IBM Security Directory Server
Version 6.3.1

Installation and Configuration Guide

SC27-2747-01

IBM Security Directory Server
Version 6.3.1

Installation and Configuration Guide

SC27-2747-01

Note
Before using this information and the product it supports, read the general information under "Notices" on page 235.

Edition notice

Note: This edition applies to version 6.3.1 of *IBM Security Directory Server* **licensed program (product number 5724-J39) and to all subsequent releases and modifications until otherwise indicated in new editions.**

Contents

Tables

About this publication

IBM® Security Directory Server, previously known as IBM Tivoli® Directory Server, is an IBM implementation of Lightweight Directory Access Protocol for the following operating systems:

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

IBM Security Directory Server, Version 6.3.1 Installation and Configuration Guide contains information for installing, configuring, and uninstalling IBM Security Directory Server. It also includes information about upgrading from a previous version.

Access to publications and terminology

This section provides:

- A list of publications in the "IBM Security Directory Server library."
- Links to "Online publications" on page x.
- A link to the "IBM Terminology website" on page x.

IBM Security Directory Server library

The following documents are available in the IBM Security Directory Server library:

- *IBM Security Directory Server, Version 6.3.1 Product Overview*, GC27-6212-00

  Provides information about the IBM Security Directory Server product, new features in the current release, and system requirements information.
- *IBM Security Directory Server, Version 6.3.1 Quick Start Guide*, GI11-9351-01

  Provides help for getting started with IBM Security Directory Server. Includes a short product description and architecture diagram, and a pointer to the product documentation website and installation instructions.
- *IBM Security Directory Server, Version 6.3.1 Installation and Configuration Guide*, SC27-2747-01

  Contains complete information for installing, configuring, and uninstalling IBM Security Directory Server. Includes information about upgrading from a previous version of IBM Security Directory Server.
- *IBM Security Directory Server, Version 6.3.1 Administration Guide*, SC27-2749-01

  Contains instructions for administrative tasks through the Web Administration tool and the command line.
- *IBM Security Directory Server, Version 6.3.1 Command Reference*, SC27-2753-01

  Describes the syntax and usage of the command-line utilities included with IBM Security Directory Server.
- *IBM Security Directory Server, Version 6.3.1 Server Plug-ins Reference* , SC27-2750-01

  Contains information about writing server plug-ins.

- *IBM Security Directory Server, Version 6.3.1 Programming Reference*, SC27-2754-01

  Contains information about writing Lightweight Directory Access Protocol (LDAP) client applications in C and Java™.
- *IBM Security Directory Server, Version 6.3.1 Performance Tuning and Capacity Planning Guide*, SC27-2748-01

  Contains information about tuning the directory server for better performance. Describes disk requirements and other hardware requirements for directories of different sizes and with various read and write rates. Describes known working scenarios for each of these levels of directory and the disk and memory used; also suggests rules of thumb.
- *IBM Security Directory Server, Version 6.3.1 Troubleshooting Guide*, GC27-2752-01

  Contains information about possible problems and corrective actions that can be taken before you contact IBM Software Support.
- *IBM Security Directory Server, Version 6.3.1 Error Message Reference*, GC27-2751-01

  Contains a list of all warning and error messages associated with IBM Security Directory Server.

Online publications

IBM posts product publications when the product is released and when the publications are updated at the following locations:

IBM Security Directory Server documentation website
The http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.IBMDS.doc/welcome.htm site displays the documentation welcome page for this product.

IBM Security Systems Documentation Central and Welcome page
IBM Security Systems Documentation Central provides an alphabetical list of all IBM Security Systems product documentation. You can also find links to the product documentation for specific versions of each product.

Welcome to IBM Security Systems documentation provides and introduction to, links to, and general information about IBM Security Systems documentation.

IBM Publications Center
The http://www-05.ibm.com/e-business/linkweb/publications/servlet/pbi.wss site offers customized search functions to help you find all the IBM publications you need.

IBM Terminology website

The IBM Terminology website consolidates terminology for product libraries in one location. You can access the Terminology website at http://www.ibm.com/software/globalization/terminology.

Accessibility

Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products successfully. With this product, you can use assistive technologies to hear and navigate the interface. You can also use the keyboard instead of the mouse to operate all features of the graphical user interface.

For more information, see the Accessibility Appendix in the *IBM Security Directory Server Product Overview*.

Technical training

For technical training information, see the following IBM Education website at http://www.ibm.com/software/tivoli/education.

Support information

IBM Support assists with code-related problems and routine, short duration installation or usage questions. You can directly access the IBM Software Support site at http://www.ibm.com/software/support/probsub.html.

IBM Security Directory Server Troubleshooting Guide provides details about:

- What information to collect before you contact IBM Support.
- The various methods for contacting IBM Support.
- How to use IBM Support Assistant.
- Instructions and problem-determination resources to isolate and fix the problem yourself.

Note: The **Community and Support** tab on the product documentation can provide additional support resources.

Statement of Good Security Practices

IT system security involves protecting systems and information through prevention, detection, and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated, or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Chapter 1. Planning for installation

You must decide hardware, software, user roles, security and other requirements for your directory server environment before installation of IBM Security Directory Server.

Planning roadmap

Use the checklist in this chapter to install a server.

If you are upgrading from a previous release, do not use this checklist. Instead, see Chapter 13, "Upgrade an instance of a previous version," on page 87 for instructions.

To install the server:

1. Read a brief overview to understand the components of IBM Security Directory Server that you will install:
2. Be sure that you have the minimum required hardware and software. For information about the requirements, see "Disk space requirements" on page 3.
3. Install IBM Security Directory Server using the IBM Installation Manager.
4. On Windows systems, if the system restarts, log on as the user you were logged on as during installation.
5. Use the Instance Administration Tool to manage directory server instances.
6. Optionally, verify the installation and configuration by loading the sample LDIF file into the database. For more information, see Loading a sample database and starting the server.
7. Start the directory server instance and, if you installed the Web Administration Tool, start it.
8. See the *IBM Security Directory Server Version 6.3.1 Administration Guide* for information about setting up and using the server and the Web Administration Tool.

If you installed a full directory server and you want to plan the organization of your database, see "Configuration planning" on page 120 for information.

Chapter 2. Installation overview

You must prepare your computer and choose the appropriateIBM Security Directory Server installation mode that is applicable for your environment.

IBM Installation Manager-based installer is provided for Windows, Linux64, and AIX. Wrapper installers are available for IBM Security Directory Server on UNIX systems except Linux 64 and AIX. With the Installation Manager-based installer, GUI and silent installation is supported for IBM Security Directory Server V6.3.1.

Disk space requirements

For successful installation of IBM Security Directory Server and the corequisite software, your computer must contain the required disk space. The disk space requirements vary based on the operating system and the IBM Security Directory Server feature and the corequisite software that you select for installation.

Disk space requirements on Windows

Note: If you select the Proxy Server or Full Directory Server feature for installation, add the sizes for the Client SDK, IBM Java Development Kit, and Java Client once.

Table 1. The disk space requirements for IBM Security Directory Server features and the corequisite software on Windows

Installable Feature	Disk Space for Installation (in MB)
Client Software Development Kit	25 MB
IBM Java Development Kit	200 MB
Java Client	124 MB
Deployed Web Administration Tool (includes embedded WebSphere® Application Server and the Web Administration Tool that is deployed into embedded WebSphere Application Server)	440 MB
Web Administration Tool deployment in existing embedded WebSphere Application Server or WebSphere Application Server	260 MB
Base Server	23 MB
Proxy Server (be sure to add the sizes for the Client SDK, Java Client, and Base Server)	40 MB
Full Directory Server (be sure to add the sizes for the Client SDK, Java Client, and Base Server)	8 MB
IBM DB2®	763 MB
IBM Global Security Kit	11 MB

Disk space requirements on AIX

Note: If you select the Proxy Server or Full Directory Server feature for installation, add the sizes for the Client SDK, IBM Java Development Kit, and Java Client once.

Table 2. The disk space requirements for IBM Security Directory Server features and the corequisite software on AIX

Installable Feature	Disk Space for Installation (in MB)
Client Software Development Kit	8 MB
IBM Java Development Kit	200 MB
Java Client	91 MB
Deployed Web Administration Tool (includes embedded WebSphere Application Server and the Web Administration Tool that is deployed into embedded WebSphere Application Server)	443 MB
Web Administration Tool deployment in existing embedded WebSphere Application Server or WebSphere Application Server	500 MB
SSL Web Administration Tool	51 MB
Base Server	39 MB
Proxy Server (be sure to add the sizes for the Client SDK, Java Client, and Base Server)	4 MB
Full Directory Server (be sure to add the sizes for the Client SDK, Java Client, and Base Server)	12 MB
IBM DB2	1250 MB
IBM Global Security Kit	16 MB

Disk space requirements on Linux

Note: If you select the Proxy Server or Full Directory Server feature for installation, add the sizes for the Client SDK, IBM Java Development Kit, and Java Client once.

Table 3. The disk space requirements for IBM Security Directory Server features and the corequisite software on Linux

Installable Feature	Disk Space for Installation (in MB)
Client Software Development Kit	9 MB
IBM Java Development Kit	200 MB
Java Client	166 MB
Deployed Web Administration Tool (includes embedded WebSphere Application Server and the Web Administration Tool that is deployed into embedded WebSphere Application Server)	443 MB
Web Administration Tool deployment in existing embedded WebSphere Application Server or WebSphere Application Server	375 MB

Table 3. The disk space requirements for IBM Security Directory Server features and the corequisite software on Linux (continued)

Installable Feature	Disk Space for Installation (in MB)
Base Server	32 MB
Proxy Server (be sure to add the sizes for the Client SDK, Java Client, and Base Server)	40 MB
Full Directory Server (be sure to add the sizes for the Client SDK, Java Client, and Base Server)	8 MB
IBM DB2 (System x Linux)	460 MB
IBM DB2 (System zLinux)	670 MB
IBM DB2 (System i and System p Linux)	520 MB
IBM DB2 (AMD64/EM64T Linux)	1300 MB
IBM Global Security Kit	40 MB

Note: (Applicable for Installation Manager-based installer.) In the shared resources directory, 200 MB of hard disk space is required. In the installation directory of IBM Security Directory Server, an additional 200 MB of hard disk space is required.

Space requirement for default temp directory of system: If DB2 is selected for installation, then 2048 MB + 500 MB free space in the temp directory is required. Without DB2, 500 MB free space in the temp directory is required.

Disk space requirements on Solaris

Note: If you select the Server and Proxy Server feature for installation, add the sizes for the C Client, IBM Java Development Kit, and Java Client once.

Table 4. The disk space requirements for IBM Security Directory Server features and the corequisite software on Solaris

Installable feature	Disk space for installation (in MB)	Remarks
C Client	11 MB	
IBM Java Development Kit		
Java Client	145 MB	
Server	47 MB	Add C Client and Java Client sizes
Proxy Server	40 MB	Add C Client and Java Client sizes
Web Administration Tool	470 MB	Includes embedded WebSphere Application Server, and Web Administration Tool that is deployed into embedded WebSphere Application Server
IBM DB2	1155 MB	
IBM Global Security Kit	34 MB	

Disk space requirements on HP-UX

Table 5. The disk space requirements for IBM Security Directory Server features and the corequisite software on HP-UX

Installable feature	Disk space for installation (in MB)
C Client	26 MB
IBM Java Development Kit	
Java Client	172 MB
IBM Global Security Kit	41 MB

Preparation of installation media

The IBM Security Directory Server product package includes IBM Security Directory Server, the corequisite software, and the installation program. You can obtain the installation media from the installation DVDs or from the Passport Advantage website.

The IBM Security Directory Server product is available in three types of files: `.zip`, `.tar`, and `.iso`. A `.iso` file contains multiple files that correspond to multiple `.zip` or `.tar` files.

Table 6. IBM Security Directory Server product is available in the following format on various operating system

AIX, Linux, Solaris, and Windows	AIX, Linux, Solaris, and HP-UX	Windows
ISO image (`.iso` file)	Tape archive files (`.tar` files)	Archive files (`.zip` files)

To use DVD as your installation media, you must complete one of the following tasks:

- Create a DVD image from the IBM Security Directory Server product image for your operating system.
- Store the IBM Security Directory Server product image on the hard disk of the computer and mount it if required.

When you download the archive files of the product, you must meet the following requirements:

1. Download all the required archive files to the same directory. Avoid downloading the archive files to a directory location that contain spaces in the path name.
2. Uncompress all the archive files in the same directory that does not contain spaces in the directory path. The directory path of the installable must not contain spaces.

To download the IBM Security Directory Server product from Passport Advantage, see "Downloading the software from Passport Advantage" on page 7.

After you prepare you installation media, you must meet the prerequisite software requirements for your operating system. See "Installation prerequisites" on page 15.

Downloading the software from Passport Advantage

For the installation of IBM Security Directory Server, you must download the software from IBM Passport Advantage.

Before you begin

You must register and obtain a customer account number and password to access IBM Passport Advantage.

Procedure

1. Go to the IBM Passport Advantage website at http://www.ibm.com/software/howtobuy/passportadvantage/pao_customers.htm.
2. Click **Customer sign in**.
3. In the **IBM ID** field, enter your IBM ID.
4. In the **Password** field, enter your password.
5. Click **Sign in**.
6. Follow the instructions to download the IBM Security Directory Server software.

Directory structure of downloaded files

You must verify the directory structure after you download the installation files for IBM Security Directory Server.

Directory structure for Windows packages

The file names for the Security Directory Server 6.3.1 for Windows packages are:

DVD image: sds631-win.iso
.zip files:
– sds631-win-base.zip (Security Directory Server 6.3.1 Client and Server)
– sds631-win-db2.zip (DB2 V9.7)
– sds631-win-ewas.zip (embedded 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)

After you create the DVD or uncompress the .zip files, the directory structure is as follows:

\sdsV6.3.1 (top-level directory for unzipped files)
– ibm_gskit\ (GSKit)
– license\ (licenses for Security Directory Server and other provided products)
– quickstart\ (Quick Start Guides in English and other languages)
– entitlement\ (entitlement files for proxy server)
– entitlement.txt
– tools\ (tools including migbkup)
– migbkup.bat
– ibm_db2_32bit\ (DB2)
– ibm_db2_64bit\ (DB2)
– ibm_ewas_32bit\ (embedded WebSphere Application Server)
– ibm_ewas_64bit\ (embedded WebSphere Application Server)
– ibm_im_32bit\ (IBM Installation Manager)
– ibm_im_64bit\ (IBM Installation Manager)

– ibm_jdk\ (IBM Java Development Kit)
– ibm_sds\ (installer files)
– atoc
– files
– native
– Offerings
– plugins
– ShareableEntities
– build.properties
– repository.config
– repository.xml
– launchpad\
– SilentInstallScripts\ (response files used in silent installation)
– autorun.inf
– imLauncherWindows.bat
– launchpad.exe
– launchpad.ini
– launchpad64.exe
– launchpad64.ini
– sds_install.xml
– write_sds_path.bat

Windows client-only package

.zip file:
– sds631-win-client.zip (Security Directory Server 6.3.1 Client)

After you uncompress the .zip file, the directory structure is as follows:

\sdsV6.3.1 (top-level directory for unzipped files)
– ibm_gskit\ (GSKit 8)
– jdk\ (IBM Java Development Kit)
– ibm_im_32bit (IBM Installation Manager)
– ibm_im_64bit (IBM Installation Manager)
– ibm_sds\ (installer files)
– launchpad\
– SilentInstallScripts\
– autorun.inf
– license\ (licenses for Security Directory Server and other provided products)
– quickstart\ (Quick Start Guides in English and other languages)
– 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

Directory structure for AIX server packages

The file names for the Security Directory Server 6.3.1 for AIX packages are:

DVD image: sds631-aix-ppc64.iso
.tar files:

– tds63-aix-ppc64-base.tar (Security Directory Server 6.3.1 Client and Server)
– sds631-aix-ppc64-db2.tar (DB2 V9.7)
– sds631-aix-ppc64-ewas.tar (embedded 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)

After you create the DVD or uncompress the .tar files, the directory structure is as follows:

/sdsV6.3.1 (top-level directory for untarred files)
– license/ (licenses for Security Directory Server and other provided products)
– quickstart/ (Quick Start Guides in English and other languages)
– ibm_im (IBM Installation Manager)
– ibm_db2/ (DB2)
– ibm_ewas/ (embedded WebSphere Application Server)
– ibm_gskit/ (GSKit 8)
– ibm_jdk/ (IBM Java Development Kit)
– ibm_sds/ (Installer files)
– atoc/
– files/
– native/
– Offerings/
– plugins/
– ShareableEntities
– build.properties
– repository.config
– repository.xml

– tools/ (tools including migbkup)
– launchpad/
– SilentInstallScripts/
– launchpad.sh
– sds_install.xml
– write_sds_path.sh
– entitlement/ entitlement files for proxy server)
– native / (native packages)

AIX client-only package

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

After you uncompress the .zip file, the directory structure is as follows:

\sdsV6.3.1 (top-level directory for unzipped files)
– ibm_gskit\ (GSKit 8)
– ibm_jdk\ (IBM Java Development Kit)
– ibm_im\ (IBM Installation Manager)
– ibm_sds\ (installer files)
– launchpad\
– SilentInstallScripts\
– autorun.inf
– license\ (licenses for Security Directory Server and other provided products)
– quickstart\ (Quick Start Guides in English and other languages)
– ibm_im\ (IBM Installation Manager)

– imLauncherWindows.bat
– launchpad.exe
– launchpad.ini
– sds_install.xml
– write_sds_path.bat

Directory structure for Linux x86_64 server packages

The file names for the Security Directory Server 6.3.1 for Linux x86_64 server packages are:

DVD image: sds631-linux-x86-64.iso
.tar files:
– sds631-linux-x86-64-base.tar (IBM Security Directory Server 6.3.1 Client and Server)
– sds631-linux-x86-64-IM.tar (IBM Installation Manager)
– sds631-linux-x86-64-gskit.tar (GSKit 8)
– sds631-linux-x86-64-db2.tar (DB2 vV9.7)
– sds631-linux-x86-64-ewas.tar (embedded WebSphere Application Server 7.0.0.29)
– sds631-linux-x86-64-jdk.tar (IBM Java Development Kit)

After you create the DVD or uncompress the .tar files, the directory structure is as follows:

/sdsV6.3.1 (top-level directory for untarred files)
– license/ (licenses for Security Directory Server and other provided products)
– quickstart/ (Quick Start Guides in English and other languages)
– ibm_im (IBM Installation Manager)
– ibm_db2/ (DB2)
– ibm_ewas/ (embedded WebSphere Application Server)
– ibm_gskit/ (GSKit 8)
– ibm_jdk/ (IBM Java Development Kit)
– ibm_sds/ (installer files)
– atoc/
– files/
– native/
– Offerings/
– plugins/
– ShareableEntities
– build.properties
– repository.config
– repository.xml

– tools/ (tools including migbkup)
– launchpad/
– SilentInstallScripts/
– launchpad.sh
– sds_install.xml
– write_sds_path.sh
– entitlement/ (entitlement files for proxy server)
– native/ (native package)

Linux x86_64 client-only package

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

After you uncompress the .zip file, the directory structure is as follows:

\sdsV6.3.1 (top-level directory for unzipped files)
– ibm_jdk\ (IBM Java Development Kit)
– ibm_im (IBM Installation Manager)
– ibm_sds\ (installer files)
– launchpad\
– SilentInstallScripts\
– autorun.inf
– license\ (Llicenses for Security Directory Server and other provided products)
– quickstart\ (Quick Start Guides in English and other languages)
– ibm_im\ (IBM Installation Manager)
– imLauncherWindows.bat
– launchpad.exe
– launchpad.ini
– sds_install.xml
– write_sds_path.bat

Directory structure for Linux x86 server packages

The file names for the Security Directory Server 6.3.1 for Linux x86 server packages are:

DVD image: sds631-linux-x86.iso
.tar files:
– sds631-linux-x86-base.tar (IBM Security Directory Server 6.3.1 Client and Server)
– sds631-linux-x86-gskit.tar (GSKit 8)
– sds631-linux-x86-db2.tar (DB2 v9.7)
– sds631-linux-x86-ewas.tar (embedded WebSphere Application Server 7.0.0.29)
– sds631-linux-x86-jdk.tar (IBM Java Development Kit)

After you create the DVD or uncompress the .tar files, the directory structure is as follows:

/sdsV6.3.1 (top-level directory for untarred files)
– appsrv/ (embedded WebSphere Application Server)
– db2 (DB2)
– gskit/ (GSKit 8)
– jdk/ (IBM Java Development Kit)
– ids_detectGskitVersion
– idsinstall_i
– idsNativeInstall.sh
– images/ (native images)
– license (licenses for Security Directory Server and other products)
– responseFile.txt (response file)

Linux x86 client-only package

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

After you uncompress the .zip file, the directory structure is as follows:

\sdsV6.3.1 (top-level directory for unzipped files)
– gskit/(GSKit 8)

– image/
– license/ (licenses for Security Directory Server and other products)
– jdk (IBM Java Development Kit)

Directory structure for Linux ppc server packages

The file names for the Security Directory Server 6.3.1 for Linux ppc server packages are:

DVD image: sds631-linux-ppc64.iso
.tar files:
– sds631-linux-ppc64-base.tar (IBM Security Directory Server 6.3.1 Client and Server)
– sds631-linux-ppc64-gskit.tar (GSKit 8)
– sds631-linux-ppc64-db2.tar (DB2 V9.7)
– sds631-linux-ppc64-ewas.tar (embedded WebSphere Application Server 7.0.0.29)
– sds631-linux-ppc64-jdk.tar (IBM Java Development Kit)

After you create the DVD or uncompress the .tar files, the directory structure is as follows:

/sdsV6.3.1 (top-level directory for untarred files)
– appsrv/ (embedded WebSphere Application Server)
– db2 (DB2)
– gskit/ (GSKit 8)
– jdk/ (IBM Java Development Kit)
– ids_detectGskitVersion
– idsinstall_i
– idsNativeInstall.sh
– images/ (native images)
– license (licenses for Security Directory Server and other products)
– responseFile.txt (response file)

Linux ppc client-only package

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

After you uncompress the .zip file, the directory structure is as follows:

\sdsV6.3.1 (top-level directory for unzipped files)
– gskit/(GSKit 8)
– image/
– license/ (licenses for Security Directory Server and other products)
– jdk (IBM Java Development Kit)

Directory structure for Linux s390 server packages

The file names for the Security Directory Server 6.3.1 for Linux s390 server packages are:

DVD image: sds631-linux-s390x.iso
.tar files:
– sds631-linux-s390x-base.tar (IBM Security Directory Server 6.3.1 Client and Server)
– sds631-linux-s390x-gskit.tar (GSKit 8)
– sds631-linux-s390x-db2.tar (DB2 V9.7)

– sds631-linux-s390x-ewas.tar (embedded WebSphere Application Server 7.0.0.29)
– sds631-linux-s390x-jdk.tar (IBM Java Development Kit)

After you create the DVD or uncompress the .tar files, the directory structure is as follows:

/sdsV6.3.1 (top-level directory for untarred files)
– appsrv/ (embedded WebSphere Application Server)
– db2 (DB2)
– gskit/ (GSKit 8)
– jdk/ (IBM Java Development Kit)
– ids_detectGskitVersion
– idsinstall_i
– idsNativeInstall.sh
– images/ (native images)
– license (licenses for Security Directory Server and other products)
– responseFile.txt (response file)

Linux s390 client-only package

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

After you uncompress the .zip file, the directory structure is as follows:

\sdsV6.3.1 (top-level directory for unzipped files)
– gskit/(GSKit 8)
– image/
– license/ (licenses for Security Directory Server and other products)
– jdk (IBM Java Development Kit)

Directory structure for Solaris x86_64 server packages

The file names for the Security Directory Server 6.3.1 for Solaris x86_64 server packages are:

DVD image: sds631-solaris-x86-64.iso
.tar files:
– sds631-solaris-x86-64-base.tar (IBM Security Directory Server 6.3.1 Client and Server)
– sds631-solaris-x86-64-gskit.tar (GSKit 8)
– sds631-solaris-x86-64-db2.tar(DB2 v9.7)
– sds631-solaris-x86-64-ewas.tar (embedded WebSphere Application Server 7.0.0.29)
– sds631-solaris-x86-64-jdk.tar (IBM Java Development Kit)

After you create the DVD or uncompress the .tar files, the directory structure is as follows:

/sdsV6.3.1 (top-level directory for untarred files)
– appsrv/ (embedded WebSphere Application Server)
– db2 (DB2)
– gskit/ (GSKit 8)
– jdk/ (IBM Java Development Kit)
– ids_detectGskitVersion
– idsinstall_i
– idsNativeInstall.sh

– images/ (native images)
– license (licenses for Security Directory Server and other products)
– responseFile.txt (response file)

Solaris x86_64 client-only package

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

After you uncompress the .zip file, the directory structure is as follows:

\sdsV6.3.1 (top-level directory for unzipped files)
– gskit/(GSKit 8)
– image/
– license/ (licenses for Security Directory Server and other products)
– jdk (IBM Java Development Kit)

Directory structure for Solaris sparc server packages

The file names for the Security Directory Server 6.3.1 for Solaris sparc server packages are:

DVD image:
.tar files:
– sds631-solaris-sparc.iso
– sds631-solaris-sparc-base.tar (IBM Security Directory Server 6.3.1 Client and Server)
– sds631-solaris-sparc-gskit.tar (GSKit 8)
– sds631-solaris-sparc-db2.tar (DB2 v9.7)
– sds631-solaris-sparc-ewas.tar (embedded WebSphere Application Server 7.0.0.29)
– sds631-solaris-sparc-jdk.tar (IBM Java Development Kit)

After you create the DVD or uncompress the .tar files, the directory structure is as follows:

/sdsV6.3.1 (top-level directory for untarred files)
– appsrv/ (embedded WebSphere Application Server)
– db2 (DB2)
– gskit/ (GSKit 8)
– jdk/ (IBM Java Development Kit)
– ids_detectGskitVersion
– idsinstall_i
– idsNativeInstall.sh
– images/ (native images)
– license (licenses for Security Directory Server and other products)
– responseFile.txt (response file)

Solaris Sparc client-only package

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

After you uncompress the .zip file, the directory structure is as follows:

\sdsV6.3.1 (top-level directory for unzipped files)
– gskit/ (GSKit 8)

– image/
– license/ (licenses for Security Directory Server and other products)
– jdk (IBM Java Development Kit)

Installation prerequisites

Installation of IBM Security Directory Server and its corequisite software might require the installation of prerequisites for your operating system. The prerequisites software must be installed before the installation of IBM Security Directory Server and its corequisite software.

Prerequisite packages that are required on various operating systems

You must update your computer with the prerequisite packages that are required for the installation of IBM Security Directory Server and its corequisite products.

The Korn shell is required on AIX, Linux, Solaris, and HP-UX (Itanium) operating systems. On SuSE Linux Enterprise Server, `PDKSH` is required.

The following prerequisite packages are required for installation of IBM Security Directory Server on the following operating systems:

AIX For installation of rpm packages on AIX, download the `rpm` package manager for AIX systems from the ftp://public.dhe.ibm.com/aix/freeSoftware/aixtoolbox/INSTALLP/ppc/rpm.rte website.

Table 7. The prerequisite packages that are required on an AIX operating system

Packages	Reason	Download address
Mozilla Firefox web browser for AIX	To open the launchpad on AIX, a supported version of browser must exist.	For more information about the web browsers for AIX, see the http://www.ibm.com/systems/power/software/aix/browsers/ website.
`gtk+ RPM (gtk2-2.10.6-4.aix5.2.ppc.rpm)`	Eclipse changed the window system requirement from `motif` to `gtk` on UNIX operating systems. For AIX, this Eclipse window system change requires the `gtk` libraries to be installed to support the GUI. For IBM Installation Manager, the GUI is the wizard mode of operation.	For more information about installation of the `gtk` libraries, see the Required gtk libraries for Installation Manager on AIX technote at the http://www.ibm.com/support/docview.wss?uid=swg21631478 website.

Table 7. The prerequisite packages that are required on an AIX operating system (continued)

Packages	Reason	Download address
GNU `tar`	To uncompress archive files that are provided with IBM Security Directory Server on AIX systems, the GNU file archive program is required. You must set the path of the GNU `tar` program before the `tar` program provided with the operating system. The GNU `tar` program is installed in the `/opt/freeware/bin` directory, and the `tar` program that is provided with the operating system in the `/usr/bin` directory. To set the `/opt/freeware/bin` path, run the following command: `export PATH=/opt/freeware/bin:$PATH`.	To download the GNU `tar` archive file (`tar`), see the http://www.ibm.com/systems/power/software/aix/linux/toolbox/alpha.html website.
`X11.adt.lib` fileset	The `X11.adt.lib` fileset is a prerequisite for installing the `idsldap.cltjava631` and `idsldap.webadmin631` packages on AIX systems.	
`xlC.rte 8.0.0.6` and `xlC.aix50.rte 8.0.0.6` or later levels	The IBM C++ Runtime Environment Components for AIX requires the `xlC.rte 8.0.0.6` and `xlC.aix50.rte 8.0.0.6` runtime levels or later.	
`bos.loc.iso.en_US 5.3.0.0`	IBM Security Directory Server, version 6.3.1 requires the minimum base level system locale fileset level at `bos.loc.iso.en_US 5.3.0.0`.	

The `idsldap` user and group

If you select the Server or the Proxy Server feature for installation, the installation program can create the `idsldap` user and group.

The installation program creates the `idsldap` user and group if they do not exist.

Note: On AIX, Linux, and Solaris, installation with the operating system utilities creates the `idsldap` user if it does not exist. However, if the `/home/idsldap` directory exists on Linux and AIX or the `/export/home/idsldap` directory exist on Solaris, it might not be possible to create the `idsldap` user. Therefore, you must ensure that the home directory for `idsldap` does not exist if the `idsldap` user does not exist.

If your environment requires that you to control the idsldap user and group, you can create them before the installation. The idsldap user and group must meet the following requirements:

- The idsldap user must be a member of the idsldap group.
- On AIX, Linux, and Solaris, the root user must be a member of the idsldap group. On Windows, the Administrator must be a member of the idsldap group.
- The idsldap user must have a home directory.
- On AIX, Linux, and Solaris, the default shell for the idsldap user must be the Korn shell.
- The idsldap user can have a password, but is not a must.
- The idsldap user can be the owner of the director server instance.

You must meet all the requirements before the IBM Security Directory Server installation. If the idsldap user exists but does not meet the requirements, the Proxy Server feature installation might fail.

Note: For more information about the user ID requirements for an instance, directory instance, database owner, see "Users and groups that are associated with a directory server instance" on page 117.

You can use Instance Administration Tool to create users and groups when you create a directory server instance. You can also use the operating system utilities to create the idsldap user and group and set them up correctly.

Examples

Run the following operating system utilities to create the idsldap group, the idsldap user, password, and to add root as a member of the idsldap group.

On AIX systems:

To create the idsldap group, run the following command:

```
mkgroup idsldap
```

To create the idsldap user ID as a member of the idsldap group and to set the Korn shell as the default shell, run the following command:

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

To set the password for the idsldap user, run the following command:

```
passwd idsldap
```

To add the root user ID as a member of the idsldap group, run the following command:

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

On Linux systems:

To create the idsldap group, run the following command:

```
groupadd idsldap
```

To create the idsldap user ID as a member of the idsldap group and to set the Korn shell as the default shell, run the following command:

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

To set the password for the idsldap user, run the following command:

```
passwd idsldap
```

To add the root user ID as a member of the idsldap group, run the following command:

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

You can retrieve the values of *rootgroups* for your computer with the `groups root` command.

