wielkości ograniczonej do 1.000.000 pozycji oraz o wieku pozycji ograniczonym do 25 godzin, uruchom komendę **idscfgchglg**:

     ```
     idscfgchglg -I
     nazwa_instancji -m 1000000 -y 1 -h 1
     ```

Więcej informacji na temat komendy **idscfgchglg** zawiera *Skorowidz komend*.

### Co dalej

Uruchom serwer katalogów. Patrz sekcja "Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzi dla wiersza komend" na stronie 157.

## Dekonfigurowanie dziennika zmian za pomocą programu Configuration Tool

Narzędzie Configuration Tool umożliwia zdekonfigurowanie bazy danych dziennika zmian dla instancji serwera katalogów.

### Zanim rozpoczniesz

Aby zdekonfigurować dziennik zmian dla instancji, instancja musi spełniać następujące wymagania:

- Dziennik zmian dla instancji musi być skonfigurowany. Patrz sekcja "Konfigurowanie dziennika zmian za pomocą programu Configuration Tool" na stronie 197.
- Zatrzymaj serwer katalogów. Patrz sekcja "Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzia Configuration Tool" na stronie 169.

### Procedura

1. Uruchom narzędzie Configuration Tool dla instancji. Patrz sekcja "Uruchamianie programu Configuration Tool" na stronie 168.
2. Na liście zadań znajdującej się w panelu nawigacyjnym po lewej stronie kliknij opcję **Zarządzanie przyrostkami**.
3. Na stronie **Zarządzanie dziennikiem zmian** wykonaj następujące kroki:
   a. Aby zdekonfigurować dziennik zmian, anuluj zaznaczenie opcji **Włącz bazę danych dziennika zmian**.
   b. Aby zastosować zmiany, kliknij przycisk **Aktualizuj**.
   c. W oknie **Zarządzanie dziennikiem zmian** kliknij przycisk **Tak**, aby potwierdzić działanie.
   d. Zweryfikuj dzienniki wygenerowane podczas dekonfigurowania bazy danych dziennika zmian.
   e. Aby wyczyścić dzienniki, kliknij przycisk **Wyczyść wyniki**.
   f. Aby zamknąć stronę **Zarządzanie dziennikiem zmian**, kliknij przycisk **Zamknij**.
4. Aby zamknąć okno programu Configuration Tool, kliknij opcje **Plik > Wyjście**.
5. Aby potwierdzić działanie, kliknij przycisk **Tak**.

### Co dalej

Uruchom serwer katalogów. Patrz sekcja "Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzia Configuration Tool" na stronie 169.

## Dekonfigurowanie dziennika zmian za pomocą programu narzędziowego dla wiersza komend

Program narzędziowy dla wiersza komend **idsucfgchglg** umożliwia zdekonfigurowanie bazy danych dziennika zmian dla instancji serwera katalogów.

### Zanim rozpoczniesz

Aby zdekonfigurować dziennik zmian dla instancji, instancja musi spełniać następujące wymagania:

- Dziennik zmian instancji musi być skonfigurowany. Patrz sekcja “Konfigurowanie dziennika zmian za pomocą programu narzędziowego dla wiersza komend” na stronie 198.
- Zatrzymaj serwer katalogów. Patrz sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzi dla wiersza komend” na stronie 157.

### Procedura

1. Zaloguj się jako właściciel instancji serwera katalogów.
2. Otwórz wiersz komend.
3. Zmień bieżący katalog roboczy na podkatalog sbin w miejscu instalacji produktu IBM Security Directory Server.
4. Aby zdekonfigurować dziennik zmian dla instancji serwera katalogów, uruchom komendę **idsucfgchglg**.

   ```
   idsucfgchglg -I nazwa_instancji
   ```

   Więcej informacji na temat komendy **idsucfgchglg** zawiera *Skorowidz komend*.

### Co dalej

Uruchom serwer katalogów. Patrz sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzi dla wiersza komend” na stronie 157.

## Konfiguracja przyrostka

Aby utworzyć hierarchię katalogów, należy skonfigurować wymagany przyrostek instancji serwera katalogów.

Przyrostek jest kontekstem nazewnictwa. Jest to nazwa wyróżniająca (DN) identyfikująca najwyższą pozycję w hierarchii katalogu. Protokół LDAP używa schematu względnych nazw. Z tego powodu nazwa wyróżniająca jest przyrostkiem wszystkich pozycji w hierarchii katalogu. W serwerze katalogów można dodać wiele przyrostków, każdy identyfikujący hierarchię katalogu. Dodanie przyrostka powoduje dodawanie do pliku konfiguracyjnego pozycji instancji serwera katalogów. Oto przykład pozycji przyrostka: o=test.

Do dodawania i usuwania przyrostków służy narzędzie konfiguracyjne. Do dodawania przyrostków można też użyć komendy **idscfgsuf**, a do usuwania - komendy **idsucfgsuf**. Przed dodaniem lub usunięciem przyrostka należy zatrzymać serwer katalogów. Więcej informacji na temat komend **idscfgsuf** i **idsucfgsuf** zawiera *Skorowidz komend*.

Z instancji serwera katalogów nie można usunąć przyrostków zdefiniowanych przez system. Przyrostki te nie są dostępne w instancjach serwera proxy. Następujące przyrostki są zdefiniowane przez system:

- cn=localhost
- cn=configuration
- cn=ibmpolicies
- cn=Deleted Objects

Podczas dodawania pozycji do serwera katalogów należy rozważyć następujące zagadnienia:

- W serwerze katalogów należy dodać pozycję przyrostka dla nazwy wyróżniającej (DN) przyrostka.
- Pozycja DN dodana do serwera katalogów musi zawierać przyrostek zgodny z wartością przyrostka DN. Następujący przykład przedstawia DN przyrostka: ou=Marketing,o=test.
- Nie można dodawać pozycji w instancji serwera proxy lub w serwerze katalogów, który nie jest skonfigurowany do pracy z bazą danych DB2.

Jeśli zapytanie zawiera przyrostek, który nie jest zgodny z żadnym przyrostkiem skonfigurowanym w lokalnej bazie danych, odnosi się ono do serwera LDAP, który jest identyfikowany przez domyślne odwołanie. Jeśli nie zostało określone żadne domyślne odwołanie LDAP, generowany jest następujący komunikat: Obiekt nie istnieje.

# Dodawanie przyrostka za pomocą narzędzia Configuration Tool

Za pomocą narzędzia Configuration Tool można dodać przyrostek dla instancji.

## Zanim rozpoczniesz

Aby dodać przyrostek dla instancji, należy wykonać następujące działania:

- Zatrzymaj serwer katalogów. Patrz sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzia Configuration Tool” na stronie 169.

## O tym zadaniu

Po dodaniu przyrostka do instancji, pozycja przyrostka jest dodawana do pliku konfiguracyjnego instancji.

## Procedura

1. Uruchom narzędzie Configuration Tool dla instancji. Patrz sekcja “Uruchamianie programu Configuration Tool” na stronie 168.
2. Na liście zadań znajdującej się w panelu nawigacyjnym po lewej stronie kliknij opcję **Zarządzanie przyrostkami**.
3. Na stronie **Zarządzanie przyrostkami** wykonaj następujące działania:
   a. W polu Nazwa DN przyrostka, wpisz przyrostek, który ma zostać dodany do instancji.
   b. Kliknij przycisk **Dodaj**.
   c. Aby zastosować zmiany, kliknij przycisk **OK**.
4. Aby zamknąć okno programu Configuration Tool, kliknij opcje **Plik** > **Wyjście**.
5. Aby potwierdzić działanie, kliknij przycisk **Tak**.

## Co dalej

Uruchom serwer katalogów. Patrz sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzia Configuration Tool” na stronie 169.

# Dodawanie przedrostka za pomocą programu narzędziowego dla wiersza komend

Za pomocą programu narzędziowego dla wiersza komend (**idscfgsuf**) można dodać przyrostek dla instancji.

## Zanim rozpoczniesz

Aby dodać przyrostek dla instancji, należy wykonać następujące działania:

- Zatrzymaj serwer katalogów. Patrz sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzi dla wiersza komend” na stronie 157.

### O tym zadaniu

Po dodaniu przyrostka do instancji, pozycja przyrostka jest dodawana do pliku konfiguracyjnego instancji.

### Procedura

1. Zaloguj się jako właściciel instancji serwera katalogów.
2. Otwórz wiersz komend.
3. Zmień bieżący katalog roboczy na podkatalog sbin w miejscu instalacji produktu IBM Security Directory Server.
4. Aby dodać do instancji przyrostek o=sample, wykonaj komendę **idscfgsuf** w następującym formacie:

   ```
   idscfgsuf -I nazwa_instancji -s "o=sample"
   ```

   Więcej informacji na temat komendy **idscfgsuf** zawiera publikacja *Skorowidz komend*.

### Co dalej

Uruchom serwer katalogów. Patrz sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzi dla wiersza komend” na stronie 157.

## Usuwanie przyrostka za pomocą narzędzia Configuration Tool

Program Configuration Tool umożliwia usunięcie przyrostka z instancji serwera katalogów.

### Zanim rozpoczniesz

Aby usunąć przyrostek z instancji serwera katalogów, należy wykonać następujące działania:

- Zatrzymaj serwer katalogów. Patrz sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzia Configuration Tool” na stronie 169.

### O tym zadaniu

Przy usuwaniu przyrostka z instancji pozycja przyrostka jest usuwana z pliku konfiguracyjnego instancji.

### Procedura

1. Uruchom narzędzie Configuration Tool dla instancji. Patrz sekcja “Uruchamianie programu Configuration Tool” na stronie 168.
2. Na liście zadań znajdującej się w panelu nawigacyjnym po lewej stronie kliknij opcję **Zarządzanie przyrostkami**.
3. Na stronie **Zarządzanie przyrostkami** wykonaj następujące działania:
   a. Z listy **Bieżące nazwy DN przyrostków** wybierz przyrostki, które chcesz usunąć. Dla pełnego serwera katalogów nie można usunąć następujących przyrostków zdefiniowanych dla systemu:
      - cn=localhost
      - cn=configuration
      - cn=ibmpolicies

- cn=Deleted Objects

b. Kliknij przycisk **Usuń**.
c. W oknie potwierdzenia **Zarządzania przyrostkami** kliknij przycisk **OK**
d. Aby zastosować zmiany, kliknij przycisk **OK**.

4. Aby zamknąć okno programu Configuration Tool, kliknij opcje **Plik > Wyjście**.
5. Aby potwierdzić działanie, kliknij przycisk **Tak**.

### Co dalej

Uruchom serwer katalogów. Patrz sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzia Configuration Tool” na stronie 169.

## Usuwanie przyrostka za pomocą programu narzędziowego dla wiersza komend

Za pomocą programu narzędziowego dla wiersza komend (**idsucfgsuf**) można usunąć przyrostek z instancji.

### Zanim rozpoczniesz

Aby usunąć przyrostek z instancji, należy wykonać następujące działania:

- Zatrzymaj serwer katalogów. Patrz sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzia Configuration Tool” na stronie 169.

### O tym zadaniu

Przy usuwaniu przyrostka z instancji pozycja przyrostka jest usuwana z pliku konfiguracyjnego instancji. Dla pełnego serwera katalogów nie można usunąć następujących przyrostków zdefiniowanych dla systemu:

- cn=localhost
- cn=configuration
- cn=ibmpolicies
- cn=Deleted Objects

### Procedura

1. Zaloguj się jako właściciel instancji serwera katalogów.
2. Otwórz wiersz komend.
3. Zmień bieżący katalog roboczy na podkatalog sbin w miejscu instalacji produktu IBM Security Directory Server.
4. Aby usunąć przyrostek o=sample z instancji, uruchom komendę **idsucfgsuf**:

   ```
   idsucfgsuf -I nazwa_instancji -s "o=sample"
   ```

   Więcej informacji na temat komendy **idsucfgsuf** zawiera *Skorowidz komend*.

### Co dalej

Uruchom serwer katalogów. Patrz sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzi dla wiersza komend” na stronie 157.

## Zarządzanie schematem

Jeśli instancja ma obsługiwać niestandardowe obiekty klas i atrybuty, należy dodać definiujący je plik schematu.

Do zarządzania plikami schematów można użyć narzędzia konfiguracyjnego lub komend **idscfgsch** albo **idsucfgsch**. Plik schematu musi istnieć na komputerze. Więcej informacji na temat komend **idscfgsch** i **idsucfgsch** zawiera *Skorowidz komend*.

Przed dodaniem lub usunięciem schematu należy zatrzymać serwer katalogów.

Gdy plik schematu jest dodawany lub usuwany, w pliku konfiguracyjnym instancji aktualizowana jest pozycja schematu. Można uruchomić następujące operacje zarządzania schematami:

- dodawanie pliku schematu do listy plików schematu, które są ładowane podczas uruchamiania serwera,
- usuwanie pliku schematu z listy plików schematu, które są aktualizowane podczas uruchamiania serwera,
- zmienianie typu przeprowadzanego sprawdzania poprawności plików schematu.

Nie można usunąć następujących zdefiniowanych przez system plików schematu:

- V3.config.at
- V3.config.oc
- V3.ibm.at
- V3.ibm.oc
- V3.system.at
- V3.system.oc
- V3.user.at
- V3.user.oc
- V3.ldapsyntaxes
- V3.matchingrules
- V3.modifiedschema

Można też użyć narzędzia konfiguracyjnego do określenia reguł sprawdzających zgodność pozycji ze schematem. Domyślna reguła sprawdzania poprawności schematu: Wersja 3 (sprawdzanie niepełne). Serwer katalogów obsługuje następujące reguły sprawdzania poprawności schematu:

**Wersja 3 (sprawdzanie ścisłe)**
Serwer uruchamia ścisłe sprawdzanie pozycji LDAP wersja 3. Ten typ sprawdzania poprawności wymaga, aby podczas dodawania pozycji obecne były wszystkie nadrzędne klasy obiektów.

**Wersja 3 (sprawdzanie niepełne)**
Serwer uruchamia niepełne sprawdzanie pozycji LDAP wersja 3. Ten typ sprawdzania poprawności nie wymaga, aby podczas dodawania pozycji obecne były wszystkie nadrzędne klasy obiektów. Niepełne sprawdzanie poprawności LDAP wersja 3 jest domyślną regułą sprawdzania poprawności.

**Wersja 2**
Serwer uruchamia sprawdzanie pozycji LDAP wersja 2.

**Brak** Serwer nie wykonuje sprawdzania poprawności.

# Zarządzanie plikiem schematu za pomocą narzędzia Configuration Tool

Za pomocą narzędzia Configuration Tool można zarządzać plikami schematów instancji.

## Zanim rozpoczniesz

Aby zarządzać plikami schematów instancji, należy wykonać następujące działania:

- Zatrzymaj serwer katalogów. Patrz sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzia Configuration Tool” na stronie 169.

## O tym zadaniu

Po dodaniu lub usunięciu pliku schematu, pozycja schematu zostanie zaktualizowana w pliku konfiguracyjnym instancji.

## Procedura

1. Uruchom narzędzie Configuration Tool dla instancji. Patrz sekcja “Uruchamianie programu Configuration Tool” na stronie 168.
2. Na liście zadań znajdującej się w panelu nawigacyjnym po lewej stronie kliknij opcję **Zarządzanie plikami schematu**.
3. Na stronie **Zarządzaj plikami schematów** wybierz operację, która ma zostać wykonana.
   - Aby dodać plik schematu do pliku konfiguracyjnego instancji, wykonaj następujące działania:
     a. W polu **Ścieżka i nazwa pliku** wpisz nazwę pliku wraz z ścieżką. Można również kliknąć plik **Przeglądaj** i wybrać położenie i nazwę pliku.
     b. Kliknij przycisk **Dodaj**.
   - Aby usunąć plik schematu do pliku konfiguracyjnego instancji, wykonaj następujące działania:
     a. Z listy **Bieżące pliki schematów** wybierz plik schematu, który ma zostać usunięty.
     b. Kliknij przycisk **Usuń**.
     c. W oknie potwierdzenia **Zarządzaj plikami schematów** kliknij przycisk **OK**.
4. Aby zastosować zmiany, kliknij przycisk **OK**.
5. Aby zamknąć okno programu Configuration Tool, kliknij opcje **Plik > Wyjście**.
6. Aby potwierdzić działanie, kliknij przycisk **Tak**.