On Solaris systems:

To create the idsldap group, run the following command:

```
groupadd idsldap
```

To create the idsldap user ID as a member of the idsldap group and to set the Korn shell as the default shell, run the following command:

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

To set the password for the idsldap user, run the following command:

```
passwd idsldap
```

To add the root user ID as a member of the idsldap group, run the following command:

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

To modify the root user ID so that root is a member of the group idsldap, use an appropriate tool.

For more information about the command to add user and group, see the documentation for your operating system.

Installation methods

For the installation of IBM Security Directory Server and its corequisite software, you must choose the appropriate installation method that suits best for your environment.

You can use the following methods for the installation of IBM Security Directory Server and its corequisite software:

- Installation with IBM Installation Manager
- Installation with operating system command-line utilities

CAUTION:

- **You must not use different modes of installation on the same computer. You must run IBM Security Directory Server installation with IBM Installation Manager or operating system command-line utilities, but not both. If you mix the two modes of installation, the installation might not include all the correct packages for a feature.**
- **You must avoid manual installation of DB2 and embedded WebSphere Application Server in their default installation path that is used by IBM Installation Manager. Such manual installation might cause installation, modification, or uninstallation failures when you run these operations with IBM Installation Manager. For more information about the default installation path, see "Default installation locations" on page 25.**

Chapter 3. Installation with IBM Installation Manager

IBM Installation Manager is a tool that you can use for the installation and maintenance of IBM Security Directory Server and its corequisite software.

IBM Installation Manager overview

IBM Installation Manager is an installation wizard that guides you through the steps to install, modify, update, roll back, or uninstall IBM products. It can use remote or local software repositories for installation.

IBM Installation Manager also helps you manage the IBM applications or packages that it installs on your computer in the following ways:

- Keeps record of what you installed
- Determines and shows packages that are available for installation
- Checks prerequisites and interdependencies

IBM Installation Manager includes six wizards that make it easy to maintain packages:

- The **Install** wizard walks you through the installation process. You can install one or more packages at a time. You can accept the default settings or you can modify the settings to create a custom installation where possible. Before you install, you get a complete summary of your selections throughout the wizard.
- The **Update** wizard searches for available updates to packages that are installed on your system. Details of the contents of the update are provided in the wizard. You can choose whether to apply an update.
- The **Modify** wizard helps you modify certain elements of a package that you already installed. During the first installation of the package, you select the features that you want to install. Later, if you require other features, you can use the modify packages wizard to add them to your package. You can also remove features.
- The **Manage Licenses** wizard helps you set up the licenses for your packages. Use this wizard to change your trial license to a full license, to set up your servers for floating licenses, and to select which type of license to use for each package.
- The **Roll Back** wizard helps you to revert to a previous version of a package.
- The **Uninstall** wizard removes a package from your computer. You can uninstall more than one package at a time.

Supported operating systems

You can use IBM Installation Manager for the installation of IBM Security Directory Server on AIX (ppc64), Linux (AMD64/EM64T architecture), and Microsoft Windows.

The following sections list the versions of the operating systems are supported for installation of IBM Security Directory Server with IBM Installation Manager.

If you want to install IBM Security Directory Server on an operating system that is not listed in the following sections:

1. Check whether the version of the operating system is supported for IBM Security Directory Server. For a list of all supported operating systems, see *IBM Security Directory Server Product Overview*.
2. If it is supported, you can use the command-line utilities of the operating system for the installation of IBM Security Directory Server.

AIX (ppc64)

- AIX Version 6.1
- AIX Version 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

IBM Security Directory Server installation package types

To choose the correct IBM Security Directory Server installation package, you must know the available installation package types.

The following IBM Security Directory Server installation package types are available for installation with IBM Installation Manager:

Table 8. IBM Security Directory Server installation package type and the available features for installation

All features	Features in full product installer	Features in client-only installer
IBM DB2	Yes	No
IBM Global Security Kit	Yes	Yes
C Client	Yes	Yes
IBM Java Development Kit	Yes	Yes
Java Client	Yes	Yes
Server	Yes	No
Proxy Server	Yes	No
Web Administration Tool	Yes	No

Note: If you choose to install Web Administration Tool, IBM Installation Manager provides an option to install embedded WebSphere Application Server.

Installation guidelines

You must consider some restrictions before you begin the installation of IBM Security Directory Server with the IBM Installation Manager.

Installation method

When you install IBM Security Directory Server, you can choose to install with either the IBM Installation Manager or the command-line utilities of the operating system. For any future installation or uninstallation of IBM Security Directory Server packages, features, and fix packs, you must use the same installation method on a system. For example, if you install IBM Security Directory Server with the IBM Installation Manager, you must not use command-line utilities to install features or to uninstall the product. If you do so, the IBM Security Directory Server setup might get corrupted or become unusable.

IBM Installation Manager version

IBM Installation Manager Version 1.7.0 and later are supported for installation of IBM Security Directory Server. An error message is displayed on the Install Packages page of IBM Installation Manager and you cannot proceed with the installation in the following scenarios:

- You try to start the installation of IBM Security Directory Server with a previous version of IBM Installation Manager.
- A previous version of IBM Installation Manager is detected when you start the installation of IBM Security Directory Server from the Launchpad program.

Multiple installations

You cannot install multiple copies of the same version of IBM Security Directory Server on the same system. When you select the installation package for the same version again, IBM Installation Manager generates a warning message and you cannot proceed with the installation. However, different versions of IBM Security Directory Server can coexist on the same system.

Installation location on AIX and Linux systems:

IBM Security Directory Server can be installed only at the predefined location on the AIX and Linux systems. The path is specified by default in the **Installation Directory** field in IBM Installation Manager. Though this field is editable in IBM Installation Manager, if you change the path that is specified by default, you cannot click **Next** to proceed with the installation. You must revert to the default installation path for IBM Security Directory Server.

This restriction does not apply to Microsoft Windows operating systems. IBM Security Directory Server can be installed at any custom location on Microsoft Windows operating systems. Even if you select a custom installation location for IBM Security Directory Server, the `idsinstinfo` directory and the `idsinstances.ldif` file that it contains are always created on the partition that is specified by `%SystemDrive%`. If IBM Security Directory Server is installed on the `E:` drive and the operating system is on the `C:` drive, you might observe the following changes:

- The `idsinstinfo` directory is created in the `C:` drive (`C:\idsinstinfo`), instead of in the `E:\Program Files\IBM\ldap` directory.

To know more about the default installation locations, see "Default installation locations" on page 25.

IBM Security Directory Server components

When you install IBM Security Directory Server with the IBM Installation Manager, you can select the components that you want to install. IBM Installation Manager displays the dependencies of each component that you select.

The following IBM Security Directory Server components are available for installation:

IBM DB2

You can install IBM DB2 as a feature. If a supported version of IBM DB2 is installed, you do not require to install DB2 that is provided with the IBM Security Directory Server package. For information about supported versions of DB2 for various operating systems, see *IBM Security Directory Server Product Overview*.

IBM DB2 is required for the full directory server because directory data is stored in a DB2 database. IBM DB2 is not required for Proxy Server.

IBM Global Security Kit

You can install IBM Global Security Kit (GSKit) as a feature along with other features of IBM Security Directory Server. GSKit is an optional feature that is required only if you want to use Secure Sockets Layer (SSL) or Transport Layer Security (TLS) communication protocol. GSKit must be installed on both server and client systems to establish and use secure connections.

C Client

You can install C Client as a feature either by itself or along with other features of IBM Security Directory Server. The C Client feature does not have any dependency on other features. However, the Server and Proxy Server features are dependent on the C Client. When you install the Server or Proxy Server feature, the C Client feature is automatically selected for installation.

C Client is client Software Development Kit (SDK) that provides the tools that are required to develop C-language LDAP applications. C Client package contains the following files and applications:

- Client libraries that provide a set of C-language application programming interfaces (APIs)
- C header files to build and compile LDAP applications
- C server and client utilities
- Sample programs in source form

IBM Java Development Kit

You can install IBM Java Development Kit as a feature either by itself or along with other features of IBM Security Directory Server. When you choose to install IBM Java Development Kit, IBM Installation Manager extracts the compressed file to the `java` subdirectory in the IBM Security Directory Server installation location. IBM Java Development Kit provides IBM Java SDK and Java 1.6 SR 14. IBM Java Development Kit is required to compile Java sample programs, and to run Java programs, such as Instance Administration Tool (**idsxinst**) and Configuration Tool (**idsxcfg**).

Java Client

You can install Java Client as a feature either by itself or along with other features of IBM Security Directory Server. The Java Client feature does not have any dependency on other features. However, the Server and Proxy

Server features are dependent on the Java Client. When you install the Server or Proxy Server feature, the Java Client feature is automatically selected for installation.

Java Client includes the IBM Security Directory Server JNDI toolkit and Java client utilities.

Server You can install Server as a feature along with other features of IBM Security Directory Server. The Server feature has dependency on the C Client and Java Client features. When you select the Server feature for installation, the C Client and Java Client features are selected for installation.

Server is required to create a full directory server or an LDAP server. You must configure a full directory server with a database instance. It processes client requests that require accessing entries that are stored in the database. DB2 is required for a full directory server.

Proxy Server

You can install Proxy Server as a feature along with other features of IBM Security Directory Server. The Proxy Server feature has dependency on the C Client and Java Client features. When you select the Proxy Server feature for installation, the C Client and Java Client features are selected for installation.

Proxy Server is an LDAP server that acts as a front end to the directory. It authenticates client requests for the entire directory and routes requests to full directory servers. Proxy Server can also be used at the front end of a server cluster or a distributed directory to provide failover and load balancing.

Web Administration Tool

You can install Web Administration Tool as a feature either by itself or along with other features of IBM Security Directory Server. Web Administration Tool is an optional feature that is required if you want to manage your directory server remotely. To use Web Administration Tool, you must deploy it on a supported version of embedded WebSphere Application Server or WebSphere Application Server.

When you install Web Administration Tool, Directory Services Markup Language (DSML) files are also copied to your computer. For more information about DSML, see Appendix A, "Directory Services Markup Language," on page 231.

You can use Web Administration Tool as a console to manage directory servers, which can be of the following types:

- IBM Security Directory Server, version 6.3.1
- IBM Security Directory Server, version 6.3
- IBM Security Directory Server, version 6.2
- IBM Security Directory Server, version 6.1
- IBM Security Directory Server, version 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

Important: On z/OS, management of directory data is supported and not server administration.

Embedded WebSphere Application Server
You can install embedded WebSphere Application Server if you choose to install Web Administration Tool. Embedded WebSphere Application Server is required only if you want to deploy and run Web Administration Tool. If a supported version of WebSphere Application Server is installed on your system, you can choose not to install embedded WebSphere Application Server. You can deploy Web Administration Tool on an existing WebSphere Application Server or embedded WebSphere Application Server that is installed your system.

IBM Security Directory Server installation customization

You can customize the IBM Security Directory Server installation to suit your product usage.

You can categorize the IBM Security Directory Server installation for the following purpose:

- Complete product
- Full directory server
- Proxy server
- Client
- Remote server management with Web Administration Tool

Table 9. IBM Security Directory Server features for installation based on the product usage

All features	Full directory server	Proxy server	Client	Remote server management with Web Administration Tool
IBM DB2	Yes	No	No	No
IBM Global Security Kit	Yes	Yes	Yes	No
C Client	Yes	Yes	Yes	No
IBM Java Development Kit	Yes	Yes	Yes	No
Java Client	Yes	Yes	Yes	No
Server	Yes	No	No	No
Proxy Server	No	Yes	No	No
Web Administration Tool	Optional	Optional	No	Yes

Note: If you choose to install Web Administration Tool, IBM Installation Manager provides an option to install embedded WebSphere Application Server.

You can optionally choose embedded WebSphere Application Server and Web Administration Tool for installation with Full directory server and Proxy server.

Default installation locations

If you run IBM Installation Manager for installation, IBM Security Directory Server and its corequisite software is installed in the predefined installation location.

Table 10. The default installation location of IBM Security Directory Server, IBM DB2, embedded WebSphere Application Server, and IBM Java Development Kit.

Operating system	IBM Security Directory Server	IBM DB2	Embedded 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`

IBM Security Directory Server can be installed only at the predefined location on the AIX and Linux systems. The path is specified by default in the **Installation Directory** field in IBM Installation Manager. Though this field is editable in IBM Installation Manager, if you change the path that is specified by default, you cannot click **Next** to proceed with the installation. You must revert to the default installation path for IBM Security Directory Server.

This restriction does not apply to Microsoft Windows operating systems. IBM Security Directory Server can be installed at any custom location on Microsoft Windows operating systems. Even if you select a custom installation location for IBM Security Directory Server, the `idsinstinfo` directory and the `idsinstances.ldif` file that it contains are always created on the partition that is specified by `%SystemDrive%`. If IBM Security Directory Server is installed on the `E:` drive and the operating system is on the `C:` drive, you might observe the following changes:

- The `idsinstinfo` directory is created in the `C:` drive (`C:\idsinstinfo`), instead of in the `E:\Program Files\IBM\ldap` directory.

Installation repositories

The installation repository is the location where the IBM Security Directory Server packages are available for installation.

You can install IBM Security Directory Server from one of the following locations:

- Product setup disk
- Remote shared drive or a local directory that contains an electronic image of the installation package

You can use the repository to start an installation in the following ways:

- Use the Launchpad to start an installation from:
  - A product setup disk
  - An electronic image of the installation package on a remote shared drive or local directory

When you use the Launchpad, the installation process is already configured with the location of the repository that contains the installation package.

- Start IBM Installation Manager directly and specify the repository preferences manually. For example:
  - The URL for the repository on a web server
  - The path to a remote shared drive that contains the product package

Starting the installation

You can start the installation of IBM Security Directory Server either by using the Launchpad or by using IBM Installation Manager set with repository preferences.

Starting the installation with the launchpad

The launchpad provides a single location to start the installation process.

About this task

You can use the launchpad to start an installation in the following scenarios:

- Installation from a product setup disk.
- Installation from a local directory or remote shared drive that contains an electronic image of the product package.

When you use the launchpad to start the installation, IBM Installation Manager is automatically installed if a supported version is not on your system.

Procedure

1. Go to the root directory of your installation package.
   - If you are using the IBM Security Directory Server product setup disk, insert the disk in the disk drive.
   - If you are installing from electronic image of the product installation package, change to the directory where the image is located.
2. Start the launchpad.

   Note: For Windows operating systems, right-click the `.exe` file for the launchpad, and select **`Run as administrator`**.

Operating system	Command to run:
Windows 32-bit	`launchpad.exe`
Windows 64-bit	`launchpad64.exe`
AIX and Linux	`./launchpad.sh`

   IBM Security Directory Server launchpad starts and the Welcome page is displayed.
3. On the **Welcome** page, select the language from the **Select a language** list, and click **OK**.
4. On the left navigation area, click **IBM Security Directory Server Installation**.
5. On the **Installation** page, click the **Launch the IBM Security Directory Server installer** link. IBM Installation Manager starts.
6. Ensure that the following packages are selected for installation:
   - IBM Installation Manager (It is listed only if a supported version is not already installed on your system.)

- IBM Security Directory Server

7. Continue with the steps to install IBM Security Directory Server. See "Installing with IBM Installation Manager" on page 28.
8. After you finish the installation, click **Exit**.

Results

When you use the launchpad to start the IBM Security Directory Server installation, the launchpad creates a temporary file, `sds631.temp`, which contains the media path name. The `sds631.temp` file is created in the following location on the operating system:

AIX and Linux
`/tmp`

Microsoft Windows
The default temporary directory of the system set in the *TEMP* variable.

You cannot install multiple copies of the same version of IBM Security Directory Server on the same system. When you select the installation package for the same version again, IBM Installation Manager generates a warning message and you cannot proceed with the installation. However, different versions of IBM Security Directory Server can coexist on the same system.

What to do next

Proceed with the steps to install IBM Security Directory Server. See "Installing with IBM Installation Manager" on page 28.

Starting the installation by setting repository preferences

If the supported version of IBM Installation Manager is installed on your system, you can start it directly and specify the repository preferences.

Before you begin

IBM Installation Manager Version 1.7.0 and later are supported for installation of IBM Security Directory Server. An error message is displayed on the Install Packages page of IBM Installation Manager and you cannot proceed with the installation in the following scenarios:

- You try to start the installation of IBM Security Directory Server with a previous version of IBM Installation Manager.
- A previous version of IBM Installation Manager is detected when you start the installation of IBM Security Directory Server from the Launchpad program.

If your system contains IBM Installation Manager earlier than version 1.7.0, you must upgrade to version 1.7.0 or later. You can choose one of the following ways to install the required IBM Installation Manager version.

- Start the IBM Installation Manager installation with the Launchpad. For more information, see "Starting the installation with the launchpad" on page 26.
- Download IBM Installation Manager, version 1.7.0 or later for your operating system. For more information about silent mode installation of IBM Installation Manager, see the IBM Installation Manager documentation at http://pic.dhe.ibm.com/infocenter/install/v1r6/topic/com.ibm.cic.agent.ui.doc/helpindex_imic.html.

About this task

You can start the installation by setting the repository preferences in the following installation scenarios:

- Installation from a local directory or remote shared drive that contains the product package that is downloaded from IBM Passport Advantage®.
- Installation from a URL for the repository on a web server.

Procedure

1. Start IBM Installation Manager.

   Windows
   From the **Start** menu, click **All Programs** > **IBM Installation Manager** > **IBM Installation Manager**.

   AIX and Linux
   Enter the following command at the command prompt. Modify the following default path if IBM Installation Manager is installed at a different location.

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

2. On the Start page of IBM Installation Manager, click **File** > **Preferences**.
3. On the Repositories page, click **Add Repository**.
4. In the Add Repository page, enter the URL of the repository location or browse to it and set a file path.
5. Click **OK**. If you provided an HTTPS or restricted repository location, then you are prompted to enter a user ID and password. The new or changed repository location is listed.
6. To verify the repository access, click **Test Connections**.
7. Click **OK** to exit the Repositories page.

Results

You cannot install multiple copies of the same version of IBM Security Directory Server on the same system. When you select the installation package for the same version again, IBM Installation Manager generates a warning message and you cannot proceed with the installation. However, different versions of IBM Security Directory Server can coexist on the same system.

What to do next

Proceed with the steps to install IBM Security Directory Server. See “Installing with IBM Installation Manager.”

Installing with IBM Installation Manager

Complete the steps to install IBM Security Directory Server with the IBM Installation Manager.

Before you begin

Start the installation.

Procedure

1. On the IBM Installation Manager Start page, click **Install**.

2. On the Install Packages page, select the IBM Security Directory Server package for installation.
3. Click **Next**. IBM Installation Manager checks for the prerequisite packages on your computer.
4. If your computer does not meet the prerequisites check, the **Validation Results** page shows the prerequisites.
   a. To verify whether the prerequisite requirements are met after you install the prerequisite packages, click **Recheck Status**. For more information about the prerequisites, see "Prerequisite packages that are required on various operating systems" on page 15.
   b. If all prerequisites are met, click **Next**.
5. Click **I accept the terms in the license agreement**, and click **Next**. The shared resources directory location is displayed.
6. Optional: Use the default path or specify a path in the **Shared Resources Directory** field. The shared resources directory is the directory where installation artifacts are stored so that they can be used by one or more product package groups. You can specify the shared resources directory only the first time that you install a package.
7. Click **Next**. The package group name and the default installation location are shown. The **Create a new package group** option is selected by default and only this option is supported for the installation of IBM Security Directory Server. A package group represents a directory in which packages share resources with other packages in the same group. A package group is assigned a name automatically.

   Restriction:

   IBM Security Directory Server can be installed only at the predefined location on the AIX and Linux systems. The path is specified by default in the **Installation Directory** field in IBM Installation Manager. Though this field is editable in IBM Installation Manager, if you change the path that is specified by default, you cannot click **Next** to proceed with the installation. You must revert to the default installation path for IBM Security Directory Server.

   For a list of the default installation locations on various operating systems, see "Default installation locations" on page 25.

   This restriction does not apply to Microsoft Windows operating systems. IBM Security Directory Server can be installed at any custom location on Microsoft Windows operating systems. Even if you select a custom installation location for IBM Security Directory Server, the `idsinstinfo` directory and the `idsinstances.ldif` file that it contains are always created on the partition that is specified by `%SystemDrive%`. If IBM Security Directory Server is installed on the `E:` drive and the operating system is on the `C:` drive, you might observe the following changes:

   - The `idsinstinfo` directory is created in the `C:` drive (`C:\idsinstinfo`), instead of in the `E:\Program Files\IBM\ldap` directory.
8. Click **Next**.
9. On the **Install Packages** page, select the features that you require. To view the dependents of a selected feature or the feature's dependencies on other features, select the **Show dependencies** check box.

Table 11. IBM Security Directory Server features available for installation in a full product or a client-only package

All features	Installation dependencies	Features in full product package	Features in client-only package
IBM DB2	None	Yes	No
IBM Global Security Kit	None	Yes	Yes
C Client	None	Yes	Yes
IBM Java Development Kit	None	Yes	Yes
Java Client	None	Yes	Yes
Server	C Client Java Client	Yes	No
Proxy Server	C Client Java Client	Yes	No
Web Administration Tool	None	Yes	No

10. Click **Next**.
11. If you select the IBM DB2 feature for installation, click **IBM DB2** and then take one of the following actions:
    - To install IBM DB2, take the following actions:
      a. Click **Install DB2**.
      b. In the **DB2 installable path** field, specify the path name of the DB2 installable. You can click **Browse** and specify the path.
      c. On Windows, enter the system user ID that you want to the `DB2ADMNS` or the `DB2USERS` groups in the **User name** field. You can use this user ID to run local DB2 applications and tools on the computer. If the user ID does not exist, the installation program creates the user account.
      d. On Windows, enter the password for the user ID in the **Password** filed. If your password does not meet the password policy set on your computer, the installation might fail.
      e. On Windows, enter the password for the user ID in the **Confirm password** filed.
      f. Click **Next**.
    - If your computer contains a supported version of IBM DB2 installed on it, take one of the following actions:
      a. To continue with an existing IBM DB2 version, click **Continue with the existing DB2**.

         Important: If you choose to continue with the existing DB2 during the installation, IBM Installation Manager updates its registry with the DB2 feature entry.
      b. From the list, select a supported DB2 version that you want to use with IBM Security Directory Server.
      c. Click **Next**.
12. If you select the IBM Global Security Kit feature for installation, click **IBM Global Security Kit** and then take one of the following actions:
    - If your computer does not contain GSKit, version 8.0 or later installed on it, take the following actions:

a. Click **Install GSKit**.
b. In the **GSKit installable path** field, specify the path name of the GSKit installable. You can click **Browse** and specify the path.

   Note: The path you specify must contain both 64-bit and 32-bit GSKit installable.
c. Click **Next**.

- If your computer contains GSKit, version 8.0 or later installed on it, take one of the following actions:
  a. To continue with an existing GSKit version, click **Continue with the existing GSKit**.

     Important: If you choose to continue with the existing GSKit during the installation, IBM Installation Manager updates its registry with the GSKit feature entry.
  b. Click **Next**.

13. If you select the IBM Java Development Kit feature for installation, click **IBM Java Development Kit**, and complete the following steps:
    a. In the **IBM Java Development Kit** field, specify the file name with path name of the JDK compressed file. You can click **Browse** and specify the path.
    b. Click **Next**.
14. If you select theWeb Administration Tool feature for installation, click **Web Administration Tool**, and complete the following steps:
    a. To install embedded WebSphere Application Server, take the following actions:
       1) Select **Install Embedded WebSphere Application Server**.
       2) In the **Embedded WebSphere Application Server installable path** field, specify the path name of the embedded WebSphere Application Server installable. You can click **Browse** and specify the path.
    b. To deploy Web Administration Tool, take one of the following actions:
       - To deploy in the embedded WebSphere Application Server that is in the default installation path, click **Deploy in the default Embedded WebSphere Application Server**.

         Note: If a previous version of Web Administration Tool exists, the installation program migrates it to the current version if the following conditions are met:
         1) The previous version of Web Administration Tool and embedded WebSphere Application Server are installed in the default installation path.
         2) The previous version of Web Administration Tool is deployed in embedded WebSphere Application Server that is in the default installation path.
         3) Web Administration Tool that is provided with IBM Security Directory Server, version 6.1, 6.2, or 6.3 are supported for migration.
       - To deploy in the WebSphere Application Server or embedded WebSphere Application Server that is in a custom installation path, click **Deploy in an existing WebSphere Application Server**.

1) In the **WebSphere Application Server or Embedded WebSphere Application Server installation path** field, specify the installation path of an existing web application server.

- To deploy Web Administration Tool later in a supported web application server, click **Deploy manually later**.

15. Click **Next**. The preinstallation summary information is displayed, which includes the installation location, list of packages, and repository information.
16. Verify the summary information, and click **Install**. The installation starts and a progress bar is displayed. After the installation, the post-installation summary page is displayed.
17. Click the **View Log File** link to verify that the installation was successful. For more information, see Chapter 5, "IBM Installation Manager log files," on page 41.
18. To start one of the following programs, take one of the following actions:
    - To start Instance Administration Tool, click **Instance Administration Tool (idsxinst)**.
    - If you do not want to start any program, click **None**.
19. Click **Finish**.
20. Click **File** > **Exit**.

Results

If the installation is successful, IBM Security Directory Server in installed in the installation location. For information about the default installation location, see "Default installation locations" on page 25. If the installation is unsuccessful for any of the selected features, installation of the IBM Security Directory Server packages is rolled back.

What to do next

After the IBM Security Directory Server installation, you must take the following actions:

- To use IBM Security Directory Server as a full directory server, create a directory server instance. For more information, see "Creating the default directory server instance" on page 130.
- To use IBM Security Directory Server as a proxy server, create a proxy server instance. For more information, see "Creating a proxy server instance with custom settings" on page 138.

Silent mode installation

You can use silent mode installation to install IBM Security Directory Server on multiple system without any manual interventions.

For silent mode installation, you must complete the following activities:

1. Install IBM Installation Manager, if not present.
2. Use the default response file or record a customized response file.
3. Install the packages.

Response file for silent installation

In silent mode installation, the user interface is not available. The response file serves as the input for installation. A response file is an XML file that contains the data that are required to complete silent installation.

Recording a customized response file

You can record response file for the following tasks:

- Installing packages
- Modifying packages
- Uninstalling packages

To record a response file, you must record the preferences and installation actions with IBM Installation Manager in user interface mode. When you first record a response file for silent installation, you can choose not to install the packages with the **-skipInstall** *agentDataLocation* parameter.

The *agentDataLocation* location stores the data for installing the product. To record a response file for silent modification or uninstallation of the product, you must use the same *agentDataLocation* location with the **-skipInstall** parameter.

For multiple installation scenario, you must record different response files with a different *agentDataLocation* location for each scenario.

For more information about recording a response file for silent installation, see the IBM Installation Manager documentation at http://pic.dhe.ibm.com/infocenter/install/v1r6/topic/com.ibm.silentinstall12.doc/topics/c_silent_response_files.html.

Verification of silent installation

After the installation is complete, you must verify the silent installation. You can verify the installation in one of the following ways:

- Checking the return code
- Checking the log file
- Checking the packages

Installing silently with a response file

Use IBM Security Directory Server silent installation to install the required packages without any manual interventions.

Before you begin

IBM Installation Manager, version 1.7.0 or later is required for the silent installation of IBM Security Directory Server packages.

About this task

You can use the default response file or record a customized response file and use it as the input file for silent installation.

Procedure

1. Log in to the system as an administrator.
2. Access the **IBMIM** command in the IBM Installation Manager installation location.

Operating system	Default location of the **IBMIM** command:
Microsoft Windows	`C:\Program Files\IBM\InstallationManager\eclipse`
AIX and Linux	`/opt/IBM/InstallationManager/eclipse`

3. Optional: Run the **IBMIM** command to record a response file for installation.

   Tip: You can use the sample response file for installation. See the default location of sample response file, "Silent mode installation" on page 32.

   a. To record the installation steps without installing the product, run the following commands on various operating systems:

      Microsoft Windows

      ```
      IBMIM.exe -record path_name\responseFile.xml -skipInstall
      agentDataLocation
      ```

      AIX and Linux

      ```
      ./IBMIM -record path_name/responseFile.xml -skipInstall
      agentDataLocation
      ```

      The command opens IBM Installation Manager.

   b. Set the IBM Security Directory Server repository. For more information, see 2 on page 28

   c. Complete the IBM Security Directory Server installation recording. For more information, see "Installing with IBM Installation Manager" on page 28

4. Run the **imcl** command to start silent installation with the response file as input. The **imcl** command should be present in <*IBM_Installation_Manager_install_dir*>/eclipse/tools.

Operating system	Command to run:
Microsoft Windows	`imcl.exe input path_name\responseFile.xml -acceptLicense -showProgess`
AIX and Linux	`./imcl input path_name/responseFile.xml -acceptLicense -showProgess`

   Note: There are many other parameters that can be used along with **imcl** command. For more details, see the **imcl** command help.

5. Verify the installation summary and the log files.

Operating system	Default log path:
Microsoft Windows	`C:\ProgramData\IBM\InstallationManager\logs`
AIX and Linux	`/var/ibm/InstallationManager/logs/`

6. Verify whether the IBM Security Directory Server packages are at the required level.

Operating system	Verifying packages:
Microsoft Windows	See "Verifying IBM Security Directory Server features with IBM Installation Manager" on page 81.

Operating system	Verifying packages:
AIX and Linux	See "Verifying IBM Security Directory Server features with IBM Installation Manager" on page 81.

Results

If the installation is successful, IBM Security Directory Server in installed in the IBM Security Directory Server installation location. For information about the default installation location, see "Default installation locations" on page 25. If the installation is unsuccessful for any of the selected features, installation of the IBM Security Directory Server packages is rolled back.

What to do next

Note: If you select Instance Administration Tool to open when you record your response file for installation, Instance Administration Tool does not open after the IBM Security Directory Server silent installation.

If you selected the Server or Proxy Server feature for installation, open Instance Administration Tool to create a directory server instance or a proxy server instance. See "Starting Instance Administration Tool" on page 127.

Chapter 4. Modification with IBM Installation Manager

You can install IBM Security Directory Server features that you did not install earlier, uninstall features that you already installed, or both with IBM Installation Manager.

You cannot remove a feature if it is a prerequisite for other installed features. You can remove a dependency only if all of the dependent features are selected for removal or are removed.

Important: If you choose to continue with an existing version of a DB2 or GSKit during the installation, IBM Installation Manager updates its registry with the feature entry. If you remove a feature that was installed with the **Continue with the existing** option, Installation Manager takes the following actions:

- Removes the feature entry from the IBM Installation Manager registry.
- Does not uninstall the feature from the computer.

Modifying features with IBM Installation Manager

Complete the steps to modify IBM Security Directory Server features with IBM Installation Manager.

Before you begin

You must stop all IBM Security Directory Server client and server processes.

- Directory server
- Administration server
- LDAP traces
- Custom LDAP applications

If any processes are in use, the programs and libraries cannot be removed.

Procedure

1. Start IBM Installation Manager.
   - AIX and Linux:
     a. Open a command-line window and change to the directory that contains IBM Installation Manager. The following directory is the default IBM Installation Manager installation location:
        `opt/IBM/InstallationManager/eclipse`
     b. Run the following command:
        `./IBMIM`
   - Microsoft Windows:
     a. Click **Start** > **All Programs** > **IBM Installation Manager** > **IBM Installation Manager**.
2. Click **Modify**.
3. Select **IBM Security Directory Server**, and then click **Next**.
4. On the **Modify Packages** page, you must take the following actions:
   a. Select the features that you want to install.

b. Clear the features that you want to uninstall.

Table 12. IBM Security Directory Server features available for modifications in full product and client-only packages

All features	Installation dependencies	Features in full product package	Features in client-only package
IBM DB2	None	Yes	No
IBM Global Security Kit	None	Yes	Yes
C Client	None	Yes	Yes
IBM Java Development Kit	None	Yes	Yes
Java Client	None	Yes	Yes
Server	C Client Java Client	Yes	No
Proxy Server	C Client Java Client	Yes	No
Web Administration Tool	None	Yes	No

Important: If you choose to continue with an existing version of a DB2 or GSKit during the installation, IBM Installation Manager updates its registry with the feature entry. If you remove a feature that was installed with the **Continue with the existing** option, Installation Manager takes the following actions:

- Removes the feature entry from the IBM Installation Manager registry.
- Does not uninstall the feature from the computer.

If DB2 instances exist that you created with the DB2 copy installed with IBM Installation Manager, you cannot remove IBM DB2. In such situation, you must manually remove the DB2 instances and then try again. It is advisable to take database backup before you remove DB2 instances.

c. Click **Next**.

5. If you select the IBM DB2 feature for installation, click **IBM DB2** and then take one of the following actions:
   - To install IBM DB2, take the following actions:
     a. Click **Install DB2**.
     b. In the **DB2 installable path** field, specify the path name of the DB2 installable. You can click **Browse** and specify the path.
     c. On Windows, enter the system user ID that you want to the `DB2ADMNS` or the `DB2USERS` groups in the **User name** field. You can use this user ID to run local DB2 applications and tools on the computer. If the user ID does not exist, the installation program creates the user account.
     d. On Windows, enter the password for the user ID in the **Password** filed. If your password does not meet the password policy set on your computer, the installation might fail.
     e. On Windows, enter the password for the user ID in the **Confirm password** filed.
     f. Click **Next**.

- If your computer contains a supported version of IBM DB2 installed on it, complete the following steps:
  a. To continue with an existing IBM DB2 version, click **Continue with the existing DB2**.

     Important: If you choose to continue with the existing DB2 during the installation, IBM Installation Manager updates its registry with the DB2 feature entry.
  b. From the list, select a supported DB2 version that you want to use with IBM Security Directory Server.
  c. Click **Next**.

6. If you select the IBM Global Security Kit feature for installation, click **IBM Global Security Kit** and then take one of the following actions:
   - If your computer does not contain GSKit, version 8.0 or later installed on it, complete the following steps:
     a. Click **Install GSKit**.
     b. In the **GSKit installable path** field, specify the path name of the GSKit installable. You can click **Browse** and specify the path.

        Note: The path you specify must contain both 64-bit and 32-bit GSKit installable.
     c. Click **Next**.
   - If your computer contains GSKit, version 8.0 or later installed on it, complete the following steps:
     a. To continue with an existing GSKit version, click **Continue with the existing GSKit**.

        Important: If you choose to continue with the existing GSKit during the installation, IBM Installation Manager updates its registry with the GSKit feature entry.
     b. Click **Next**.
7. If you select the IBM Java Development Kit feature for installation, click **IBM Java Development Kit**, and complete the following steps:
   a. In the **IBM Java Development Kit** field, specify the file name with path name of the JDK compressed file. You can click **Browse** and specify the path.
   b. Click **Next**.
8. If you select theWeb Administration Tool feature for installation, click **Web Administration Tool** and complete the following steps:
   a. To install embedded WebSphere Application Server, take the following actions:
      1) Select **Install Embedded WebSphere Application Server**.
      2) In the **Embedded WebSphere Application Server installable path** field, specify the path name of the embedded WebSphere Application Server installable. You can click **Browse** and specify the path.
   b. To deploy Web Administration Tool, take one of the following actions:
      - To deploy in the embedded WebSphere Application Server that is in the default installation path, click **Deploy in the default Embedded WebSphere Application Server**.

Note: If a previous version of Web Administration Tool exists, the installation program migrates it to the current version if the following conditions are met:

1) The previous version of Web Administration Tool and embedded WebSphere Application Server are installed in the default installation path.
2) The previous version of Web Administration Tool is deployed in embedded WebSphere Application Server that is in the default installation path.
3) Web Administration Tool that is provided with IBM Security Directory Server, version 6.1, 6.2, or 6.3 are supported for migration.

- To deploy in the WebSphere Application Server or embedded WebSphere Application Server that is in a custom installation path, click **Deploy in an existing WebSphere Application Server**.
  1) In the **WebSphere Application Server or Embedded WebSphere Application Server installation path** field, specify the installation path of an existing web application server.
- To deploy Web Administration Tool later in a supported web application server, click **Deploy manually later**.

9. Click **Next**.

   Important: If you choose to continue with an existing version of a DB2 or GSKit during the installation, IBM Installation Manager updates its registry with the feature entry. If you remove a feature that was installed with the **Continue with the existing** option, Installation Manager takes the following actions:

   - Removes the feature entry from the IBM Installation Manager registry.
   - Does not uninstall the feature from the computer.

10. Verify the summary information and click **Modify**.
11. Optional: If an error occurs during modification, click **View Log File** to read the details. For more information, see Chapter 5, "IBM Installation Manager log files," on page 41.
12. Click **Finish**.
13. Click **File** > **Exit**.

Results

If the modification is successful, you can observe the following change:

- IBM Security Directory Server features that you selected to add are installed in the installation location. For information about the default installation location, see "Default installation locations" on page 25.
- IBM Security Directory Server features that you selected to remove are uninstalled.

Chapter 5. IBM Installation Manager log files

You can verify the installation, modification, or uninstallation of IBM Security Directory Server and its components by checking the log file that the IBM Installation Manager creates.

If an error occurs during the installation, modification, or uninstallation of IBM Security Directory Server and its components, you must check the log files. IBM Installation Manager creates the log files in the default location.

Table 13. The default location of IBM Installation Manager log files on various operating systems

Operating system	**Default log location of IBM Installation Manager**
AIX and Linux	`/var/ibm/InstallationManager/logs`
Microsoft Windows	`C:\ProgramData\IBM\InstallationManager\logs`

The default locations are applicable to all supported versions of AIX, Linux, and Microsoft Windows.

Chapter 6. Native installation and configuration using scripts

You can install and configure IBM Security Directory Server using scripts.

Installation roadmap

Use the checklist in this topic to install IBM Security Directory Server on Linux x86, Linux i/pSeries, Linux s390, Solaris, and HP-UX systems.

1. Be sure that your system meets the minimum required hardware and software. For more information, see the *IBM Security Directory Server Version 6.3.1 System Requirements Guide*.
2. Install the prerequisite software, such as DB2. If not already installed, be sure that the path to DB2 installable is accessible and have the required permissions.
3. If you plan to use any of the following features, you must install the optional prerequisite software. If not already installed, be sure that the path to the optional prerequisite software is accessible and have the required permissions.
   - For using the Web Administration tool, a supported embedded version of WebSphere Application Server or WebSphere Application Server is required. Also, a supported version of browser is required.
   - For Secure Socket Layer (SSL) or Transport Layer Security (TLS) encryption, a supported version of IBM Global Security Kit (GSKit) is required.
4. On Linux x86, Linux i/pSeries, Linux s390, Solaris, and HP-UX systems, use the **idsNativeInstall** installation program to install IBM Security Directory Server packages and other required software.
5. After installing IBM Security Directory Server, use the **idsdefinst** command to create and configure a directory server instance.
6. Start the directory server instance.
7. Load the sample LDIF file into the database. See the *IBM Security Directory Server Version 6.3.1 Administration Guide* for information about using the directory server instance.

Note: The native installation script, **idsNativeInstall** is not provided for Windows, AIX, and Linux x86_64 (64-bit) operating systems. You can use the IBM Installation Manager or the operating system's command-line utilities to install manually on these operating systems.

Installing IBM Security Directory Server packages on Linux, Solaris, and HP-UX platforms

Use steps provided to install or upgrade IBM Security Directory Server packages on Linux x86, Linux i/pSeries, Linux s390, Solaris, and HP-UX systems.

Before you begin

Before you begin installing IBM Security Directory Server packages, you must do the following steps:

1. Log on the system with root privileges.
2. Extract the IBM Security Directory Server Version 6.3.1 archive file to a directory, for example/`sdsV6.3.1`, with adequate disk space.

3. Stop all IBM Security Directory Server client and server processes, including the directory server, administration server, and custom LDAP applications. Programs and libraries cannot be replaced while they are in use. If tracing is set, run `ldtrc off` to stop the trace process. See the "Basic server administration tasks" and "Directory administration server" sections in the *Administration Guide* for instructions to stop the directory server instances and administration servers.

About this task

You can use the **idsNativeInstall** command to install or upgrade IBM Security Directory Server packages on Linux x86, Linux i/pSeries, Linux s390, Solaris, and HP-UX systems. You can also use the **idsNativeInstall** command to optionally install DB2, GSKit, and embedded WebSphere Application Server, if they are not already installed on your system.

Note:

- The native installation script, **idsNativeInstall** is not provided for Windows, AIX, and Linux x86_64 (64-bit) operating systems. You can use the IBM Installation Manager or the operating system's command-line utilities to install manually on these operating systems.
- On HP-UX systems, IBM Security Directory Server client-only packages are available for installation.

Procedure

1. Go to the directory with the **idsNativeInstall** installation program and the `responseFile.txt` file. The `idsNativeInstall` and `responseFile.txt` files must be present in the same directory.
2. Update the `responseFile.txt` file for the following entries. By default, the values of the feature installation variables are set to `false` and their corresponding path variables are not set.
   - To install DB2, set the *db2FeatureInstall* variable to `true` and update the *db2InstallimagePath* variable with the absolute path of DB2 installable. For example:

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

     Important: For full directory server, DB2 must be installed on the system. If you set the DB2 variables, *db2FeatureInstall* and *db2InstallimagePath*, then DB2 is installed in `/opt/ibm/sdsV6.3.1db2` on Linux or `/opt/IBM/sdsV6.3.1db2` on Solaris. If a DB2 version is already installed in the specified location, then the installation overwrites the existing files.
   - To install GSKit, set the *gskitFeatureInstall* variable to `true` and update the *gskitInstallimagePath* variable with the absolute path of GSKit installable. For example:

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

     Important: To configure a directory server instance to communicate over SSL or TLS, a required version of GSKit must be installed on the system.
   - To install IBM Java Development Kit, set the *JDKFeatureInstall* variable to `true` and update the *JDKInstallimagePath* variable with the absolute path of IBM Java Development Kit installable. For example:

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

IBM Java Development Kit is installed in `/opt/ibm/ldap/V6.3.1/java` on Linux and `/opt/ibm/ldap/V6.3.1/java` on Solaris systems.

- To install embedded version of WebSphere Application Server, set the *eWasFeatureInstall* variable to `true` and update the *eWasInstallimagePath* variable with the absolute path of embedded version of WebSphere Application Server installable. For example:

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

  The embedded version of WebSphere Application Server is installed in `/opt/ibm/ldap/V6.3/appsrv` on Linux and `/opt/ibm/ldap/V6.3/appsrv` on Solaris systems.
- To install IBM Security Directory Server Version 6.3.1 general availability (GA), update the *tdsInstallimagePath* variable with the absolute path of IBM Security Directory Server Version 6.3.1 GA installable. For example:

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

  If you specify `/sdsV6.3.1` as your IBM Security Directory Server Version 6.3.1 installable location, ensure that the following files are present in the `/sdsV6.3.1` directory.

  ```
  idsinstall
  idsinstall_i
  ids_detectGskitVersion
  ```

  The IBM Security Directory Server Version 6.3.1 packages must be present in the `/sdsV6.3.1/tdsfiles` directory.

3. Run the **idsNativeInstall** command at the command prompt.

Results

After you finish running the **idsNativeInstall** command, it installs IBM Security Directory Server 6.3.1 packages. The **idsNativeInstall** command also installs DB2, GSKit, IBM Java Development Kit, or embedded WebSphere Application Server based on the values in the response file.

Note: If IBM Security Directory Server Version 6.3.1 is not installed on the system, then all the components of IBM Security Directory Server Version 6.3.1 are installed. IBM Security Directory Server Version 6.3.1 is installed in `/opt/ibm/ldap/V6.3.1/` on Linux and `/opt/ibm/ldap/V6.3.1/` on Solaris and HP-UX systems.

What to do next

After installing IBM Security Directory Server, you must verify whether the IBM Security Directory Server packages are installed. For more information about verifying logs, see"Verifying installation logs."

Verifying installation logs

Determine the log file that you must check to verify the installation status on Linux x86, Linux i/pSeries, Linux s390, Solaris, and HP-UX systems.

After you finish the installation, the **idsNativeInstall** command shows appropriate messages which indicate whether the installation was successful or not. To verify whether the IBM Security Directory Server packages are installed, check the following log file for the installation logs.

The log file is `/var/idsldap/V6.3/idsNativeInstall_timestamp.log`.

After verifying the installation log, ensure that all packages are installed successfully and are at the required level. For more information about querying the version number of the installed packages, see"Querying the IBM Security Directory Server packages."

Querying the IBM Security Directory Server packages

Verify the IBM Security Directory Server packages by querying IBM Security Directory Server packages on supported platforms.

About this task

After you install the IBM Security Directory Server packages, you must ensure that all the packages are at the required level. This task helps you to query the version number of installed IBM Security Directory Server packages.

Procedure

Log on to the system on which you installed the IBM Security Directory Server packages and run the commands with root privileges.

- On AIX systems: Run the **lslpp** command. For example:
  ```
  lslpp -l 'idsldap*'
  ```
- On Linux systems: Run the **rpm** command. For example:
  ```
  rpm -qa | grep idsldap
  ```
- On Solaris systems:
  1. To list the installed packages, run the **pkginfo** command. For example:
     ```
     pkginfo | grep IDSl
     ```
  2. To query the version of a particular IBM Security Directory Server package, run the **pkgparam** command. For example:
     ```
     pkgparam IDSlbc63 VERSION
     ```
- On HP-UX (Itanium) systems: Run the **swlist** command. For example:
  ```
  swlist | grep idsldap
  ```

IBM Security Directory Server uninstallation

Points you must consider before uninstalling IBM Security Directory Server.

When you uninstall IBM Security Directory Server, the instances and their configuration files are not removed.

Uninstalling IBM Security Directory Server: An overview

This task provides an overview on uninstalling IBM Security Directory Server product.

Before you begin

To uninstall IBM Security Directory Server, you must log on with root privileges on AIX, Linux, Solaris, or HP-UX systems; and as an administrator group member on Windows systems.

About this task

This task provides an overview of steps that you must do to uninstall IBM Security Directory Server.

Procedure

1. Stop all IBM Security Directory Server client or server processes, including the directory server, administration daemon, and custom LDAP applications. Programs and libraries cannot be replaced while they are in use. If tracing is set, run the **ldtrc off** command to turn tracing off.
2. Based on the operating system and mode of IBM Security Directory Server installation, use the same mode to uninstall IBM Security Directory Server. The available methods to uninstall IBM Security Directory Server packages are:
   a. GUI uninstallation program.
   b. Operating system utilities. The package names on Linux systems are slightly different for updates than for the GA version. For example, the package name for the base client for the GA version on xSeries Linux is `idsldap-cltbase63-6.3.0-0.i386.rpm`. You can use the **rpm -qa** command to list all packages.
3. After uninstalling IBM Security Directory Server, query if the all IBM Security Directory Server packages are removed successfully. For more information, see "Querying the IBM Security Directory Server packages" on page 46.

Related information:

 http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.IBMDS.doc/toc.xml
For more information about uninstalling IBM Security Directory Server, see the *Uninstalling IBM Security Directory Server* chapter in the *IBM Security Directory Server Version 6.3.1 Installation and Configuration Guide*.

Chapter 7. Installation of IBM DB2

To create an IBM Security Directory Server instance with a DB2 database configured with it, your computer must contain a supported version of IBM DB2 installed on it.

The IBM Security Directory Server installation media provides a supported version of IBM DB2. If you are using the operating system utilities for IBM Security Directory Server installation, you must complete IBM DB2 installation. When you run IBM Security Directory Server installation, the property files are updated with the details of the supported IBM DB2 version. If your computer contains a supported version of IBM DB2 installed on it, you can use the DB2 and configure with your directory server instance. For more information about the updating the `ldapdb.properties` file, see Updating the `ldapdb.properties` file manually.

For installing IBM DB2, access the IBM Security Directory Server installation media and go to directory that contains the IBM DB2 installable.

You must meet the DB2 prerequisites before you run IBM DB2 installation. To verify whether your computer meets the DB2 prerequisites check, run the **db2prereqcheck** command. If there are any missing packages on your computer, you must update your computer for the required packages.

On AIX, Linux, and Solaris, you can use the **db2_install** command for the installation of IBM DB2. On Windows, use the **setup.exe** command for the installation of IBM DB2.

On System x Linux on Intel 32-bit architecture, you must choose Workspace Server Edition by entering WSE. For other supported operating systems, choose Enterprise Server Edition by entering ESE.

After the IBM DB2 installation, check the `/tmp/db2_install_log.`*XXXXX* file to verify that the installation was successful. The *XXXXX* is a random number that is associated with the installation.

For more information about DB2 prerequisites and IBM DB2 installation, see the IBM DB2 documentation at http://pic.dhe.ibm.com/infocenter/db2luw/v9r7/topic/com.ibm.db2.luw.doc/welcome.html.

Kernel parameters on Solaris systems

On Solaris systems, you might required to update the kernel parameters in the `/etc/system` file before the IBM DB2 installation. You can use the **db2osconf** command to determine the correct kernel parameter values for your computer. You can use the **projmod** command to configure the Solaris kernel parameters values before the DB2 installation on Solaris.

On a Solaris system with zones configured, the **db2osconf** command can be run only from the global zone on Solaris.

For more information about the **db2osconf** command, search for `db2osconf` in the IBM DB2 documentation at http://pic.dhe.ibm.com/infocenter/db2luw/v9r7.

Chapter 8. IBM Java Development Kit for IBM Security Directory Server

To compile Java sample programs, and to run Java programs, such as Instance Administration Tool and Configuration Tool, you must uncompress IBM Java Development Kit in the IBM Security Directory Server installation location.

The IBM Security Directory Server installation media provides a supported version of IBM Java Development Kit, IBM Java 1.6 SR 14. If you are using the operating system utilities for IBM Security Directory Server installation, you must complete IBM Java Development Kit installation.

For installing IBM Java Development Kit, access the IBM Security Directory Server installation media and go to directory that contains the IBM Java Development Kit compressed file.

You must uncompress the IBM Java Development Kit archive file to the IBM Security Directory Server installation location. The IBM Java Development Kit archive file is uncompressed to the `java` directory. For more information about IBM Security Directory Server installation location, see "Default installation locations" on page 25.

On AIX, you can use the GNU `tar` to uncompress the IBM Java Development Kit archive file to the IBM Security Directory Server installation location. Otherwise, you might require to move the `java` directory, which you uncompressed, to the IBM Security Directory Server installation location. For more information about the prerequisite packages, see "Prerequisite packages that are required on various operating systems" on page 15.

Table 14. IBM Java Development Kit packages that are available on various operating system

Operating system	Package name
AIX	`ibm-java-16sr14-aix-ppc-64.tar`
System x Linux (Intel 32-bit)	`ibm-java-16sr14-linux-i386.tar`
System i and System p Linux	`ibm-java-16sr14-linux-ppc-64.tar`
System z Linux	`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 on AMD64/EM64T	`ibm-java-16sr14-solaris-amd-64.tar`
Solaris SPARC	`ibm-java-16sr14-solaris-sparc-64.tar`
Windows 32-bit	`ibm-java-16sr14-win-i386.zip`
Windows on AMD64/EM64T	`ibm-java-16sr14-win-x86_64.zip`

Examples

Example 1:

To uncompress the IBM Java Development Kit archive file to the IBM Security Directory Server installation location on a Linux system, run the following command:

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

Chapter 9. Installation of IBM Global Security Kit

To use Secure Sockets Layer (SSL) and Transaction Layer Security (TLS) with IBM Security Directory Server, your computer must contain a supported version of IBM Global Security Kit (GSKit).

If your operating systems do not support installation with IBM Installation Manager, you can use the operating system utilities for IBM Global Security Kit installation. You must install GSKit on both the server and client systems to establish and use secure connections.

The GSKit crypt package is required for low level encryption support. The GSKit SSL package is required for secure communication handshake operations. The GSKit crypt package is a prerequisite for the GSKit SSL package.

IBM Security Directory Server installation media provides the following GSKit packages for various operating systems:

Note: For Solaris x64 and SPARC architectures, the GSKit package names are the same.

AIX

Package names of GSKit (64-bit)

```
GSKit8.gskcrypt64.ppc.rte

GSKit8.gskssl64.ppc.rte
```

Package names of GSKit (32-bit)

```
GSKit8.gskcrypt32.ppc.rte

GSKit8.gskssl32.ppc.rte
```

System x Linux

Package names of GSKit (32-bit)

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

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

System z Linux

Package names of GSKit (64-bit)

```
gskcrypt64-8.0.14.26.linux.s390x.rpm

gskssl64-8.0.14.26.linux.s390x.rpm
```

Package names of GSKit (32-bit)

```
gskcrypt31-8.0.14.26.linux.s390.rpm

gskssl31-8.0.14.26.linux.s390.rpm
```

System i and System p Linux

Package names of GSKit (64-bit)

```
gskcrypt64-8.0.14.26.linux.ppc.rpm

gskssl64-8.0.14.26.linux.ppc.rpm
```

Package names of GSKit (32-bit)

```
gskcrypt32-8.0.14.26.linux.ppc.rpm
```

gskssl32-8.0.14.26.linux.ppc.rpm

Linux IA64 (Itanium) and AMD64/EM64T Linux

Package names of GSKit (64-bit)

gskcrypt64-8.0.14.26.linux.x86_64.rpm

gskssl64-8.0.14.26.linux.x86_64.rpm

Package names of GSKit (32-bit)

gskcrypt32-8.0.14.26.linux.x86.rpm

gskssl32-8.0.14.26.linux.x86.rpm

Solaris

Package names of GSKit (64-bit)

gsk8cry64.pkg

gsk8ssl64.pkg

Package names of GSKit (32-bit)

gsk8cry32.pkg

gsk8ssl32.pkg

HP-UX (Itanium)

Package names of GSKit (64-bit)

gskcrypt64

gskssl64

Package names of GSKit (32-bit)

gskcrypt32

gskssl32

Microsoft Windows

Package names of GSKit (64-bit)

gsk8crypt64.exe

gsk8ssl64.exe

Package names of GSKit (32-bit)

gsk8crypt32.exe

gsk8ssl32.exe

Installing IBM Global Security Kit with `installp`

You can use the **installp** command to complete the IBM Global Security Kit installation on an AIX system.

Before you begin

Access the IBM Security Directory Server installation media to obtain the IBM Global Security Kit installable. See "Preparation of installation media" on page 6.

About this task

The **installp** installation program installs IBM Global Security Kit (GSKit) on an AIX system.

Procedure

1. Log in as the root user.
2. Access the command prompt.
3. Change the current working directory to the `gskit` directory where the IBM Global Security Kit installable is stored.
4. Run the **installp** command to install the IBM Global Security Kit packages.
   a. To install GSKit 64-bit packages, run the following commands:
      ```
      installp -acgXd . GSKit8.gskcrypt64.ppc.rte
      installp -acgXd . GSKit8.gskssl64.ppc.rte
      ```
   b. To install GSKit 32-bit packages, run the following commands:
      ```
      installp -acgXd . GSKit8.gskcrypt32.ppc.rte
      installp -acgXd . GSKit8.gskssl32.ppc.rte
      ```
5. Run the following command to verify whether the IBM Global Security Kit installation is successful:
   ```
   lslpp -aL GSKit8*
   ```

Results

The installation program installs IBM Global Security Kit in the following locations on an AIX system:

GSKit 64-bit
`/usr/opt/ibm/gsk8_64/`

GSKit 32-bit
`/usr/opt/ibm/gsk8/`

Installing IBM Global Security Kit with Linux utilities

Use the **rpm** command to complete the IBM Global Security Kit installation on a Linux system.

Before you begin

Access the IBM Security Directory Server installation media to obtain the IBM Global Security Kit installable. See “Preparation of installation media” on page 6.

About this task

The **rpm** command installs IBM Global Security Kit (GSKit) on a Linux system. In the example, installation of IBM Global Security Kit on AMD64 Opteron/EM64T Linux is shown. For System z, System i or System p, or System x Linux, you must substitute with the appropriate package names.

Procedure

1. Log in as the root user.
2. Access the command prompt.
3. Change the current working directory to the `gskit` directory where the IBM Global Security Kit installable is stored.
4. Run the **rpm** command to install the IBM Global Security Kit packages.
   a. To install GSKit 64-bit packages, run the following commands:
      ```
      rpm -ivh gskcrypt64-8.0.14.26.linux.x86_64.rpm
      rpm -ivh gskssl64-8.0.14.26.linux.x86_64.rpm
      ```

b. To install GSKit 32-bit packages, run the following commands:

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

5. Run the following command to verify whether the IBM Global Security Kit installation is successful:

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

Results

The installation program installs IBM Global Security Kit in the following locations on a Linux system:

GSKit 64-bit
/usr/local/ibm/gsk8_64/

GSKit 32-bit
/usr/local/ibm/gsk8/

Installing IBM Global Security Kit with Solaris utilities

Use the **pkgadd** command to complete the IBM Global Security Kit installation on a Solaris system.

Before you begin

Access the IBM Security Directory Server installation media. See "Preparation of installation media" on page 6.

About this task

The **pkgadd** command installs IBM Global Security Kit (GSKit) on a Solaris system. The package names and the file names are the same for Solaris SPARC and Solaris X64 operating systems.

Procedure

1. Log in as the root user.
2. Access the command prompt.
3. Change the current working directory to the `gskit` directory where the IBM Global Security Kit installable is stored.
4. Run the **pkgadd** command to install the IBM Global Security Kit packages.
   a. To install GSKit 64-bit packages, run the following commands:

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

   b. To install GSKit 32-bit packages, run the following commands:

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

5. Run the following command to verify whether the IBM Global Security Kit installation is successful:

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

   Substitute the `package_name` value with the GSKit package name to verify the version.

Installing IBM Global Security Kit with HP-UX utilities

Use the **swinstall** command to complete the IBM Global Security Kit installation on an HP-UX system.

Before you begin

Access the IBM Security Directory Server installation media to obtain the IBM Global Security Kit installable. See "Preparation of installation media" on page 6.

Procedure

1. Log in as the root user.
2. Access the command prompt.
3. Change the current working directory to the `gskit` directory where the IBM Global Security Kit installable is stored.
4. Run the **swinstall** command to install the IBM Global Security Kit packages.
   a. To install GSKit 64-bit packages, run the following commands:

      ```
      swinstall -s path_to_gskit_installable/gskcrypt64 gskcrypt64
      swinstall -s path_to_gskit_installable/gskssl64 gskssl64
      ```

      You must provide the absolute path name of the GSKit installable with the **-s** parameter.
   b. To install GSKit 32-bit packages, run the following commands:

      ```
      swinstall -s path_to_gskit_installable/gskcrypt32 gskcrypt32
      swinstall -s path_to_gskit_installable/gskssl32 gskssl32
      ```
5. Run the following command to verify whether the IBM Global Security Kit installation is successful:

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

Installing IBM Global Security Kit on Windows

Run the IBM Global Security Kit installation program to complete the IBM Global Security Kit installation on a Windows system.

Before you begin

Access the IBM Security Directory Server installation media to obtain the IBM Global Security Kit installable. See "Preparation of installation media" on page 6.

About this task

In the example, installation of GSKit crypt 64-bit and GSKit SSL 64-bit is shown. For the installation of GSKit 32-bit, use the appropriate packages. On Windows 64-bit operating system, you can install both 64-bit and 32-bit GSKit packages.

Procedure

1. Log in as a member of the administrator group.
2. Change the current working directory to the `gskit` directory where the IBM Global Security Kit installable is stored.
3. To install GSKit 64-bit packages, run the GSKit installation program.
   a. Run the GSKit8 crypt installation package, `gsk8crypt64.exe`.
   b. On the GSKit8 crypt installation window, complete the following steps:

1) Specify the installation path for GSKit8 crypt.
2) Click **Next**.
3) Click **Install**.
4) Click **Finish**.

c. Run the GSKit8 SSL installation package, `gsk8ssl64.exe`.
d. On the GSKit8 SSL installation window, complete the following steps:
1) Specify the installation path for GSKit8 SSL.
2) Click **Next**.
3) Click **Install**.
4) Click **Finish**.

4. To run GSKit commands from the command-line, set the *PATH* variable with the `bin` and `lib64` directories on Windows x86_64 system.

Note: On Windows 32-bit, set the *PATH* variable with the `bin` and `lib` directories.
If the GSKit installation location is `C:\Program Files\IBM\gsk8`, set the *PATH* variable with the following values:

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

Installing IBM Global Security Kit silently on Windows

Run the IBM Global Security Kit installation program from the command prompt to complete the IBM Global Security Kit installation silently on a Windows system.

Before you begin

Access the IBM Security Directory Server installation media to obtain the IBM Global Security Kit installable. See "Preparation of installation media" on page 6.

About this task

In the example, installation of GSKit crypt 64-bit and GSKit SSL 64-bit is shown. For the installation of GSKit 32-bit, use the appropriate packages. On Windows 64-bit operating system, you can install both 64-bit and 32-bit GSKit packages.

Procedure

1. Log in as a member of the administrator group.
2. Access the command prompt.
3. Change the current working directory to the `gskit` directory where the IBM Global Security Kit installable is stored.
4. To install GSKit 64-bit packages silently, run the following commands:

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

5. To run GSKit commands from the command-line, set the *PATH* variable with the `bin` and `lib64` directories on Windows x86_64 system.

Note: On Windows 32-bit, set the *PATH* variable with the `bin` and `lib` directories.
If the GSKit installation location is `C:\Program Files\IBM\gsk8`, set the *PATH* variable with the following values:

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

Chapter 10. Installation of language packs

To generate the directory server messages in languages other than English, you must install language packs for the languages you want to use.

IBM Installation Manager can install all the language packs that are available for the operating system if you select an installation feature from the full installer. The language packs are installed in the `nls` subdirectory in the IBM Security Directory Server installation location.

Note: You do not require to install language packs for the client. You can install language packs for the client if you want to generate messages in a language other than English for the **idslink** and **idsrmlink** commands. For information about the **idslink** and **idsrmlink** commands, see the *Command Reference*.

You can install language packs with IBM Installation Manager or with operating system utilities on AIX and Linux systems. Language pack installation with IBM Installation Manager is provided with the IBM Security Directory Server full product installer.

Remember: Language pack installation with IBM Installation Manager is supported only on AIX, Linux on the AMD64/EM64T architecture, and Microsoft Windows computers. On operating systems that support IBM Security Directory Server installation with IBM Installation Manager, you must not manually install language packs with operating system utilities. If for your operating system installation of language packs with IBM Installation Manager is not supported, use the operating utilities for installation of language packs.