## Co dalej

Uruchom serwer katalogów. Patrz sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzia Configuration Tool” na stronie 169.

# Zarządzanie plikiem schematu za pomocą programu narzędziowego dla wiersza komend

Za pomocą programów narzędziowych wiersza komend można zarządzać plikami schematów instancji serwera katalogów.

## Zanim rozpoczniesz

Aby zarządzać plikami schematów instancji, należy wykonać następujące działania:

- Zatrzymaj serwer katalogów. Patrz sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzi dla wiersza komend” na stronie 157.

### O tym zadaniu

Po dodaniu lub usunięciu pliku schematu, pozycja schematu zostanie zaktualizowana w pliku konfiguracyjnym instancji.

### Procedura

1. Zaloguj się jako właściciel instancji serwera katalogów.
2. Otwórz wiersz komend.
3. Zmień bieżący katalog roboczy na podkatalog sbin w miejscu instalacji produktu IBM Security Directory Server.
4. Aby zarządzać plikami schematów instancji, wybierz operację, która ma zostać wykonana.
   - Aby dodać plik schematu dla instancji, uruchom komendę **idscfgsch** w następującym formacie:

     ```
     idscfgsch -I nazwa_instancji -s plik_schematu.oc
     ```
   - Aby usunąć plik schematu dla instancji, uruchom komendę **idsucfgsch** w następującym formacie:

     ```
     idsucfgsch -I nazwa_instancji -s plik_schematu.oc
     ```

   Więcej informacji na temat komend **idscfgsch** i **idsucfgsch** zawiera *Skorowidz komend*.

### Co dalej

Uruchom serwer katalogów. Patrz sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzi dla wiersza komend” na stronie 157.

## Konfigurowanie sprawdzania poprawności schematu za pomocą programu Configuration Tool

Program Configuration Tool umożliwia skonfigurowanie sprawdzania poprawności schematu dla instancji.

### Zanim rozpoczniesz

Aby skonfigurować regułę sprawdzania poprawności schematu dla instancji, należy wykonać następujące kroki:

- Zatrzymaj serwer katalogów. Patrz sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzia Configuration Tool” na stronie 169.

### O tym zadaniu

Przy konfigurowaniu sprawdzania poprawności schematu plik konfiguracyjny instancji zostaje zaktualizowany o wartość.

### Procedura

1. Uruchom narzędzie Configuration Tool dla instancji. Patrz sekcja “Uruchamianie programu Configuration Tool” na stronie 168.

2. Na liście zadań znajdującej się w panelu nawigacyjnym po lewej stronie kliknij opcję **Zarządzanie plikami schematu**.
3. W obszarze **Reguły sprawdzania poprawności schematu** na stronie **Zarządzanie plikami schematu** wybierz jedną z następujących reguł sprawdzania poprawności schematu do skonfigurowania:
   - Aby skonfigurować ścisłe sprawdzanie poprawności LDAP w wersji 3, kliknij opcję **Wersja 3 (sprawdzanie ścisłe)**.
   - Aby skonfigurować niepełne sprawdzanie poprawności LDAP w wersji 3, kliknij opcję **Wersja 3 (sprawdzanie niepełne)**.
   - Aby skonfigurować sprawdzanie LDAP w wersji 2, kliknij opcję **Wersja 2**.
   - Aby skonfigurować sprawdzanie LDAP w wersji 2, kliknij opcję **Brak**.
4. Aby zastosować zmiany, kliknij przycisk **OK**.
5. Aby zamknąć okno programu Configuration Tool, kliknij opcje **Plik > Wyjście**.
6. Aby potwierdzić działanie, kliknij przycisk **Tak**.

### Co dalej

Uruchom serwer katalogów. Patrz sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzia Configuration Tool” na stronie 169.

## Zarządzanie danymi LDIF

Aby można było używać dane katalogu, należy dodać dane do instalacji serwera katalogów z istniejącej instancji lub z pliku LDIF (LDAP Data Interchange Format).

Do zaimportowania danych z pliku LDIF lub do wyeksportowania danych z bazy danych do pliku LDIF można użyć programu konfiguracyjnego. Format LDIF jest używany do reprezentowania pozycji LDAP w formie tekstowej. Podczas importowania można dodawać pozycje do pustej bazy danych katalogu lub do bazy danych zawierającej już pozycje. Narzędzia konfiguracyjnego można używać także do sprawdzania poprawności danych zawartych w pliku w formacie LDIF bez rzeczywistego dodawania danych do katalogu.

Dane mogą być dodawane do instancji, która jest skonfigurowana do działania z bazą danych DB2. Nie można dodawać danych katalogu do instancji serwera proxy, ponieważ nie jest to obsługiwane.

Aby zaimportować dane w formacie LDIF z innej instancji serwera, należy kryptograficznie zsynchronizować instancje. Należy synchronizować dwukierunkowe szyfrowanie między instancjami serwera katalogów, aby zmniejszyć czas wymagany do szyfrowania i deszyfrowania danych w komunikacji między serwerami. Podczas importowania danych LDIF, które nie są kryptograficznie zsynchronizowane, pozycje w pliku zaszyfrowane algorytmem AES nie są importowane. Więcej informacji na temat synchronizowania dwukierunkowego szyfrowania zawiera *Skorowidz komend*.

Jeśli instancje serwera nie są kryptograficznie zsynchronizowane, podaj klucz początkowy (seed) i dodatkowy (salt) szyfrowania serwera docelowego, eksportując plik LDIF z serwera źródłowego. Dane zaszyfrowane algorytmem AES są deszyfrowane za pomocą kluczy AES serwera źródłowego, a następnie są szyfrowane z użyciem początkowego i dodatkowego klucza szyfrowania serwera docelowego. Tak zaszyfrowane dane zostaną zapisane do pliku w formacie LDIF.

Aby zaimportować dane, należy przed rozpoczęciem procesu spełnić następujące wymagania:

- Importowanie lub eksportowanie danych LDIF nie jest obsługiwana dla instancji serwera proxy lub instancji, która nie jest skonfigurowana do działania z bazą danych DB2.

- Dodaj wymagane przyrostki na serwerze docelowym, do którego chcesz zaimportować dane. Patrz sekcja “Konfiguracja przyrostka” na stronie 200.
- Należy zatrzymać serwer docelowy, do którego mają zostać zaimportowane dane.

Po zakończeniu ładowania dużych ilości danych, takich jak zapełnianie bazy danych za pomocą komendy **idsbulkload**, należy zoptymalizować bazę danych. Ta operacja może zwiększyć wydajność bazy danych.

Można także użyć interfejsu wiersza komend w celu zaimportowania, wyeksportowania lub sprawdzenia poprawności danych LDIF:

- Aby zaimportować dane z pliku w formacie LDIF, użyj komendy **idsldif2db** lub programu narzędziowego **idsbulkload**.
- Aby wyeksportować dane do pliku w formacie LDIF, należy użyć programu narzędziowego **idsdb2ldif**.
- Aby sprawdzić poprawność danych znajdujących się w pliku w formacie LDIF, należy użyć programu narzędziowego **idsbulkload**.

Więcej informacji na temat programów narzędziowych wiersza komend zawiera *Skorowidz komend*.

### Przykłady

Aby pobrać wartość dodatkowego klucza szyfrowania serwera, uruchom komendę **idsldapsearch** w następującym formacie:

```
idsldapsearch -h nazwa_hosta -p port -D DN_administratora -w Hasło_administratora \
 -b "cn=crypto,cn=localhost" objectclass=* ibm-slapdCryptoSalt

ibm-slapdCryptoSalt=:SxaQ+.qdKor
```

Tekst po znaku równości (=) za atrybutem ibm-slapdCryptoSalt jest dodatkowym kluczem szyfrowania (salt). W tym przykładzie jest to :SxaQ+.qdKor.

## Importowanie danych LDIF za pomocą programu Configuration Tool

W celu zaimportowania danych do instancji serwera katalogu z pliku LDIF należy użyć programu Configuration Tool.

### Zanim rozpoczniesz

Aby zaimportować dane z pliku w formacie LDIF do instancji, instancja musi spełniać następujące wymagania:

- Musi istnieć instancja serwera katalogów, dla której skonfigurowano bazę danych DB2. Patrz sekcja “Konfigurowanie bazy danych dla instancji za pomocą narzędzia Configuration Tool” na stronie 174.
- Muszą istnieć skonfigurowane wymagane pozycje przyrostka. Patrz sekcja “Dodawanie przyrostka za pomocą narzędzia Configuration Tool” na stronie 201.
- Zatrzymaj serwer katalogów. Patrz sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzia Configuration Tool” na stronie 169.

### Procedura

1. Uruchom narzędzie Configuration Tool dla instancji. Patrz sekcja “Uruchamianie programu Configuration Tool” na stronie 168.

2. Na liście zadań znajdującej się na lewym panelu nawigacyjnym kliknij opcję **Zadania LDIF > Importowanie danych w formacie LDIF**.
3. Na stronie **Importowanie danych w formacie LDIF** wykonaj następujące kroki:
   a. W polu **Nazwa i ścieżka pliku LDIF** podaj ścieżkę i nazwę pliku LDIF, z którego chcesz zaimportować dane. Możesz również kliknąć przycisk **Przeglądaj** i wybrać plik oraz katalog.
   b. Jeśli chcesz usunąć końcowe znaki spacji z danych, zaznacz opcję **Usuń końcowe znaki spacji w opcji Standardowy import lub Bulkload**.
   c. W zależności od liczby pozycji, które chcesz zaimportować, wybierz odpowiednią opcję:
      - Aby zaimportować dane za pomocą programu narzędziowego **idsldif2db**, kliknij opcję **Standardowy import**. Użyj tej opcji, jeśli plik LDIF zawiera niewiele pozycji.
      - Aby zaimportować dane za pomocą programu narzędziowego **idsbulkload**, kliknij opcję **Bulkload**. W przypadku plików LDIF z dużą liczbą pozycji importowanie danych za pomocą programu narzędziowego **idsbulkload** jest szybsze niż za pomocą programu narzędziowego **idsldif2db**.
   d. Jeśli do zaimportowania danych została wybrana opcja **Bulkload**, podaj typy sprawdzenia poprawności, jakie mają zostać uruchomione dla danych LDIF.
      1) Aby sprawdzić zgodność danych LDIF ze schematem, wybierz opcję **Włącz sprawdzenie schematu**.
      2) Aby sprawdzić, czy dane LDIF zawierają odpowiednie listy ACL, wybierz opcję **Włącz sprawdzenie list ACL**.
   e. Aby uruchomić operację importowania, kliknij przycisk **Importuj**.
   f. Aby potwierdzić zakończenie zadania, kliknij przycisk **OK**.
   g. Zweryfikuj dzienniki wygenerowane dla operacji importowania pliku LDIF.
   h. Aby wyczyścić dzienniki, kliknij przycisk **Wyczyść wyniki**.
   i. Aby zamknąć stronę **Importowanie danych w formacie LDIF**, kliknij przycisk **Zamknij**.
4. Aby zamknąć okno programu Configuration Tool, kliknij opcje **Plik > Wyjście**.
5. Aby potwierdzić działanie, kliknij przycisk **Tak**.

### Co dalej

Uruchom serwer katalogów. Patrz sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzia Configuration Tool” na stronie 169. Po zakończeniu ładowania dużych ilości danych, takich jak zapełnianie bazy danych za pomocą komendy **idsbulkload**, należy zoptymalizować bazę danych. Więcej informacji o optymalizowaniu bazy danych zawiera sekcja “Optymalizowanie bazy danych za pomocą programu Configuration Tool” na stronie 184.

## Sprawdzenie poprawności danych LDIF za pomocą programu Configuration Tool

Program Configuration Tool umożliwia sprawdzania poprawności danych zawartych w pliku w formacie LDIF bez rzeczywistego dodawania danych do bazy danych.

### Zanim rozpoczniesz

Aby sprawdzić poprawność danych umieszczonych w pliku LDIF w odniesieniu do schematu serwera katalogów, instancja musi spełniać następujące wymagania:

- Musi istnieć instancja serwera katalogów, dla której skonfigurowano bazę danych DB2. Patrz sekcja “Konfigurowanie bazy danych dla instancji za pomocą narzędzia Configuration Tool” na stronie 174.
- Zatrzymaj serwer katalogów. Patrz sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzia Configuration Tool” na stronie 169.

### Procedura

1. Uruchom narzędzie Configuration Tool dla instancji. Patrz sekcja “Uruchamianie programu Configuration Tool” na stronie 168.
2. Na liście zadań znajdującej się na lewym panelu nawigacyjnym kliknij opcję **Zadania LDIF > Importowanie danych w formacie LDIF**.
3. Na stronie **Importowanie danych w formacie LDIF** wykonaj następujące kroki:
   a. W polu **Nazwa i ścieżka pliku LDIF** podaj ścieżkę i nazwę pliku LDIF, z którego chcesz zaimportować dane. Możesz również kliknąć przycisk **Przeglądaj** i wybrać plik oraz katalog.
   b. Kliknij przycisk **Tylko sprawdzanie poprawności danych**.
   c. Aby uruchomić operację sprawdzania poprawności danych, kliknij przycisk **Importuj**.
   d. Aby potwierdzić zakończenie zadania, kliknij przycisk **OK**.
   e. Zweryfikuj dzienniki wygenerowane dla operacji sprawdzania poprawności.
   f. Aby wyczyścić dzienniki, kliknij przycisk **Wyczyść wyniki**.
   g. Aby zamknąć stronę **Importowanie danych w formacie LDIF**, kliknij przycisk **Zamknij**.
4. Aby zamknąć okno programu Configuration Tool, kliknij opcje **Plik > Wyjście**.
5. Aby potwierdzić działanie, kliknij przycisk **Tak**.

### Co dalej

Uruchom serwer katalogów. Patrz sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzia Configuration Tool” na stronie 169.

## Eksportowanie danych LDIF za pomocą programu Configuration Tool

Program Configuration Tool umożliwia wyeksportowanie danych katalogu z instancji serwera do pliku LDIF.

### Zanim rozpoczniesz

Aby wyeksportować dane z instancji do pliku w formacie LDIF, instancja musi spełniać następujące wymagania:

- Musi istnieć instancja serwera katalogów, dla której skonfigurowano bazę danych DB2. Patrz sekcja “Konfigurowanie bazy danych dla instancji za pomocą narzędzia Configuration Tool” na stronie 174.
- Instancja musi zawierać pozycje katalogu.

### Procedura

1. Uruchom narzędzie Configuration Tool dla instancji. Patrz sekcja “Uruchamianie programu Configuration Tool” na stronie 168.
2. Na liście zadań znajdującej się na lewym panelu nawigacyjnym kliknij opcję **Zadania LDIF > Eksportuj dane do pliku LDIF**.