Table 15. The list of supported languages on AIX, Linux, Solaris, and Windows operating systems

Languages	AIX	Linux	Solaris	Microsoft Windows
Czechoslovakian	✓			
French	✓	✓	✓	✓
German	✓	✓	✓	✓
Hungarian	✓			
Italian	✓	✓	✓	✓
Japanese	✓	✓	✓	✓
Korean	✓	✓	✓	✓
Polish	✓			
Portuguese (Brazil)	✓	✓	✓	✓
Russian	✓			
Slovakian	✓			
Spanish	✓	✓	✓	✓
Simplified Chinese	✓	✓	✓	✓
Traditional Chinese	✓	✓	✓	✓

Language pack packages for installation

You must identify package names that are associated with each language for a supported operating system before you install a language pack.

Language and language pack names

Remember: The language packs for Linux are supported for the following architectures:

- System x Linux
- System z Linux
- AMD64 Opteron / Intel EM64T Linux
- System i and System p Linux

Remember: The language packs for Solaris are supported for the following architectures:

- Solaris SPARC
- Solaris X64

Table 16. The list of supported languages with the language pack names on AIX, Linux, and Solaris operating systems

Languages	AIX	Linux	Solaris
Czechoslovakian	idsldap.msg631.cs_CZ		
French	idsldap.msg631.fr_FR	idsldap-msg631-fr-6.3.1-0.noarch.rpm	idsldap.msg631.fr.pkg
German	idsldap.msg631.de_DE	idsldap-msg631-de-6.3.1-0.noarch.rpm	idsldap.msg631.de.pkg
Hungarian	idsldap.msg631.hu_HU		
Italian	idsldap.msg631.it_IT	idsldap-msg631-it-6.3.1-0.noarch.rpm	idsldap.msg631.it.pkg
Japanese	idsldap.msg631.ja_JP	idsldap-msg631-ja-6.3.1-0.noarch.rpm	idsldap.msg631.ja.pkg
Korean	idsldap.msg631.ko_KO	idsldap-msg631-ko-6.3.1-0.noarch.rpm	idsldap.msg631.ko.pkg
Polish	idsldap.msg631.pl_PL		
Portuguese (Brazil)	idsldap.msg631.pt_BR	idsldap-msg631-pt_BR-6.3.1-0.noarch.rpm	idsldap.msg631.pt_BR.pkg
Russian	idsldap.msg631.ru_RU		
Slovakian	idsldap.msg631.sk_SK		
Spanish	idsldap.msg631.es_ES	idsldap-msg631-es-6.3.1-0.noarch.rpm	idsldap.msg631.es.pkg
Simplified Chinese	idsldap.msg631.zh_CN	idsldap-msg631-zh_CN-6.3.1-0.noarch.rpm	idsldap.msg631.zh_CN.pkg
Traditional Chinese	idsldap.msg631.zh_TW	idsldap-msg631-zh_TW-6.3.1-0.noarch.rpm	idsldap.msg631.zh_TW.pkg

Installing language packs with operating system utilities

Use the operating system utilities for the language pack installation if the operating system does not support installation with IBM Installation Manager.

Before you begin

You must prepare the IBM Security Directory Server installation media. See "Preparation of installation media" on page 6.

About this task

To generate the directory server messages in languages other than English, you must install language packs for the languages you want to use.

Procedure

1. Log in as the root user.
2. Access the command prompt.
3. Change the current working directory to the directory where IBM Security Directory Server installable are stored.
4. Go to the `tdsLangpack` subdirectory.
5. To install the language pack for a language, run the package installation commands. In the following example, the installation of language pack for the French language is shown. You can install any language pack by replacing with the appropriate package name for the operating system.

Operating system	Command to run:
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. Verify whether the language pack installation is successful. For more information, see "Verifying IBM Security Directory Server packages" on page 83.

Results

The installation program installs the language packs in the following directories:

Table 17. The default installation location of the language packs of IBM Security Directory Server

Operating system	Language pack installation location
Linux	`/opt/ibm/ldap/V6.3.1/nls/msg`
AIX and Solaris	`/opt/IBM/ldap/V6.3.1/nls/msg`

Chapter 11. Installation with operating system command-line utilities

You can run IBM Security Directory Server installation with operating system command-line utilities if your system does not provide X11 support.

CAUTION:

- **You must not use different modes of installation on the same computer. You must run IBM Security Directory Server installation with IBM Installation Manager or operating system command-line utilities, but not both. If you mix the two modes of installation, the installation might not include all the correct packages for a feature.**
- **You must avoid manual installation of DB2 and embedded WebSphere Application Server in their default installation path that is used by IBM Installation Manager. Such manual installation might cause installation, modification, or uninstallation failures when you run these operations with IBM Installation Manager. For more information about the default installation path, see "Default installation locations" on page 25.**

You must obtain the IBM Security Directory Server installation source before you install the product. IBM Security Directory Server product is available in archive files or as an installable image. You can create installation DVDs from the installable image.

You must prepare the installation media. For more information, see "Preparation of installation media" on page 6.

Important: To use IBM Security Directory Server as a full directory server, install a supported version of IBM DB2 on the computer if it is not installed. You must configure the `ldapdb.properties` file with the path name and version of IBM DB2.

Installation with AIX utilities

You can use AIX command-line utilities to install IBM Security Directory Server on an AIX system.

You can use one of the following utilities for IBM Security Directory Server installation:

SMIT The preferred installation method is to use the utility. For more information, see "Installing with SMIT" on page 67.

installp
For more information, see "Installing with **installp**" on page 69.

Packages for installation on an AIX system

To use IBM Security Directory Server as a full directory server, proxy server, or client on an AIX system, you must install appropriate packages.

Packages and file sets

IBM Security Directory Server provides the packages for an AIX system. Each package contains one or more file sets.

Table 18. Packages and the file sets contained in the packages

Packages	File sets that are associated with the package
idsldap.license631	idsldap.license631.rte - License
idsldap.cltbase631	• idsldap.cltbase631.rte - Base client run time • idsldap.cltbase631.adt - Base client SDK
idsldap.clt32bit631	• idsldap.clt32bit631.rte - 32-bit C Client (without SSL and TLS)
idsldap.clt64bit631	• idsldap.clt64bit631.rte - 64-bit C Client (without SSL and TLS)
idsldap.clt_max_crypto32bit631	• idsldap.clt_max_crypto32bit631.rte - 32-bit C Client (with SSL and TLS)
idsldap.clt_max_crypto64bit631	• idsldap.clt_max_crypto64bit631.rte - 64-bit C Client (with SSL and TLS)
idsldap.cltjava631	• idsldap.cltjava631.rte - Java Client
idsldap.srvbase64bit631	• idsldap.srvbase64bit631.rte - Base Server
idsldap.srv_max_cryptobase64bit631	• idsldap.srv_max_cryptobase64bit631.rte - Base Server (SSL)
idsldap.srvproxy64bit631	• idsldap.srvproxy64bit631.rte - Proxy Server (64-bit)
idsldap.srv64bit631	• idsldap.srv64bit631.rte - Directory Server (64-bit)
idsldap.webadmin631	• idsldap.webadmin631.rte - Web Administration Tool (without SSL and TLS)
idsldap.webadmin_max_crypto631	• idsldap.webadmin_max_crypto631.rte - Web Administration Tool (with SSL and TLS)
idsldap.msg631.en_US	Not available
idsldap.ent631	• idsldap.ent631.rte - IBM Directory Server Entitlement (provided only on Passport Advantage)

Installation sequence

You can install all the features at the same time. If you install them separately, you must install them in a specific order.

Important:

- If you want to use Secure Socket Layer (SSL) or Transport Layer Security (TLS), you must install a supported version of IBM Global Security Kit.
- For Kerberos support on AIX systems, a supported version of Network Authentication Service is required.

Note: If the computer does not support X11, you can skip the JDK component installation that is provided in the IBM JDK. If JDK component is not installed, you might not be able to use Instance Administration Tool or Configuration Tool.

Table 19. The installation sequence for the client feature

32-bit client (without SSL and TLS)	32-bit client (with SSL and TLS)	64-bit client (without SSL and TLS)	64-bit client (with SSL and TLS)
1. idsldap.cltbase631 2. idsldap.clt32bit631 3. idsldap.cltjava631	1. idsldap.cltbase631 2. idsldap.clt32bit631 3. idsldap.clt_max_crypto32bit631 4. idsldap.cltjava631	1. idsldap.cltbase631 2. idsldap.clt64bit631 3. idsldap.cltjava631	1. idsldap.cltbase631 2. idsldap.clt64bit631 3. idsldap.clt_max_crypto32bit631 4. idsldap.cltjava631

Note: When you use the Client-Server with entitlement archived file or an ISO image with entitlement for installation of IBM Security Directory Server, you must first accept license terms and install the idsldap.license631 package.

Table 20. The installation sequence for the full directory server feature

Full directory server 64-bit (without SSL and TLS)	Full directory server 64-bit (with SSL and TLS)
1. idsldap.license631 2. idsldap.cltbase631 3. idsldap.clt64bit631 4. idsldap.cltjava631 5. idsldap.srvbase64bit631 6. idsldap.srv64bit631 7. idsldap.msg631.en_US 8. idsldap.ent631	1. idsldap.license631 2. idsldap.cltbase631 3. idsldap.clt64bit631 4. idsldap.clt_max_crypto64bit631 5. idsldap.cltjava631 6. idsldap.srvbase64bit631 7. idsldap.srv_max_cryptobase64bit631 8. idsldap.srv64bit631 9. idsldap.msg631.en_US 10. idsldap.ent631

Table 21. The installation sequence for the proxy server feature

Proxy server 64-bit (without SSL and TLS)	Proxy server 64-bit (with SSL and TLS)
1. idsldap.license631 2. idsldap.cltbase631 3. idsldap.clt64bit631 4. idsldap.cltjava631 5. idsldap.srvbase64bit631 6. idsldap.srvproxy64bit631 7. idsldap.msg631.en_US 8. idsldap.ent631	1. idsldap.license631 2. idsldap.cltbase631 3. idsldap.clt64bit631 4. idsldap.clt_max_crypto64bit631 5. idsldap.cltjava631 6. idsldap.srvbase64bit631 7. idsldap.srv_max_cryptobase64bit631 8. idsldap.srvproxy64bit631 9. idsldap.msg631.en_US 10. idsldap.ent631

Note: To use Web Administration Tool, you must deploy it in a web application server. For more information about installing embedded WebSphere Application Server, see "Installing embedded WebSphere Application Server manually" on page 107.

Table 22. Web Administration Tool installation package

Web Administration Tool (without SSL and TLS)	Web Administration Tool (with SSL and TLS)
1. idsldap.license631 2. idsldap.webadmin631	1. idsldap.license631 2. idsldap.webadmin_max_crypto631

When you install Web Administration Tool, Directory Services Markup Language (DSML) files are also copied to your computer. For more information about DSML, see Appendix A, "Directory Services Markup Language," on page 231.

Installing with SMIT

Use the **smit** command to complete the IBM Security Directory Server installation on an AIX system.

Before you begin

You must prepare the IBM Security Directory Server installation media. See "Preparation of installation media" on page 6.

About this task

The **smit** installation program installs IBM Security Directory Server on an AIX system. If a supported version of IBM DB2 is installed on the system, the installation process updates the `ldapdb.properties` file with the DB2 path name and version.

Procedure

1. Log in as the root user.
2. Access the command prompt.
3. Run the **idsLicense** command.
   ```
   ./idsLicense
   ```
4. If you agree to accept the terms in the Software license agreement, enter 1. The following options are available to you:
   - 1: To accept the license agreement.
   - 2: To decline the license agreement and exit the installation.
   - 3: To print the license agreement.
   - 4: To read non-IBM terms in the license agreement.
   - 99: To go back to the previous screen.

   On accepting the terms in the license agreement, a `LAPID` file and a `license` folder is created in the IBM Security Directory Server installation location. The license folder contains IBM Security Directory Server license files in all supported languages.

   Important: Do not modify or delete the `LAPID` file and the license files in the license folder.
5. Run the **smit install** command. The **Software Installation and Maintenance** window opens.
6. Click **Install and Update Software** > **Install and Update from ALL Available Software**.
7. Select your installation media.
   - If you are installing from the DVD, take the following actions:
     a. Click **List** to access the device that contains IBM Security Directory Server images.
   - If you are installing from the uncompressed archive file, enter **.** in the **INPUT device/directory for software** field.
8. Click **Do**.
9. Move the cursor to **Software to install**, and take the following actions:
   a. To install the `idsldap` file set, type `idsldap`.
   b. Click **List** to list all the file sets, and select the file sets that you want to install.
   c. Click **OK**.
10. To start the installation, click **OK**.
11. Check the installation summary at the end of the output to verify successful installation of the file sets.
12. After the installation is complete, click **Done**.
13. To exit the **SMIT** program, press the `F12` key.

14. Verify whether the IBM Security Directory Server installation is successful. For more information, see "Verifying IBM Security Directory Server packages" on page 83.

Results

The installation program installs IBM Security Directory Server in the `/opt/IBM/ldap/V6.3.1` directory on the AIX system. If a supported version of IBM DB2 is installed on the system, the installation process updates the `ldapdb.properties` file with the DB2 path name and version.

What to do next

After the IBM Security Directory Server installation, you must take the following action:

- To use IBM Security Directory Server as a full directory server, create a directory server instance. See "Creating the default directory server instance" on page 130.
- To use IBM Security Directory Server as a proxy server, create a proxy server instance. See "Creating a proxy server instance with custom settings" on page 138.

Installing with `installp`

Use the **`installp`** command to complete the IBM Security Directory Server installation on an AIX system.

Before you begin

You must prepare the IBM Security Directory Server installation media. See "Preparation of installation media" on page 6.

About this task

The **`installp`** installation program installs IBM Security Directory Server on an AIX system. If a supported version of IBM DB2 is installed on the system, the installation process updates the `ldapdb.properties` file with the DB2 path name and version.

Procedure

1. Log in as the root user.
2. Access the command prompt.
3. Change the current working directory to the directory where the IBM Security Directory Server installable are stored.
4. Run the **`idsLicense`** command.

   ```
   ./idsLicense
   ```

5. If you agree to accept the terms in the Software license agreement, enter 1. The following options are available to you:
   - 1: To accept the license agreement.
   - 2: To decline the license agreement and exit the installation.
   - 3: To print the license agreement.
   - 4: To read non-IBM terms in the license agreement.
   - 99: To go back to the previous screen.

On accepting the terms in the license agreement, a `LAPID` file and a `license` folder is created in the IBM Security Directory Server installation location. The license folder contains IBM Security Directory Server license files in all supported languages.

Important: Do not modify or delete the `LAPID` file and the license files in the license folder.

6. Determine which IBM Security Directory Server packages you want to install.
   ```
   installp -ld . | grep idsldap
   ```
   A list of all the installable IBM Security Directory Server packages are shown.
7. Run the following command to install the packages:
   ```
   installp -acgXd . package_names
   ```
   To install all IBM Security Directory Server packages from the current path, run the following command:
   ```
   installp -acgXd . idsldap
   ```
8. After the completion of installation, the system generates an installation summary.
9. Verify whether the IBM Security Directory Server installation is successful. For more information, see "Verifying IBM Security Directory Server packages" on page 83.

Results

The installation program installs IBM Security Directory Server in the `/opt/IBM/ldap/V6.3.1` directory on the AIX system. If a supported version of IBM DB2 is installed on the system, the installation process updates the `ldapdb.properties` file with the DB2 path name and version.

What to do next

After the IBM Security Directory Server installation, you must take the following actions:

- To use IBM Security Directory Server as a full directory server, create a directory server instance. For more information, see "Creating the default directory server instance" on page 130.
- To use IBM Security Directory Server as a proxy server, create a proxy server instance. For more information, see "Creating a proxy server instance with custom settings" on page 138.

Installation with Linux utilities

You can use Linux command-line utilities to install IBM Security Directory Server on a Linux system.

IBM Security Directory Server provides separate packages for computers with different operating systems and architecture. You must select the appropriate packages for installation on your computer. For more information about the package names, see "Packages for installation on a Linux system" on page 71.

Packages for installation on a Linux system

To use IBM Security Directory Server as a full directory server, proxy server, or client on a Linux system, you must install appropriate packages.

Packages provided for various Linux systems

Table 23. Packages that are provided with IBM Security Directory Server for various Linux systems

IBM Security Directory Server packages	AMD64 Opteron/EM64T Linux	System i or System p	System x	System z
IBM Directory Server - License	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 - Base Client	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 - 32-bit Client	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 - 64-bit Client	idsldap-clt64bit631-6.3.1-0.x86_64.rpm	idsldap-clt64bit631-6.3.1-0.ppc64.rpm	Not available	idsldap-clt64bit631-6.3.1-0.s390x.rpm
IBM Directory Server - Java Client	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 - Base Server	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 - Proxy Server	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 - 32-bit Server	Not available	Not available	idsldap-srv32bit631-6.3.1-0.i386.rpm	Not available
IBM Directory Server - 64-bit Server	idsldap-srv64bit631-6.3.1-0.x86_64.rpm	idsldap-srv64bit631-6.3.1-0.ppc64.rpm	Not available	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 - Messages US English	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 (provided only on 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

Package dependency

For installation of certain packages, you must install the dependencies first.

Note: When you use the Client-Server with entitlement archived file or an ISO image with entitlement for installation of IBM Security Directory Server, you must first accept license terms and install the `idsldap-license631-6.3.1-0.`*`arch`*`.rpm` package.

In the table, package dependency on AMD64 Opteron/EM64T Linux is shown. For System z, System i or System p, or System x Linux, substitute with the appropriate package names.

Table 24. Package and its dependant packages

Package name	Depends on
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 2. idsldap-cltbase631-6.3.1-0.x86_64.rpm 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 2. idsldap-cltbase631-6.3.1-0.x86_64.rpm 3. idsldap-clt64bit631-6.3.1-0.x86_64.rpm 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 2. idsldap-cltbase631-6.3.1-0.x86_64.rpm 3. idsldap-clt64bit631-6.3.1-0.x86_64.rpm 4. idsldap-srvbase64bit631-6.3.1-0.x86_64.rpm

Installation sequence

You can install all the features at the same time. If you install them separately, you must install them in a specific order.

Important: If you want to use Secure Socket Layer (SSL) or Transport Layer Security (TLS), you must install a supported version of IBM Global Security Kit.

In the installation sequence example, AMD64 Opteron/EM64T Linux is used. For System z, System i or System p, or System x Linux, substitute with the appropriate package names.

Table 25. The installation sequence for the client feature

32-bit client	64-bit client
1. idsldap-cltbase631-6.3.1-0.x86_64.rpm 2. idsldap-clt32bit631-6.3.1-0.x86_64.rpm 3. idsldap-cltjava631-6.3.1-0.x86_64.rpm	1. idsldap-cltbase631-6.3.1-0.x86_64.rpm 2. idsldap-clt64bit631-6.3.1-0.x86_64.rpm 3. idsldap-cltjava631-6.3.1-0.x86_64.rpm

Table 26. The installation sequence for the full directory server and proxy server feature

Full directory server 64-bit	Proxy server 64-bit
1. idsldap-license631-6.3.1-0.x86_64.rpm 2. idsldap-cltbase631-6.3.1-0.x86_64.rpm 3. idsldap-clt64bit631-6.3.1-0.x86_64.rpm 4. idsldap-cltjava631-6.3.1-0.x86_64.rpm 5. idsldap-srvbase64bit631-6.3.1-0.x86_64.rpm 6. idsldap-srv64bit631-6.3.1-0.x86_64.rpm 7. idsldap-msg631-en-6.3.1-0.x86_64.rpm 8. idsldap-ent631-6.3.1-0.x86_64.rpm	1. idsldap-license631-6.3.1-0.x86_64.rpm 2. idsldap-cltbase631-6.3.1-0.x86_64.rpm 3. idsldap-clt64bit631-6.3.1-0.x86_64.rpm 4. idsldap-cltjava631-6.3.1-0.x86_64.rpm 5. idsldap-srvbase64bit631-6.3.1-0.x86_64.rpm 6. idsldap-srvproxy64bit631-6.3.1-0.x86_64.rpm 7. idsldap-msg631-en-6.3.1-0.x86_64.rpm 8. idsldap-ent631-6.3.1-0.x86_64.rpm

Note: To use Web Administration Tool, you must deploy it in a web application server. For more information about installing embedded WebSphere Application Server, see "Installing embedded WebSphere Application Server manually" on page 107.

Table 27. Web Administration Tool installation package

Web Administration Tool
1. idsldap-license631-6.3.1-0.x86_64.rpm 2. idsldap-webadmin631-6.3.1-0.x86_64.rpm

When you install Web Administration Tool, Directory Services Markup Language (DSML) files are also copied to your computer. For more information about DSML, see Appendix A, "Directory Services Markup Language," on page 231.

Installing with Linux utilities

Use the **rpm** command to complete the IBM Security Directory Server installation on a Linux system.

Before you begin

You must prepare the IBM Security Directory Server installation media. See "Preparation of installation media" on page 6.

About this task

The **rpm** installation program installs IBM Security Directory Server on a Linux system. If a supported version of IBM DB2 is installed on the system, the installation process updates the `ldapdb.properties` file with the DB2 path name and version.

Procedure

1. Log in as the root user.
2. Access the command prompt.
3. Change the current working directory to the directory where IBM Security Directory Server installable are stored.
4. Run the **idsLicense** command.

   ```
   ./idsLicense
   ```

5. If you agree to accept the terms in the Software license agreement, enter 1. The following options are available to you:
   - 1: To accept the license agreement.
   - 2: To decline the license agreement and exit the installation.
   - 3: To print the license agreement.
   - 4: To read non-IBM terms in the license agreement.
   - 99: To go back to the previous screen.

   On accepting the terms in the license agreement, a `LAPID` file and a `license` folder is created in the IBM Security Directory Server installation location. The license folder contains IBM Security Directory Server license files in all supported languages.

   Important: Do not modify or delete the `LAPID` file and the license files in the license folder.

6. Run the following command to install the package:

   ```
   rpm -ivh package_name
   ```

   To install all IBM Security Directory Server packages, run the following command:

   ```
   rpm -ivh idsldap*
   ```

7. Verify whether the IBM Security Directory Server installation is successful. For more information, see "Verifying IBM Security Directory Server packages" on page 83.

Results

The installation program installs IBM Security Directory Server in the `/opt/ibm/ldap/V6.3.1` directory on the Linux system. If a supported version of IBM DB2 is installed on the system, the installation process updates the `ldapdb.properties` file with the DB2 path name and version.

What to do next

After the IBM Security Directory Server installation, you must take the following action:

- To use IBM Security Directory Server as a full directory server, create a directory server instance. For more information, see "Creating the default directory server instance" on page 130.
- To use IBM Security Directory Server as a proxy server, create a proxy server instance. For more information, see "Creating a proxy server instance with custom settings" on page 138.

Installation with Solaris utilities

You can use Solaris command-line utilities to install IBM Security Directory Server on a Solaris system.

IBM Security Directory Server provides same set of packages for computers with different architecture. There are packages available for Sun SPARC Solaris and AMD64 Opteron/EM64T Solaris operating systems. The package names and the file names are the same for both operating systems. For more information about the package names, see "Packages for installation on a Solaris system."

When you install IBM Security Directory Server packages, you must not use the system default of ALL. If you use choose ALL packages, the system does not sequence the packages correctly and the installation fails.

Packages for installation on a Solaris system

To use IBM Security Directory Server as a full directory server, proxy server, or client on a Solaris system, you must install appropriate packages.

Packages provided for Solaris systems

Important: The package names and the file names are the same for Solaris SPARC and AMD64 Opteron/EM64T Solaris operating systems.

Table 28. Packages that are provided with IBM Security Directory Server for various Solaris systems

IBM Security Directory Server packages	Package names	File name
IBM Directory Server - License	IDSllicense631	idsldap-license631.pkg
IBM Directory Server - Base Client	IDSlbc631	idsldap.cltbase631.pkg
IBM Directory Server - 32-bit Client	IDSl32c631	idsldap.clt32bit631.pkg
IBM Directory Server - 64-bit Client	IDSl64c631	idsldap.clt64bit631.pkg
IBM Directory Server - Java Client	IDSljc631	idsldap.cltjava631.pkg
IBM Directory Server - Base Server	IDSlbs631	idsldap.srvbase64bit631.pkg
IBM Directory Server - Proxy Server	IDSl64p631	idsldap.srvproxy64bit631.pkg
IBM Directory Server - 64-bit Server	IDSl64s631	idsldap.srv64bit631.pkg
IBM Directory Server - Web Administration Tool	IDSlweb631	idsldap.webadmin631.pkg
IBM Directory Server - Messages US English	IDSlen631	idsldap.msg631.en.pkg
IBM Directory Server Entitlement (provided only on Passport Advantage)	IDSlent631	idsldap.ent631.pkg

Package dependency

For installation of certain packages, you must install the dependencies first.

Table 29. Package and its dependant packages

Package name	Depends on
idsldap.clt32bit631.pkg	idsldap.cltbase631.pkg
idsldap.clt64bit631.pkg	idsldap.cltbase631.pkg
idsldap.srvbase64bit631.pkg	1. idsldap-license631.pkg 2. idsldap.cltbase631.pkg 3. idsldap.clt64bit631.pkg
idsldap.srv64bit631.pkg	1. idsldap-license631.pkg 2. idsldap.cltbase631.pkg 3. idsldap.clt64bit631.pkg 4. idsldap.srvbase64bit631.pkg
idsldap.srvproxy64bit631.pkg	1. idsldap-license631.pkg 2. idsldap.cltbase631.pkg 3. idsldap.clt64bit631.pkg 4. idsldap.srvbase64bit631.pkg

Installation sequence

When you install the packages on a Solaris system, you must install them in a specific order.

Important: If you want to use Secure Socket Layer (SSL) or Transport Layer Security (TLS), you must install a supported version of IBM Global Security Kit.

Table 30. The installation sequence for the client feature

32-bit client	64-bit client
1. idsldap.cltbase631.pkg	1. idsldap.cltbase631.pkg
2. idsldap.clt32bit631.pkg	2. idsldap.clt64bit631.pkg
3. idsldap.cltjava631.pkg	3. idsldap.cltjava631.pkg

Note: When you use the Client-Server with entitlement archived file or an ISO image with entitlement for installation of IBM Security Directory Server, you must first accept license terms and install the `idsldap-license631.pkg` package.

Table 31. The installation sequence for the full directory server and proxy server feature

Full directory server 64-bit	Proxy server 64-bit
1. idsldap-license631.pkg	1. idsldap-license631.pkg
2. idsldap.cltbase631.pkg	2. idsldap.cltbase631.pkg
3. idsldap.clt64bit631.pkg	3. idsldap.clt64bit631.pkg
4. idsldap.cltjava631.pkg	4. idsldap.cltjava631.pkg
5. idsldap.srvbase64bit631.pkg	5. idsldap.srvbase64bit631.pkg
6. idsldap.srv64bit631.pkg	6. idsldap.srvproxy64bit631.pkg
7. idsldap.msg631.en.pkg	7. idsldap.msg631.en.pkg
8. idsldap.ent631.pkg	8. idsldap.ent631.pkg

Note: To use Web Administration Tool, you must deploy it in a web application server. For more information about installing embedded WebSphere Application Server, see "Installing embedded WebSphere Application Server manually" on page 107.

Table 32. Web Administration Tool installation package

Web Administration Tool
1. idsldap-license631.pkg
2. idsldap.webadmin631.pkg

When you install Web Administration Tool, Directory Services Markup Language (DSML) files are also copied to your computer. For more information about DSML, see Appendix A, "Directory Services Markup Language," on page 231.

Installing with Solaris utilities

Use the **pkgadd** command to complete the IBM Security Directory Server installation on a Solaris system.

Before you begin

Access the IBM Security Directory Server installation media. See "Preparation of installation media" on page 6.

About this task

The **pkgadd** installation program installs IBM Security Directory Server on a Solaris system. If a supported version of IBM DB2 is installed on the system, the installation process updates the `ldapdb.properties` file with the DB2 path name and version.

Procedure

1. Log in as the root user.
2. Access the command prompt.
3. Change the current working directory to the directory where IBM Security Directory Server installable is stored.
4. Run the **idsLicense** command.

   ```
   ./idsLicense
   ```
5. If you agree to accept the terms in the Software license agreement, enter 1. The following options are available to you:
   - 1: To accept the license agreement.
   - 2: To decline the license agreement and exit the installation.
   - 3: To print the license agreement.
   - 4: To read non-IBM terms in the license agreement.
   - 99: To go back to the previous screen.

   On accepting the terms in the license agreement, a `LAPID` file and a `license` folder is created in the IBM Security Directory Server installation location. The license folder contains IBM Security Directory Server license files in all supported languages.

   Important: Do not modify or delete the `LAPID` file and the license files in the license folder.
6. Run the following command to install a package:

   Note: You must install IBM Security Directory Server packages on a Solaris system in a specific order. For more information, see "Packages for installation on a Solaris system" on page 74.

   ```
   pkgadd -d package_name
   ```
7. Verify whether the IBM Security Directory Server installation is successful. For more information, see "Verifying IBM Security Directory Server packages" on page 83.

Results

The installation program installs IBM Security Directory Server in the `/opt/IBM/ldap/V6.3.1` directory on the Solaris system. If a supported version of IBM DB2 is installed on the system, the installation process updates the `ldapdb.properties` file with the DB2 path name and version.

What to do next

After the IBM Security Directory Server installation, you must take the following action:

- To use IBM Security Directory Server as a full directory server, create a directory server instance. For more information, see "Creating the default directory server instance" on page 130.
- To use IBM Security Directory Server as a proxy server, create a proxy server instance. For more information, see "Creating a proxy server instance with custom settings" on page 138.

Installation with HP-UX utilities

You can use HP-UX command-line utilities to install IBM Security Directory Server on an HP-UX system.

IBM Security Directory Server provides client only packages for HP-UX on Itanium systems (Intel IA64 processor-based servers). For more information, see "Packages for installation on an HP-UX Itanium system."

Packages for installation on an HP-UX Itanium system

To use IBM Security Directory Server as a client on an HP-UX system, you must install appropriate packages.

Packages provided for HP-UX systems

IBM Security Directory Server provides client only package for HP-UX on Itanium systems (Intel IA64 processor-based servers).

Table 33. Packages that are provided with IBM Security Directory Server for HP-UX systems

IBM Security Directory Server packages	Package names
IBM Directory Server - Base Client	idsldap.cltbase631.depot
IBM Directory Server - 32-bit Client	idsldap.clt32bit631.depot
IBM Directory Server - 64-bit Client	idsldap.clt64bit631.depot
IBM Directory Server - Java Client	idsldap.cltjava631.depot
IBM Directory Server - License	idsldap.license631.depot

Package dependency

For installation of certain packages, you must install the dependencies first.

Table 34. Package and its dependant packages

Package name	Depends on
idsldap.clt32bit631.depot	idsldap.cltbase631.depot
idsldap.clt64bit631.depot	idsldap.cltbase631.depot

Installation sequence

When you install the packages on an HP-UX system, you must install them in a specific order.

Important: If you want to use Secure Socket Layer (SSL) or Transport Layer Security (TLS), you must install a supported version of IBM Global Security Kit.