3. Na stronie **Eksportowanie danych do pliku LDIF** wykonaj następujące kroki:
   a. W polu **Nazwa i ścieżka pliku LDIF** podaj ścieżkę i nazwę pliku LDIF, do którego chcesz wyeksportować dane. Możesz również kliknąć przycisk **Przeglądaj** i wybrać plik oraz katalog.
   b. Jeśli plik istnieje i chcesz go nadpisać, zaznacz opcję **Nadpisz jeśli plik istnieje**.
   c. Jeśli chcesz wyeksportować atrybuty operacyjne, takie jak creatorsName, createTimestamp, modifiersName i modifyTimestamp, zaznacz opcję **Eksportuj atrybuty operacyjne**. Atrybuty operacyjne są tworzone i modyfikowane przez serwer w chwili, gdy pozycja katalogu jest tworzona lub zmodyfikowana. Zawierają one informacje na temat użytkownika, który utworzył lub zmodyfikował pozycję, oraz o czasie utworzenia lub modyfikacji pozycji. Pozycje te zapisane są w pliku LDIF jako pola sterujące zakodowane w standardzie base-64-encoded.
   d. Aby zaimportować dane do serwera docelowego obsługującego AES (Advanced Encryption Standard) i jeśli serwer ten nie jest kryptograficznie zsynchronizowany z serwerem źródłowym, wybierz opcję **Eksportuj dane dla serwera docelowego z obsługą AES**.
   e. Aby wyeksportować pozycje, które zostały usunięte, ale są nadal przechowywane w poddrzewie obiektów reliktowych, wybierz opcję **Eksportuj usunięte pozycje**. Więcej informacji na temat poddrzewa obiektów reliktowych znajduje się w sekcji Administrowanie dokumentacji produktu IBM Security Directory Server.
   f. Jeśli wybrano opcję **Eksportuj dane dla serwera docelowego z obsługą AES**, określ następujące wartości:
      - W polu **Klucz początkowy szyfrowania** wprowadź klucz początkowy szyfrowania dla serwera docelowego.
      - W polu **Klucz dodatkowy szyfrowania** wprowadź klucz dodatkowy szyfrowania dla serwera docelowego. Więcej informacji na temat sposobu pobierania dodatkowego klucza szyfrowania zawiera sekcja “Zarządzanie danymi LDIF” na stronie 207.
   g. Aby określić filtr dla pozycji, które są eksportowane do pliku LDIF, wprowadź nazwę DN dla poprawnego filtru replikacji w polu **Nazwa DN pozycji filtru**. Filtr umożliwia wyeksportowanie do pliku LDIF tylko pozycji bazy danych, które spełniają podane kryteria. Więcej informacji na temat filtrów replikacji znajduje się w sekcji Administrowanie dokumentacji produktu IBM Security Directory Server.
   h. Aby dodać komentarze do pliku LDIF, wpisz komentarz w polu **Komentarze**.
   i. Jeśli chcesz wyeksportować pozycje należące do określonego poddrzewa, podaj w polu **Nazwa DN poddrzewa** nazwę DN tego poddrzewa. Nazwa DN poddrzewa określa najwyższy punkt w poddrzewie, które ma zostać zapisane do pliku LDIF. Poddrzewo i wszystkie pozycje poniżej niego w hierarchii katalogów zostaną zapisane do pliku. Jeśli użytkownik nie określi nazwy DN poddrzewa, do pliku wyjściowego zostaną zapisane wszystkie pozycje katalogu, które są przechowywane w bazie danych. Pozycje są identyfikowane na podstawie przyrostków, które są podane w pliku konfiguracyjnym instancji serwera katalogów.
   j. Aby uruchomić operację eksportowania, kliknij przycisk **Eksportuj**.
   k. Aby potwierdzić zakończenie zadania, kliknij przycisk **OK**.
   l. Zweryfikuj dzienniki wygenerowane dla operacji eksportowania danych do pliku LDIF.
   m. Aby wyczyścić dzienniki, kliknij przycisk **Wyczyść wyniki**.
   n. Aby zamknąć stronę **Eksportowanie danych do pliku LDIF**, kliknij przycisk **Zamknij**.
4. Aby zamknąć okno programu Configuration Tool, kliknij opcje **Plik > Wyjście**.
5. Aby potwierdzić działanie, kliknij przycisk **Tak**.

## Synchronizowanie z Active Directory

Istnieje możliwość synchronizowania pozycji kontenerów użytkowników i grup utworzonych w programie Microsoft Active Directory z instancją produktu IBM Security Directory Server. Synchronizacja danych jest jednokierunkowa: z Active Directory do instancji serwera katalogów.

**Uwaga:** W produkcie IBM Security Directory Server od wersji 6.3.1 synchronizacja z Active Directory jest funkcją nieaktualną. Zamiast tego należy użyć rozwiązania LDAPSync.

Do skonfigurowania i uruchamiania synchronizacji z Active Directory można użyć narzędzia konfiguracyjnego lub komend **idsadscfg** i **idsadsrun**.

**Uwaga:** Synchronizacja użytkowników i grup z Active Directory do instancji IBM Security Directory Server za pośrednictwem serwera proxy produktu BM Security Directory nie jest obsługiwana.

Funkcja synchronizacji z Active Directory używa programu IBM Security Directory Integrator do synchronizowania kontenerów użytkowników i grup. Program IBM Security Directory Integrator należy zainstalować przed użyciem funkcji synchronizacji z Active Directory.

Program IBM Security Directory Integrator jest niezbędny do wykonania następujących działań:

- Uruchamianie konfigurowania
- Uruchamianie, zatrzymywanie, restartowanie i monitorowanie operacji

Konfigurując synchronizację z Active Directory, należy wziąć pod uwagę następujące informacje:

- Aplikacja synchronizacji z Active Directory i program IBM Security Directory Integrator muszą być na tym samym komputerze, co instancja serwera katalogów.
- Narzędzie synchronizacji z Active Directory przeprowadza wyłącznie synchronizację kontenerów użytkowników i grup. Narzędzie nie synchronizuje innych obiektów ani kontenerów.
- Rozwiązanie również sprawdza przynależność pozycji użytkownika do grup. Pozycja użytkownika jest dodawana do wszystkich grup w instancji, które są synchronizowane z Active Directory. Gdy istniejąca pozycja użytkownika jest przenoszona poza kontener użytkowników, zostanie ona usunięta z instancji. Pozycja użytkownika jest również usuwana ze wszystkich grup w instancji.
- Narzędzie synchronizacji z Active Directory nie synchronizuje zagnieżdżonych jednostek organizacyjnych (ou).
- Nie można odwzorować wielu atrybutów z katalogu Active Directory na jeden atrybut instancji serwera katalogów.
- Atrybut userpassword w Active Directory nie może być odwzorowany na instancję serwera katalogów. W tym rozwiązaniu hasła użytkowników nie są synchronizowane.
- Synchronizacja z Active Directory umożliwia synchronizację użytkowników i grup z jednego lub kilku kontenerów Active Directory z jedną jednostką organizacyjną (ou) serwera katalogów. Narzędzie nie synchronizuje jednak wielu kontenerów użytkowników i grup z Active Directory z jednostką organizacyjną (ou) serwera katalogów.
- Można określić kilka kontenerów użytkowników, które mają być synchronizowane z jedną jednostką organizacyjną (ou) serwera katalogów, stosując jako separator znak średnika (;). Używanie innych separatorów nie jest obsługiwane. Używając średnika (;) jako separatora, należy ująć argumenty w cudzysłów ("). Poniżej zamieszczono przykład stosowana

średnika (;) jako separatora:
"ou=SWUGroups,dc=adsync,dc=com;ou=STGGroups,dc=adsync,dc=com".

- Atrybut SAMAccountName z Active Directory jest używany do utworzenia atrybutu $dn w programie IBM Security Directory Server. Atrybut SAMAccountName jest unikalny w domenie, podczas synchronizowania wielu kontenerów użytkowników Active Directory do jednej jednostki organizacyjnej serwera katalogów nie będą występować konflikty.
- Rozwiązanie obsługuje bezpieczne połączenie z Active Directory, ale nie obsługuje bezpiecznego połączenia z instancją serwera katalogów.
- Jeśli po skonfigurowaniu synchronizacji z Active Directory przeprowadzona zostanie zmiana nazwy DN lub hasła administratora instancji serwera katalogów, synchronizację należy zrekonfigurować.
- Jeśli kontenery użytkowników lub grup w Active Directory zostały zmienione podczas synchronizowania, należy ponownie skonfigurować synchronizację z Active Directory, używając zmienionych nazw. W przeciwnym razie synchronizacja z Active Directory może przestać działać.
- Jeśli użytkownicy lub grupy w programie IBM Security Directory Server zostaną zmodyfikowane z użyciem innego narzędzia niż narzędzie do synchronizacji z Active Directory, synchronizacja ta może przestać działać poprawnie.

# Konfigurowanie i uruchamianie synchronizacji z Active Directory

Aby zsynchronizować kontenery użytkowników i grup Active Directory z instancją produktu IBM Security Directory Server, należy skonfigurować i uruchomić synchronizację Active Directory.

## Zanim rozpoczniesz

Aby skonfigurować i uruchomić synchronizację Active Directory, należy zainstalować następujące oprogramowanie:

- IBM Security Directory Server
- IBM Security Directory Integrator

## Procedura

1. Jeśli produkt IBM Security Directory Integrator został zainstalowany w ścieżce niestandardowej, należy ustawić ścieżkę instalacji w zmiennej środowiskowej *IDS_LDAP_TDI_HOME*.

   **Uwaga:** W systemie Windows należy ustawić zmienną środowiskową ze ścieżką instalacji, która nie zawiera spacji i cudzysłowów. Przy podawaniu ścieżki należy użyć nazwy skróconej.
   Poniższa ścieżka jest domyślną ścieżką instalacji produktu IBM Security Directory Integrator:

   **AIX i Solaris**
   /opt/IBM/TDI/V7.1

   **Linux** /opt/ibm/TDI/V7.1

   **Windows**
   C:\Program Files\IBM\TDI\V7.1
2. Opcjonalne: Załaduj przykładowe pliki users.ldif oraz groups.ldif do Active Directory.

3. Uruchom komendę **idsadscfg** w celu skonfigurowania synchronizacji Active Directory. Do skonfigurowania synchronizacji Active Directory można również uruchomić narzędzie Configuration Tool. Komenda utworzy pliki adsync_private.prop oraz adsync_public.prop.
4. Zmodyfikuj plik adsync_public.prop, aby dostosować opcjonalne atrybuty i parametry SSL. Więcej informacji na temat bezpiecznej komunikacji znajduje się w sekcji *Administrowanie* w dokumentacji serwera IBM Security Directory Server.
5. Uruchom komendę **idsadsrun**, aby rozpocząć synchronizację Active Directory. Komenda wyświetli zapytanie, czy wykonać pełną synchronizację, a następnie synchronizację w czasie rzeczywistym, czy uruchomić synchronizację w czasie rzeczywistym. Narzędzie do synchronizacji Active Directory identyfikuje zmiany pozycji Active Directory i synchronizuje je z pozycjami w produkcie IBM Security Directory Server.
6. Opcjonalne: Uruchom konsolę administrowania i monitorowania produktu IBM Security Directory Integrator do administrowania synchronizacją i jej monitorowania.

# Konfigurowanie synchronizacji z katalogiem Active Directory za pomocą narzędzia Configuration Tool

Za pomocą narzędzia Configuration Tool można skonfigurować synchronizację katalogu Active Directory z instancją serwera katalogów.

## Zanim rozpoczniesz

Aby skonfigurować synchronizację z Active Directory, muszą być spełnione następujące wymagania:

- Zainstaluj serwer IBM Security Directory Integrator.
- Zatrzymaj serwer katalogów. Patrz sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzia Configuration Tool” na stronie 169.

## Procedura

1. Uruchom narzędzie Configuration Tool dla instancji. Patrz sekcja “Uruchamianie programu Configuration Tool” na stronie 168.
2. Na liście zadań znajdującej się w panelu nawigacyjnym po lewej stronie kliknij opcję **Synchronizacja Active Directory**.
3. Na stronie **Synchronizacja Active Directory: szczegóły instancji** podaj szczegóły konfiguracyjne instancji produktu IBM Security Directory Server. Podane informacje zostaną zapisane w plikach adsync_private.properties i adsync_public.properties. Pliki znajdują się w podkatalogu etc/tdisoldir katalogu głównego instancji.
4. W polu **Przyrostek katalogu** wpisz przyrostek serwera katalogu, który ma być używany podczas synchronizowania z katalogiem Active Directory. W polu **Adres URL LDAP** zostanie wyświetlony adres URL instancji serwera katalogów. Nie można modyfikować tego pola.
5. W polu **Nazwa DN pozycji kontenera grup** wpisz nazwę DN kontenera, do którego mają być skopiowane grupy z Active Directory. Grupy oraz przynależność użytkowników do grup są synchronizowane pomiędzy Active Directory i serwerem IBM Security Directory Server. Po dodaniu lub usunięciu użytkownika z grupy w Active Directory, pozycja jest również dodawana lub usuwana z odpowiedniej grupy w instancji serwera IBM Security Directory Server.
6. W polu **Nazwa DN pozycji kontenera użytkowników** wpisz nazwę DN kontenera, do którego mają być skopiowani użytkownicy z Active Directory.

7. Aby w połączeniach z Active Directory korzystać z protokołu SSL, zaznacz pole wyboru **Połączenie SSL z katalogiem Active Directory**. Połączenie SSL z serwerem IBM Security Directory Server nie jest obsługiwane. Informacje na temat procedury służącej do konfigurowania połączenia SSL z Active Directory znajdują się w sekcji *Administrowanie* dokumentacji produktu IBM Security Directory Server.
8. Kliknij przycisk **Dalej**. Zostanie otwarta strona **Synchronizacja z Active Directory: szczegóły dotyczące Active Directory**.
9. W polu **Adres hosta** wpisz nazwę hosta lub adres IP kontrolera domeny Active Directory.
10. W polu **Port hosta** wpisz port używany przez Active Directory.
11. W polu **Nazwa użytkownika** wpisz nazwę logowania, którą IBM Security Directory Integrator musi powiązać z katalogiem Active Directory. Ten identyfikator musi dysponować wystarczającymi uprawnieniami umożliwiającymi odczyt pozycji Active Directory, które należy przesłać do instancji serwera katalogów.
12. W polu Hasło wpisz hasło, które IBM Security Directory Integrator musi powiązać z katalogiem Active Directory.
13. W polu **Podstawa wyszukiwania** wpisz poddrzewo Active Directory, z którego zmiany będą propagowane do instancji. Zmiany w pozycjach użytkowników z tego poddrzewa będą propagowane do instancji serwera katalogów. Aby propagować do instancji wszystkich użytkowników w grupach Active Directory, ustaw jako podstawę wyszukiwania szczyt hierarchii Active Directory.
14. W polu **Nazwa DN pozycji kontenera grup** wpisz nazwę DN kontenera Active Directory, z którego mają być synchronizowane grupy z instancją.
15. W polu **Nazwa DN pozycji kontenera użytkowników** wpisz nazwę DN kontenera Active Directory, z którego mają być synchronizowani użytkownicy z instancją.
16. Kliknij przycisk **Zakończ**. Otwarte zostanie okno **Synchronizacja z Active Directory: wyniki**.
17. Sprawdź komunikaty dziennika utworzone dla konfiguracji synchronizacji z Active Directory.
18. Aby wyczyścić dzienniki, kliknij przycisk **Wyczyść wyniki**.
19. Aby zamknąć stronę **Synchronizacja z Active Directory**, kliknij przycisk **Zamknij**.
20. Aby zamknąć okno programu Configuration Tool, kliknij opcje **Plik > Wyjście**.
21. Aby potwierdzić działanie, kliknij przycisk **Tak**.

# Konfigurowanie synchronizacji z katalogiem Active Directory za pomocą programu narzędziowego dla wiersza komend

Za pomocą programu narzędziowego dla wiersza komend (**idsadscfg**) można skonfigurować synchronizację katalogu Active Directory z instancją serwera katalogów.

## Zanim rozpoczniesz

Aby skonfigurować synchronizację z Active Directory, muszą być spełnione następujące wymagania:

- Zainstaluj serwer IBM Security Directory Integrator.
- Zatrzymaj serwer katalogów. Patrz sekcja “Uruchamianie i zatrzymywanie serwera katalogów i serwera administracyjnego za pomocą narzędzi dla wiersza komend” na stronie 157.

## Procedura

1. Zaloguj się jako użytkownik root w systemach AIX, Linux lub Solaris i jako członek grupy administratorów w systemie Windows.

2. Otwórz wiersz komend.
3. Zmień bieżący katalog roboczy na podkatalog sbin w miejscu instalacji produktu IBM Security Directory Server.
4. Aby skonfigurować synchronizację Active Directory z instancją, wykonaj komendę **idsadscfg** w następującym formacie:

   ```
   idsadscfg -I nazwa_instancji -adH ldap://LDAP_server1:389 -adb dc=adsynctest,dc=com
   -adD cn=administrator,cn=users,dc=adsynctest,dc=com -adw secret -adg ou=testgroup1,
   dc=adsynctest,dc=com -adu ou=testuser1,dc=adsynctest,dc=com -idss o=sample -idsg
   ou=Testgroup1,ou=groups,o=sample -idsu ou=Testuser1,ou=users,o=sample
   ```

   Więcej informacji na temat komendy **idsadscfg** zawiera publikacja *Skorowidz komend*.

## Co dalej

Uruchom komendę **idsadsrun**, aby rozpocząć synchronizację Active Directory. Więcej informacji na temat komendy **idsadsrun** zawiera publikacja *Skorowidz komend*.

# Rozdział 21. Automatyczne uruchamianie instancji serwera katalogów podczas uruchamiania systemu operacyjnego

Można skonfigurować instancje serwera katalogów do automatycznego uruchamiania, gdy komputer jest restartowany po tym, jak został zamknięty w celu przeprowadzenia konserwacji lub aktualizacji.

Gdy tworzona jest instancja serwera katalogów, serwer administracyjny jest uruchamiany, jeśli tworzenie instancji się powiodło. Aby uruchomić serwer katalogów wraz z bazą danych DB2, należy uruchomić procesu ibmslapd lub idsslapd dla instancji.

Gdy komputer jest restartowany, należy uruchomić zarówno serwer administracyjny, jak i proces ibmslapd powiązany z instancją. Można też skonfigurować automatyczne uruchamianie wraz z systemem operacyjnym usług i procesów powiązanych z instancją.

Aby w systemach AIX, Linux lub Solaris skonfigurować automatyczne uruchamianie instancji serwera katalogów, należy odpowiednio zaktualizować plik /etc/inittab. Plik inittab definiuje procesy, które muszą być uruchamiane podczas uruchamiania systemu i działać podczas normalnej pracy systemu. Do pliku inittab należy dodać wpis opisujący serwer katalogów w następującym formacie:

```
id:poziomy_działania:działanie:proces
```

Znaczenie atrybutów w pliku inittab jest następujące:

**id** Unikalny identyfikator w tym pliku składający się z 1-4 cyfr.

**poziomy_działania**
Atrybut poziomy_działania wskazuje tryb poziomu działania (runlevel) systemu operacyjnego, w którym proces jest automatycznie uruchamiany. Poziom działania odnosi się do trybu działania systemu operacyjnego AIX, Linux lub Solaris. Konfiguracja atrybutu poziomy_działania przebiega odmiennie w zależności od systemu operacyjnego. Szczegółowe informacje dotyczące konfigurowania poziomu działania (runlevel) używanego systemu operacyjnego zawiera jego dokumentacja.

**działanie**
Atrybut działanie określa typ działania.

**proces**
Atrybut proces określa, który proces ma być uruchamiany.

## Konfigurowanie automatycznego uruchamiania dla instancji serwera katalogów w systemie Windows

W oknie **Usługi** można skonfigurować automatyczne uruchamianie instancji serwera katalogów w systemie Windows.

### Zanim rozpoczniesz

Aby skonfigurować automatyczne uruchamianie instancji serwera katalogów po uruchomieniu systemu operacyjnego, komputer musi spełniać następujące wymagania:

- Komputer musi zawierać instancję serwera katalogów, która może być uruchomiona w trybie normalnym.

## O tym zadaniu

W systemie Windows można uruchomić serwer katalogów (proces idsslapd) w oknie **Usługi** lub za pomocą komendy **idsslapd**. Dla instancji serwera katalogów z bazą danych DB2, należy ustawić usługę powiązaną z serwerem katalogów w zależności od usługi instancji DB2. Dla instancji serwera katalogów z bazą danych DB2, należy uruchomić bazę danych DB2 przed uruchomieniem procesu idsslapd. Jeśli nie zostanie ustawiona zależność i dla usługi powiązanej z serwerem w polu **Typ uruchomienia** zostanie wybrana wartość Automatyczny, może wystąpić błąd podczas restartowania komputera. Dla instancji serwera proxy nie trzeba konfigurować zależności dla usługi powiązanej z instancją bazy danych DB2.

Dla instancji serwera proxy użyj kroków 1, 2, 4, 5 i 6.

## Procedura

1. Zaloguj się jako członek grupy administratorów.
2. Aby otworzyć okno **Usługi**, wykonaj następujące działania:
   a. Kliknij opcje **Start > Uruchom**.
   b. W polu **Otwórz** wpisz services.msc.
   c. Kliknij przycisk **OK**.
3. Znajdź nazwę usługi DB2 powiązanej z instancją serwera katalogów, która ma być uruchamiana automatycznie. Nazwa usługi powinna rozpoczynać się od DB2 - SDSV631DB2 -. Jeśli nazwa instancji bazy danych DB2 to DSRDBM01, pozycja tej jej usługi ma nazwę DB2 - SDSV631DB2 - DSRDBM01. Kliknij dwukrotnie usługę i zapamiętaj wartość występującą po DB2 - SDSV631DB2 - w polu **Wyświetlana nazwa**. W tym przykładzie będzie to DSRDBM01.
4. Znajdź usługę dla instancji serwera katalogów, która ma być uruchamiana automatycznie. Nazwa usługi rozpoczyna się od IBM Security Directory Server Instance 6.3.1. Jeśli nazwa instancji to dsrdbm01, pozycja ma nazwę IBM Security Directory Server Instance 6.3.1 - dsrdbm01. Kliknij dwukrotnie usługę i zapamiętaj wartość występującą po IBM Security Directory Server Instance 6.3.1 - w polu **Wyświetlana nazwa**. W tym przykładzie dla instancji dsrdbm01 będzie to idsslapd-dsrdbm01.
5. W oknie właściwości usługi IBM Security Directory Server Instance 6.3.1 - dsrdbm01 w polu **Typ uruchomienia** wybierz wartość Automatyczny.
6. Kliknij przycisk **OK**.
7. Aby zamknąć okno **Usługi** kliknij opcje **Plik > Zakończ**.
8. Aby otworzyć rejestr systemu Windows, wykonaj następujące działania:
   a. Kliknij opcje **Start > Uruchom**.
   b. W polu **Otwórz** wpisz regedit.
   c. Kliknij przycisk **OK**.
9. W panelu nawigacyjnym po lewej stronie kliknij pozycje **Komputer > HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Services**.
10. Znajdź usługę powiązaną z instancją serwera katalogów. W tym przykładzie jest to idsslapd-dsrdbm01.
11. Kliknij usługę powiązaną z instancją serwera katalogów.
12. W panelu po prawej stronie kliknij dwukrotnie atrybut DependOnService.
13. W oknie **Edytowanie ciągu** dodaj nazwę usługi DB2 powiązanej z instancją wymienioną w sekcji **LanmanServer**. W tym przykładzie jest to DSRDBM01.
14. Kliknij przycisk **OK**. Zostanie utworzona zależność od usługi DB2.

15. Aby zamknąć rejestr Windows, kliknij opcje **Plik > Zakończ**.

### Wyniki

Po zrestartowaniu komputera, instancja serwera katalogów zostanie uruchomiona automatycznie.

## Konfigurowanie automatycznego uruchamiania dla instancji serwera katalogów w systemie UNIX

Zaktualizuj w pliku /etc/inittab pozycje serwera katalogów, aby skonfigurować automatyczne uruchamianie instancji serwera katalogów w systemie AIX, Linux lub Solaris.

### Zanim rozpoczniesz

Aby skonfigurować automatyczne uruchamianie instancji serwera katalogów po uruchomieniu systemu operacyjnego, komputer musi spełniać następujące wymagania:

- Komputer musi zawierać instancję serwera katalogów, która może być uruchomiona w trybie normalnym.

### Procedura

1. Zaloguj się jako użytkownik root.
2. Aby skonfigurować automatyczne uruchamianie instancji serwera katalogów lub instancji serwera proxy, dodaj do pliku /etc/inittab następujące pozycje:
   a. Aby dodać proces idsslapd i serwer administracyjny powiązany z instancją serwera katalogów, dodaj następujące pozycje:

      **AIX** srv1:2:once:/opt/IBM/ldap/V6.3.1/sbin/idsslapd -I *nazwa_instancji* > /dev/null 2>&1 #Autostart IBM Directory Server Instance

      adm1:2:once:/opt/IBM/ldap/V6.3.1/sbin/ibmdiradm -I *nazwa_instancji* > /dev/null 2>&1 #Autostart IBM Directory Administartion Server

      **Linux** srv1:2345:once:/opt/ibm/ldap/V6.3.1/sbin/ibmslapd -I *nazwa_instancji* > /dev/null 2>&1 #Autostart IBM Directory Server Instance

      adm1:2345:once:/opt/ibm/ldap/V6.3.1/sbin/ibmdiradm -I *nazwa_instancji* > /dev/null 2>&1 #Autostart IBM Directory Administartion Server

      **Solaris** srv1:234:once:/opt/IBM/ldap/V6.3.1/sbin/ibmslapd -I *nazwa_instancji* > /dev/null 2>&1 #Autostart IBM Directory Server Instance

      adm1:234:once:/opt/IBM/ldap/V6.3.1/sbin/ibmdiradm -I *nazwa_instancji* > /dev/null 2>&1 #Autostart IBM Directory Administartion Server

      Zastąp zmienną *nazwa_instancji* nazwą instancji.

   b. Aby dodać proces idsslapd i serwer administracyjny powiązany z instancją serwera proxy, należy najpierw uruchomić instancje serwera katalogów. Przed uruchomieniem serwera proxy należy uruchomić wszystkie serwery katalogów z bazą danych DB2. Jeśli komputer zawiera pełne serwery katalogów oraz serwer proxy, dodaj opóźnienie między uruchomieniem pełnego serwera katalogów i serwera proxy. W poniższym przykładzie w pliku /etc/inittab wprowadzono opóźnienie w postaci dodatkowej pozycji w formacie id:2345:wait.

**AIX** srv1:2345:once:/opt/IBM/ldap/V6.3.1/sbin/idsslapd -I *nazwa_instancji_1* > /dev/null 2>&1 #Autostart IBM Directory Server Instance

adm1:2345:once:/opt/IBM/ldap/V6.3.1/sbin/ibmdiradm -I *nazwa_instancji_1* > /dev/null 2>&1 #Autostart IBM Directory Administartion Server

srv2:2345:once:/opt/IBM/ldap/V6.3.1/sbin/idsslapd -I *nazwa_instancji_2* > /dev/null 2>&1 #Autostart IBM Directory Server Instance

adm2:2345:once:/opt/IBM/ldap/V6.3.1/sbin/ibmdiradm -I *nazwa_instancji_2* > /dev/null 2>&1 #Autostart IBM Directory Administartion Server

srv3:2345:wait:/opt/IBM/ldap/V6.3.1/sbin/idsslapd -I *instancja_proxy_1* -k > /dev/null 2>&1 #Autostart IBM Directory Proxy Server Instance

adm3:2345:wait:/opt/IBM/ldap/V6.3.1/sbin/ibmdiradm -I *instancja_proxy_1* -k > /dev/null 2>&1 #Autostart IBM Directory Administartion Server

srv4:2345:wait:/opt/IBM/ldap/V6.3.1/sbin/idsslapd -I *instancja_proxy_1* > /dev/null 2>&1 #Autostart IBM Directory Proxy Server Instance

adm4:2345:wait:/opt/IBM/ldap/V6.3.1/sbin/ibmdiradm -I *instancja_proxy_1* > /dev/null 2>&1 #Autostart IBM Directory Administartion Server

Zastąp zmienne *nazwa_instancji_1* i *nazwa_instancji_1* nazwami instancji serwera katalogów. Zastąp zmienną *instancja_proxy_1* nazwą instancji serwera proxy.

## Wyniki

Po dodaniu pozycji do pliku /etc/inittab, instancja serwera katalogów (pełna lub proxy) będzie automatycznie uruchamiania po uruchomieniu systemu.

# Rozdział 22. Strategia związana ze strategią poprawek

Poniżej znajdują się informacje na temat pakietów poprawek produktu IBM Security Directory Server.

Dla systemów AIX, Linux, Solaris i HP-UX dostępne są poprawki lub pakiet poprawek dla instalacji rodzimej z użyciem skryptu.

W systemie Windows dostępne są poprawki i pakiety poprawek instalowane za pomocą programu IBM Installation Manager.

Poprawki i pakiety poprawek instalowane za pomocą IBM Installation Manager mogą być instalowane z użyciem interfejsu GUI lub w trybie instalacji cichej.

Za pomocą programu IBM Installation Manager można określić wersję zainstalowanej poprawki lub pakietu poprawek:

- Wybierz opcje **Plik > Wyświetl zainstalowane pakiety**.
- Użyj komendy **imcl** znajdującej się w podkatalogu tools w katalogu instalacyjnym programu IBM Installation Manager.

W systemach UNIX sprawdź wersję pakietów rodzimych, aby określić wersję zainstalowanej poprawki lub pakietu poprawek.

**Uwaga:** Po zastosowaniu w wersji podstawowej rodzimego pakietu poprawek, nie można wykonywać żadnych zmian za pomocą programu IBM Installation Manager. Po zastosowaniu rodzimego pakietu poprawek dalsze operacje mogą być wykonywane tylko w trybie rodzimym.

## Instalowanie pakietów poprawek przy użyciu programu IBM Installation Manager

Program IBM Installation Manager pozwala na instalowanie pakietów poprawek lub udoskonaleń w systemach operacyjnych Microsoft Windows.

### Zanim rozpoczniesz

- Zapoznaj się z informacjami na temat strategii pakietów poprawek.
- Upewnij się, że w systemie zainstalowany jest program IBM Installation Manager w wersji 1.7.0 lub nowszej. Patrz serwis IBM Installation Manager Documentation.
- Przed zainstalowaniem pakietu poprawek należy zatrzymać wszystkie uruchomione procesy i usługi produktu IBM Security Directory Server. Można to zrobić ręcznie, można też kliknąć opcję **Stop all blocking processes** (Zatrzymaj wszystkie blokujące procesy) w programie Installation Manager.

### O tym zadaniu

Pakiet poprawek aktualizuje tylko te funkcje, które były wcześniej zainstalowane. Produkt należy zaktualizować przed użyciem kreatora **Modyfikuj** w celu zainstalowania nowych funkcji.

Pakiet poprawek nie aktualizuje następujących komponentów: IBM DB2, IBM GSKit, IBM WebSphere Application Server (wersja wbudowana), IBM Java Development Kit. Do zaktualizowania tego oprogramowania należy użyć kreatora **Modyfikuj**.

## Procedura

1. Pobierz pakiet poprawek z serwisu http://www-01.ibm.com/support/docview.wss?uid=swg21496581#v631.
2. Ustaw preferencje repozytorium w programie IBM Installation Manager.
   a. Aby uruchomić program IBM Installation Manager, z menu **Start** wybierz kolejno opcje **Wszystkie programy > IBM Installation Manager > IBM Installation Manager**.
   b. Na stronie Start programu IBM Installation Manager kliknij kolejno opcje **File > Preferences**.
   c. Na stronie Repositories (Repozytoria) kliknij opcję **Add Repository** (Dodaj repozytorium).
   d. Na stronie Add Repository (Dodaj repozytorium) podaj położenia jednego z następujących repozytoriów:
      - Ścieżka lokalnego katalogu lub zdalnego dysku sieciowego z pakietem produktu pobranym z serwisu wsparcia IBM.
      - Adres URL repozytorium na serwerze WWW.
   e. Kliknij przycisk **OK**. Jeśli podano lokalizację repozytorium HTTPS lub repozytorium wymagającego logowania, a następnie należy wprowadzić ID użytkownika i hasło. Zostanie wyświetlona lokalizacja nowego lub zmienionego repozytorium.
   f. Aby sprawdzić poprawność dostępu repozytorium, kliknij przycisk **Test Connections**.
   g. Kliknij przycisk **OK**, aby zamknąć stronę Repositories.
3. Uruchom instalację.
   - Jeśli produkt IBM Security Directory Server 6.3.1 nie jest zainstalowany w systemie, wykonaj następujące czynności:
     a. Na stronie Start (Uruchamianie) programu IBM Installation Manager kliknij opcję **Install** (Zainstaluj). Kreator **instalowania** przeprowadza użytkownika przez proces instalowania.
     b. Wykonaj procedurę instalacji opisaną w sekcji “Instalowanie przy użyciu programu IBM Installation Manager” na stronie 31.
   - Jeśli produkt IBM Security Directory Server 6.3.1 jest już zainstalowany w systemie, wykonaj następujące czynności, aby zainstalować pakiet poprawek:
     a. Na stronie Start (Uruchamianie) programu IBM Installation Manager kliknij opcję **Update** (Zaktualizuj). Kreator **aktualizowania** wyszukuje dostępne aktualizacje pakietów zainstalowanych w systemie.
     b. Wybierz opcję **IBM Security Directory Server**. Wyświetlony katalog instalacyjny jest katalogiem instalacyjnym wersji 6.3.1 produktu i nie można go zmienić. Kliknij przycisk **Dalej**.
     c. Wybierz produkt **IBM Security Directory Server** do zaktualizowania, następnie wybierz poprawkę (**wersja 6.3.1.5**). Kliknij przycisk **Dalej**.
     d. Zaakceptuj licencję pakietu poprawek i kliknij przycisk **Dalej**.
     e. Domyślnie wybrane są funkcje, które mogą być zaktualizowane. Tylko te funkcje, które zostały wcześniej zainstalowane w systemie, są wyświetlane. Kliknij przycisk **Dalej**.