Table 35. The installation sequence for the client feature

32-bit client	64-bit client
1. idsldap.cltbase631.depot 2. idsldap.clt32bit631.depot 3. idsldap.cltjava631.depot	1. idsldap.cltbase631.depot 2. idsldap.clt64bit631.depot 3. idsldap.cltjava631.depot

Installing with HP-UX utilities

You can use the **swinstall** command to complete the IBM Security Directory Server installation on an HP-UX system.

Before you begin

You must prepare the IBM Security Directory Server installation media. See "Preparation of installation media" on page 6.

About this task

The **pkgadd** installation program installs IBM Security Directory Server on a Solaris system. If a supported version of IBM DB2 is installed on the system, the installation process updates the `ldapdb.properties` file with the DB2 path name and version.

Procedure

1. Log in as the root user.
2. Access the command prompt.
3. Change the current working directory to the directory where IBM Security Directory Server installable are stored.
4. Run the following command to install the packages:

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

5. Verify whether the IBM Security Directory Server installation is successful. For more information, see "Verifying IBM Security Directory Server packages" on page 83.

Results

The installation program installs IBM Security Directory Server in the `/opt/IBM/ldap/V6.3.1` directory on the HP-UX system.

Chapter 12. Verification of IBM Security Directory Server features

After the IBM Security Directory Server installation, modification, or uninstallation, you must verify whether the IBM Security Directory Server features are correctly installed, modified, or uninstalled.

You can use IBM Installation Manager or operating system utilities to verify whether the installation, modification, or uninstallation is successful.

Verifying IBM Security Directory Server features with IBM Installation Manager

Use IBM Installation Manager to verify the IBM Security Directory Server features and corequisite products that you installed with IBM Installation Manager.

Procedure

1. Start IBM Installation Manager.

   Windows
   From the **Start** menu, click **All Programs** > **IBM Installation Manager** > **IBM Installation Manager**.

   AIX and Linux
   Enter the following command at the command prompt. Modify the following default path if IBM Installation Manager is installed at a different location.

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

2. In the **IBM Installation Manager** page, click **File** > **View Installed Packages**.
3. From the **Installed Packages and Fixes** list in the **Installed Package** page, expand **IBM Security Directory Server**.
4. From the **Installed Packages and Fixes** list, click the IBM Security Directory Server version for which you want see the features.
5. Under the **Details** area, verify the installation of features and corequisite products.
6. To close the **Installed Package** page, click **Close**.
7. To close **IBM Installation Manager**, click **File** > **Exit**.

Verifying IBM Security Directory Server features on Windows

You can verify whether the IBM Security Directory Server installation, modification, or uninstallation was successful by checking the Microsoft Windows registry.

About this task

Microsoft Windows maintains registry entries to track the software that are on a Windows system. After a successful IBM Security Directory Server features installation, modification, or uninstallation, the registry entries are modified to record the most recent update on the system. An example of the registry entries is shown after a successful installation of IBM Security Directory Server features.

When you modify or uninstall IBM Security Directory Server features, the registry entries that track the features are modified to show the most recent status. The registry entries are shown for Microsoft Windows on the AMD64/EM64T architecture.

Procedure

1. Log on to the Windows system with the administrator privileges.
2. Access the command prompt, and run the following command:

   ```
   regedit
   ```
3. In the **Registry Editor** window, click **My Computer** > **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **Wow6432NODE** > **IBM** > **IDSLDAP** > **6.3.1**

   Note: To verify the IBM Security Directory Server installation on Microsoft Windows systems that are on Intel x86 (IA32) architecture, expand **My Computer** > **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **IBM** > **IDSLDAP** > **6.3.1** .
   `My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432NODE\IBM\IDSLDAP\6.3.1` shows the major versions of IBM Security Directory Server features that are installed on the system.

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

   The minor versions of IBM Security Directory Server features that are installed on the system and shown under `My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432NODE\IBM\IDSLDAP\6.3.1`. For example:

   ```
   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. To close the **Registry Editor** window, click **File** > **Exit**.

Verifying IBM Security Directory Server packages

You can verify whether the IBM Security Directory Server installation is successful by checking the system for IBM Security Directory Server packages.

About this task

After the IBM Security Directory Server installation, you must ensure that the packages are at the required level. You can query the version number of IBM Security Directory Server packages.

Procedure

1. Log in as the root user.
2. Access a command prompt, and run the following command:

Operating system	Command to query the packages:
AIX	`lslpp -l 'idsldap*'`
Linux	`rpm -qa | grep -i idsldap`
Solaris	`pkginfo | grep IDSl` `pkgparam package_name VERSION`
HP-UX	`swlist | grep -i idsldap`

Results

The command lists IBM Security Directory Server packages that are installed on the system.

Verifying the version of Web Administration Tool

To verify whether Web Administration Tool installation or upgrading is successful, you must verify the Web Administration Tool version.

Procedure

1. Log in with the administrator privileges.
2. Go to the *ds_install_location*/idstools directory. The *ds_install_location* is the IBM Security Directory Server installation location. The following locations are the default for various operating systems:

Table 36. The default IBM Security Directory Server installation location on various operating systems

Operating systems	Default installation locations:
Microsoft Windows	`c:\Program Files\IBM\ldap\V6.3.1`
AIX and Solaris	`/opt/IBM/ldap/V6.3.1`
Linux	`/opt/ibm/ldap/V6.3.1`

3. Run the following command:

Operating systems	Command to run:
Microsoft Windows	`deploy_IDSWebApp.bat -v`
AIX, Linux, and Solaris	`deploy_IDSWebApp -v`

The command shows the following information:

- The version and date values of the **deploy_IDSWebApp** command.
- The version and date values of the installed IDSWebApp.war file.
- The version and date values of the currently deployed IDSWebApp.war file.

What to do next

You must check the following values:

1. If the version and date values of installed IDSWebApp.war file is different from the version and date values of the currently deployed IDSWebApp.war file.
2. If the values are different, deploy the latest Web Administration Tool into the web application server.

Verifying IBM Global Security Kit installation on Windows

Verify the IBM Global Security Kit (GSKit) installation status to confirm whether the installation was successful on Windows.

Procedure

1. Access the gskitinst.log file.

Operating system	Default path:
Windows	C:\Program Files\IBM\ldap\V6.3.1\var

2. Verify whether the following directory is created: C:\Program Files\IBM\gsk8
3. Verify whether the gskitinst.log file contains the EXIT 0 value. If IBM Global Security Kit installation was successful, 0 is set otherwise, a non-zero value is set.
4. Optional: If IBM Global Security Kit installation was not successful, error details are stored in the C:\Program Files\IBM\ldap\V6.3.1\var\gskitinsterr.log file.

Verifying IBM Global Security Kit installation on AIX, Linux, Solaris, and HP-UX

Verify the IBM Global Security Kit (GSKit) installation to confirm whether the installation was successful.

About this task

After the IBM Global Security Kit installation, you must ensure that the packages are at the required level. You can query the version number of IBM Global Security Kit.

Procedure

1. Log in as the root user.
2. Access a command prompt, and run the following command:

Operating system	Command to run:
AIX	lslpp -al | grep -i gsk
Linux	rpm -qa | grep -i gsk
Solaris	pkginfo | grep gsk pkgparam package_name VERSION

Operating system	Command to run:
HP-UX	`swlist | grep -i gsk`

Chapter 13. Upgrade an instance of a previous version

To convert an existing instance to a functional instance of a latest release and to continue with the existing configuration files, you must upgrade an instance.

The upgrade process preserves changes to the schema definitions, changes to configuration files, and the data of a directory server instance.

Upgrading an instance from a previous version requires you to complete the following process:

1. Complete the installation of IBM Security Directory Server.
2. Upgrade an existing instance from a previous version.

IBM Security Directory Server, version 6.3.1 server and client can coexist with servers and clients of versions 6.0, 6.1, 6.2, and 6.3.

You can directly upgrade directory server instances of the following versions to IBM Security Directory Server, version 6.3.1:

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

Important: Direct upgrade of IBM Security Directory Server, version 6.0 instances to IBM Security Directory Server, version 6.3.1 is not supported. You can upgrade 6.0 instances to 6.1, 6.2, or 6.3, and then to 6.3.1.

You can upgrade an instance of a previous version in the following ways:

- Upgrading an existing instance on a local computer with IBM Security Directory Server Instance Administration Tool (**idsxinst**) or the **idsimigr** command. You must not remove the directory server instance that you want to upgrade. For a full directory server instance, do not unconfigure the database. Upgrade is not supported if the directory server instance is removed or its database is unconfigured.
- Upgrading an instance on a remote computer with the **migbkup** and **idsimigr** commands. For more information, see "Upgrading a remote instance of a previous version with the **idsimigr** command" on page 92.

Attention: You must back up the schema, configuration files, and database of an instance to recover from any upgrade failures.

DB2 database upgrade

When you upgrade an instance, its associated DB2 database is also upgraded if the DB2 version is lower than the version supported by IBM Security Directory Server, version 6.3.1. The **idsdbmigr** command is run internally to upgrade the DB2 database.

Important: Direct upgrade of a directory server instance that is configured with DB2, version 9.1 to an instance with DB2, version 10.1.0.2 or later is not supported. You can upgrade an instance that is configured with DB2, version 9.1 to an instance with DB2, version 10.1.0.2 or later in one of the following ways:

- Upgrade the instance with DB2, version 9.1 to an instance with DB2, version 9.5, and then to an instance with DB2, version 10.1.0.2 or later.
- Upgrade the instance with DB2, version 9.1 to an instance with DB2, version 9.7, and then to an instance with DB2, version 10.1.0.2 or later.

Client installation upgrade

If you installed client-only features with IBM Security Directory Server client installer, you do not require to upgrade. Clients from version 6.0, 6.1, 6.2, and 6.3 can coexist with the 6.3.1 server and client.

Setting the environment before you upgrade an instance

You must set up the directory server environment before you upgrade an existing instance.

Before you begin

You must complete the following tasks before you set the environment:

- Access the IBM Security Directory Server installation media.
- Complete IBM Security Directory Server, version 6.3.1 installation. See "Starting the installation" on page 26.
- Log in as a root user on AIX, Linux, or Solaris operating system, and as a member of the Administrator group on the Windows operating system.

Procedure

1. Ensure that the operating system on which the instance for upgrade is present is supported by IBM Security Directory Server, version 6.3.1.
2. Ensure that the instance of a previous version that you want to upgrade starts successfully. If you want to upgrade a directory server instance, you must configure the database, if it not already configured.

   Attention: Upgrade of a proxy server or a directory server is not supported, if the server fails to start successfully.
3. Take offline backup of the instance that you want to upgrade. For a directory server instance, back up the DB2 databases and DB2 settings. For more information, see the **idsdbback** command in the *Command Reference*.
4. To back up the schema and configuration files, run the **migbkup** command:

Operating system	Command to run:
Microsoft Windows	**migbkup.bat** drive_name\idsslapd-instance_name backup_directory
AIX, Linux, and Solaris	**migbkup** user_home_dir/idsslapd-instance_name backup_directory

The **migbkup** command is in the `tools` subdirectory of the IBM Security Directory Server installation media. If you completed the installation of IBM Security Directory Server, the **migbkup** command is in `sbin` folder of the IBM Security Directory Server installation location. The following directory is the default installation location on various operating systems:

Microsoft Windows

```
C:\Program Files\IBM\ldap\V6.3.1
```

AIX and Solaris

```
/opt/IBM/ldap/V6.3.1
```

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

The **migbkup** command backs up the following files:

- `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` (for Windows)
- `ibmslapdService.cmd` (for Windows)

The **migbkup** command creates the following files:

- `db2info` contains the path name and version information of the DB2 that is used by the directory server instance. The **idsimigr** command or Instance Administration Tool uses this file to upgrade DB2 instance and database when you upgrade a directory server instance. For a proxy server instance, this file is not available.
- `platforminfo` contains the information about the operating system and process type.

5. If you manually modified the `V3.modifiedschema` file of an instance for upgrade, the file must not contain any duplicate object identifiers (OIDs) for object classes or attributes. If the file contains duplicate OIDs, they are not preserved during the upgrade. If schema files contains duplicate OIDs, the OID in the `V3.modifiedschema` is preserved. If the schema files do not contain the attributes or object classes, the administration server and the `idsslapd` process might fail to start. In such situations, you must manually add the missing attributes or object classes to the schema files before you start the servers.
6. If you configured the instance with custom schema files, copy the files manually to the backup directory. When you back up schema and configuration files, the **migbkup** command backs up the custom schema files. However, these schema files might not be used when you upgrade the instance.

What to do next

After you set up the environment, run the **idsimigr** command or Instance Administration Tool to upgrade an instance from previous version. To upgrade an instance, use one of the following methods:

- "Upgrading an instance of a previous version with the **idsimigr** command" on page 90

- "Upgrading an instance of a previous version with Instance Administration Tool" on page 143

Upgrading an instance of a previous version with the `idsimigr` command

Use the **idsimigr** command to upgrade a directory server instance or a proxy server instance of a previous version to version 6.3.1.

Before you begin

You must complete the following tasks before you upgrade an instance with the **idsimigr** command:

- Complete IBM Security Directory Server, version 6.3.1 installation. See "Starting the installation" on page 26.
- Set up the environment before you upgrade an instance. See "Setting the environment before you upgrade an instance" on page 88.
- Log in as a root user on AIX, Linux, or Solaris operating system, and as a member of the Administrator group on the Windows operating system.

You can also upgrade an instance that is existing on a computer with Instance Administration Tool. For more information, see "Upgrading an instance of a previous version with Instance Administration Tool" on page 143.

About this task

After you upgrade an instance of a previous version, the instance is converted to a fully functional instance of IBM Security Directory Server, version 6.3.1.

Procedure

1. Access the command prompt.
2. Change the current working directory to `sbin`. The default location is the default on various operating systems:

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

   AIX and Solaris
   `/opt/IBM/ldap/V6.3.1/sbin`

   Linux `/opt/ibm/ldap/V6.3.1/sbin`
3. Stop the `ibmslapd` process and the administration server of the instance that you plan to upgrade.

   ```
   ibmslapd -I instance_name -k
   ibmdiradm -I instance_name -k
   ```
4. Do not uninstall the IBM Security Directory Server product version that is associated with the instance that you plan to upgrade.
5. Run the **idsimigr** command to upgrade the instance from a previous version to IBM Security Directory Server, version 6.3.1.

   ```
   idsimigr -I instance_name
   ```
6. Start the `ibmslapd` process and the administration server of the instance.

   ```
   ibmslapd -I instance_name -n
   ibmdiradm -I instance_name
   ```
7. Take offline backup of the instance. See "Directory server backup" on page 180.

Upgrade an instance of a previous version to a different computer

You can upgrade an existing instance of a previous version that is on a computer to a later version on a different computer.

You might want to upgrade an existing instance remotely for one of the following reasons:

- The operating system on a computer where an instance of a previous version exists might not be a supported operating system by IBM Security Directory Server, version 6.3.1. You might not want to upgrade or change the operating system on the computer.
- You want to install IBM Security Directory Server, version 6.3.1 on a computer with an operating system that is different from the operating system on which a previous version exists. However, you want to create an instance with the information as the existing instance of a previous version. For example, you an existing instance of a previous version on an AMD64/EM64T Linux system, but you want the 6.3.1 server to on an AIX system. In such case, the two operating systems must be of the same endian type. If the first computer is little endian, the second system must also be little endian. The endian type is concerned with the ordering of bits used to represent data in memory. If the operating systems do not have the same endian type, the upgrade of an instance is not supported.

The procedure for remote upgrade is similar to the procedure for upgrade on the same computer. The exception is that you must copy the backup files from the computer to a computer where you install IBM Security Directory Server, version 6.3.1.

Note: If you upgrade a remote instance from a computer that participates in replication, take the following actions:

- Enable replication with the source system as the supplier.
- Enable replication with the target system as the consumer.

The replication ensures that the updates are queued and can be replicated when the target system is brought online. You must enable replication before you take the backup of an instance on the source system.

Supported operating systems for upgrading a remote instance

To upgrade a remote instance on an appropriate target operating system, you must identify the operating systems that are the source and target for an instance.

Table 37. Supported source and target operating systems for remote instance upgrade

	Operating system: target system (IBM Security Directory Server, version 6.3.1)								
Operating system: source system (IBM Security Directory Server, 6.3 or earlier) ↓	**Intel 32-bit Windows**	**AMD64/ EM64T Windows**	**System x Linux (32-bit)**	**AMD64/ EM64T Linux**	**System i and System p Linux**	**System z Linux**	**AIX**	**Solaris SPARC**	**Solaris X64**
Intel 32-bit Windows	✔	✔	✔	✔					✔

Table 37. Supported source and target operating systems for remote instance upgrade (continued)

	Operating system: target system (IBM Security Directory Server, version 6.3.1)								
Operating system: source system (IBM Security Directory Server, 6.3 or earlier) ↓	**Intel 32-bit Windows**	**AMD64/ EM64T Windows**	**System x Linux (32-bit)**	**AMD64/ EM64T Linux**	**System i and System p Linux**	**System z Linux**	**AIX**	**Solaris SPARC**	**Solaris X64**
AMD/ EM64T Windows	✓	✓	✓	✓					✓
System x Linux (32-bit)	✓	✓	✓	✓					✓
AMD/ EM64T Linux	✓	✓	✓	✓					✓
System i and System p Linux					✓	✓	✓	✓	
System z Linux					✓	✓	✓	✓	
AIX					✓	✓	✓	✓	
Solaris SPARC					✓	✓	✓	✓	
Solaris X64	✓	✓	✓	✓					✓

Upgrading a remote instance of a previous version with the `idsimigr` command

Use the **idsimigr** command with the **-u** parameter to upgrade a remote directory server instance or proxy server instance of a previous version to version 6.3.1.

Before you begin

You must complete the following tasks before you upgrade an instance with the **idsimigr** command with the **-u** parameter:

- Set up the environment before you upgrade an instance. See, "Setting the environment before you upgrade an instance" on page 88.
- Log in as a root user on AIX, Linux, or Solaris operating system, and as a member of the Administrator group on the Windows operating system.

You can also upgrade a remote instance with backup files by using Instance Administration Tool. For more information, see "Upgrading a remote instance of a previous version with Instance Administration Tool" on page 144.

About this task

After you complete the upgrade process, the **idsimigr** command creates an instance of 6.3.1 on the computer with the information from the remote instance.

Procedure

1. Back up the database of a directory server instance that is on a remote computer with the **idsdb2ldif** command.

   Important: If you are upgrading a proxy server instance, do not back up database. Proxy server does not contain a database that is associated with it.

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

   For more information about the **idsdb2ldif** command, see the *Command Reference*.
2. Complete IBM Security Directory Server, version 6.3.1 installation on a computer to which you want to upgrade the remote instance. See, "Starting the installation" on page 26.
3. To back up the schema and configuration files of the remote instance, run the **migbkup** command of the version to which you want to upgrade:

Operating system	Command to run:
Microsoft Windows	**migbkup.bat** drive_name\idsslapd-instance_name backup_directory
AIX, Linux, and Solaris	**migbkup** user_home_dir/idsslapd-instance_name backup_directory

   The **migbkup** command is in the tools subdirectory of the IBM Security Directory Server installation media.
4. Copy the backup directory, backup_directory, which you created with **migbkup**, from the remote computer to the computer with IBM Security Directory Server, version 6.3.1.
5. Optional: Copy the database backup file, inst_out.ldif, from the remote computer to the computer with IBM Security Directory Server, version 6.3.1.
6. Run the **idsimigr** command with the **-u** parameter to create an instance with the backup data of the remote instance.

   ```
   idsimigr -u backup_directory
   ```
7. Configure a database, suffix, and administrator DN and password for the directory server instance.

   Important: If you are upgrading a proxy server instance, do not run the **idscfgdb** command to configure a database.

   ```
   idscfgdb -I instance_name –a db_admin_id –w db_admin_pwd –t db_name –l db_location
   idscfgsuf -I instance_name –s suffix
   idsdnpw -I instance_name –u admin_DN –p admin_PWD
   ```
8. Optional: Run the **idsldif2db** command to import the database backup file, inst_out.ldif, to the upgraded directory server instance.
9. Start the ibmslapd process and the administration server of the instance.

   ```
   ibmslapd -I instance_name -n
   ibmdiradm -I instance_name
   ```
10. Take backup of the instance. For more information, see "Directory server backup" on page 180.

Links to client and server utilities

You can use the **idslink** command to set the links to the directory server command-line utilities and libraries.

After the IBM Security Directory Server installation, you can set links for client and server utilities. These links are not set automatically during the installation.

If you configured links to utilities of a previous version of IBM Security Directory Server, the links remain unless you change them. To remove the links that are set by the `idslink` command, use the **idsrmlink** command.

You can use the **idslink** command to set the links to the command-line utilities, such as **idsldapmodify** and **idsldapadd**, and libraries, such as `libibmldap.so`. These links point to the location where the IBM Security Directory Server, version 6.3.1 utilities and libraries are stored.

For more information about the **idslink** and **idsrmlink** commands, see the *Command Reference*.

Chapter 14. Migration of data and solutions from an instance of a previous version

You can migrate directory data, solutions, or both that you configured with an instance of a previous version to use with a 6.3.1 instance.

Migration of DB2 data from IBM DB2 Enterprise Server Edition (ESE) to IBM DB2 Workspace Server Edition (WSE)

On System x Linux (Intel 32-bit architecture), IBM DB2 ESE, version 9.7 or later is not supported. On System x Linux, IBM Security Directory Server uses IBM DB2 WSE, version 9.7, Fix Pack 6 or later to create and configure database.

When you upgrade an instance of 6.1 or 6.2 with data to 6.3.1, you might require to run remote upgrade of an instance. You can upgrade a 6.3 instance with DB2 WSE, version 9.7 or later to a 6.3.1 instance with DB2 WSE, version 9.7 or later. On System x Linux, direct upgrade of a 6.1 or 6.2 instance with DB2 ESE, version 9.1 or later to a 6.3.1 instance with DB2 WSE, version 9.7 or later might fail. For more information about how to migrate DB2 ESE database to DB2 WSE, see "Migrating an instance with DB2 ESE database to an instance with DB2 WSE database" on page 96.

Migration of directory server solutions that are based on IBM Tivoli Directory Integrator

To use solutions that are configured with a previous version of instance with a 6.3.1 instance, you must migrate these solutions.

The following solutions are supported:

- Log management tool
- Simple Network Management Protocol (SNMP)
- Active Directory synchronization

For more information about the directory server solutions, see the *IBM Security Directory Server version 6.3.1 Administration Guide*.

For the solution to function, your computer must contain IBM Tivoli Directory Integrator, version 7.1. For more information about the installation and administration of IBM Tivoli Directory Integrator, see*IBM Tivoli Directory Integrator version 7.1 Installation and Administrator Guide*. You can download *IBM Tivoli Directory Integrator version 7.1 Installation and Administrator Guide* from the IBM Security Directory Integrator documentation website at http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.IBMDI.doc_7.1/toc.xml.

If IBM Tivoli Directory Integrator installation path in different from the default installation path, set the *IDS_LDAP_TDI_HOME* variable with the IBM Tivoli Directory Integrator installation location. The following installation paths are the default for IBM Tivoli Directory Integrator, version 7.1 on various operating system:

AIX, Linux, and Solaris

```
/opt/IBM/TDI/V7.1
```

Windows

```
C:\Program Files\IBM\TDI\V7.1
```

Migrating an instance with DB2 ESE database to an instance with DB2 WSE database

To upgrade a 6.1 o 6.2 instance with DB2 ESE to a 6.3.1 instance with DB2 WSE, migrate data from the DB2 ESE database to DB2 WSE database.

Before you begin

You must complete the following tasks before you migrate data from an instance of a previous version to a 6.3.1 instance:

- Complete IBM Security Directory Server, version 6.3.1 installation with IBM DB2 WSE. See "Starting the installation" on page 26.
- Set up the environment before you upgrade an instance. See "Setting the environment before you upgrade an instance" on page 88.
- Log in as a root user on AIX, Linux, or Solaris operating system, and as a member of the Administrator group on the Windows operating system.

Procedure

1. Stop the directory server instance from which you want to migrate directory data.
2. Run the **migbkup** command that is provided with IBM Security Directory Server, version 6.3.1 to back up the instance. See "Setting the environment before you upgrade an instance" on page 88. For more information about the **migbkup** command, see *Command Reference*.
3. Back up the database of the directory server instance from which you want to migrate data. To back up the database of an instance, `dsrdbm01`, complete the following steps:
   a. Switch the user context to DB2 instance owner.
      ```
      su - dsrdbm01
      ```
   b. Run the `db2profile` for the user.
      ```
      sqllib/db2profile
      ```
   c. Back up the DB2 database for the instance.
      ```
      db2 backup database dsrdbm01 to database_backup_directory
      ```
      The database owner must contain read, write, and execute permissions on the database backup directory, `database_backup_directory`.
   d. Back up the change log database if it is configured for the directory server instance.
      ```
      db2 backup db ldapclog to changelog_backup_directory
      ```
      The database owner must contain read, write, and execute permissions on the change log backup directory, `changelog_backup_directory`.
   e. Run the `exit` command to exit the user context.
4. Delete the directory server instance with the database. For more information about deleting an instance with database, see "Deleting an instance with the command-line utility" on page 158.
5. Change the current working directory to the `sbin` subdirectory in the IBM Security Directory Server, version 6.3.1 installation location.
6. To use the instance backup directory for remote upgrade of an instance, run the **idsimigr** command in the following format:
   ```
   idsimigr -I dsrdbm01 -u instance_backup_location -l instance_home_directory -n
   ```

7. To configure the instance, run the **idscfgdb** command in the following format:

```
idscfgdb -I dsrdbm01 -a database_owner -w passwd
 -t dsrdbm01 -l instance_home_directory -n
```

8. If the change log database was configured for the instance, configure the change log database for the instance:

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

9. Restore the database from the backup image. To restore the database of an instance, `dsrdbm01`, complete the following steps:
   a. Switch the user context to DB2 instance owner.

```
su - dsrdbm01
```

   b. Restore the DB2 database for the instance.

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

   c. Restore the change log database if it is configured for the directory server instance.

```
db2 restore db ldapclog from  changelog_backup_directory
```

   d. Run the `exit` command to exit the user context.
10. To catalog the restored database, run the following commands:

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

11. To catalog the restored change log database, run the following commands:

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

12. Start the directory server and the administration server.

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

Migrating the log management solution

You can migrate the log management solution that is configured with an instance of a previous version to an instance of 6.3.1.

Before you begin

You must complete the following tasks before you migrate the log management solution from an instance of a previous version to a 6.3.1 instance:

- Complete IBM Security Directory Server, version 6.3.1 installation. See "Starting the installation" on page 26.
- Complete IBM Tivoli Directory Integrator, version 7.1 installation, if it not installed on the computer.
- Log in as a root user on AIX, Linux, or Solaris operating system, and as a member of the Administrator group on the Windows operating system.

Procedure

1. Back up the `solution.properties` file that is in the *DS_instance_home*/`idsslapd-`*instance_name*`/etc/logmgmt` directory for your existing directory server instance.
2. Upgrade your previous version of instance to 6.3.1 instance. See Chapter 13, "Upgrade an instance of a previous version," on page 87.

3. Remove all the files and subdirectories from the *DS_instance_home*/idsslapd-*instance_name*/etc/logmgmt directory for the upgraded instance.
4. If your IBM Tivoli Directory Integrator is earlier that version 7.1, complete the IBM Tivoli Directory Integrator, version 7.1 installation.
5. Switch the user context as directory server instance owner.

   ```
   su - instance_owner
   ```
6. Copy the following files:
   a. Copy the files and directories from *Directory_Integrator_v7.1_installation_location*/etc to *DS_instance_home*/idsslapd-*instance_name*/etc/logmgmt.
   b. Copy the files and directories from *Directory_Integrator_v7.1_installation_location*/serverapi to *DS_instance_home*/idsslapd-*instance_name*/etc/logmgmt.
   c. Copy *Directory_Integrator_v7.1_installation_location*/idisrv.sth to *DS_instance_home*/idsslapd-*instance_name*/etc/logmgmt.
   d. Copy *Directory_Integrator_v7.1_installation_location*/testserver.jks to *DS_instance_home*/idsslapd-*instance_name*/etc/logmgmt.
7. Create a directory with the name logs in *DS_instance_home*/idsslapd-*instance_name*/etc/logmgmt.
8. Add the systemqueue.on=false entry at the end of the *DS_instance_home*/idsslapd-*instance_name*/etc/logmgmt/solutions.properties file.
9. If the IBM Tivoli Directory Integrator, version 7.1 installation path in different from the default path, set the *IDS_LDAP_TDI_HOME* variable with the installation location.
10. Run the log management solution.

Migrating the SNMP solution

You can migrate the Simple Network Management Protocol (SNMP) solution that is configured with an instance of a previous version to an instance of 6.3.1.

Before you begin

You must complete the following tasks before you migrate the SNMP solution from an instance of a previous version to a 6.3.1 instance:

- Complete IBM Security Directory Server, version 6.3.1 installation. See "Starting the installation" on page 26.
- Complete IBM Tivoli Directory Integrator, version 7.1 installation, if it not installed on the computer.
- Log in as a root user on AIX, Linux, or Solaris operating system, and as a member of the Administrator group on the Windows operating system.

Procedure

1. Back up the snmp directory that is in the IBM Security Directory Server installation location that is associated with your existing instance of previous version.
2. Upgrade your previous version of instance to 6.3.1 instance. See Chapter 13, "Upgrade an instance of a previous version," on page 87.

3. Replace the /idstools/snmp/idssnmp.conf file that in the IBM Security Directory Server, version 6.3.1 installation path with the /idstools/snmp/idssnmp.conf file that in the installation path of previous version of IBM Security Directory Server.
4. Replace the /idstools/snmp/idssnmp.properties file that in the IBM Security Directory Server, version 6.3.1 installation path with the /idstools/snmp/idssnmp.properties file that in the installation path of previous version of IBM Security Directory Server.
5. Replace the /idstools/snmp/IBM-DIRECTORYSERVER-MIB file that in the IBM Security Directory Server, version 6.3.1 installation path with the /idstools/snmp/IBM-DIRECTORYSERVER-MIB file that in the installation path of previous version of IBM Security Directory Server.
6. Replace the /idstools/snmp/INET-ADDRESS-MIB file that in the IBM Security Directory Server, version 6.3.1 installation path with the /idstools/snmp/INET-ADDRESS-MIB file that in the installation path of previous version of IBM Security Directory Server.
7. If the IBM Tivoli Directory Integrator, version 7.1 installation path in different from the default path, set the *IDS_LDAP_TDI_HOME* variable with the installation location.
8. Run the SNMP solution.

Migrating the Active Directory synchronization solution

You can migrate the Active Directory synchronization solution that is configured with an instance of a previous version to an instance of 6.3.1.

Before you begin

You must complete the following tasks before you migrate the Active Directory synchronization solution from an instance of a previous version to a 6.3.1 instance:

- Complete IBM Security Directory Server, version 6.3.1 installation. See "Starting the installation" on page 26.
- Complete IBM Tivoli Directory Integrator, version 7.1 installation, if it not installed on the computer.
- Log in as a root user on AIX, Linux, or Solaris operating system, and as a member of the Administrator group on the Windows operating system.

From IBM Security Directory Server, version 6.3.1, the Active Directory synchronization solution is deprecated.

Procedure

1. Upgrade your previous version of instance to 6.3.1 instance. See Chapter 13, "Upgrade an instance of a previous version," on page 87.
2. Create a directory server instance. See "Instance creation with Instance Administration Tool" on page 129.
3. Configure the directory server instance for Active Directory synchronization. See "Active Directory synchronization" on page 203.
4. Restore the changes to the *DS_instance_home*/idsslapd-*instance_name*/etc/tdisoldir/solution.properties file before you upgraded the instance.

   Note: If you replace the newly created solution.properties file with the earlier file, Active Directory synchronization might fail. The format of the

`solution.properties` file that gets created when you run the **idsadscfg** command is different from the earlier file.

5. Run the Active Directory synchronization solution. For more information about the **idsadsrun** command, see *Command Reference*.

Migrate a previous version of Web Administration Tool configuration

Migrate a previous version Web Administration Tool configuration to continue to use the same settings with a later version of Web Administration Tool.

To migrate an existing Web Administration Tool configuration of a previous version with the **idswmigr** command, the following conditions must be met:

1. The previous version of Web Administration Tool is installed on the computer.
2. The previous version of embedded WebSphere Application Server is installed on the computer.
3. The previous version of Web Administration Tool is deployed in the previous version of embedded WebSphere Application Server.
4. Install Web Administration Tool that is provided with IBM Security Directory Server, version 6.3.1.
5. Install embedded WebSphere Application Server that is provided with IBM Security Directory Server, version 6.3.1.
6. Do not deploy Web Administration Tool that is provided with 6.3.1 in the embedded WebSphere Application Server.

Web Administration Tool of the following IBM Security Directory Server versions that is deployed on the following embedded WebSphere Application Server version is supported for migration:

- IBM Security Directory Server, version 6.1 and embedded WebSphere Application Server, version 6.1.0.7 or later
- IBM Security Directory Server, version 6.2 and embedded WebSphere Application Server, version 6.1.0.13 or later (on UNIX) or embedded WebSphere Application Server, version 6.1.0.17 (on Windows) or later
- IBM Security Directory Server, version 6.3 and embedded WebSphere Application Server, version 7.0.0.7 or later

When you use the **idswmigr** command to migrate configuration settings of a previous version of Web Administration Tool, the command does the following operations:

1. Saves the configuration files for the previous version of Web Administration Tool.
2. Undeploys the previous version of Web Administration Tool from the previous version of embedded WebSphere Application Server.
3. Backs up the configuration of the previous version of embedded WebSphere Application Server to a temporary location that you specify.
4. Restores the configuration of the previous version of embedded WebSphere Application Server to a location.
5. Deploys Web Administration Tool in the current version of embedded WebSphere Application Server that is provided with IBM Security Directory Server, version 6.3.1.
6. Migrates the previous Web Administration Tool configuration files and restores these files in the later version of embedded WebSphere Application Server.

Note: Migration of Web Administration Tool will be possible using IBM Installation Manager only if the major version of embedded WebSphere Application Server to be migrated is smaller than the major version of embedded WebSphere Application Server (newly installed).

idswmigr

Use the **idswmigr** command to migrate an existing Web Administration Tool configuration of a previous version to a later version of Web Administration Tool.

Description

To migrate an existing Web Administration Tool configuration of a previous version with the **idswmigr** command, the following conditions must be met:

1. The previous version of Web Administration Tool is installed on the computer.
2. The previous version of embedded WebSphere Application Server is installed on the computer.
3. The previous version of Web Administration Tool is deployed in the previous version of embedded WebSphere Application Server.
4. Install the later version of Web Administration Tool.
5. Install the later version of embedded WebSphere Application Server.
6. Do not deploy Web Administration Tool that is of later version in the embedded WebSphere Application Server.

Synopsis