        **Uwaga:** Anulowanie zaznaczenia funkcji oznacza, że funkcja zostanie odinstalowana.

        **Ograniczenie:** Pomimo tego, że baza danych IBM DB2 jest wyświetlana na stronie jako funkcja do aktualizowania, nie jest ona aktualizowana. Oprogramowanie wymagane wstępnie nie jest aktualizowane przez kreator

**aktualizacji** programu IBM Installation Manager. Nie anuluj zaznaczenia opcji IBM DB2, gdyż spowoduje to wyczyszczenie funkcji serwera.

f. Przejrzyj informacje wyświetlane na stronie podsumowania, następnie kliknij przycisk **Dalej**, aby rozpocząć instalowanie.

4. Sprawdź poprawność instalacji. Więcej informacji na temat sprawdzania poprawności za pomocą programu IBM Installation Manager w używanym systemie operacyjnym zawiera sekcja Rozdział 13, “Sprawdzanie funkcji serwera IBM Security Directory Server”, na stronie 83.

### Co dalej

Aby odinstalować pakiet poprawek, należy użyć kreatora **Roll Back** (Wycofaj), który przywraca poprzednią wersję pakietu.

## Instalacja pakietów poprawek w trybie cichym

Program IBM Installation Manager może być użyty do zainstalowania pakietów poprawek w trybie cichym.

**Uwaga:** W pliku odpowiedzi dla aktualizacji nie można podać funkcji, która nie jest zainstalowana. Podanie niezainstalowanej funkcji spowoduje, że proces się nie powiedzie.

### Wygeneruj nowy plik odpowiedzi dla instalacji pakietu poprawek.

Jeśli plik odpowiedzi, który był użyty do instalacji produktu, nie jest dostępny, utwórz nowy plik odpowiedzi.

1. Uruchom program IBM Installation Manager w trybie symulowania instalacji. Na przykład:

   ```
   C:\Program Files\IBM\Installation Manager\eclipse\IBMIM.exe
        -record c:\SDS_6310\install_resp.xml -skipInstall położenie
   ```

   gdzie

   *położenie* jest miejscem, w którym przechowywane są dane instalowanego produktu.

2. Ustaw preferencje repozytorium na wersję 6.3.1.0.
3. Dokończ proces symulowanej instalacji.
4. Zamknij program IBM Installation Manager. Został utworzony plik odpowiedzi bez instalowania produktu.
5. Wykonaj czynności opisane w następnej sekcji.

### Zainstaluj z użyciem pliku odpowiedzi użytego podczas instalowania produktu

1. Zmodyfikuj plik odpowiedzi install_resp.xml, wprowadzając następujące zmiany:
   a. Zaktualizuj ścieżkę repozytorium, podając ścieżkę repozytorium dla wersji 6.3.1.5.

      ```
      <repository location='C:\SDS_6315\ibm_sds'/>
      ```

   b. Zaktualizuj wersję oferty do 6.3.1.5.

      ```
      <offering id='com.ibm.security.directoryserver.v631' version='6.3.1.5' profile=.......
      ```

2. Uruchom instalację cichą, aby zainstalować pakiet poprawek. Na przykład:

   ```
   C:\Program Files\IBM\Installation Manager\eclipse\tools\imcl.exe
        input c:\SDS_6310\install_resp.xml -acceptLicense -showProgress
   ```

   W tej komendzie można też użyć opcji -stopBlockingProcesses, aby bezwarunkowo zatrzymać blokujące wszystkie procesy przed zainstalowaniem pakietu poprawek.

# Instalowanie pakietów poprawek przy użyciu skryptów rodzimych

Uruchom w wierszu komend podany skrypt, aby zainstalować pakiety poprawek lub zainstalować udoskonalenia serwisowe w systemach AIX, Linux, i Solaris.

## Zanim rozpoczniesz

Zapoznaj się z informacjami na temat strategii pakietów poprawek.

## Procedura

1. Pobierz pakiet poprawek z serwisu http://www-01.ibm.com/support/docview.wss?uid=swg21496581#v631.
2. Wyodrębnij archiwum pakietu poprawek do katalogu, w którym jest wystarczająca ilość wolnego miejsca. Szczegółowe informacje na temat zawartości pakietu poprawek, w tym nazwy katalogów i plików, znajdują się w pliku *README* dostarczanym wraz z pakietem poprawek.
3. Zatrzymaj wszystkie procesy klienta i serwera produktu IBM Security Directory Server. Zestaw procesów obejmuje serwer katalogów, serwer administracyjny, serwer proxy (jeśli jest używany) i niestandardowe aplikacje LDAP. Nie można zastąpić programów i bibliotek w czasie, gdy są one używane. Jeśli śledzenie jest włączone, uruchom komendę **ldtrc off**, aby je wyłączyć. Więcej informacji na temat zatrzymywania instalacji serwera katalogów i procesów administracyjnych zawiera dokumentacja produktu IBM Security Directory Server w sekcji Podstawowe zadania administracyjne serwera.
4. W wierszu komend przejdź do katalogu, w którym wyodrębniono archiwum poprawek.
5. Wydaj następującą komendę jako użytkownik root:

   ```
   idsinstall -u -f
   ```

   Program instalacyjny zainstaluje aktualizacje już zainstalowanych komponentów.
6. Sprawdź poprawność instalacji.
   a. Program instalacyjny wyświetla komunikat informujący o tym, czy instalacja się powiodła. Sprawdź dziennik instalacji /tmp/idsinstall_*datownik*.
   b. Jeśli instalacja się nie powiodła albo jeśli wyświetlony został komunikat, że nie wszystkie pakiety zostały zainstalowane, popraw błędy opisane w dzienniku instalacji, na przykład zwiększ ilość wolnego miejsca na dysku. Następnie ponownie uruchom program instalacyjny i upewnij się, że wszystkie pakiety zostały pomyślnie zainstalowane.
   c. Sprawdź numery wersji pakietów, upewniając się, że są one poprawne. Instrukcje zawiera sekcja Rozdział 6, “Odpytywanie o pakiety serwera IBM Security Directory Server”, na stronie 45.

# Rozdział 23. Deinstalowanie IBM Security Directory Server: przegląd

Przeczytaj przegląd informacji na temat deinstalowania produktu IBM Security Directory Server i ważne punkty, które należy rozważyć przed deinstalacją.

## Zanim rozpoczniesz

Aby zdeinstalować produkt IBM Security Directory Server, zaloguj się jako użytkownik z uprawnieniami root w systemie AIX, Linux, Solaris lub HP-UX albo jako członek grupy administratorów w systemie Windows.

## O tym zadaniu

Podczas deinstalowania produktu IBM Security Directory Server nie są usuwane instancje i ich pliki konfiguracyjne.

## Procedura

1. Zatrzymaj wszystkie procesy klienta i serwera IBM Security Directory Server, w tym serwer katalogów, demon administracyjny i niestandardowe aplikacje LDAP. Nie można zastąpić programów i bibliotek w czasie, gdy są one używane. Jeśli włączono śledzenie, wykonaj komendę **ldtrc off**, aby je wyłączyć.
2. W zależności od systemu operacyjnego i trybu, w którym zainstalowano produkt IBM Security Directory Server, należy użyć tego samego trybu do zdeinstalowania produktu IBM Security Directory Server. Dostępne metody deinstalacji pakietów produktu IBM Security Directory Server:
   a. Program deinstalacyjny w interfejsie GUI.
   b. Programy narzędziowe systemu operacyjnego. Nazwy pakietów w systemie Linux są trochę inne w przypadku aktualizacji, niż w przypadku wersji GA. Na przykład, nazwa pakietu klienta podstawowego w wersji GA w systemie xSeries Linux to idsldap-cltbase63-6.3.0-0.i386.rpm. Za pomocą komendy **rpm -qa** można wyświetlić listę wszystkich pakietów.
3. Po zdeinstalowaniu produktu IBM Security Directory Server, sprawdź, czy pomyślnie usunięto wszystkie pakiety produktu IBM Security Directory Server. Aby uzyskać więcej informacji, patrz Rozdział 6, “Odpytywanie o pakiety serwera IBM Security Directory Server”, na stronie 45.

**Informacje pokrewne**:

http://www-01.ibm.com/support/knowledgecenter/SSVJJU/welcome
Więcej informacji znajduje się w rozdziale *Deinstalowanie produktu IBM Security Directory Server* w sekcji *Instalowanie i konfigurowanie* dokumentacji produktu IBM Security Directory Server.

# Rozdział 24. Deinstalowanie serwera IBM Security Directory Server i innego wymaganego oprogramowania

Jeśli komputer ma być wykorzystany w innym celu, można usunąć z niego produkt IBM Security Directory Server i powiązane oprogramowanie.

Aby zdeinstalować produkt IBM Security Directory Server, można użyć programu IBM Installation Manager lub programów narzędziowych systemu operacyjnego. Należy zdeinstalować produkt w tym samym trybie, w którym został zainstalowany. Jeśli zainstalowano produkt za pomocą IBM Installation Manager, należy zdeinstalować produkt również za pomocą programu IBM Installation Manager. Nie można mieszać trybów instalacji i deinstalacji.

Przed usunięciem z komputera produktu IBM Security Directory Server należy wziąć pod uwagę następujące warunki:

1. Należy zatrzymać wszystkie procesy klienta i serwera IBM Security Directory Server.
   - Serwer katalogów
   - Serwer administracyjny
   - Śledzenie LDAP
   - Narzędzie Web Administration Tool i powiązany z nim serwer aplikacji
   - Niestandardowe aplikacje LDAP
2. Jeśli na komputerze ma być ponownie zainstalowany produkt IBM Security Directory Server, nie trzeba usuwać instancji serwera katalogów ani dekonfigurować z instancji bazy danych DB2. Jeśli produkt IBM Security Directory Server zostanie usunięty z komputera, instancje serwera katalogów pozostaną bez zmian do momentu samodzielnego ich usunięcia lub zdekonfigurowania.
3. Po deinstalacji użytkownik idsldap i grupa utworzona podczas instalacji produktu IBM Security Directory Server pozostają w systemie. Przed deinstalacją produktu IBM Security Directory Server z systemów AIX, Linux i Solaris należy wziąć pod uwagę dodatkowe warunki.
   - Jeśli użytkownik idsldap i zdefiniowana grupa nie są potrzebne, należy usunąć te elementy za pomocą programów narzędziowych systemu operacyjnego. Użytkownik idsldap i grupa są wymagane przez serwer proxy oraz pełny serwer katalogów i muszą znajdować się na komputerze, jeśli zainstalowany jest produkt IBM Security Directory Server.
   - Jeśli zostanie usunięty użytkownik idsldap, ale nie zostanie usunięty jego katalog osobisty, mogą wystąpić problemy z utworzeniem użytkownika idsldap podczas instalowania produktu IBM Security Directory Server. Z tego powodu, jeśli użytkownik idsldap zostanie usunięty, należy usunąć jego katalog osobisty. Jeśli użytkownik idsldap będzie usuwany za pomocą komendy **userdel**, należy pamiętać, aby użyć parametru **-r** w celu usunięcia jego katalogu osobistego (userdel -r idsldap).
4. W systemie Windows usługi serwera administracyjnego i serwera katalogów są usuwane podczas deinstalowania produktu IBM Security Directory Server. Usługi nie są zastępowane podczas instalowania produktu IBM Security Directory Server. Można użyć komendy **idsslapd** w celu dodania usługi serwera i komendy **idsdiradm** w celu dodania usługi serwera administracyjnego. Więcej informacji na temat komend **idsslapd** i **idsdiradm** znajduje się w publikacji *IBM Security Directory Server - Spis komend*.

# Deinstalowanie przy użyciu programu IBM Installation Manager

Jeśli produkt IBM Security Directory Server został zainstalowany za pomocą programu IBM Installation Manager, należy użyć tego programu do zdeinstalowania produktu IBM Security Directory Server i jego komponentów.

Podczas deinstalowania produktu IBM Security Directory Server za pomocą programu IBM Installation Manager, usuwany jest produkt IBM Security Directory Server i całe oprogramowanie, które było z nim zainstalowane. Podczas deinstalacji za pomocą programu IBM Installation Manager nie można wybrać, które funkcje produktu IBM Security Directory Server zostaną usunięte.

Jeśli zainstalowano bazę danych IBM DB2 dostarczoną z produktem IBM Security Directory Server, należy usunąć wszystkie instancje DB2, które zostały utworzone przez kopię DB2. Jeśli na komputerze pozostanie instancja bazy danych DB2, która została utworzone przez kopię DB2, podczas deinstalacji produktu IBM Security Directory Server baza danych DB2 nie zostanie usunięta. IBM Installation Manager rejestruje komunikaty o błędach w pliku dziennika.

Instalacja, modyfikacja i deinstalacja produktu IBM Security Directory Server i jego komponentów musi być wykonywana w tym samym trybie (za pomocą produktu IBM Installation Manager lub programów narzędziowych systemu operacyjnego). Nie można zainstalować, zmodyfikować lub zdeinstalować produktu IBM Security Directory Server, używając programu IBM Installation Manager i programów narzędziowych systemu operacyjnego.

## Deinstalacja przy użyciu programu IBM Installation Manager

Program IBM Installation Manager umożliwia wykonanie deinstalacji produktu IBM Security Directory Server, jeśli program ten został użyty do jego zainstalowania.

### Zanim rozpoczniesz

Należy zatrzymać wszystkie procesy klienta i serwera IBM Security Directory Server.

- Serwer katalogów
- Serwer administracyjny
- Śledzenie LDAP
- Niestandardowe aplikacje LDAP

Jeśli którykolwiek proces jest używany, nie można usunąć programów i bibliotek.

### Procedura

1. Uruchom program IBM Installation Manager.
   - AIX i Linux:
     a. Otwórz okno wiersza komend i przejdź do katalogu, który zawiera program IBM Installation Manager. Następujący katalog jest domyślnym położeniem instalacji programu IBM Installation Manager:
        ```
        opt/IBM/InstallationManager/eclipse
        ```
     b. Uruchom komendę:
        ```
        ./IBMIM
        ```
   - Microsoft Windows:
     a. Kliknij kolejno opcje **Start > Wszystkie programy > IBM Installation Manager > IBM Installation Manager**.

2. Kliknij przycisk **Deinstaluj**.
3. Wybierz opcję **IBM Security Directory Server** i odpowiednią wersję, a następnie kliknij przycisk **Dalej**.
4. W oknie **Deinstalacja pakietów** sprawdź pakiety wybrane do zdeinstalowania.

   **Ważne:** Jeśli podczas instalowania wybrana zostanie opcja użycia istniejącej wersji bazy danych DB2 albo pakietu GSKit, program IBM Installation Manager zaktualizuje odpowiednio swój rejestr. Podczas usuwania funkcji zainstalowanej z użyciem opcji **Kontynuuj z istniejącą**, program Installation Manager wykonuje następujące działania:

   - Pozycja funkcji jest usuwana z rejestru programu IBM Installation Manager.
   - Funkcja nie jest deinstalowana z komputera.

   Jeśli istnieją instancje DB2 utworzone za pomocą kopii bazy danych DB2 zainstalowanej przy użyciu programu IBM Installation Manager, nie można usunąć produktu IBM Security Directory Server. W takiej sytuacji należy samodzielnie usunąć instancje DB2, a następnie spróbować ponownie. Zaleca się wykonanie kopii zapasowej bazy danych przed usunięciem instancji DB2.
5. Kliknij przycisk **Deinstaluj**. Po zakończeniu deinstalacji program IBM Installation Manager informuje, czy zakończyła się ona powodzeniem.
6. Opcjonalne: Jeśli podczas deinstalacji wystąpi błąd, kliknij opcję **Wyświetl plik dziennika**, aby zapoznać się ze szczegółami. Aby uzyskać więcej informacji, patrz Rozdział 5, “Pliki dziennika programu IBM Installation Manager”, na stronie 43.
7. Kliknij przycisk **Zakończ**.
8. Kliknij kolejno opcje **Plik > Wyjście**.

### Wyniki

Program IBM Installation Manager wykona deinstalację produktu IBM Security Directory Server oraz jego komponentów.

## Deinstalacja cicha przy użyciu pliku odpowiedzi

Wykonaj poniższe czynności, aby wykonać deinstalację komponentów produktu IBM Security Directory Server w trybie cichym przy użyciu pliku odpowiedzi.

### Zanim rozpoczniesz

Do wykonania cichej instalacji pakietów produktu IBM Security Directory Server wymagany jest program IBM Installation Manager w wersji 1.7.0 lub nowszej.

### O tym zadaniu

Można użyć domyślnego pliku odpowiedzi lub zarejestrować zmodyfikowany plik odpowiedzi i użyć go jako pliku wejściowego dla cichej deinstalacji.

### Procedura

1. Zaloguj się do systemu jako administrator.
2. Uzyskaj dostęp do komendy **IBMIM** w katalogu instalacyjnym IBM Installation Manager.

| System operacyjny | Domyślne położenie komendy IBMIM: |
|---|---|
| **Microsoft Windows** | C:\Program Files\IBM\InstallationManager\eclipse |
| **AIX i Linux** | /opt/IBM/InstallationManager/eclipse |

3. Opcjonalne: Uruchom komendę **IBMIM**, aby zarejestrować plik odpowiedzi dla deinstalacji cichej.
   a. Uruchom następujące komendy w różnych systemach operacyjnych:

      **Microsoft Windows**
      IBMIM.exe -record *ścieżka\uninstall_responseFile.xml* -skipInstall *agentDataLocation*

      **AIX i Linux**
      ./IBMIM -record *ścieżka/uninstall_responseFile.xml* -skipInstall *agentDataLocation*

      Ta komenda uruchamia program IBM Installation Manager.
   b. Wykonaj rejestrowanie operacji deinstalacji produktu IBM Security Directory Server Więcej informacji na ten temat zawiera krok 2 na stronie 229.
4. Uruchom komendę **IBMIM**, aby uruchomić deinstalację cichą z plikiem odpowiedzi podanym jako dane wejściowe.

| System operacyjny | Komenda do uruchomienia: |
|---|---|
| **Microsoft Windows** | IBMIM.exe -silent -input *ścieżka\uninstsll_responseFile.xml* -noSplash |
| **AIX i Linux** | ./IBMIM -silent -input *ścieżka/uninstall_responseFile.xml* -noSplash |

5. Sprawdź podsumowanie deinstalacji i pliki dziennika.

| System operacyjny | Domyślna ścieżka dziennika: |
|---|---|
| **Microsoft Windows** | C:\ProgramData\IBM\InstallationManager\logs |
| **AIX i Linux** | /var/ibm/InstallationManager/logs/ |

6. Sprawdź, czy pakiety produktu IBM Security Directory Server zostały zdeinstalowane.

| System operacyjny | Weryfikowanie pakietów: |
|---|---|
| **Microsoft Windows** | Patrz sekcja “Weryfikowanie funkcji serwera IBM Security Directory Server w systemie Windows” na stronie 83. |
| **AIX i Linux** | Patrz sekcja “Weryfikowanie pakietów serwera katalogów IBM Security” na stronie 85. |

### Wyniki

Program IBM Installation Manager wykona cichą deinstalację komponentów produktu IBM Security Directory Server.

## Deinstalowanie w trybie cichym za pomocą komendy imcl uninstall

Wykonaj poniższe czynności, aby wykonać deinstalację komponentów produktu IBM Security Directory Server w trybie cichym za pomocą komendy **imcl uninstall**.

### Zanim rozpoczniesz

Do wykonania cichej instalacji pakietów produktu IBM Security Directory Server wymagany jest program IBM Installation Manager w wersji 1.7.0 lub nowszej.

### O tym zadaniu

Można użyć komendy **imcl uninstall** do zdeinstalowania produktu IBM Security Directory Server w trybie cichym.

### Procedura

1. Zaloguj się do systemu jako administrator.
2. 
3. Uruchom komendę **imcl listInstalledPackages** z katalogu <*katalog_instalacyjny_IBM_Installation_Manager*>/eclipse/tools.

| System operacyjny | Komenda do uruchomienia: |
|---|---|
| **Microsoft Windows** | imcl.exe listInstalledPackages |
| **AIX i Linux** | ./imcl listInstalledPackages |

   Ta komenda wyświetla listę wszystkich pakietów zainstalowanych przez program IBM Installation Manager.
4. Uruchom komendę **imcl uninstall com.ibm.security.directoryserver.v631_6.3.1.0**. Użyj pozycji dla serwera Security Directory, która będzie znajdować się w danych wyjściowych podanej powyżej komendy **imcl listInstalledPackages**.

| System operacyjny | Komenda do uruchomienia: |
|---|---|
| **Microsoft Windows** | imcl.exe uninstall com.ibm.security.directoryserver.v631_6.3.1.0 |
| **AIX i Linux** | ./imcl uninstall com.ibm.security.directoryserver.v631_6.3.1.0 |

### Wyniki

Program IBM Installation Manager wykona cichą deinstalację komponentów produktu IBM Security Directory Server.

## Deinstalacja serwera IBM Security Directory Server za pomocą programów narzędziowych systemu operacyjnego

Jeśli produkt IBM Security Directory Server został zainstalowany za pomocą programów narzędziowych systemu operacyjnego, należy go zdeinstalować również za pomocą programów narzędziowych systemu operacyjnego.

Za pomocą programów narzędziowych systemu operacyjnego można zdeinstalować produkt IBM Security Directory Server z komputerów z systemem operacyjnym AIX, Linux, Solaris lub HP-UX. W systemie Windows produkt IBM Security Directory Server należy instalować i deinstalować za pomocą programu IBM Installation Manager. Informacje na ten temat zawiera sekcja “Deinstalacja przy użyciu programu IBM Installation Manager” na stronie 228.

Jeśli do zdeinstalowania produktu IBM Security Directory Server zostaną użyte programy narzędziowe systemu operacyjnego, program usunie z komputera produkt IBM Security Directory Server. Podczas deinstalowania produktu IBM Security Directory Server można wybrać funkcje, które zostaną usunięte.

Przed zdeinstalowaniem produktu IBM Security Directory Server należy zatrzymać wszystkie procesy klienta i serwera IBM Security Directory Server.

- Serwer katalogów
- Serwer administracyjny
- Śledzenie LDAP
- Narzędzie Web Administration Tool i powiązany z nim serwer aplikacji
- Niestandardowe aplikacje LDAP

Jeśli utworzono i skonfigurowano instancję serwera katalogów z bazą danych DB2, ani serwer ani baza danych nie są usuwane podczas deinstalowania produktu IBM Security Directory Server za pomocą programów narzędziowych systemu operacyjnego.

# Deinstalowanie z użyciem programów narzędziowych w systemie AIX

Za pomocą programów narzędziowych wiersza komend systemu AIX można zdeinstalować produkt IBM Security Directory Server z systemu AIX.

Do zdeinstalowania produktu IBM Security Directory Server można użyć jednego z następujących programów narzędziowych:

**SMIT** Jest to preferowana metoda deinstalacji. Aby uzyskać więcej informacji, patrz "Deinstalacja za pomocą programu SMIT".

**installp**
Aby uzyskać więcej informacji, patrz "Deinstalacja za pomocą komendy **installp**" na stronie 233.

## Deinstalacja za pomocą programu SMIT

Użyj komendy **smit**, aby wykonać deinstalację produktu IBM Security Directory Server z systemu AIX.

### Zanim rozpoczniesz

Należy zatrzymać wszystkie procesy klienta i serwera IBM Security Directory Server.

- Serwer katalogów
- Serwer administracyjny
- Śledzenie LDAP
- Narzędzie Web Administration Tool i powiązany z nim serwer aplikacji
- Niestandardowe aplikacje LDAP

### Procedura

1. Zaloguj się do systemu jako użytkownik root.
2. Otwórz wiersz komend.
3. Uruchom komendę **smit**. Zostanie otwarte okno **Instalacja i konserwacja oprogramowania**.
4. Wybierz opcję **Instalacja i konserwacja oprogramowania > Obsługa oprogramowania i narzędzia**.

5. Wybierz opcję **Usuń zainstalowane oprogramowanie**.
6. W polu **Nazwa oprogramowania** naciśnij klawisz **F4**, aby wyświetlić listę zainstalowanego oprogramowania. Możesz podać wartość idsldap w polu, aby wyświetlić wszystkie pakiety IBM Security Directory Server.
7. Wybierz pakiety, które chcesz usunąć, i naciśnij klawisz Enter.

### Wyniki

Program narzędziowy SMIT usuwa serwer IBM Security Directory Server z systemu AIX. Jeśli wybrano usunięcie wszystkich pakietów serwera IBM Security Directory Server, program narzędziowy usuwa również jego katalog instalacyjny /opt/IBM/ldap/6.3.1 z systemu AIX.

### Co dalej

Sprawdź, czy deinstalacja produktu IBM Security Directory Server powiodła się. Aby uzyskać więcej informacji, patrz sekcja “Weryfikowanie pakietów serwera katalogów IBM Security” na stronie 85.

## Deinstalacja za pomocą komendy installp

Użyj komendy **installp**, aby wykonać deinstalację produktu IBM Security Directory Server z systemu AIX.

### Zanim rozpoczniesz

Należy zatrzymać wszystkie procesy klienta i serwera IBM Security Directory Server.

- Serwer katalogów
- Serwer administracyjny
- Śledzenie LDAP
- Narzędzie Web Administration Tool i powiązany z nim serwer aplikacji
- Niestandardowe aplikacje LDAP

### Procedura

1. Zaloguj się do systemu jako użytkownik root.
2. Otwórz wiersz komend.
3. Uruchom następującą komendę, aby określić pakiety IBM Security Directory Server, które chcesz usunąć:

   ```
   lslpp -l 'idsldap*'
   ```

4. Aby usunąć pakiet IBM Security Directory Server, uruchom następującą komendę:

   ```
   installp -u nazwa_pakietu
   ```

   Aby całkowicie usunąć serwer IBM Security Directory Server, usuń wszystkie jego pakiety. Przy deinstalowaniu serwera IBM Security Directory Server należy zdeinstalować wszystkie jego pakiety w odwrotnej kolejności w stosunku do instalacji. Więcej informacji na temat kolejności zawiera sekcja “Pakiety przeznaczone do instalacji w systemie AIX” na stronie 67. Aby usunąć pakiet idsldap.ent631, uruchom następującą komendę:

   ```
   installp -u idsldap.ent631
   ```

### Co dalej

Sprawdź, czy deinstalacja produktu IBM Security Directory Server powiodła się. Aby uzyskać więcej informacji, patrz sekcja “Weryfikowanie pakietów serwera katalogów IBM Security” na stronie 85.

## Deinstalowanie z użyciem programów narzędziowych w systemie Linux

Za pomocą programów narzędziowych wiersza komend systemu Linux można zdeinstalować produkt IBM Security Directory Server z systemu Linux.

Nazwy pakietów IBM Security Directory Server są inne na komputerach z różnymi systemami operacyjnymi i architekturami. Przed zdeinstalowaniem należy sprawdzić zainstalowane pakiety produktu IBM Security Directory Server.

### Deinstalacja z użyciem programów narzędziowych w systemie Linux

Za pomocą komendy **rpm** można wykonać deinstalację produktu IBM Security Directory Server w systemie Linux.

#### Zanim rozpoczniesz

Należy zatrzymać wszystkie procesy klienta i serwera IBM Security Directory Server.

- Serwer katalogów
- Serwer administracyjny
- Śledzenie LDAP
- Narzędzie Web Administration Tool i powiązany z nim serwer aplikacji
- Niestandardowe aplikacje LDAP

#### O tym zadaniu

Poniższy przykład przedstawia deinstalację pakietów IBM Security Directory Server z systemu Linux dla platformy AMD64 Opteron/EM64T. Dla systemów Linux dla System z, System i, System p lub System x należy podstawić odpowiednie nazwy pakietów.

#### Procedura

1. Zaloguj się do systemu jako użytkownik root.
2. Otwórz wiersz komend.
3. Uruchom następującą komendę, aby określić pakiety IBM Security Directory Server, które chcesz usunąć:
   ```
   rpm -qa | grep -i idsldap
   ```
4. Aby usunąć pakiet IBM Security Directory Server, uruchom następującą komendę:
   ```
   rpm -ev nazwa_pakietu
   ```

   Aby całkowicie usunąć serwer IBM Security Directory Server, usuń wszystkie jego pakiety. Przy deinstalowaniu serwera IBM Security Directory Server należy zdeinstalować wszystkie jego pakiety w odwrotnej kolejności w stosunku do instalacji. Więcej informacji na temat kolejności zawiera sekcja “Pakiety przeznaczone do instalacji w systemie Linux” na stronie 73. Aby usunąć pakiet idsldap-srv64bit631-6.3.1-0.x86_64.rpm, uruchom następującą komendę:
   ```
   rpm -ev idsldap-srv64bit631-6.3.1-0.x86_64.rpm
   ```

### Co dalej

Sprawdź, czy deinstalacja produktu IBM Security Directory Server powiodła się. Aby uzyskać więcej informacji, patrz sekcja “Weryfikowanie pakietów serwera katalogów IBM Security” na stronie 85.

## Deinstalowanie z użyciem programów narzędziowych w systemie Solaris

Za pomocą programów narzędziowych wiersza komend systemu Solaris można zdeinstalować produkt IBM Security Directory Server z systemu Solaris.

Nazwy pakietów IBM Security Directory Server są takie same w systemach Solaris SPARC i Solaris X64.

### Deinstalacja przy użyciu programów narzędziowych systemu Solaris

Użyj komendy **pkgrm**, aby wykonać deinstalację produktu IBM Security Directory Server z systemu Solaris.

#### Zanim rozpoczniesz

Należy zatrzymać wszystkie procesy klienta i serwera IBM Security Directory Server.

- Serwer katalogów
- Serwer administracyjny
- Śledzenie LDAP
- Narzędzie Web Administration Tool i powiązany z nim serwer aplikacji
- Niestandardowe aplikacje LDAP

#### Procedura

1. Zaloguj się do systemu jako użytkownik root.
2. Otwórz wiersz komend.
3. Uruchom następującą komendę, aby określić pakiety IBM Security Directory Server, które chcesz usunąć:

   ```
   pkginfo | grep -i IDSl
   ```
4. Aby usunąć pakiet IBM Security Directory Server, uruchom następującą komendę:

   ```
   pkgrm nazwa_pakietu
   ```

   Aby całkowicie usunąć serwer IBM Security Directory Server, usuń wszystkie jego pakiety. Przy deinstalowaniu serwera IBM Security Directory Server należy zdeinstalować wszystkie jego pakiety w odwrotnej kolejności w stosunku do instalacji. Więcej informacji na temat kolejności zawiera sekcja “Pakiety przeznaczone do instalacji w systemie Solaris” na stronie 76. Aby usunąć pakiet IDSlent631, uruchom następującą komendę:

   ```
   pkgrm IDSlent631
   ```

#### Co dalej

Sprawdź, czy deinstalacja produktu IBM Security Directory Server powiodła się. Aby uzyskać więcej informacji, patrz sekcja “Weryfikowanie pakietów serwera katalogów IBM Security” na stronie 85.