```
idswmigr -l temp_path [-s source_path -t target_path
          -r profile_name -a app_name -v -o ports_path]
```

Options

The **idswmigr** command takes the following parameters:

-a *app_name*
Specified is the application name. If not specified, the default is `IDSWebApp.war`.

-l *temp_path*
Specifies a location to store the temporary files.

-o *ports_path*
Specifies the fully qualified path of the ports definition file. If not specified, the following default path is used:

Windows
`C:\Program Files\IBM\ldap\V6.3.1\idstools\TDSWEBPortDef.props`

AIX and Solaris
`/opt/IBM/ldap/V6.3.1/idstools/TDSWEBPortDef.props`

Linux `/opt/ibm/ldap/V6.3.1/idstools/TDSWEBPortDef.props`

-r *profile_name*
Specifies the profile name that is associated with the application. If not specified, the default is `TDSWebAdminProfile`.

-s *source_path*
Specifies the source location for the previous version of embedded WebSphere Application Server.

-t *target_path*
Specifies the installation location of a later version of embedded WebSphere Application Server.

-v
Displays the version information.

Examples

Example 1

To migrate an existing Web Administration Tool configuration of version 6.2 to version 6.3.1, run the following command:

```
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
```

Manually migrating the Web Administration Tool

You can manually migrate the Web Administration Tool.

Before you begin

To migrate the Web Administration Tool manually, the Web Administration Tool must be installed first. Follow the steps to migrate the Web Administration Tool manually. In the example that is shown, the Web Administration Tool on IBM Security Directory Server V6.3 is migrated to IBM Security Directory Server V6.3.1.

On AIX, the migration commands are similar to the commands on Linux, except the path `/opt/ibm/ldap` should be replaced by `/opt/IBM/ldap`.

Procedure

1. For Windows, add the WebSphere Application Server service using following command:

   ```
   "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. Back up the Web Administration Tool files from the previous release.
   - On Windows, find these files under the directory:

     ```
     C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\
      installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\
      WEB-INF\classes\
     ```

     or

     ```
     C:\Program Files\IBM\LDAP\V6.3\appsrv\installedApps\DefaultNode
     \IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\classes
     ```

   - On Linux, find these files under the following directory:

     ```
     /opt/ibm/ldap/V6.3/appsrv/profiles/TDSWebAdminProfile/installedApps
     /DefaultNode/IDSWebApp.war.ear/IDSWebApp.war/WEB-INF/classes
     ```

     or

     ```
     /opt/ibm/ldap/V6.3/appsrv/installedApps/DefaultNode
     /IDSWebApp.war.ear/IDSWebApp.war/WEB-INF/classes
     ```

   Copy only the following five files from the directories:

   ```
   security\console_passwd
   IDSConfig\IDSSessionConfig\IDSSessionMgmt.xml
   ```

IDSConfig\IDSServersConfig\IDSServersInfo.xml

IDSConfig\IDSAppReg\IDSAppReg.xml

IDSConfig\IDSSearchSettings\IDSSearchMgmt.xml

For example:

```
  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. Uninstall the war file from the previous release.
   - On Windows, the command is present under the following directory:

     ```
     C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\bin\wsadmin.bat
     ```

     or

     ```
     C:\Program Files\IBM\LDAP\V6.3\appsrv\bin\wsadmin.bat
     ```

   - On Linux, the command is present under the following directory:

     ```
     /opt/ibm/ldap/V6.3/appsrv/profiles/TDSWebAdminProfile/bin/wsadmin.sh
     ```

     or

     ```
     /opt/ibm/ldap/V6.3/appsrv/bin/wsadmin.sh
     ```

   ```
   wsadmin.bat -conntype NONE -c "$AdminApp uninstall IDSWebApp.war"
   ```

   For example:

   ```
   "C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\bin\wsadmin.bat"
    -conntype NONE -c "$AdminApp uninstall IDSWebApp.war"
   ```

4. If the server of the previous embedded WebSphere Application Server is running, then stop the application server.
   - On Windows, the command is present under the following directory:

     ```
     C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\bin\
     stopServer.bat
     ```

     or

     ```
     C:\Program Files\IBM\LDAP\V6.3\appsrv\bin\stopServer.bat
     ```

   - On Linux, the command is present under the following directory:

     ```
     /opt/ibm/ldap/V6.3/appsrv/profiles/TDSWebAdminProfile/bin/stopServer.sh
     ```

     or

     ```
     /opt/ibm/ldap/V6.3/appsrv/bin/stopServer.sh
     ```

   For example:

   ```
   "C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\bin\
   stopServer.bat" server1
   ```

5. Check for the existence of the profile on the new embedded WebSphere Application Server. If the profile does not exist, create a new profile.

- On Windows, run the following command to create new profile:

```
"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"
```

- On Linux, run the following command to create new profile:

```
/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. Copy the new war file into the new WebSphere Application Server directory.
   - On Windows, run the following command:

```
copy "C:\Program Files\IBM\LDAP\V6.3.1\idstools\IDSWebApp.war"
 "C:\Program Files\IBM\LDAP\V6.3.1\appsrv\profiles\TDSWebAdminProfile\
 installableApps"
```

   - On Linux, run the following command:

```
cp "/opt/ibm/ldap/V6.3.1/idstools/IDSWebApp.war"
 "/opt/ibm/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/installableApps"
```

7. Install the new WAR file into the new WebSphere Application Server product.
   - On Windows, run the following command:

```
"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\"}"
```

   - On Linux, run the following command:

```
"/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. Restore the Web Administration Tool configuration files that were saved previously.
   - On Windows, replace following files with the backup copy files:

```
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
```

   - On Linux, replace following files with the backup copy files:

```
/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. On Windows, start the service that was added.

```
"C:\Program Files\IBM\ldap\V6.3.1\appsrv\bin\WASService.exe"
 -start TDSWebAdmin-V6.3.1
```

10. On Linux, start the server.

```
/opt/ibm/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/bin/startServer.sh server1
```

Chapter 15. Manual deployment of Web Administration Tool

To manage and administer directory server instances with Web Administration Tool, you must deploy Web Administration Tool in a supported web application server.

For deploying Web Administration Tool, your computer must contain a supported version of web application server. IBM Security Directory Server installation media provides embedded WebSphere Application Server, version 7.0.0.25. You can use IBM Installation Manager to complete Web Administration Tool installation, and deploy it in embedded WebSphere Application Server.

If your operating system does not support IBM Security Directory Server installation with IBM Installation Manager, complete the embedded WebSphere Application Server installation manually. After the installation of embedded WebSphere Application Server, you must deploy Web Administration Tool in embedded WebSphere Application Server.

If your computer contains a supported version of WebSphere Application Server, you can deploy Web Administration Tool in it.

WebSphere Application Server is the IBM runtime environment for Java-based applications. For more information about WebSphere Application Server, see the WebSphere Application server documentation at http://pic.dhe.ibm.com/infocenter/wasinfo/v7r0/index.jsp.

Installing embedded WebSphere Application Server manually

To deploy Web Administration Tool, you must complete the installation of embedded WebSphere Application Server on your computer.

Before you begin

For the installation of embedded WebSphere Application Server, complete the following steps:

1. Access IBM Security Directory Server installation media that contains the embedded WebSphere Application Server installable. See "Preparation of installation media" on page 6.

About this task

To deploy Web Administration Tool with the `deploy_IDSWebApp` command without using any parameters, you must provide the following values:

1. Specify the `appsrv` directory in the IBM Security Directory Server installation path as the installation location for embedded WebSphere Application Server. For more information about the default IBM Security Directory Server installation path, see "Default installation locations" on page 25.

You can provide any other installation location for embedded WebSphere Application Server. In such a case, you must specify the **-w**, **-p**, **-r**, and **-o** parameters and values with the `deploy_IDSWebApp` command for the Web Administration Tool deployment.

Procedure

1. Log in with administrator privileges.
2. Access the command prompt.
3. Change the current working directory to the directory that contains the embedded WebSphere Application Server installable.
4. To install embedded WebSphere Application Server in the default IBM Security Directory Server installation path, run the following command:

Operating systems	Command to run:
Microsoft Windows	`install.bat -installRoot c:\Program Files\IBM\ldap\V6.3.1\appsrv`
AIX and Solaris	`install.sh -installRoot /opt/IBM/ldap/V6.3.1/appsrv`
Linux	`install.sh -installRoot /opt/ibm/ldap/V6.3.1/appsrv`

What to do next

If Web Administration Tool is not installed on your computer, complete the installation of Web Administration Tool. See Chapter 11, "Installation with operating system command-line utilities," on page 65.

If Web Administration Tool is installed on your computer, complete the deployment of Web Administration Tool. See "Deploying Web Administration Tool in embedded WebSphere Application Server" on page 109.

Default ports for Web Administration Tool

To avoid port conflicts of ports between Web Administration Tool and other applications, you must know the default ports that are used by Web Administration Tool.

Embedded WebSphere Application Server uses the following default port settings for Web Administration Tool:

- HTTP Transport (port 1): 12100
- HTTPS Transport (port 2): 12101
- Admin Console (for administering WebSphere Application Server) port: 12104
- Secure Admin Console (for administering WebSphere Application Server) port: 12105

Embedded WebSphere Application Server uses the following default port settings for other applications:

- Bootstrap/rmi port: 12102
- Soap connector port: 12103

The other port numbers that might be used by embedded WebSphere Application Server: 9405, 9406, 9407, 9375, 9105, 7276, 7286, 5558, 5577, 5075, 5076.

If a port conflict exists with another application that might be using one or more of the default ports, take one of the following actions that is appropriate for your environment:

- Change the default ports to unused ports, and start the application the unused port.
- If the application that is using the default ports is not an important service or server, change its port number and free the default port.

To change the default port numbers that embedded WebSphere Application Server initializes for application, you must set appropriate port number in the `portdef.props` file. The `portdef.props` file is in the `\appsrv\profiles\TDSWebAdminProfile\properties\` directory in the IBM Security Directory Server installation location. For more information about the default IBM Security Directory Server installation location, see "Default installation locations" on page 25.

HTTP Transport port 1
To modify the port for HTTP Transport port 1, change the entry with the port number 12100 to the port number that is not in use.

HTTPS Transport port 2
To modify the port for HTTPS Transport port 2, change the entry with the port number 12101 to the port number that is not in use.

Bootstrap/rmi port
To modify the port for Bootstrap/rmi port, change the entry with the port number 12102 to the port number that is not in use.

Soap connector port
To modify the port for Soap connector port, change the entry with the port number 12103 to the port number that is not in use.

Admin Console port
To modify the port for Admin Console port, change the entry with the port number 12104 to the port number that is not in use.

Admin Secure Console port
To modify the port for Admin Secure Console port, change the entry with the port number 12105 to the port number that is not in use.

Deploying Web Administration Tool in embedded WebSphere Application Server

To use Web Administration Tool, you must deploy it in a web application server.

Before you begin

You must take the following actions before you deploy Web Administration Tool:

1. Complete the installation of Web Administration Tool package for your operating system.
2. Complete the installation of a supported version of web application server.
3. If you plan to migrate an existing Web Administration Tool configuration of a previous version, then you must not deploy a later version of Web Administration Tool.

About this task

When you deploy Web Administration Tool, the command does the following actions:

1. Removes an earlier version of Web Administration Tool, if any.

2. Deploys Web Administration Tool in a web application server.
3. Starts the web application server.

Procedure

1. Log in with the administrator privileges.
2. Go to the *DS_install_location*/idstools directory. The *DS_install_location* is the IBM Security Directory Server installation location. The following locations are the default for various operating systems:

Operating systems	Default installation locations:
Microsoft Windows	c:\Program Files\IBM\ldap\V6.3.1
AIX and Solaris	/opt/IBM/ldap/V6.3.1
Linux	/opt/ibm/ldap/V6.3.1

3. Run the following command:

   Note: If you installed embedded WebSphere Application Server in the default IBM Security Directory Server installation location, do not provide any parameters to the deploy_IDSWebApp command. For more information about the deploy_IDSWebApp command, see the command usage, deploy_IDSWebApp -h.

Operating systems	Command to run:
Microsoft Windows	deploy_IDSWebApp.bat -w *path_to_war_file* -p *was_installation_path* -r *profile* -o ports_file
AIX, Linux, and Solaris	deploy_IDSWebApp -w *path_to_war_file* -p *was_installation_path* -r *profile* -o ports_file

Results

The command deploys Web Administration Tool in the web application server that is specified by *was_installation_path*.

What to do next

To access Web Administration Tool, open a browser window and enter http://*host_name*:12100/IDSWebApp. The *host_name* variable indicates the host name or IP address of the computer where you installed Web Administration Tool.

Deploying Web Administration Tool in WebSphere Application Server

If you want to manage applications on your computer with WebSphere Application Server, you can deploy Web Administration Tool in WebSphere Application Server.

Before you begin

To deploy Web Administration Tool in WebSphere Application Server, you must meet the following requirements:

1. Complete the installation of Web Administration Tool package for your operating system. See “Installing with IBM Installation Manager” on page 28.
2. Your computer must contain a supported version of WebSphere Application Server.

About this task

IBM Security Directory Server installation media provides Web Administration Tool and embedded WebSphere Application Server. If your computer contains WebSphere Application Server, you can deploy Web Administration Tool in WebSphere Application Server. To deploy Web Administration Tool, you must deploy the `IDSWebApp.war` file that is in the `idstools` directory of the IBM Security Directory Server installation location.

Procedure

1. Use the URL `http://`*`hostname_WAS_server`*`:9060/ibm/console` to log in the WebSphere Admin console. Substitute the *hostname_WAS_server* variable with the host name or IP address of your computer on which WebSphere Application Server is installed. If you specified a custom port to access WebSphere Admin console, substitute the default port, `9060`, with your port number.
2. Enter the user ID and password of the user. The user must contain the required permission to run operations on WebSphere Application Server.
3. On the left navigational pane, click **Application** > **New Application**.
4. In the **New Application** page, click **New Enterprise Application**.
5. In the **Path to the new application** page, choose one of the following options that are based on from where you accessed the WebSphere Admin console:
   - If you accessed the WebSphere Admin console from a local computer, select **Local file system**, and enter the path of the `IDSWebApp.war` file in the **Full path** field. You can also click **Browse** to specify the path.
   - If you accessed the WebSphere Admin console from a remote computer, select **Remote file system**, and enter the path of the `IDSWebApp.war` file in the **Full path** field. You can also click **Browse** to specify the path.
6. In the **How do you want to install the application** page, select the **Fast Path** option and click **Next**.
7. In the **Select installation options** page, the default options are selected.
8. Click **Next**.
9. In the **Map modules to server** page, you can map modules to the servers that are specified in the **Clusters and servers** field.
   a. Select the check box for the required module, and click **Apply**.
   b. After you complete the mapping, click **Next**.
10. In the **Map virtual hosts for Web modules** page, you can map the web application to the specific virtual servers. If there are more virtual hosts, the server requires information about the WebSphere environment to select the right module. In this example, the `default_host` option is available for selection.
11. Click **Next**.
12. In the **Map context roots for Web modules** page, enter the context root as `/IDSWebApp` in the field.
13. A summary with your selection is shown.
14. Click **Finish**. It initiates the installation of your application. A summary of installation is shown.
15. To save the changes to the master configuration, click **Save**.
16. On the left navigational pane, click **Applications** > **Application Types** > **WebSphere enterprise applications**.

17. In the **Enterprise Applications** page, select the check box next to `IDSWebApp_war`, and click **Start**.
18. Start Web Administration Tool.
19. To access Web Administration Tool, open a browser and enter the following address:
    - For non-secured access (HTTP), enter `http://WAS_server_hostname:9080/IDSWebApp`.
    - For secured access (HTTPS), enter `https://WAS_server_hostname:9443/IDSWebApp`

    The port, 9080, is the default HTTP port for WebSphere Application Server, and port, 9443, is the default HTTPS port. If these ports are not the configured port for your WebSphere Application Server, provide the appropriate port number. If Global or Administrative security is configured for WebSphere Application Server, then you must meet the following requirements:
    a. Deploy Web Administration Tool in WebSphere Application Server as a new profile.
    b. Configure SSL for Web Administration Tool.
    c. If it is not possible to deploy Web Administration Tool in a profile, add the directory server certificate to the truststore of the profile. For the server-client authentication, add the WebSphere Application Server profile certificate to the truststore of the directory server.

Starting embedded WebSphere Application Server to use Web Administration Tool

Start the web application server that is associated with Web Administration Tool to add, manage, and administer directory server instances.

Before you begin

You must complete the following tasks before you start web application server that is associated with Web Administration Tool:

1. Complete the installation of Web Administration Tool.
2. Deploy Web Administration Tool in a supported web application server.

Note: If you use IBM Installation Manager for the installation and deployment of Web Administration Tool in embedded WebSphere Application Server, the application server starts after the you complete Web Administration Tool deployment.

Procedure

1. To start the application server that is associated with Web Administration Tool, run the following command on various operating system:

   Windows

   If the application server is not started, run the following command:

   installation_path`\idstools\bin\startWebadminApp.bat`

   The default installation path is `C:\Program Files\IBM\ldap\V6.3.1`.

   AIX and Solaris

   `/opt/IBM/ldap/V6.3.1/idstools/bin/startWebadminApp`

Linux

```
/opt/ibm/ldap/V6.3.1/idstools/bin/startWebadminApp
```

2. Open a web browser.
3. Enter the following URL on the address bar of web browser:

   Note: If you installed and deployed Web Administration Tool on a remote system, substitute the host name or IP address of the system instead of `localhost`.

   ```
   http://localhost:12100/IDSWebApp
   ```

What to do next

To manage and administer directory server instances, add servers in the Web Administration Tool console. See "Accessing Web Administration Tool."

Accessing Web Administration Tool

To manage directory server instances remotely, open Web Administration Tool and configure directory server instance for remote management.

Before you begin

You must complete the following tasks before you can access Web Administration Tool:

1. Complete the installation of Web Administration Tool.
2. Deploy Web Administration Tool in a supported web application server.
3. Start the web application server that is associated with Web Administration Tool.

Procedure

1. To access Web Administration Tool, use one of the following options:
   - Open a web browser and enter the following URL:
     - For unsecured access, enter `http://hostname:12100/IDSWebApp`.
     - For secured access, enter `https://hostname:12101/IDSWebApp`.
   - Open the following file in a web browser:

     Windows

     For unsecured access, open *ds_installation_path*`\idstools\bin\idswebadmin.html`. You can also click **Start** > **All Programs** > **IBM Security Directory Server 6.3.1** > **Web Administration Tool**.

     For secured access, open *ds_installation_path*`\idstools\bin\idswebadminssl.html`. You can also click **Start** > **All Programs** > **IBM Security Directory Server 6.3.1** > **Web Administration Tool (secure)**.

     AIX, Linux, and Solaris

     For unsecured access, open *ds_installation_path*`/idstools/bin/idswebadmin.html`.

     For secured access, enter *ds_installation_path*`/idstools/bin/idswebadminssl.html`.

The *ds_installation_path* variable represents the IBM Security Directory Server installation location. For more information about the default location, see "Default installation locations" on page 25.

2. Log in to the Web Administration Tool console as the console administrator.
   a. In the **User ID** field, enter `superadmin`.
   b. In the **Password** field, enter **secret**.

      Note: You must change the console administrator password after you log in for the first time.
   c. Click **Login**.
3. To add a directory server to the console, complete the following steps:
   a. On the **Introduction** page, click **Manage console servers**.
   b. On the **Manage console servers** page, click **Add**.
   c. In the **Server name** field, enter a unique name to identify your server. If you do not provide a value, the application assigns a `hostname:port` value or an `IP_address:port` value.
   d. In the **Hostname** field, the host name or the IP address of the directory server.
   e. In the **Port** field, enter the server port number.
   f. To specify whether the console must communicate with the server securely, select **Enable SSL encryption**.
   g. To enable the Administration port control, select **Administration server supported**.
   h. In the **Administration port** field, enter the administration server port number.
   i. To apply changes, click **OK**.
4. To logout of the Web Administration Tool console, click **Logout**.

Stopping web application server

Before the uninstallation of Web Administration Tool, you must logout of Web Administration Tool and stop the web application server that is associated with it.

Before you begin

You must complete the following tasks before you can stop web application server that is associated with Web Administration Tool:

1. Deploy Web Administration Tool in a supported web application server.
2. Start the web application server that is associated with Web Administration Tool.

Procedure

1. Log in a root on UNIX systems, and as a member of administrator group on Windows.
2. Access the command prompt.
3. Go to `bin` subdirectory in the Web Administration Tool profile. The following location is the default installation path of the embedded WebSphere Application Server where Web Administration Tool is deployed. If you specified a custom installation path for embedded WebSphere Application Server, you must make appropriate changes.

Operating system	Path
Windows	`C:\Program Files\IBM\ldap\V6.3.1\appsrv\profiles\TDSWebAdminProfile\bin`
AIX and Solaris	`/opt/IBM/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/bin`
Linux	`/opt/ibm/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/bin`

4. To stop web application server that is associated with Web Administration Tool, run the following command:

Operating system	Command to run:
Windows	`stopServer.bat server1`
AIX, Linux, and Solaris	`./stopServer server1`

Note: On Windows, you can also stop the service that is associated with your web application server from the **Services** window.

HTTPS with embedded WebSphere Application Server

To secure web access to your application, you can configure and start your application in HTTPS mode.

After you deploy Web Administration Tool in embedded WebSphere Application Server, you can start your application. You can connect to Web Administration Tool securely by providing HTTPS web address and the secure port.

To use HTTPS, provide the following web address to accessWeb Administration Tool:

`https://`*`hostname`*`:12101/IDSWebApp`

To use non-HTTPS connection, provide the following web address to accessWeb Administration Tool:

`http://`*`hostname`*`:12100/IDSWebApp`

You can also change the default JKS files with certificates that are provided with the web application server for SSL/TLS secure communication. You can create new key and truststore database files to use with application that is deployed in embedded WebSphere Application Server. The default key and truststore database files are separate and are in the *WAS_HOME*`/profiles/TDSWebAdminProfile/etc/` directory. The *WAS_HOME* variable is the installation location of embedded WebSphere Application Server. The default key database file is `DummyServerKeyFile.jks`, and the default truststore database file is `DummyServerTrustFile.jks`.

If you created your JKS files, you can change the key and truststore database files. To configure your JKS files, passwords, and file formats, add, or modify the following entries (highlighted in **bold**) in the *WAS_HOME*`/profiles/TDSWebAdminProfile/config/cells/DefaultNode/security.xml` file:

```
<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"/>
```

Undeploying Web Administration Tool from embedded WebSphere Application Server

To replace an existing Web Administration Tool (`IDSWebApp.war` file) with a later version, you must undeploy the existing Web Administration Tool.

Procedure

1. Start the web application server that is associated with Web Administration Tool, if it is in stopped state. See "Starting embedded WebSphere Application Server to use Web Administration Tool" on page 112.
2. Go to the *DS_install_location*`/idstools` directory. The *DS_install_location* is the IBM Security Directory Server installation location. The following locations are the default for various operating systems:

Operating systems	Default installation locations:
Microsoft Windows	`c:\Program Files\IBM\ldap\V6.3.1`
AIX and Solaris	`/opt/IBM/ldap/V6.3.1`
Linux	`/opt/ibm/ldap/V6.3.1`

3. Run the following command:

   Note: If you installed embedded WebSphere Application Server in a custom location, you must also provide the **-a**, **-w**, **-p**, and **-r** parameters to the `deploy_IDSWebApp` command. For more information about the `deploy_IDSWebApp` command, see the command usage, `deploy_IDSWebApp -h`.

Operating systems	Command to run:
Microsoft Windows	`deploy_IDSWebApp.bat -u`
AIX, Linux, and Solaris	`deploy_IDSWebApp -u`

Chapter 16. Planning for an instance configuration

You must decide the configuration settings for your computer before you create and configure the LDAP environment.

To create a directory server instance or a proxy server instance, you must first create a system user ID who owns the instance. For storing directory data in a directory server instance, you must decide the code page that you want to use.

Installation of IBM Security Directory Server and corequisite software products and creation of a directory server instance requires you to create user and group on the computer. Installation of IBM Security Directory Server corequisite software products, such as IBM DB2, requires creation of system user ID for DB2 administrator.

Users and groups that are associated with a directory server instance

To create a directory server instance or a proxy server instance, you must create user and group with the required permissions.

If you want to create an instance on your computer, you must associate the instance with a system user ID. This user ID is the owner of the directory server instance. If a system user ID does not exist for an instance, you must create a user ID on the computer. To create a user ID for the directory server instance owner, database instance owner, and database owner, you must follow the naming rules. For more information about the naming rules, see "Naming rules" on page 118.

For a full directory server, you must also associate system user IDs as the owners of the database instance and the database. You can use the same user ID for all three roles. If you use the same user ID, the directory server instance, database instance, and database owner all contain the same owner name.

If you use Instance Administration Tool to create a directory server instance, you can create the directory server instance owner user ID with the tool. You can also use the **idsadduser** command to create the directory server instance owner user ID. The command creates a user ID that meets all the requirements.

The user ID that you associate with the directory server instance owner, database instance owner, and database owner contain the following roles:

Directory server instance owner

A system user ID must exist on the computer that serves as the directory server instance owner. The user ID for the directory server instance owner is also the name of the directory server instance. This user is assigned the authority to manage the directory server instance.

On Windows, a member of the Administrators group also has the authority to manage the directory server instance. On AIX, Linux, and Solaris, the primary group of the directory server instance owner also contains the authority to manage the directory server instance.

Note: On AIX, Linux, and Solaris, the instance owner names are case-sensitive. You must always specify the directory server instance name

and owner exactly as the user ID is specified. The following example shows two different owner names, `JoeSmith` and `joesmith`.

Database instance owner
The user ID that serves as database instance owner owns the database instance that is configured for a directory server instance. The database instance name and the database instance owner name are the same. This user manages the database instance. The directory server instance owner can also manage the database instance. By default, this user ID is the same as the user ID that owns directory server instance.

Database owner
This user ID owns the database that is used by the directory server instance to store the directory data. The database is stored in the database instance that is owned by the database instance owner. The directory server instance uses the database owner user ID and the password to connect to the database.

Naming rules

The user ID and the primary group for a directory server instance must meet the naming rule guidelines.

The naming rules requirement apply to the following user IDs:

- The directory server instance name (the user ID that owns the directory server instance).
- The database instance name (the user ID that owns the database instance). This user ID is usually the same as the directory server instance name.
- On AIX, Linux, and Solaris, the primary groups of the directory server instance owner user ID and the database instance owner user ID.

Note: When you create the user ID and group, you must assign the appropriate permissions. See "Users and groups creation requirements" on page 119.

The user and group IDs must meet the following requirements:

- Cannot be longer than 8 characters
- Cannot be any of the following names:
  - `USERS`
  - `ADMINS`
  - `GUESTS`
  - `PUBLIC`
  - `LOCAL`
  - `idsldap`
- Cannot begin with any of the following prefix:
  - `IBM`
  - `SQL`
  - `SYS`
- Cannot include accented characters
- Can include the following characters:
  - A - Z
  - a - z
  - 0 - 9

  - _ (Underscore)
- Must begin with one of the following characters:
  - A - Z
  - a - z

Users and groups creation requirements

When you create users and groups for your instance, you must assign users and groups with appropriate permissions and add as a member of appropriate groups.

After you create the required users and groups for your instance, you must assign appropriate permissions and add the users in appropriate groups. You must meet the following requirements for user and group IDs:

Windows

- Add the directory server instance owner and the database instance owner as the members of the Administrators group.
- Set a valid locale for the database instance owner must to a language in which you want the server to generate messages. If necessary, log in as the user and change the locale with the appropriate value.