# Deinstalowanie z użyciem programów narzędziowych w systemie HP-UX

Za pomocą programów narzędziowych wiersza komend systemu HP-UX można zdeinstalować produkt IBM Security Directory Server z systemu HP-UX.

Na komputerach z systemem HP-UX (Itanium) obsługiwane są tylko pakiety klienta IBM Security Directory Server.

## Deinstalacja przy użyciu programów narzędziowych systemu HP-UX

Użyj komendy **swremove**, aby wykonać deinstalację produktu IBM Security Directory Server z systemu HP-UX.

### Zanim rozpoczniesz

Należy zatrzymać wszystkie procesy klienta IBM Security Directory Server.

- Śledzenie LDAP
- Niestandardowe aplikacje LDAP

### Procedura

1. Zaloguj się do systemu jako użytkownik root.
2. Otwórz wiersz komend.
3. Uruchom następującą komendę, aby określić pakiety IBM Security Directory Server, które chcesz usunąć:

   ```
   swlist | grep -i idsldap
   ```
4. Aby usunąć pakiet IBM Security Directory Server, uruchom następującą komendę:

   ```
   swremove nazwa_pakietu
   ```

   Aby całkowicie usunąć serwer IBM Security Directory Server, usuń wszystkie jego pakiety. Przy deinstalowaniu serwera IBM Security Directory Server należy zdeinstalować wszystkie jego pakiety w odwrotnej kolejności w stosunku do instalacji. Więcej informacji na temat kolejności zawiera sekcja “Pakiety przeznaczone do instalacji w systemie HP-UX Itanium” na stronie 80. Aby usunąć pakiet idsldap.cltjava631.depot, uruchom następującą komendę:

   ```
   swremove idsldap.cltjava631.depot
   ```

### Co dalej

Sprawdź, czy deinstalacja produktu IBM Security Directory Server powiodła się. Aby uzyskać więcej informacji, patrz sekcja “Weryfikowanie pakietów serwera katalogów IBM Security” na stronie 85.

# Deinstalacja bazy danych IBM DB2 za pomocą komend DB2

Jeśli samodzielnie zainstalowano kopię bazy danych IBM DB2 dostarczoną z produktem IBM Security Directory Server, można ją usunąć z komputera za pomocą komend DB2.

Jeśli kopia bazy danych IBM DB2 została zainstalowana za pomocą programu IBM Installation Manager podczas instalowania produktu IBM Security Directory Server, baza IBM DB2 jest instalowana w predefiniowanym położeniu. Więcej informacji na temat położenia domyślnego znajduje się w sekcji “Domyślne położenia instalacji” na stronie 27. Jeśli zainstalowano kopię bazy danych IBM DB2 za pomocą programu IBM Installation Manager, należy zdeinstalować bazę danych IBM DB2, również korzystając z tego programu.

Jeśli komputer zawiera instancje bazy danych DB2 dla kopii IBM DB2, przed zdeinstalowaniem bazy IBM DB2 należy usunąć instancje DB2. Przed zdeinstalowaniem zaleca się wykonanie kopii zapasowej baz danych DB2 i danych.

Jeśli za pomocą komend DB2 samodzielnie zainstalowano bazę danych IBM DB2 w położeniu niestandardowym, użyj komend DB2 do zdeinstalowania takiej bazy danych. W systemach AIX, Linux i Solaris wykonaj w katalogu *położenie_instalacji_DB2*/install/ komendę **db2_deinstall**, aby zdeinstalować bazę danych IBM DB2. W systemach Windows uruchom w katalogu *położenie_instalacji_DB2*\bin komendę **db2unins**, aby zdeinstalować bazę danych IBM DB2. Więcej informacji na temat deinstalowania bazy danych IBM DB2, znajduje się w dokumentacji produktu IBM DB2 dostępnej pod adresem http://www-01.ibm.com/support/knowledgecenter/SSEPGG/welcome.

# Deinstalacja pakietu IBM Global Security Kit za pomocą programów narzędziowych systemu operacyjnego

Jeśli zainstalowano pakiet IBM Global Security Kit (GSKit) za pomocą programów narzędziowych systemu operacyjnego, należy go zdeinstalować również za pomocą programów narzędziowych systemu operacyjnego.

Za pomocą programów narzędziowych systemu operacyjnego można zdeinstalować pakiet GSKit z komputerów z systemem operacyjnym AIX, Linux, Solaris lub HP-UX.

W systemach Windows można samodzielnie zdeinstalować pakiet GSKit, tylko jeśli podczas instalowania za pomocą programu IBM Installation Manager wybrano używanie pakietu GSKit. Jeśli produkt IBM Security Directory Server jest zainstalowany na komputerze, nie można zdeinstalować pakietu GSKit. Aby użyć najnowszej wersji pakietu GSKit, za pomocą programu IBM Installation Manager należy zmodyfikować funkcje pakietu GSKit i usunąć go z rejestru. Następnie można uruchomić deinstalowanie pakietu GSKit.

## Deinstalacja pakietu IBM Global Security Kit za pomocą programu SMIT

Użyj komendy **smit**, aby wykonać deinstalację produktu IBM Global Security Kit (GSKit) z systemu AIX.

### Procedura

1. Zaloguj się do systemu jako użytkownik root.
2. Otwórz wiersz komend.
3. Uruchom komendę **smit**. Zostanie otwarte okno **Instalacja i konserwacja oprogramowania**.
4. Wybierz opcję **Instalacja i konserwacja oprogramowania > Obsługa oprogramowania i narzędzia**.
5. Wybierz opcję **Usuń zainstalowane oprogramowanie**.
6. W polu **Nazwa oprogramowania** naciśnij klawisz **F4**, aby wyświetlić listę zainstalowanego oprogramowania. Możesz podać wartość GSKit w polu, aby wyświetlić wszystkie pakiety GSKit.
7. Ustaw wartość **Usuń zależne oprogramowanie** na YES, aby usunąć wszystkie produkty oprogramowania i aktualizacje, które są zależne od usuwanego produktu.
8. Wybierz pakiety, które chcesz usunąć, i naciśnij klawisz Enter.
9. Sprawdź, czy deinstalacja pakietu GSKit została wykonana pomyślnie.

   ```
   lslpp -l 'GSK*'
   ```

# Deinstalacja pakietu IBM Global Security Kit komendą installp

Użyj komendy **installp**, aby wykonać deinstalację produktu IBM Global Security Kit (GSKit) z systemu AIX.

## Procedura

1. Zaloguj się do systemu jako użytkownik root.
2. Otwórz wiersz komend.
3. Uruchom następującą komendę, aby określić pakiety GSKit, które chcesz usunąć:
   ```
   lslpp -l 'GSK*'
   ```
4. Aby usunąć pakiet GSKit, uruchom następującą komendę:
   ```
   installp -u nazwa_pakietu
   ```

   Aby usunąć pakiet GSKit całkowicie, usuń wszystkie pakiety GSKit w tej samej wersji. Przy deinstalacji pakietu GSKit należy najpierw usunąć pakiet GSKit SSL, a następnie pakiet GSKit crypt. Aby usunąć pakiety GSKit8.gskssl64.ppc.rte i GSKit8.gskcrypt64.ppc.rte, uruchom następującą komendę:
   ```
   installp -u GSKit8.gskssl64.ppc.rte
   installp -u GSKit8.gskcrypt64.ppc.rte
   ```
5. Sprawdź, czy deinstalacja pakietu GSKit została wykonana pomyślnie.
   ```
   lslpp -l 'GSK*'
   ```

# Deinstalacja pakietu IBM Global Security Kit z użyciem programów narzędziowych w systemie Linux

Użyj komendy **rpm**, aby wykonać deinstalację produktu IBM Global Security Kit (GSKit) z systemu Linux.

## O tym zadaniu

Poniższy przykład przedstawia deinstalację pakietów GSKit z systemu Linux dla AMD64 Opteron/EM64T. Dla systemów Linux dla System z, System i, System p lub System x należy podstawić odpowiednie nazwy pakietów.

## Procedura

1. Zaloguj się do systemu jako użytkownik root.
2. Otwórz wiersz komend.
3. Uruchom następującą komendę, aby określić pakiety GSKit, które chcesz usunąć:
   ```
   rpm -qa | grep -i gsk
   ```
4. Aby usunąć pakiet GSKit, uruchom następującą komendę:
   ```
   rpm -ev nazwa_pakietu
   ```

   Aby usunąć pakiet GSKit całkowicie, usuń wszystkie pakiety GSKit w tej samej wersji. Przy deinstalacji pakietu GSKit należy najpierw usunąć pakiet GSKit SSL, a następnie pakiet GSKit crypt. Aby usunąć pakiety gskssl64-8.0-14.26.x86_64 i gskcrypt64-8.0-14.26.x86_64, uruchom następującą komendę:
   ```
   rpm -ev gskssl64-8.0-14.26.x86_64
   rpm -ev gskcrypt64-8.0-14.26.x86_64
   ```
5. Sprawdź, czy deinstalacja pakietu GSKit została wykonana pomyślnie.
   ```
   rpm -qa | grep -i gsk
   ```

# Deinstalacja pakietu IBM Global Security Kit z użyciem programów narzędziowych w systemie Solaris

Użyj komendy **pkgrm**, aby wykonać deinstalację produktu IBM Global Security Kit (GSKit) z systemu Solaris.

## Procedura

1. Zaloguj się do systemu jako użytkownik root.
2. Otwórz wiersz komend.
3. Uruchom następującą komendę, aby określić pakiety GSKit, które chcesz usunąć:
   ```
   pkginfo | grep -i gsk
   ```
4. Aby usunąć pakiet GSKit, uruchom następującą komendę:
   ```
   pkgrm nazwa_pakietu
   ```

   Aby usunąć pakiet GSKit całkowicie, usuń wszystkie pakiety GSKit w tej samej wersji. Przy deinstalacji pakietu GSKit należy najpierw usunąć pakiet GSKit SSL, a następnie pakiet GSKit crypt. Aby usunąć pakiety gsk8ssl64 i gsk8cry64, uruchom następującą komendę:
   ```
   pkgrm gsk8ssl64
   pkgrm gsk8cry64
   ```
5. Sprawdź, czy deinstalacja pakietu GSKit została wykonana pomyślnie.
   ```
   pkginfo | grep -i gsk
   ```

# Deinstalacja pakietu IBM Global Security Kit z użyciem programów narzędziowych w systemie HP-UX

Użyj komendy **swremove**, aby wykonać deinstalację produktu IBM Global Security Kit (GSKit) z systemu HP-UX.

## Procedura

1. Zaloguj się do systemu jako użytkownik root.
2. Otwórz wiersz komend.
3. Uruchom następującą komendę, aby określić pakiety GSKit, które chcesz usunąć:
   ```
   swlist | grep -i gsk
   ```
4. Aby usunąć pakiet GSKit, uruchom następującą komendę:
   ```
   swremove nazwa_pakietu
   ```

   Aby usunąć pakiet GSKit całkowicie, usuń wszystkie pakiety GSKit w tej samej wersji. Przy deinstalacji pakietu GSKit należy najpierw usunąć pakiet GSKit SSL, a następnie pakiet GSKit crypt. Aby usunąć pakiety gskssl64 i gskcrypt64, uruchom następującą komendę:
   ```
   swremove gskssl64
   swremove gskcrypt64
   ```
5. Sprawdź, czy deinstalacja pakietu GSKit została wykonana pomyślnie.
   ```
   swlist | grep -i gsk
   ```

# Deinstalacja pakietu IBM Global Security Kit w systemie Windows

Użyj komend programu IBM Global Security Kit (GSKit), aby wykonać deinstalację pakietu GSKit z systemu Windows.

### O tym zadaniu

W tym przykładzie deinstalacji cichej pakietu GSKit przedstawiono 64-bitowy pakiet SSL i 64-bitowy pakiet GSKit crypt w systemie Windows na platformie AMD64/EM64T. Dla systemu operacyjnego Windows na platformie IA32/x86 nazwy pakietu GSKit są inne. Informacje na temat nazw pakietów GSKit zawiera sekcja Rozdział 10, “Instalowanie pakietu IBM Global Security Kit”, na stronie 55.

**Uwaga:** Pakiet GSKit można też usunąć, używając opcji **Start > Panel sterowania > Dodaj lub usuń programy**.

### Procedura

1. Zaloguj się do systemu jako członek grupy administratorów.
2. Otwórz wiersz komend.
3. Zmień bieżący katalog roboczy na katalog gskit, w którym znajdują się pliki instalacyjne pakietu IBM Global Security Kit.
4. Aby zdeinstalować 64-bitowe pakiety GSKit w trybie cichym, uruchom następujące komendy: Aby usunąć pakiet GSKit całkowicie, usuń wszystkie pakiety GSKit w tej samej wersji. Przy deinstalacji pakietu GSKit należy najpierw usunąć pakiet GSKit SSL, a następnie pakiet GSKit crypt.

   ```
   gsk8ssl64.exe /s /x /v"/quiet"
   gsk8crypt64.exe /s /x /v"/quiet"
   ```

## Deinstalowanie pakietów językowych

Aby odinstalować produkt IBM Security Directory Server, należy odinstalować zainstalowane wcześniej pakiety językowe.

Jeśli produkt IBM Security Directory Server i jego pakiety językowe zainstalowano za pomocą programu IBM Installation Manager, do deinstalacji pakietów językowych również należy użyć programu IBM Installation Manager.

Jeśli pakiety językowe zostały zainstalowane za pomocą programów narzędziowych systemu operacyjnego, należy ich użyć również do deinstalacji.

Jeśli do instalacji nie zostanie wybrana opcja serwera proxy lub serwera, z systemu zostaną zdeinstalowane wszystkie pakiety językowe.

## Deinstalacja pakietów językowych za pomocą programów narzędziowych systemu operacyjnego

Użyj narzędzia systemu operacyjnego do wykonania deinstalacji pakietu językowego, jeśli pakiet językowy zainstalowano za pomocą programów narzędziowych systemu operacyjnego.

### Zanim rozpoczniesz

Przed zdeinstalowaniem pakietów językowych dla serwera IBM Security Directory Server należy zatrzymać wszystkie procesy klienta i serwera IBM Security Directory Server.

- Serwer katalogów
- Serwer administracyjny
- Śledzenie LDAP
- Niestandardowe aplikacje LDAP

## Procedura

1. Zaloguj się do systemu jako użytkownik root.
2. Otwórz wiersz komend.
3. Określ, jakie pakiety językowe są dostępne do usunięcia na komputerze:

| System operacyjny | Komenda do uruchomienia: |
|---|---|
| **AIX** | lslpp -l 'idsldap.msg631*' |
| **Linux** | rpm -qa \| grep -i idsldap-msg631 |
| **Solaris** | pkginfo \| grep IDSl |

4. Aby zdeinstalować pakiet językowy dla języka, uruchom komendy deinstalacji pakietu. W poniższym przykładzie przedstawiona została deinstalacja pakietu językowego dla języka francuskiego. Zastępując odpowiednią nazwę pakietu dla systemu operacyjnego, można zdeinstalować dowolny pakiet językowy.

| System operacyjny | Komenda do uruchomienia: |
|---|---|
| **AIX** | installp -u idsldap.msg631.fr_FR |
| **Linux** | rpm -ev idsldap-msg631-fr-6.3.1-0.noarch.rpm |
| **Solaris** | pkgrm IDSlfr631 |

5. Sprawdź, czy instalacja pakietu językowego zakończyła się pomyślnie. Aby uzyskać więcej informacji, patrz sekcja "Weryfikowanie pakietów serwera katalogów IBM Security" na stronie 85.

# Dodatek A. Język DSML

Język DSML (Directory Services Markup Language) służy do reprezentowania informacji o strukturze katalogu, przesyłania zapytań do serwera katalogów, aktualizowania danych oraz określania wyników tych operacji w postaci danych XML.