AIX, Linux, and Solaris

- Add the root ID as a member of the primary group of the directory server instance owner and the database instance owner.
- Add the root ID as a member of the `idsldap` group.
- Add the directory server instance owner and the database instance owner as the members of the `idsldap` group.
- Create home directories for the directory server instance owner and the database instance owner.
- Assign appropriate permissions for the home directory of the directory server instance owner.
  - The user ownership for the instance is the directory server instance owner.
  - The group ownership for the instance is the primary group of directory server instance owner.
  - You must assign read, write, and execute permissions to the home directory for the directory server instance owner and its primary group.
- Assign read, write, and execute access on the location where the database is created for the directory server instance owner and its primary group.
- The directory server instance owner and the database instance owner for a directory server instance can be different users. In such a case, the directory server instance owner must be a member of the database instance owner primary group.
- If directory server instance owner, DB2 instance owner, and database owner are different, they all must to be members of the same group.
- Set the Korn shell script (`/usr/bin/ksh`) as the login shell of the directory server instance owner, the database instance owner, and the database owner.

You must set the password of the directory server instance owner, the database instance owner, and the database owner correctly and must be ready to use. The

password must not be expired or waiting for a first-time validation of any kind. You can verify whether the password is correctly set by accessing telnet on the computer and log in with the user ID and password.

When you configure the database, it is not necessary but customary, to specify the home directory of the database instance owner as the database location. If you specify some other location, the home directory of the database instance owner must contain 3 - 4 MB of space available. DB2 creates links and adds files into the home directory of the database instance owner even though the database itself is elsewhere. If your computer does not contain the required space in the database instance owner home directory, you can add space or change the home directory.

Examples

To create an instance owner that meets the requirements for a directory server instance owner, you can run the **idsadduser** command. The **idsadduser** command is in the `sbin` subdirectory of the IBM Security Directory Server installation location.

Example 1:

To create a user account on AIX, Linux, or Solaris, with the following values, run the **idsadduser** command:

- User name: `JoeSmith`
- Primary group: `employees`
- Home directory: `/home/joe` (On Solaris, use `/export/home/joe`)
- Password: `joespw`

```
idsadduser –u JoeSmith –g employees –l /home/joe –w joespw
```

Example 2:

To create a user account as a member of the Administrators group on Windows with the following values, run the **idsadduser** command:

- User name: `JoeSmith`
- Password: `joespw`

```
idsadduser –u JoeSmith –w joespw
```

Configuration planning

For your directory server environment, you must decide the data type you plan to store, the data structure, and the data security to set.

You must make the following decisions before you configure and populate your database:

The data type that you want to store in the directory server

You must decide the schema that you want to use for your directory server and the data type you want to store in your directory server. A standard set of attribute-type definitions and object class definitions are included in the directory server. To customize your data, you might want to add your custom attribute type and object class definitions before you add entries to the directory server.

You can make addition or modification to schema after the directory is populated with data. In some situations, schema changes might require you to unload and reload your data.

The code page that you are want to use

Decide whether to create your database by using the local code page or by

using the Universal Character Set (UTF-8). If you select a local code page, it enables IBM Security Directory Server applications and users to retrieve search results as expected for the collation sequence of the language. However, if you use a local code page data in that specific code page is stored in the directory. If you use UTF-8, you can store any UTF-8 character data in the directory. For more information about UTF-8, see "UTF-8 support."

Note: If you want to use language tags, you must use UTF-8 as the code page for the database.

Define a hierarchy structure to store r your directory data
IBM Security Directory Server stores directory data in a hierarchical tree structure. The names of entries in the directory are based on the relative position of the entries within the tree structure. It is important to define a logical organization to the directory that is appropriate for your LDAP environment. A logical organization makes it easier for clients to determine which branch of the tree to search to locate the required information.

Define your data security requirements
To prevent access to the directory data over unsecured port, you can configure your directory server for secure communication. For more about how to secure your data, see *IBM Security Directory Server Version 6.3.1 Administration Guide*.

Define the required access permissions for the directory data
For information about using access permissions, see the access control lists in the *IBM Security Directory Server Version 6.3.1 Administration Guide*.

Access whether you require a proxy server
If the directory data is large and the environment is write-intensive, you must consider whether to use a proxy server. Large directory environments that are read-heavy might be able to achieve the required scaling by configuring replication. See the list of supported features in a proxy server in the *IBM Security Directory Server Version 6.3.1 Administration Guide* before you decide to use a proxy server.

UTF-8 support

You can configure a directory server to store any national language characters that can be represented in UTF-8.

IBM Security Directory Server supports a wide variety of national language characters through the UTF-8 (UCS Transformation Format) character set. In LDAP Version 3 protocol all character data that an LDAP client and server communicates is in UTF-8.

The server determines the types of characters that can be stored and searched based on the code page that is used for configuring a database. You can specify the database character set as UTF-8 or set to use the local character set of the system on which the server exists. The local character set is based on the locale, language, and code page environment on the system.

If you specify UTF-8, you can store any UTF-8 character data in the directory. LDAP clients on a system that support any UTF-8 supported language can access and search the directory properly. If the LDAP clients are on a system with a local character set, the client might not correctly show the results that are retrieved from the server in a particular character set.

If you use a UTF-8 database, the database performance improves because no data conversion is required when you store data or retrieve data from the database.

Note: If you want to use language tags, the database must be a UTF-8 database.

Use of UTF-8 in a directory server

To decide which code page to use, you must understand how a directory server uses code page to store and access directory data.

A UTF-8 database has a fixed collation sequence and that sequence is the binary order of the UTF-8 characters. It is not possible to do language-sensitive collation with a UTF-8 database.

For your LDAP applications or users to obtain the following results, then UTF-8 might not be the appropriate character set for your database:

- A search with an ordering filter, such as `"name >= SMITH"`, and if you expect the order similar to your locale.
- A search with the control to sort the results, and if you expect the order similar to your locale.

In such situations, the LDAP server system and all the client systems must be run with the same character set and locale.

For example, an LDAP server database that is configured with the Spanish locale returns search results based on order of the character, as Spanish-language clients expect. Such configuration limits your directory user community to a single character set in that locale and collation sequence.

Creation of an LDIF file with UTF-8 values by using server utilities

You can use a `charset` extension to create an LDIF format with UTF-8 values.

Manual creation of an LDIF file that contains UTF-8 values is difficult. In the LDIF file header, you can specify the extension that supports an Internet Assigned Numbers Authority (IANA) character set name along with the version number. For more information about the supported IANA character sets, see "Supported IANA character sets" on page 123.

Examples

Example 1:

For the server utilities to automatically convert from the specified character set to UTF-8, you can use the `charset` tag.

```
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: [title in Spanish]
jpegPhoto:< file:///usr/local/photos/jgriego.jpg
```

In the following example, all attribute names with values that are separated by a single colon are translated from the `ISO-8859-1` character

set to UTF-8. All attribute names with values that are separated by a double colon, such as `description:: V2hhdCBhIGNhcmVmdWwgcmVhZGVyIHlvd`, must be `base 64-encoded` and are must be in binary or UTF-8 character strings. If values are read from a file, such as the `jpegPhoto` attribute, which is specified by the web address must also be in binary or UTF-8. For such attribute values, no translation is done from the specified `charset` to UTF-8.

Example 2:

In the following example, an LDIF file without the `charset` tag the content is expected to be in UTF-8:

```
# IBM Directorysample LDIF file
#
# The suffix "o=sample" should be defined before attempting to load
# this data.

 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
```

In IBM Security Directory Server, the LDIF file with the following content can be used without the `version: 1` header information:

```
# IBM Directorysample LDIF file
#
#The suffix "o=sample" should be defined before attempting to load
#this data.

 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
```

Supported IANA character sets

You can use Internet Assigned Number Authority (IANA) character set names in an LDIF file or with the C Client interface to identify the character set of directory data.

IBM Security Directory Server supports the Internet Assigned Number Authority (IANA) character set names by operating systems.

For more information about IANA-registered character sets, see the Character Sets website at www.iana.org/assignments/character-sets.

Table 38. IANA-defined character sets

Character	Locale					DB2 code page	
Set name	**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	n/a	X	X	X		
IBM437	n/a	n/a	X	n/a	n/a	437	437
IBM850	n/a	n/a	X	X	n/a	850	850
IBM852	n/a	n/a	X	n/a	n/a	852	852
IBM857	n/a	n/a	X	n/a	n/a	857	857
IBM862	n/a	n/a	X	n/a	n/a	862	862
IBM864	n/a	n/a	X	n/a	n/a	864	864
IBM866	n/a	n/a	X	n/a	n/a	866	866
IBM869	n/a	n/a	X	n/a	n/a	869	869
IBM1250	n/a	n/a	X	n/a	n/a		
IBM1251	n/a	n/a	X	n/a	n/a		
IBM1253	n/a	n/a	X	n/a	n/a		
IBM1254	n/a	n/a	X	n/a	n/a		
IBM1255	n/a	n/a	X	n/a	n/a		
IBM1256	n/a	n/a	X	n/a	n/a		
TIS-620	n/a	n/a	X	X	n/a	874	874
EUC-JP	X	X	n/a	X	X	954	n/a
EUC-KR	n/a	n/a	n/a	X	X	970	n/a
EUC-CN	n/a	n/a	n/a	X	X	1383	n/a
EUC-TW	X	n/a	n/a	X	X	964	n/a
Shift-JIS	n/a	X	X	X	X	932	943
KSC	n/a	n/a	X	n/a	n/a	n/a	949
GBK	n/a	n/a	X	X	n/a	1386	1386
Big5	X	n/a	X	X	X	950	950
GB18030	n/a	X	X	X	X		
HP15CN	X (with non-GB18030)						

Note:

- The Chinese character set standard, GB18030, is supported by appropriate patches available from www.oracle.com and www.microsoft.com

- On Windows operating systems, you must set the *zhCNGB18030* environment variable to TRUE.

ASCII characters from 33 to 126

Use the ASCII characters table to determine the characters to use for directory server instance encryption seed and encryption salt.

You can use the ASCII characters from 33 to 126 in the encryption seed string and encryption salt.

Table 39. ASCII characters from 33 to 126

ASCII code	Character	ASCII code	Character	ASCII code	Character
33	! exclamation point	34	" double quotation	35	# number sign
36	$ dollar sign	37	% percent sign	38	& ampersand
39	' apostrophe	40	(left parenthesis	41	) right parenthesis
42	* asterisk	43	+ plus sign	44	, comma
45	- hyphen	46	. period	47	/ slash
48	0	49	1	50	2
51	3	52	4	53	5
54	6	55	7	56	8
57	9	58	: colon	59	; semicolon
60	< less-than sign	61	= equals sign	62	> greater-than sign
63	? question mark	64	@ at sign	65	A uppercase a
66	B uppercase b	67	C uppercase c	68	D uppercase d
69	E uppercase e	70	F uppercase f	71	G uppercase g
72	H uppercase h	73	I uppercase i	74	J uppercase j
75	K uppercase k	76	L uppercase l	77	M uppercase m
78	N uppercase n	79	O uppercase o	80	P uppercase p
81	Q uppercase q	82	R uppercase r	83	S uppercase s
84	T uppercase t	85	U uppercase u	86	V uppercase v
87	W uppercase w	88	X uppercase x	89	Y uppercase y
90	Z uppercase z	91	[left square bracket	92	\ backslash
93	] right square bracket	94	^ caret	95	_ underscore
96	` grave accent	97	a lowercase a	98	b lowercase b
99	c lowercase c	100	d lowercase d	101	e lowercase e
102	f lowercase f	103	g lowercase g	104	h lowercase h
105	i lowercase i	106	j lowercase j	107	k lowercase k
108	l lowercase l	109	m lowercase m	110	n lowercase n
111	o lowercase o	112	p lowercase p	113	q lowercase q
114	r lowercase r	115	s lowercase s	116	t lowercase t
117	u lowercase u	118	v lowercase v	119	w lowercase w
120	x lowercase x	121	y lowercase y	122	z lowercase z
123	{ left curly brace	124	| vertical bar	125	} right curly brace
126	~ tilde				

Chapter 17. Instance creation and administration

To use a directory server in an identity infrastructure, you must create a directory server instance as per your requirements.

After you complete IBM Security Directory Server installation, you must create a directory server instance and then set the administrator DN and password for the instance. You can create a full directory server or a proxy server. To create a directory server instance or a proxy server instance, you must create a system user ID on the computer. The system user ID is the owner of the directory server instance or the proxy server instance.

For a full directory server, you must create a DB2 database and configure the database with the directory server instance. To create a DB2 database, you must install a supported DB2 version on the computer. You must verify whether the `ldapdb.properties` file is updated with the DB2 installation path and version. For more information, see Updating the `ldapdb.properties` file manually.

Note: When you use IBM Security Directory Server Instance Administration Tool (**idsxinst**) to create a full directory server instance, it also creates a `ldapdb.properties` file in the instance home directory. On Windows, the `ldapdb.properties` file is in the *instance_home*`\idsslapd-`*instance_name*`\etc` directory. On AIX, Linux, or Solaris, the file is in the *instance_home*`/idsslapd-`*instance_name*`/etc` directory.

For a proxy server instance, do not create and configure a DB2 database with the proxy server instance.

Instance Administration Tool is a graphical user interface (GUI) that you can use to create and manage directory server instances. To use Instance Administration Tool, IBM Java Development Kit is required. When you use Instance Administration Tool, the tool provides wizard to help you complete the task.

You can use Instance Administration Tool to create, view, copy, change information about, and delete instances. You can also use the tool to create or edit the users who own directory server instances and to upgrade instances from previous versions of IBM Security Directory Server. You can use Instance Administration Tool to start or stop the server or the administration server for your instances. In addition, you can open Configuration Tool from Instance Administration Tool.

You can also use command-line utilities to create and manage directory server instances.

Starting Instance Administration Tool

Start Instance Administration Tool to create and administer a directory server instance or a proxy server instance.

Before you begin

To use Instance Administration Tool, you must install IBM Security Directory Server with the Server, Proxy Server, or both features. To run Instance Administration Tool, log in with the following credentials:

AIX, Linux, and Solaris
Log in as the root user.

Windows
Log in as a member of the administrator group.

IBM Java Development Kit must exist in the IBM Security Directory Server installation path. For the default IBM Security Directory Server installation path, see "Default installation locations" on page 25.

Procedure

To start Instance Administration Tool, use one of the following options:

Options to open Instance Administration Tool	Command to run:
Installation of the IBM Security Directory Server Server feature	On **Summary** page, click **Instance Administration Tool (idsxinst)**. For information, see "Installing with IBM Installation Manager" on page 28.
The `idsxinst` command	**Windows** 1. Change the current directory to the `sbin` directory in the IBM Security Directory Server installation location. 2. Run the **`idsxinst`** command. **Note:** You can also click **Start** > **All Programs** > **IBM Security Directory Server 6.3.1** > **Instance Administration Tool**. **AIX, Linux, and Solaris** 1. Change the current directory to the `sbin` directory in the IBM Security Directory Server installation location. 2. Run the **`idsxinst`** command. For more information about the IBM Security Directory Server installation path, see "Default installation locations" on page 25.

Starting Instance Administration Tool to upgrade an instance

Run Instance Administration Tool with parameters to open Instance Administration Tool to upgrade a remote instance that contains backup data.

Before you begin

To upgrade a remote instance, you must meet the following requirements:

- You computer must contain the backup data of the instance created with the **`migbkup`** command. You must use the **`migbkup`** command of an version to which you want to upgrade the remote instance.

- Log in as a root user on AIX, Linux, and Solaris systems. On Windows, log in as a member of administrator group.

Procedure

1. Access the command prompt.
2. Change your current working directory to `sbin` directory in the IBM Security Directory Server installation location. For more information about the default installation path, see "Default installation locations" on page 25.
3. Run the **idsxinst** command in the following format:

   ```
   idsxinst -migrate backup_directory
   ```

   Substitute the *backup_directory* variable with the location where you stored the backup data of the instance created with the **migbkup** command.

Directory server instance creation

To use a directory server instance in an LDAP environment, create an instance that is cryptographically synchronized with the existing instance to obtain optimum performance

If you create a directory server instance as a copy of an existing directory server instance, the two directory server instances are cryptographically synchronized. You do not require to synchronize them.

If you create an instance that is not a copy of an existing instance cryptographically synchronize the instance with the existing instance. You must cryptographically synchronize the server instances to obtain the best performance in the following environment:

- Replication
- Distributed directory
- Import and export LDIF data between server instances

You must synchronize the server instances before you do any of the following operations:

- Start the new server instance.
- Run the **idsbulkload** command on the server instance.
- Run the **idsldif2db** command on the server instance.

For more information about synchronizing directory servers, see *IBM Security Directory Server Administration Guide*.

After you create a directory server instance and configure it with a DB2 database, back up the directory server instance. You must back up configuration, schema, DB2 database, and directory key stash files. You can use the **idsdbback** command to create directory server instance backup. You can use the **idsdbrestore** command to restore the key stash files if necessary. For more information about the backup and restore commands, see *Command Reference*.

Instance creation with Instance Administration Tool

You must assess the requirements of your environment and create a directory server instance at a stage that is appropriate for your environment.

You can use Instance Administration Tool to create an instance in several different ways:

- Create a default instance with a default name and other settings. See "Creating the default directory server instance."
- Create an instance with custom settings. See "Creating a directory server instance with custom settings" on page 132.
- Upgrade an instance from a previous version of IBM Security Directory Server. See "Upgrading an instance of a previous version with the **idsimigr** command" on page 90 or "Upgrading an instance of a previous version with Instance Administration Tool" on page 143.
- Create an instance that is a copy of an existing instance on the computer or on another computer. See "Creating a copy of an existing instance with Instance Administration Tool" on page 148.

Creating the default directory server instance

Use the default instance creation option to create a directory server instance with the predefined instance name and the default settings.

Before you begin

To create a default instance, you must complete the following tasks:

1. Install IBM Security Directory Server with the Server feature. See "Installing with IBM Installation Manager" on page 28.
2. Install IBM DB2. See "Installing with IBM Installation Manager" on page 28.
3. Verify whether the `ldapdb.properties` file contains DB2 installation path and version information. See Updating the `ldapdb.properties` file manually.

About this task

If your computer contains an existing directory server instance with the default instance name, then you cannot create the default directory server instance.

The default directory server instance contains the following settings, which you cannot change:

Table 40. The settings for a default directory server instance

Settings	Microsoft Windows	AIX and Linux	Solaris
Name	`dsrdbm01`	`dsrdbm01`	`dsrdbm01`
Instance location	`c:\idsslapd-dsrdbm01`	`/home/dsrdbm01`	`/export/home/dsrdbm01`
Group name	`Administrators`	`grrdbm01`	`grrdbm01`
Administrator DN	`cn=root`	`cn=root`	`cn=root`
Database name	`dsrdbm01`	`dsrdbm01`	`dsrdbm01`

The DB2 table space for the default directory server instance is Database Managed Storage (DMS).

For the default directory server instance, Instance Administration Tool creates the `o=sample` suffix. You can add more suffixes later with Configuration Tool or the **idscfgsuf** command. For more information, see "Suffix configuration" on page 193.

Procedure

1. Start Instance Administration Tool. See "Starting Instance Administration Tool" on page 127.
2. Click **Create an instance**.
3. On the **Create new directory server instance** window, complete the following steps:
   a. Click **Create default instance**.
   b. Click **Next**.
   c. In the **User password** field, enter a password for the user account who owns the directory server instance.
   d. In the **Confirm password** field, enter the password again for the user account who owns the directory server instance.
   e. In the **Encryption seed** field, enter an encryption seed for the directory server instance.

      Remember: You must remember the encryption seed of a directory server instance since it might be required for other configuration tasks.
      The encryption seed must contain only printable `ISO-8859-1 ASCII` characters with values in the range of 33 to 126. The encryption seed must contain a minimum of 12 and a maximum of 1016 characters. For information about the characters to use, see "ASCII characters from 33 to 126" on page 125. The directory server uses the encryption seed to generate a set of Advanced Encryption Standard (AES) secret key values. The key stash file of a directory server instance store the key values, and are used to encrypt and decrypt password and attributes.
   f. In the **Confirm encryption seed** field, enter the encryption seed for the directory server instance.
   g. In the **Administrator DN password** filed, enter a password for the directory server instance administrator.
   h. In the **Confirm password** filed, enter the password for the directory server instance administrator.
   i. Click **Next** .
   j. Verify the information about the default directory server instance. and
   k. To start creating the default directory server instance, click **Finish**. The Result window with the log information is displayed.
4. Verify the log information is displayed in the **Results** window.
5. To close the **Results** window, click **Close**.
6. To close Instance Administration Tool, click **Close**.

Results

Instance Administration Tool creates the default directory server instance, `dsrdbm01`, on the computer.

What to do next

You must start the `ibmslapd` process and the administration server that is associated with the directory server instance. See "Start or stop a directory server and an administration server" on page 151.

Creating a directory server instance with custom settings

Use Instance Administration Server to create a directory server instance with custom values as per your requirement.

Before you begin

To create a directory server instance, you must complete the following tasks:

1. Install IBM Security Directory Server with the Server feature. See "Installing with IBM Installation Manager" on page 28.
2. To create a full directory server with RDBM backend, install IBM DB2. See "Installing with IBM Installation Manager" on page 28.
3. Verify whether the `ldapdb.properties` file contains DB2 installation path and version information. See Updating the `ldapdb.properties` file manually.

Procedure

1. Start Instance Administration Tool. See "Starting Instance Administration Tool" on page 127.
2. Click **Create an instance**.
3. In the **Create or migrate** panel of the **Create new directory server instance** window, click **Create a new directory server instance**.
4. Click **Next**.
5. In the**Instance details** panel of the **Create new directory server instance** window, specify the following values:
   a. From the **User name** list, select the user name that owns the directory server instance. The directory server instance is assigned the same name as the user name.
   b. If you want to associate a new user account with the instance, click **Create user**. In the **Create new user for directory server instance** window, complete the following steps:
      1) In the **User Name** field, enter the user name.
      2) In the **Password** field, enter a password for the user account.
      3) In the **Confirm password** field, enter the password for the user account.
      4) In the **Home directory** field, enter the home directory to configure for the user account. You can click **Browse** and specify the home directory.
      5) In the **Primary group** field, enter the primary group name of the user.
      6) To create the user account, click **Create**.
   c. To modify an existing user account, select the user name from the **User name** list and click **Edit user**. In the **Edit the user for directory server instance** window, complete the following steps:
      1) The **User Name** field is populated with the user name.
      2) In the **Password** field, enter a password for the user account.
      3) In the **Confirm password** field, enter the password for the user account.
      4) In the **Home directory** field, enter the home directory to configure for the user account. You can click **Browse** and specify the home directory.
      5) In the **Primary group** field, enter the primary group name of the user.
      6) To edit the user account, click **Edit**.

6. In the **Instance location** field, enter the location of the directory server instance. You can click **Browse** and specify the instance home directory. The location must contain at least 30 MB of free disk space. On Windows systems, the location is a disk drive, such as `C:`. The directory instance files are stored in the `\idsslapd-`*`instance_name`* directory on the disk drive you specify. The *instance_name* variable is the name of the directory server instance. On AIX, Linux, and Solaris systems, the home directory of the directory server instance owner is the default instance location, but you can specify a different path.
7. In the **Encryption seed string** field, enter the encryption seed for the directory server instance.

   Remember: You must remember the encryption seed of a directory server instance since it might be required for other configuration tasks.
   The encryption seed must contain only printable `ISO-8859-1 ASCII` characters with values in the range of 33 to 126. The encryption seed must contain a minimum of 12 and a maximum of 1016 characters. For information about the characters to use, see "ASCII characters from 33 to 126" on page 125. The directory server uses the encryption seed to generate a set of Advanced Encryption Standard (AES) secret key values. The key stash file of a directory server instance store the key values, and are used to encrypt and decrypt password and attributes.
8. In the **Confirm encryption seed** field, enter the encryption seed for the directory server instance.
9. If you want to provide an encryption salt value, click **Use encryption salt value**.
   a. In the **Encryption salt string** field, enter an encryption salt value for the directory server instance. The encryption salt must contain only printable `ISO-8859-1 ASCII` characters with values in the range of 33 to 126. The encryption salt must contain 12 characters. For information about the characters to use, see "ASCII characters from 33 to 126" on page 125. To cryptographically synchronize a directory server with another directory server instance, you must use the same encryption seed and salt values.
   b. In the **Confirm encryption salt** field, enter the encryption salt value for the directory server instance.
10. Optional: In the **Instance description** field, a description of the directory server instance. The description helps in identifying the instance.
11. Click **Next**.
12. In the **DB2 instance name** field on the **DB2 instance details** panel, specify the DB2 instance name for the directory server instance.

    Note: The DB2 instance for the directory server instance must not be configured or used by other programs or products.

    By default, the DB2 instance name is the same as the directory server instance name. However, you can specify a different name for the DB2 instance. If you specify a different name, a system user ID with the same name must exist on the computer. This user account name must not be associated with another directory server instance.
13. Click **Next**.
14. In the **TCP/IP settings for multihomed hosts** panel, select one of the following options:
    - If you want the directory server instance to listen on all IP addresses, select **Listen on all configured IP addresses**.

- If you want the instance to listen on a particular set of IP addresses that are configured on the computer, complete the following steps:
  a. Clear **Listen on all configured IP addresses**.
  b. From the **Select the specific IP addresses to listen on** list, select the IP address or addresses that you want the instance to listen on.

15. Click **Next**.
16. In the **TCP/IP port settings** panel, specify the following values:

    Note: You must assign a unique port numbers to the directory server ports and must not conflict with existing ports that are in use on the computer. ON AIX, Linux, and Solaris systems, port numbers in the range of 1 - 1000 can be used only by root.

    a. In the **Server port** field, enter the port number that you want the server to use as its unsecured port. The number must be in range of 1 - 65535.
    b. In the **Server secure port** field, enter the port number that you want the server to use as its secured port. The number must be in the range of 1 - 65535.
    c. In the **Administration server port** field, enter the port number that you want the administration server to use as its unsecured port. The number must be in the range of 1 - 65535.
    d. In the **Administration server secure port** field, enter the port number that you want the administration server to use as its secured port. The number must be in the range of 1 - 65535.
    e. Click **Next**.
17. In the **Optional steps** panel, complete the following steps:
    a. To configure the administrator DN and password for the directory server instance, select **Configure administrator DN and password**. You must set the administrator DN and password for a proxy server and full directory server.
    b. To configure the database for the directory server instance, select **Configure database**.
    c. Click **Next**.
18. In the **Configure administrator DN and password** panel, complete the following steps:
    a. In the **Administrator DN** field, enter a valid DN or accept the default DN, `cn=root`. The administrator DN value is not case-sensitive. The administrator DN user has full access to all data in the directory server instance.
    b. In the **Administrator Password** field, enter the password for the administrator DN. Passwords are case-sensitive. Double byte character set (DBCS) characters in the password are not valid.
    c. In the **Confirm password** field, enter the password for the administrator DN. You must remember the password for future reference.
    d. Click **Next**.
19. In the **Configure database** panel, complete the following tasks to configure the database for the directory server instance: Instance Administration Tool adds the database information in the configuration file, `ibmslapd.conf`, for the directory server instance. If the database does not exist, Instance Administration Tool creates the database.

a. In the **Database user name** field, enter a valid DB2 administrator ID. The DB2 administrator ID must exist on the computer and must contain the required access permission before you configure the database.

   Note: The DB2 administrator ID must set the appropriate locale for the language in which you want server messages to be displayed before the server startup.

b. In the **Password** field, enter the password for the DB2 administrator. The password is case-sensitive.

   Note: If you change the system password for the DB2 administrator, you cannot update it with Instance Administration Tool. You must use Configuration Tool or the **idscfgdb** command with the **-w** parameter. For more information, see "Management of the DB2 database administrator password" on page 173.

c. In the **Database name** field, enter a DB2 database name. The name must be in the range of 1 - 8 characters long.

d. Optional: If you want to set any of the following DB2 configuration settings, select **Show advanced tablespace options**.

   Note: DB2 can use System Managed Storage (SMS) or Database Managed Storage (DMS) data storage type when it creates table spaces. The default for IBM Security Directory Server, version 6.3.1 is Database Managed Storage (DMS). Version of IBM Security Directory Server earlier than 6.2 use SMS for all databases. If you clear **Show advanced tablespace options**, the USERSPACE1 and LDAPSPACE table spaces are created by using DMS with default sizes and locations. On AIX, Linux, and Solaris, the default path and file name for the USERSPACE1 table space is *database_location*/*instance_name*/NODE0000/SQL00001/USPACE. On Windows, the default path and file name for the USERSPACE1 table space is *database_location**instance_name*\NODE0000\SQL00001\USPACE. On AIX, Linux, and Solaris, the default path and file name for the LDAPSPACE table space is *database_location*/ldap32kcont_*instance_name*/ldapspace. On Windows, the default path and file name for the LDAPSPACE table space is *database_location*\ldap32kcont_*instance_name*\ldapspace.

   - You want the database to use the System Managed Storage (SMS) data storage for the DB2 table spaces. When SMS is used, the file system manager of the operating system allocates and manages the table space where DB2 tables are stored.
   - You want the database to use the Database Managed Storage (DMS) data storage for the DB2 table spaces. Also, you want to configure the database for the USERSPACE1 and LDAPSPACE table spaces, size, and location. When DMS is used, the table spaces are managed by the database manager. The database administrator decides which devices and files to use, and DB2 manages the space on those devices and files.

e. Click **Next**.

20. In the **Database options** panel, complete the following steps:

    a. In the **Database install location** field, enter the database location path. You can click **Browse** to specify a directory. On Windows, you must provide a disk drive location, C:. On AIX, Linux, and Solaris, the location must be a directory name, such as /home/ldapdb.

       Note: The minimum disk space that is required for a DMS database is 1 GB. For an SMS database, a minimum of 150 MB of disk space is required.

These requirements are for an empty database. When you store data in the database, more disk space is required.

b. To configure the directory server with database for online backup, complete the following steps:

   1) Select **Configure for online backup**.

   2) In the **Database backup location** field, enter the location where you want to store the backup image. You can click **Browse** to specify the location.

   Note: Do not exit Instance Administration Tool when the backup operation is running.
   When you configure the database for online backup after the database configuration is complete an initial, offline backup of the database is run. After the offline backup operation is complete, the administration server is restarted. You can also configure online backup for a directory server instance with the **idscfgdb** command. However, you cannot unconfigure online backup with the **idscfgdb** command and the **-c** parameter. If you configure online backup for an instance with Instance Administration Tool or Configuration Tool, you can unconfigure it with Configuration Tool or the **idscfgdb** command.

c. In the **Character-set option** area, choose one of the following options to create a database type:

   Note: Create a universal DB2 database if you plan to store data in multiple languages in the directory server. A DB2 Universal Database is also most efficient because less data translation is needed. If you want to use language tags, the database must be a UTF-8 database. For more information about UTF-8, see "UTF-8 support" on page 121.

   - To create an UCS Transformation Format (UTF-8) database in which LDAP clients can store UTF-8 character data, click **Create a universal DB2 database** .
   - To create a database in the local code page, click **Create a local codepage DB2 database**.

d. Click **Next**.

21. If you selected **Show advanced tablespace options** in the **Configure database** panel, you must complete the following values in the **Configure Database Tablespaces** panel:

    a. From the **Select database tablespace type** list, select a database type. The DMS database table space type is the default. If you select SMS database table space type, all other fields are disabled. DMS table space support is used only for the USERSPACE1 and LDAPSPACE table spaces. All other table spaces, such as catalog and temporary table spaces, are of type SMS.

    a. Under the **USERSPACE1 tablespace details** area, specify the following details:

       1) From the **Tablespace container** list, select the container type. If you want the USERSPACE1 table space location on the file system, select **File**. If the database table space container location is in a file system, a DMS cooked table space is created. You can specify the initial size for the table space and an extendable unit size, and the table space is automatically expanded when required. If you want to create the USERSPACE1 table space on a raw device, select **Raw device**. A raw device is a device where no file system is installed, such as a hard disk that does not contain a file system. If the database table space container

location is in a raw device, a DMS raw table space is created. In this case, the size of the database table space container is fixed and cannot be expanded. If you select **Raw device**, specify the size along with the container location instead of accepting the default values.