Po zakończeniu instalowania programu Web Administration Tool produktu IBM Security Directory Server na komputerze docelowym znajduje się plik archiwum DSML.zip z plikami DSML (Directory Services Markup Language). Plik DSML.zip jest przechowywany w podkatalogu idstools katalogu instalacyjnego produktu IBM Security Directory Server. Więcej informacji na temat domyślnego katalogu instalacyjnego produktu IBM Security Directory Server zawiera sekcja “Domyślne położenia instalacji” na stronie 27.

Plik DSML.zip zawiera program instalacyjny DSML i dokumentację instalowania, konfigurowania i używania języka DSML. W archiwum DSML.zip znajdują się następujące pliki:

**DSMLReadme.txt**
Pliki DSMLReadme.txt zawierają listę plików w pakiecie oraz instrukcje instalowania i konfigurowania języka DSML.

**dsml.pdf**
Plik dsml.pdf jest dokumentem w formacie PDF opisującym używanie języka DSML.

**dsml.htm**
Plik dsml.htm jest dokumentem w formacie HTML opisującym używanie języka DSML.

# Dodatek B. Ładowanie przykładowej bazy danych i uruchamianie serwera

Załaduj przykładową bazę danych i uruchom serwer katalogów, aby dodać, zaktualizować lub wyszukać pozycje.

## Zanim rozpoczniesz

Utwórz instancję serwera katalogów. Informacje na ten temat zawiera sekcja “Tworzenie instancji serwera katalogów” na stronie 133.

## O tym zadaniu

Za pomocą programu Configuration Tool można załadować dane LDIF na serwer katalogów i uruchomić serwer.

## Procedura

1. Aby uruchomić program Configuration Tool, uruchom następującą komendę:
   ```
   idsxcfg -I nazwa_instancji
   ```
2. W obszarze nawigacyjnym po lewej stronie kliknij opcję **Zadania LDIF > Importowanie danych w formacie LDIF**.
3. W polu **Nazwa i ścieżka pliku LDIF** podaj plik danych LDIF ze ścieżką. Aby wskazać plik danych LDIF, możesz także kliknąć przycisk Przeglądaj. Poniżej przedstawiono domyślne nazwy ścieżek i pliki danych LDIF w różnych systemach operacyjnych:

   **Windows**
   *ścieżka_instalacyjna*\examples\sample.ldif

   **AIX i Solaris**
   /opt/IBM/ldap/V6.3.1/examples/sample.ldif

   **Linux** /opt/ibm/ldap/V6.3.1/examples/sample.ldif
4. Kliknij przycisk **Standardowy import**.
5. Kliknij przycisk **Importuj**.
6. Aby uruchomić instancję serwera katalogów, wykonaj następujące czynności:
   a. W obszarze nawigacyjnym po lewej stronie kliknij opcję **Zarządzanie stanem serwera**.
   b. Kliknij opcję **Uruchamianie serwera**.

# Dodatek C. Samodzielne aktualizowanie pliku ldapdb.properties

Jeśli program IBM Security Directory Server jest instalowany na komputerze, na którym nie ma obsługiwanej wersji bazy danych IBM DB2, plik ldapdb.properties nie będzie aktualizowany podczas instalacji. W takiej sytuacji należy zainstalować obsługiwaną wersję bazy danych IBM DB2, a następnie zaktualizować plik ldapdb.properties samodzielnie.

## Zanim rozpoczniesz

Należy upewnić się, że jest zainstalowany pakiet pełnego serwera katalogów.

## Procedura

1. Zainstaluj obsługiwaną wersję bazy danych IBM DB2, jeśli jeszcze nie została zainstalowany.
2. Uruchom komendę **db2ls**, aby wyświetlić listę wersji DB2 zainstalowanych na komputerze i ich ścieżki instalacji.
3. Zaktualizuj plik ldapdb.properties podając w nim obsługiwaną wersję DB2 i ścieżkę instalacji. Domyślne położenie pliku ldapdb.properties i przykładowe wartości dla różnych systemów operacyjnych:

   **Microsoft Windows**
   C:\Program Files\IBM\ldap\V6.3.1\etc\ldapdb.properties

   ```
   currentDB2InstallPath=C:\Program Files\IBM\SQLLIB
   currentDB2Version=9.7.0.6
   ```

   **AIX i Solaris**
   /opt/IBM/ldap/V6.3.1/etc/ldapdb.properties

   ```
   currentDB2InstallPath=/opt/IBM/db2/V9.7
   currentDB2Version=9.7.0.6
   ```

   **Linux** /opt/ibm/ldap/V6.3.1/etc/ldapdb.properties

   ```
   currentDB2InstallPath=/opt/ibm/db2/V9.7
   currentDB2Version=9.7.0.6
   ```

4. Zapisz plik ldapdb.properties.

# Dodatek D. Ułatwienia dostępu w produkcie Security Directory Server

Opcje ułatwień dostępu pomagają użytkownikom nie w pełni sprawnym, np. mającym trudności w poruszaniu się lub słabszy wzrok, korzystać skutecznie z produktów informatycznych.

Główne opcje ułatwień dostępu zawarte w tym produkcie umożliwiają użytkownikom wykonanie podanych poniżej czynności:

- Użycie techniki wspomagającej, na przykład lektora ekranowego, aby usłyszeć to, co jest wyświetlane na ekranie. Szczegółowe informacje na temat korzystania z techniki wspomagającej w tym produkcie zawiera dokumentacja produktu.
- Wykonywanie konkretnych lub odpowiednich funkcji tylko za pomocą klawiatury.
- Powiększanie informacji wyświetlanych na ekranie.

Ponadto zmodyfikowano dokumentację produktu w taki sposób, aby zawierała następujące funkcje ułatwień dostępu:

- Cała dokumentacja jest dostępna w formacie HTML, aby maksymalnie umożliwić użytkownikom korzystanie z lektorów ekranowych.
- Wszystkie obrazki są udostępniane z alternatywnym tekstem, aby użytkownicy z upośledzeniem wzroku mogli zrozumieć treść tych obrazków.

## Ułatwienia dostępu

Poniższa lista zawiera główne ułatwienia dostępu w produkcie IBM Security Directory Server.

- Umożliwia obsługę tylko przy użyciu klawiatury.
- Obsługuje interfejsy powszechnie używane przez lektory ekranowe.
- Klawisze są wyczuwalne dotykowo i nie aktywują się od samego dotknięcia.

Dokumentacja produktu IBM Security Directory Server obsługuje ułatwienia dostępu. Funkcje ułatwienia dostępu dokumentacji są opisane w zestawie dokumentacji elektronicznej.

## Poruszanie się za pomocą klawiatury

W tym produkcie wykorzystywane są skróty standardowe i klawisze skrótu. Ich opis znajduje się w dokumentacji systemu operacyjnego. Aby uzyskać więcej informacji, zapoznaj się z tą dokumentacją systemu operacyjnego.

W tym produkcie używane są standardowe klawisze nawigacyjne systemu Microsoft Windows.

## Powiększanie informacji wyświetlanych na ekranie

Informacje prezentowane w oknach produktu można powiększać, korzystając z funkcji udostępnianych przez systemy operacyjne, na których działa produkt. W środowisku Microsoft Windows można, na przykład, zmniejszyć rozdzielczość ekranu, aby zwiększyć rozmiar czcionki tekstu wyświetlanego na ekranie. Aby uzyskać więcej informacji, zapoznaj się z tą dokumentacją systemu operacyjnego.

## IBM i ułatwienia dostępu

Więcej informacji na temat zaangażowania firmy IBM w pracę nad ułatwieniami dostępu zawiera serwis IBM Human Ability and Accessibility Center: http://www.ibm.com/able

# Indeks

# F



# H



# I

## J



## K



## L



## M



## N

## O



## P

# R



# S

## T



## U



## W



## Z

# 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/regionie można uzyskać od lokalnego przedstawiciela IBM. Odwołanie do produktu, programu lub usługi IBM nie oznacza, że można użyć wyłącznie tego produktu, programu lub usługi IBM. Zamiast nich można zastosować ich odpowiednik funkcjonalny, pod warunkiem, że nie narusza to praw własności intelektualnej IBM. Jednakże cała odpowiedzialność za ocenę przydatności i sprawdzenie działania produktu, programu lub usługi pochodzących od producenta innego niż IBM spoczywa na użytkowniku.

IBM może posiadać patenty lub złożone wnioski patentowe na towary i usługi, o których mowa w niniejszej publikacji. Przedstawienie niniejszej publikacji nie daje żadnych uprawnień licencyjnych do tychże patentów. Pisemne zapytania w sprawie licencji można przesyłać na adres:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 USA

Zapytania dotyczące zestawów znaków dwubajtowych (DBCS) należy kierować do lokalnych działów własności intelektualnej IBM (IBM Intellectual Property Department) w kraju lub wysłać je na piśmie na adres:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

**Poniższy akapit nie obowiązuje w Wielkiej Brytanii, a także w innych krajach, w których jego treść pozostaje w sprzeczności z przepisami prawa miejscowego:**

INTERNATIONAL BUSINESS MACHINES CORPORATION DOSTARCZA TĘ PUBLIKACJĘ W STANIE, W JAKIM SIĘ ZNAJDUJE ("AS IS"), BEZ UDZIELANIA JAKICHKOLWIEK GWARANCJI (W TYM TAKŻE RĘKOJMI), WYRAŹNYCH LUB DOMNIEMANYCH, A W SZCZEGÓLNOŚCI DOMNIEMANYCH GWARANCJI PRZYDATNOŚCI HANDLOWEJ ORAZ PRZYDATNOŚCI DO OKREŚLONEGO CELU LUB GWARANCJI, ŻE PUBLIKACJA TA NIE NARUSZA PRAW OSÓB TRZECICH.

Ustawodawstwa niektórych krajów nie dopuszczają zastrzeżeń dotyczących gwarancji wyraźnych lub domniemanych w odniesieniu do pewnych transakcji; w takiej sytuacji powyższe zdanie nie ma zastosowania.

Informacje zawarte w niniejszej publikacji mogą zawierać nieścisłości techniczne lub błędy typograficzne. Informacje te są okresowo aktualizowane, a zmiany te zostaną ujęte w kolejnych wydaniach tej publikacji. Firma IBM zastrzega sobie prawo do wprowadzania ulepszeń i/lub zmian w produktach i/lub programach opisanych w tej publikacji w dowolnym czasie, bez wcześniejszego powiadomienia.

Wszelkie wzmianki w tej publikacji na temat stron internetowych innych firm zostały wprowadzone wyłącznie dla wygody użytkowników i w żadnym wypadku nie stanowią zachęty do ich odwiedzania. Materiały dostępne na tych stronach nie są częścią materiałów opracowanych do tego produktu IBM, a użytkownik korzysta z nich na własną odpowiedzialność.

IBM ma prawo do używania i rozpowszechniania informacji przysłanych przez użytkownika w dowolny sposób, jaki uzna za właściwy, bez żadnych zobowiązań wobec ich autora.

Licencjobiorcy tego programu, którzy chcieliby uzyskać informacje na temat programu w celu: (i) wdrożenia wymiany informacji między niezależnie utworzonymi programami i innymi programami (łącznie z tym opisywanym) oraz (ii) wykorzystywania wymienianych informacji, powinni skontaktować się z:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 USA

Informacje takie mogą być udostępnione, o ile spełnione zostaną odpowiednie warunki, w tym, w niektórych przypadkach, uiszczenie odpowiedniej opłaty.

Licencjonowany program opisany w tym dokumencie 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 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 innych firm pochodzą od dostawców tych produktów, z opublikowanych przez nich zapowiedzi lub innych powszechnie dostępnych źródeł. Firma IBM nie testowała tych produktów i nie może potwierdzić dokładności pomiarów wydajności, kompatybilności ani żadnych innych danych związanych z tymi produktami. Pytania dotyczące produktów firm innych niż IBM należy kierować do dostawców tych produktów.

Wszelkie stwierdzenia dotyczące przyszłych kierunków rozwoju i zamierzeń IBM mogą zostać zmienione lub wycofane bez powiadomienia.

Wszystkie 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.

Niniejsze informacje zawierają przykłady danych i raportów używanych w codziennych czynnościach służbowych. W celu możliwie najpełniejszej ich ilustracji w przykładach tych używane są nazwiska osób, nazwy firm, marki i nazwy produktów. Wszystkie te nazwy są fikcyjne i jakiekolwiek ich podobieństwo do nazwisk, nazw i adresów używanych w rzeczywistych przedsiębiorstwach jest całkowicie przypadkowe.

LICENCJA W ZAKRESIE PRAW AUTORSKICH:

Niniejsza publikacja zawiera przykładowe aplikacje w języku 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 lub sugerować niezawodności, użyteczności i funkcjonalności tych programów. Użytkownik może kopiować, modyfikować i rozpowszechniać te programy przykładowe w dowolnej formie bez uiszczania opłat w celu rozbudowy, używania, handlowym lub w celu rozpowszechniania aplikacji zgodnych z aplikacyjnym interfejsem programowym.

Każda kopia tych przykładowych programów lub jakiejkolwiek ich części, a także jakakolwiek praca pochodna, musi zawierać następującą klauzulę dotyczącą praw autorskich:

© (nazwa przedsiębiorstwa użytkownika) (rok). Części niniejszego kodu pochodzą z programów przykładowych IBM Corp. Sample Programs. © Copyright IBM Corp. _wpisać rok lub lata_. Wszelkie prawa zastrzeżone.

Podczas przeglądania niniejszych informacji w postaci elektronicznej zdjęcia oraz kolorowe ilustracje mogą być niewidoczne.

## Znaki towarowe

IBM, logo IBM i ibm.com są znakami towarowymi lub zastrzeżonymi znakami towarowymi International Business Machines Corp. zarejestrowanymi w wielu systemach prawnych na całym świecie. Nazwy innych produktów lub usług mogą być znakami towarowymi IBM lub innych podmiotów. Aktualna lista znaków towarowych IBM dostępna jest w sekcji "Copyright and trademark information" (Informacje o prawach autorskich i znakach towarowych), pod adresem www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript i wszystkie oparte na Adobe znaki towarowe są zastrzeżonymi znakami towarowymi lub znakami towarowymi Adobe Systems Incorporated w Stanach Zjednoczonych i w innych krajach.

IT Infrastructure Library jest zastrzeżonym znakiem towarowym Central Computer and Telecommunications Agency, która obecnie wchodzi w skład Departamentu Ministerstwa Skarbu Wielkiej Brytanii.

Intel, Intel logo, Intel Inside, logo Intel Inside, Intel Centrino, logo Intel Centrino, Celeron, Intel Xeon, Intel SpeedStep, Itanium i Pentium są zastrzeżonymi znakami towarowymi firmy Intel Corporation lub jej firm zależnych w Stanach Zjednoczonych i w innych krajach.

Linux jest znakiem towarowym Linusa Torvaldsa w Stanach Zjednoczonych i w innych krajach.

Microsoft, Windows, Windows NT oraz logo Windows są znakami towarowymi Microsoft Corporation w Stanach Zjednoczonych lub w innych krajach.

ITIL jest zastrzeżonym znakiem towarowym i zastrzeżonym wspólnotowym znakiem towarowym Departamentu Ministerstwa Skarbu Wielkiej Brytanii oraz jest zarejestrowany w Urzędzie Patentów i Znaków Towarowych Stanów Zjednoczonych.

UNIX jest zastrzeżonym znakiem towarowym The Open Group w Stanach Zjednoczonych i w innych krajach.


Java oraz wszystkie znaki towarowe i logo dotyczące języka Java są znakami towarowymi lub zastrzeżonymi znakami towarowymi Oracle i/lub przedsiębiorstw afiliowanych Oracle.

Cell Broadband Engine jest znakiem towarowym Sony Computer Entertainment, Inc. w Stanach Zjednoczonych i w innych krajach, używanym na warunkach licencji Sony Computer Entertainment, Inc.

Linear Tape-Open, LTO, logo LTO, Ultrium i logo Ultrium są znakami towarowymi HP, IBM Corp. i Quantum w Stanach Zjednoczonych i w innych krajach.

Drukowane w USA

SC85-0425-02