2) If you selected **File** in the **Tablespace container** list, specify the following details:
   a) In the **Directory path** field, specify the directory path where you want create the USERSPACE1 table space. You can click **Browse** to select the directory.
   b) In the **File name** field, enter the file name of the table space that you want to create, or accept the default file name, USPACE.
   c) In the **Initial size** field, enter the initial size for the USERSPACE1 table space in pages or accept the default value. For the **File** type table space container, the USERSPACE1 table space container is of auto-incremental type. You can provide the initial size in the **Initial size** field, and an extendable unit size in the **Extendable size** field. The default value for the initial size is 16 K pages, and the default extendable unit size is 8 K pages. The page size for the USERSPACE1 table space container is 4 KB per page.
3) If you selected **Raw device** in the **Tablespace container** list, specify the following details:
   a) In the **Device path** field, enter the location of the raw device. On Windows, the path must start with \\.\. An example that shows the path with device name, \\.*device_name*. On AIX, Linux, and Solaris, the device path must be a valid path.
   b) In the **Initial size** field, enter the initial size for the USERSPACE1 table space or accept the default value. For the **Raw Device** type table space container, the size of the USERSPACE1 table space container is fixed. The default size is 16 K pages. For better results, specify the size you want.

b. Under the **LDAPSPACE tablespace details** area, specify the following details:
   1) From the **Tablespace container** list, select the container type. If you want the LDAPSPACE table space location on a file system, select **File**. If you want to create the LDAPSPACE table space on a raw device, select **Raw device**. A raw device is a device where no file system is installed, such as a hard disk that does not contain a file system.
   2) If you selected **File** in the **Tablespace container** list, specify the following details:
      a) In the **Directory path** field, specify the directory path where you want create the LDAPSPACE table space. You can click **Browse** to select the directory.
      b) In the **File name** field, enter the file name of the table space that you want to create, or accept the default file name, ldapspace.
      c) In the **Initial size** field, enter the initial size for the LDAPSPACE table space in pages or accept the default value. For the **File** type table space container, the LDAPSPACE table space container is of auto-incremental type. You can provide the initial size in the **Initial size** field, and an extendable unit size in the **Extendable size** field. The default value for the initial size is 16 K pages, and the default extendable unit size is 8 K pages. The page size for the LDAPSPACE table space container is 32 KB per page.

3) If you selected **Raw device** in the **Tablespace container** list, specify the following details:
   a) In the **Device path** field, enter the location of the raw device. On Windows, the path must start with `\\.\`. An example that shows the path with device name, `\\.\`*`device_name`*. On AIX, Linux, and Solaris, the device path must be a valid path.
   b) In the **Initial size** field, enter the initial size for the `LDAPSPACE` table space or accept the default value. For the **Raw Device** type table space container, the size of the `LDAPSPACE` table space container is fixed. The default size is 16 K pages. For better results, specify the size you want.

c. If you selected **File** in one or both of the **Tablespace container** fields, specify the number of pages by which to expand the table space containers in the **Extendable size** field.

d. Click **Next**.

22. In the **Verify settings** panel, verify the summary that is generated.
23. To start the directory server instance creation, click **Finish**.
24. In the **Results** window, verify the log messages that are generated for the instance creation operations.
25. To close the **Results** window, click **Close**.
26. To close Instance Administration Tool, click **Close**.

Results

Instance Administration Tool creates a directory server instance on the computer.

What to do next

You must start the `ibmslapd` process and the administration server that is associated with the directory server instance. See "Start or stop a directory server and an administration server" on page 151.

Creating a proxy server instance with custom settings

Use Instance Administration Server to create a proxy server instance with custom values as per your requirement.

Before you begin

To create a proxy server instance, you must complete the following tasks:

1. Install IBM Security Directory Server with the Proxy Server feature. See "Installing with IBM Installation Manager" on page 28.

Procedure

1. Start Instance Administration Tool. See "Starting Instance Administration Tool" on page 127.
2. Click **Create an instance**.
3. In the **Create or migrate** panel of the **Create new directory server instance** window, complete the following steps to create a proxy server instance:
   a. Click **Create a new directory server instance**.
   b. Click **Set up as proxy**.
4. Click **Next**.

5. In the**Instance details** panel of the **Create new directory server instance** window, specify the following values:
   a. From the **User name** list, select the user name that owns the instance. The instance is assigned the same name as the user name.
   b. If you want to associate a new user account with the instance, click **Create user**. In the **Create new user for directory server instance** window, complete the following steps:
      1) In the **User Name** field, enter the user name.
      2) In the **Password** field, enter a password for the user account.
      3) In the **Confirm password** field, enter the password for the user account.
      4) In the **Home directory** field, enter the home directory to configure for the user account. You can click **Browse** and specify the home directory.
      5) In the **Primary group** field, enter the primary group name of the user.
      6) To create the user account, click **Create**.
   c. To modify an existing user account, select the user name from the **User name** list and click **Edit user**. In the **Edit the user for directory server instance** window, complete the following steps:
      1) The **User Name** field is populated with the user name.
      2) In the **Password** field, enter a password for the user account.
      3) In the **Confirm password** field, enter the password for the user account.
      4) In the **Home directory** field, enter the home directory to configure for the user account. You can click **Browse** and specify the home directory.
      5) In the **Primary group** field, enter the primary group name of the user.
      6) To edit the user account, click **Edit**.
      7) In the **Edit the user for directory server instance** confirmation window, click **Yes**.
6. In the **Instance location** field, enter the location of the proxy server instance. You can click **Browse** and specify the instance home directory. The location must contain at least 30 MB of free disk space. On Windows systems, the location is a disk drive, such as `C:`. The directory instance files are stored in the `\idsslapd-`*`instance_name`* directory on the disk drive you specify. The *instance_name* variable is the name of the proxy server instance. On AIX, Linux, and Solaris systems, the home directory of the proxy server instance owner is the default instance location, but you can specify a different path.
7. In the **Encryption seed string** field, enter the encryption seed for the instance.

   Remember: You must remember the encryption seed of the instance, since it might be required for other configuration tasks.
   The encryption seed must contain only printable `ISO-8859-1 ASCII` characters with values in the range of 33 to 126. The encryption seed must contain a minimum of 12 and a maximum of 1016 characters. For information about the characters to use, see “ASCII characters from 33 to 126” on page 125. The directory server uses the encryption seed to generate a set of Advanced Encryption Standard (AES) secret key values. The key stash file of a directory server instance store the key values, and are used to encrypt and decrypt password and attributes.
8. In the **Confirm encryption seed** field, enter the encryption seed for the instance.

9. If you want to provide an encryption salt value, click **Use encryption salt value**.
   a. In the **Encryption salt string** field, enter an encryption salt value for the instance. The encryption salt must contain only printable `ISO-8859-1 ASCII` characters with values in the range of 33 to 126. The encryption salt must contain 12 characters. For information about the characters to use, see "ASCII characters from 33 to 126" on page 125.
   b. In the **Confirm encryption salt** field, enter the encryption salt value for the instance.
10. Optional: In the **Instance description** field, a description of the instance. The description helps in identifying the instance.
11. Click **Next**.
12. In the **TCP/IP settings for multihomed hosts** panel, select one of the following options:
    - If you want the instance to listen on all IP addresses, select **Listen on all configured IP addresses**.
    - If you want the instance to listen on a particular set of IP addresses that are configured on the computer, complete the following steps:
      a. Clear **Listen on all configured IP addresses**.
      b. From the **Select the specific IP addresses to listen on** list, select the IP address or addresses that you want the instance to listen on.
13. Click **Next**.
14. In the **TCP/IP port settings** panel, specify the following values:

    Note: You must assign a unique port numbers to the directory server ports and must not conflict with existing ports that are in use on the computer. ON AIX, Linux, and Solaris systems, port numbers in the range of 1 - 1000 can be used only by root.
    a. In the **Server port** field, enter the port number that you want the server to use as its unsecured port. The number must be in range of 1 - 65535.
    b. In the **Server secure port** field, enter the port number that you want the server to use as its secured port. The number must be in the range of 1 - 65535.
    c. In the **Administration server port** field, enter the port number that you want the administration server to use as its unsecured port. The number must be in the range of 1 - 65535.
    d. In the **Administration server secure port** field, enter the port number that you want the administration server to use as its secured port. The number must be in the range of 1 - 65535.
    e. Click **Next**.
15. In the **Optional steps** panel, complete the following steps:
    a. To configure the administrator DN and password for the instance, select **Configure administrator DN and password**. You must set the administrator DN and password for a proxy server instance.
    b. Click **Next**.
16. In the **Configure administrator DN and password** panel, complete the following steps:
    a. In the **Administrator DN** field, enter a valid DN or accept the default DN, `cn=root`. The administrator DN value is not case-sensitive. The administrator DN user has full access to all data in the instance.

b. In the **Administrator Password** field, enter the password for the administrator DN. Passwords are case-sensitive. Double byte character set (DBCS) characters in the password are not valid.
c. In the **Confirm password** field, enter the password for the administrator DN. You must remember the password for future reference.
d. Click **Next**.

17. In the **Verify settings** panel, verify the summary that is generated.
18. To start the proxy server instance creation, click **Finish**.
19. In the **Results** window, verify the log messages that are generated for the instance creation operations.
20. To close the **Results** window, click **Close**.
21. To close Instance Administration Tool, click **Close**.

Results

Instance Administration Tool creates a proxy server instance on the computer.

What to do next

You must start the administration server and the`ibmslapd` process in configuration only mode and configure back-end servers. See the *Administration Guide*.

Creating an instance with the command-line utility

Use the command-line utility, **`idsicrt`**, to create an instance.

Before you begin

To create an instance with the command-line utility, you must meet the following conditions:

1. Install IBM Security Directory Server with the Server, Proxy Server, or both features. See "Installing with IBM Installation Manager" on page 28.
2. A system user ID must exist that must own the instance. For more information about creating a system user ID, see "Users and groups that are associated with a directory server instance" on page 117.

About this task

When the **`idsicrt`** command is run, the command creates an instance and a DB2 database instance for the full directory server instance.

Procedure

1. Log in as root user on AIX, Linux, or Solaris, and as an administrator member on Windows.
2. Change the current working directory to the `sbin` subdirectory in the IBM Security Directory Server installation location.
3. To create an instance, run the following command: Substitute the *instance_name* variable with the name of a valid system user ID.

Task to complete	Command to run:
Create a directory server instance	`idsicrt -I instance_name -e mysecretkey! -l instance_home`

Task to complete	Command to run:
Create a proxy server instance	`idsicrt -I instance_name -e mysecretkey! -l instance_home -x`

For more information about the **idsicrt** command, see *Command Reference*.

Examples

Example 1:

To create a directory server instance with the following values on AIX, Linux, or Solaris, run the following command:

- Instance name: `myinst`
- Unsecured port: `389`
- Secured port: `636`
- Encryption seed: `mysecretkey!`
- Encryption salt: `mysecretsalt`
- Instance home: `/home/myinst` on AIX and Linux, and `/export/home/myinst` on Solaris

```
idsicrt -I myinst -p 389 -s 636 -e mysecretkey!\
-g mysecretsalt -l /home/myinst
```

To create a directory server instance with the following values on Windows, run the following command:

- Instance name: `myinst`
- Unsecured port: `389`
- Secured port: `636`
- Encryption seed: `mysecretkey!`
- Encryption salt: `mysecretsalt`
- Instance home: `C:`

```
idsicrt -I myinst -p 389 -s 636 -e mysecretkey!
-g mysecretsalt -l C:
```

Example 2:

To create a proxy server instance with the following values on AIX, Linux, or Solaris, run the following command:

- Instance name: `myproxy`
- Unsecured port: `389`
- Secured port: `636`
- Encryption seed: `mysecretkey!`
- Encryption salt: `mysecretsalt`
- Instance home: `/home/myproxy` on AIX and Linux, and `/export/home/myproxy` on Solaris

```
idsicrt -I myproxy -p 389 -s 636 -e mysecretkey!\
-g mysecretsalt -l /home/myproxy -x
```

To create a proxy server instance with the following values on Windows, run the following command:

- Instance name: `myproxy`
- Unsecured port: `389`
- Secured port: `636`
- Encryption seed: `mysecretkey!`
- Encryption salt: `mysecretsalt`

- Instance home: `C:`

```
idsicrt -I myproxy -p 389 -s 636 -e mysecretkey!
-g mysecretsalt -l C: -x
```

What to do next

Complete the following configuration to create a functional instance:

1. Configure a DB2 database instance for a full directory server instance.
2. Configure the administrator DN and password for the instance.
3. Configure the suffixes for the instance.

Upgrading an instance of a previous version with Instance Administration Tool

Use Instance Administration Tool to upgrade a directory server instance or a proxy server instance of a previous version to version 6.3.1.

Before you begin

You must complete the following tasks before you upgrade an instance with Instance Administration Tool:

- Complete IBM Security Directory Server, version 6.3.1 installation. See, "Starting the installation" on page 26.
- Set up the environment before you upgrade an instance. See, "Setting the environment before you upgrade an instance" on page 88.
- Log in as a root user on AIX, Linux, or Solaris operating system, and as a member of the Administrator group on the Windows operating system.

About this task

After you upgrade an instance of a previous version, the instance is converted to a fully functional instance of IBM Security Directory Server, version 6.3.1.

Procedure

1. Access the command prompt.
2. Change the current working directory to `sbin`. The following location is the default on various operating systems:

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

   AIX and Solaris
   `/opt/IBM/ldap/V6.3.1/sbin`

   Linux `/opt/ibm/ldap/V6.3.1/sbin`
3. To start Instance Administration Tool, run the following command:

   Note: On Windows system, you can start from the **Start** menu. Click **Start** > **All Programs** > **IBM Security Directory Server 6.3.1** > **Instance Administration Tool**.

   ```
   idsxinst
   ```
4. Select a previous version of an instance that you want to upgrade.
5. Click **Migrate**.
6. In the **Migrate directory server instance** window, click **Migrate**.

7. When Instance Administration Tool prompts after it completes the upgrade operation, click **OK**.
8. Verify the summary information.
9. To close the **Migrate directory server instance** window, click **Close**.
10. Take offline backup of the instance. For more information, see "Directory server backup" on page 180.
11. To close Instance Administration Tool, click **Close**.

Results

Instance Administration Tool upgrade a previous version of directory server instance to 6.3.1.

What to do next

You must start the `ibmslapd` process and the administration server that is associated with the directory server instance. See "Start or stop a directory server and an administration server" on page 151.

Upgrading a remote instance of a previous version with Instance Administration Tool

Use Instance Administration Tool to upgrade a remote directory server instance or proxy server instance of a previous version to version 6.3.1.

Before you begin

You must complete the following tasks before you upgrade an instance with Instance Administration Tool:

- Set up the environment before you upgrade an instance. See, "Setting the environment before you upgrade an instance" on page 88.
- Log in as a root user on AIX, Linux, or Solaris operating system, and as a member of the Administrator group on the Windows operating system.

About this task

After you complete the upgrade process, Instance Administration Tool creates an instance of 6.3.1 on the computer with the remote instance information.

Procedure

1. Back up the database of a directory server instance that is on a remote computer with the **idsdb2ldif** command.

   Important: If you are upgrading a proxy server instance, do not back up database. Proxy server does not contain a database that is associated with it.

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

   For more information about the **idsdb2ldif** command, see the *Command Reference*.
2. Complete IBM Security Directory Server, version 6.3.1 installation on a computer on which you want to upgrade the remote instance. See, "Starting the installation" on page 26.
3. To back up the schema and configuration files of the remote instance, run the **migbkup** command of the version 6.3.1 to which you want to upgrade:

Operating system	Command to run:
Microsoft Windows	**migbkup.bat** drive_name\idsslapd-instance_name backup_directory
AIX, Linux, and Solaris	**migbkup** user_home_dir/idsslapd-instance_name backup_directory

The **migbkup** command is in the `tools` subdirectory of the IBM Security Directory Server installation media.

4. Copy the backup directory, `backup_directory`, which you created with **migbkup**, from the remote computer to the computer with IBM Security Directory Server, version 6.3.1.
5. Optional: Copy the database backup file, `inst_out.ldif`, from the remote computer to the computer with IBM Security Directory Server, version 6.3.1.
6. Start Instance Administration Tool. See "Starting Instance Administration Tool" on page 127.
7. Click **Create an instance**.
8. On the **Create or migrate** panel, complete the following tasks:
   a. Click **Migrate from a previous version of directory server**.
   b. In the **Enter path of the backed up files** field, enter the path where you copied the backup of the remote instance configuration and schema files. You can click **Browse** and specify the backup location.
   c. Click **Next**.
9. On the **Instance details** panel of the **Create new directory server instance** window, specify the following values:

   Note: If you are upgrading an instance, you cannot edit an existing user information.

   a. From the **User name** list, select the user name that must own the directory server instance. The directory server instance is assigned the same name as the user name.
   b. If you want to associate a new user account with the instance, click **Create user**. In the **Create new user for directory server instance** window, complete the following steps:
      1) In the **User Name** field, enter the user name.
      2) In the **Password** field, enter a password for the user account.
      3) In the **Confirm password** field, enter the password for the user account.
      4) In the **Home directory** field, enter the home directory to configure for the user account. You can click **Browse** and specify the home directory.
      5) In the **Primary group** field, enter the primary group name of the user.
      6) To create the user account, click **Create**.
10. In the **Instance location** field, enter the location of the directory server instance. You can click **Browse** and specify the instance home directory. The location must contain at least 30 MB of free disk space. On Windows systems, the location is a disk drive, such as `C:`. The directory instance files are stored in the `\idsslapd-`*`instance_name`* directory on the disk drive you specify. The *instance_name* variable is the name of the directory server instance. On AIX, Linux, and Solaris systems, the home directory of the directory server instance owner is the default instance, but you can specify a different path.
11. Optional: In the **Instance description** field, a description of the directory server instance. The description helps in identifying the instance.

12. Click **Next**.
13. If you are upgrading a remote directory server instance with the DB2 database details, click **Next** on the **DB2 instance details** panel. If the backup files are of a remote proxy server instance, the **DB2 instance details** panel might not be displayed.
14. In the **TCP/IP settings for multihomed hosts** panel, select one of the following options:
    - If you want the directory server instance to listen on all IP addresses, select **Listen on all configured IP addresses**.
    - If you want the directory server instance to listen on a particular set of IP addresses that are configured on the computer, clear **Listen on all configured IP addresses**. Select the IP address or addresses in the list that you want the directory server instance to listen on.
15. Click **Next**.
16. In the **TCP/IP port settings** panel, specify the following values:

    Note: You must assign a unique port numbers to the directory server ports and must not conflict with existing ports that are in use on the computer. ON AIX, Linux, and Solaris systems, port numbers in the range of 1 - 1000 can be used only by root.
    a. In the **Server port** field, enter the port number that you want the server to use as its unsecured port. The number must be in range of 1 - 65535.
    b. In the **Server secure port** field, enter the port number that you want the server to use as its secured port. The number must be in the range of 1 - 65535.
    c. In the **Administration server port** field, enter the port number that you want the administration server to use as its unsecured port. The number must be in the range of 1 - 65535.
    d. In the **Administration server secure port** field, enter the port number that you want the administration server to use as its secured port. The number must be in the range of 1 - 65535.
    e. Click **Next**.
17. In the **Verify settings** panel, verify the summary that is generated.
18. To start the directory server instance creation with the backed up configuration and schema files, click **Finish**.
19. In the **Results** window, verify the log messages that are generated for the instance creation operations.
20. To close the **Results** window, click **Close**.
21. To close Instance Administration Tool, click **Close**.

Results

Instance Administration Tool creates a directory server instance on the computer.

What to do next

You must start the `ibmslapd` process and the administration server that is associated with the directory server instance. See “Starting or stopping a directory server and an administration server” on page 151.

Take backup of the instance. For information about backing up a directory server instance, see “Directory server backup” on page 180.

Instance creation from an existing instance

You can use Instance Administration Tool to create a directory server instance from an existing instance that is on a local computer or a remote computer. The source directory server serves as a template for the target directory server instance.

IBM Security Directory Server Instance Administration Tool supports copying of a source directory server instance only if the tool and instance and of same version. The target directory server is created on the computer on which Instance Administration Tool is run. If the source directory server is on a different computer, the operating systems of the two computers can be different. For example, you can create a directory server instance on a Windows system that is a copy of an instance on a Linux system.

When you use the tool to copy a source instance, the tool can do the following operations that are based on your input:

- You can create a target directory server with the same configuration settings and schema files of the source directory server instance. It also synchronizes directory key stash files on the target server from the source server.
- If the source directory server instance is a full directory server, the target directory server instance that is created is also a full directory server. You can choose to copy the data from the existing directory server instance. If the source directory server is configured for online backup, you can create a functional target directory server with entries in its database.
- If the source directory server instance is a proxy server, the target directory server instance that is created is also a proxy server.
- If the source directory server is in a replication environment, you can configure the target instance as a replica server or as a peer server to the source server.
- If the source directory server is in a distributed environment, you can configure the target directory server instance as a proxy server.
- If the source directory server instance is configured for secure communication, Instance Administration Tool copies the key database files to the target directory server.

You must ensure that the source directory server meets the following conditions before you create a directory server from the source directory server:

- The source directory server must be of IBM Security Directory Server, version 6.3.1. The source directory server cannot be of an instance of previous version.
- The source directory server must be running in the normal mode. Copying of an instance that is running in the configuration mode is not supported.
- The source directory server must be accessible from the computer on which you are running Instance Administration Tool.
- To create the target directory server as a replica or peer, a replication context must exist on the source directory server instance. You cannot use Instance Administration Tool to set up the first replica or peer in a replication topology. The source directory server instance must contain at least one replication context, replication group, and replication subentry defined. If you want to configure the instance as a replica, the source instance must contain the initial replication topology, including an agreement to at least one other server. If you want to configure the instance as a peer, the source server must be defined as a master for one or more of the subentries in the replication configuration.

- If you want to create the instance as a peer or a replica, a new replication subentry is created under the `ibm-replicaGroup=default,`*`replicationContext`* DN. If the DN is not present, the instance cannot be copied.

If you want to copy data from the source directory server instance to the target directory server instance, you must meet the following requirements:

- The DB2 version can be different for both directory server instances. A database backup on an operating system can be restored on any computer with the same operating system type. For example, you can restore a database that is created on DB2 UDB version 9 on Windows systems to a system with DB2, version 10. On AIX, Linux, and Solaris systems, you can restore backups that were produced on DB2 UDB, version 9 to DB2, version 10 if the endianness (big endian or little endian) of the backup and restore operating systems are same.
- You must configure the source directory server instance for online backup. You can configure online backup during initial database configuration. You can use Instance Administration Tool or Configuration Tool to configure online backup.
- You must take an initial offline backup of the source directory server instance before you use Instance Administration Tool to copy the directory server instance. The path that you specify for backup must contain only one backup image.
- The path with the backup image must be accessible to both the source directory server instance and the target directory server instance.

Creating a copy of an existing instance with Instance Administration Tool

Use Instance Administration Tool to create a copy of an existing instance.

Before you begin

To create a copy of an existing instance, you must meet the following requirements:

- Start the `ibmslapd` process and administration server of the instance in normal mode.
- Ensure that the source directory server is accessible from Instance Administration Tool.

Procedure

1. Start Instance Administration Tool. See "Starting Instance Administration Tool" on page 127.
2. Choose one of the following options to create a copy of an existing instance:
   - To create a copy of an existing instance that is on the local computer, click **Copy local instance**.
   - To create a copy of an existing instance that is on a remote computer, click **Copy remote instance**.
3. On the **Copy directory server instance** panel, provide the following values:
   a. In the **Host** field, enter the IP address or the host name if the source directory server is on a remote computer. If the source directory server is on a local computer, the field is populated with `localhost` and you cannot edit it.

b. In the **Port** field, enter the port number of the directory server if the port number in the field is not valid. If you want to use secure connection, you must specify the secured port number of the source directory server instance.

c. In the **Administrator DN** field, enter the administrator DN of the source directory server if the instance is on a remote computer. If the source directory server is on a local computer, the field is populated with the administrator DN value and you cannot edit it.

d. In the **Password** field, enter the password of the administrator DN.

e. In the **Encryption seed** field, enter the encryption seed for the source directory server instance.

f. If the source directory server is configured for secure communications and you want to configure the target directory server with it, click **Use SSL connection**.

   1) In the **Key file** field, enter the file name with path of the key database file. You can click **Browse** and specify the location.

   2) In the **Key name** field, enter the private key name to use from the key file of the source directory server.

   3) In the **Key password** field, enter the key database password of the key file.

g. Click **Next**.

4. In the **Instance setup - step 1** panel, complete the following steps:

   a. Verify the **Source URL** and **Source instance type** fields for information about source directory server. The **Source instance type** can be a full directory server or a proxy server instance.

   b. To configure the target directory server as a peer or a replica in an existing replication topology, select **Configure as Peer or Replica server** and select one of the following options:

      - To configure the target directory server as a replica, click **Replica**.
      - To configure the target directory server as a peer, click **Peer**.

   c. In the **User name** field, enter the system user ID that must own the target directory server instance. The name cannot be longer than 8 characters. The same name is also set for the directory server instance name, DB2 administrator ID, database instance name, and database name. The user ID must exist on the computer and must not be associated with any other directory server instance on the computer. See "Users and groups that are associated with a directory server instance" on page 117 for detailed information about the user ID.

   d. In the **Password** field, enter the password for the user ID.

   e. In the **Instance location** field, enter the location of the directory server instance. You can click **Browse** and specify the instance home directory. The location must contain at least 30 MB of free disk space. On Windows systems, the location is a disk drive, such as `C:`. The directory instance files are stored in the `\idsslapd-`*`instance_name`* directory on the disk drive you specify. The *instance_name* variable is the name of the directory server instance. On AIX, Linux, and Solaris systems, the home directory of the directory server instance owner is the default instance, but you can specify a different path.

   f. Click **Next**.

5. In the **Instance setup - step 2** panel, complete the following steps:

a. In the **Administrator DN** field, enter a valid DN for the target directory server instance. The administrator DN value is not case-sensitive. The administrator DN user has full access to all data in the directory server instance.
b. In the **Password** field, enter the password for the administrator DN. Passwords are case-sensitive. Double byte character set (DBCS) characters in the password are not valid.
c. In the **Confirm password** field, enter the password for the administrator DN. You must remember the password for future reference.
d. To copy data from the database of the source server to the target server, select **Copy data from source instance to new instance** and complete the following steps:

   Note: If selected to create the target directory server as a peer or a replica, this check box is selected and you cannot clear it.

   1) In the **Path for backup images** field, enter the path name of the backup image of the source server. You can click **Browse** to specify the location. If the source instance is on a remote computer, the backup path must be a shared and must be accessible from both the source and target computers. An example of shared path is a read/write NFS file system.

e. Click **Next**.

6. In the **Verify settings** panel, verify the summary that is generated.
7. To start the creation of copy of the source directory servers, click **Finish**.
8. In the **Results** window, verify the log messages that are generated for the instance creation operations.
9. To close the **Results** window, click **Close**.
10. To close Instance Administration Tool, click **Close**.

Results

Instance Administration Tool creates a copy of the source directory server instance on the computer.

What to do next

You must start the `ibmslapd` process and the administration server that is associated with the directory server instance. See “Starting or stopping a directory server and an administration server” on page 151.

Take backup of the instance. For information about backing up a directory server instance, see “Directory server backup” on page 180.

Creating a copy of an existing instance with the command-line utility

Use the command-line utility, **`idsideploy`** , to create a copy of an instance.

Before you begin

To create a copy of an existing instance, you must meet the following requirements:

- Start the ibmslapd process and administration server of the source instance in normal mode. See "Starting or stopping a directory server and an administration server with command-line utilities" on page 152.
- Ensure that the source directory server is accessible from the computer on which you want to create the instance copy.

Procedure

1. Log in as root user on AIX, Linux, or Solaris, and as an administrator member on Windows.
2. Change the current working directory to the sbin subdirectory in the IBM Security Directory Server installation location.
3. To create an instance copy without the data from an existing directory server instance, run the following command:

```
idsideploy -sU ldap://host:port -sD src_adminDN -sw src_adminPWD
-e encryptionseed -I instance_name -a instPWD -D adminDN
-w adminPWD -l inst_location
```

   For more information about the **idsideploy** command, see *Command Reference*.

Start or stop a directory server and an administration server

To use a directory server instance, you must start the ibmslapd process and the administration server that is associated with the instance.

If you modify the configuration of a directory server, you might require to stop and start the server and the administration server to apply the changes. You can stop the directory server and the administration server only if it is running in normal or configuration mode.

You can use Instance Administration Server or server utilities, such as **ibmslapd** and **ibmdiradm**, to start and stop the servers. The ibmslapd process is associated with the directory server. You can start the directory server instance only in normal mode with Instance Administration Tool. To start a directory server in configuration only mode, use the command-line options.

A directory server can be in one of the following states:

- Started
- Stopped
- Started (Config only)

An administration server can be in one of the following states:

- Started
- Stopped

Starting or stopping a directory server and an administration server

Use Instance Administration Tool to start or stop the directory server, administration server, or both that are associated with an instance.

Before you begin

To start or stop a directory server and administration server of an instance, you must meet the following conditions:

1. An instance with the same version of Instance Administration Tool must exist.
2. If an instance does not exist, create an instance. See "Creating the default directory server instance" on page 130 or "Creating a directory server instance with custom settings" on page 132.

Procedure

1. Start Instance Administration Tool. See "Starting Instance Administration Tool" on page 127.
2. From the **List of directory server instances installed on the system** list, select an instance with the same version of Instance Administration Tool.
3. To start or stop directory server, administration server, or both, click **Start/Stop**.
4. In the **Manage server state** window, take the following actions:
   - To start the directory server, administration server, or both of an instance, complete the following steps:
     - To start the directory server, click **Start server**.
     - To start the administration server, click **Start administration server**.
     - Click **OK**.
   - To stop the directory server, administration server, or both, complete the following steps:
     - To stop the directory server, click **Stop server**.
     - To stop the administration server, click **Stop administration server**.
     - Click **OK**.
5. To close the **Manage server state** window, click **Close**.
6. To close Instance Administration Tool, click **Close**.

Starting or stopping a directory server and an administration server with command-line utilities

Use command-line utilities to start or stop the directory server, administration server, or both that are associated with an instance.

Before you begin

To start or stop a directory server and administration server of an instance, you must meet the following conditions:

- An instance with the same version of command-line utilities must exist. If an instance does not exist, create an instance. See "Creating the default directory server instance" on page 130 or "Creating a directory server instance with custom settings" on page 132.

Procedure

1. Log in the computer with the required permission. See Chapter 19, "Instance configuration," on page 161.
2. Access the command prompt.
3. Change the current working directory to the `sbin` subdirectory in the IBM Security Directory Server installation location.
4. To start the server and the administration server of an instance, *instance_name*, run the following commands: Substitute the `instance_name` value with your instance name.

   ```
   ibmslapd -I instance_name
   ibmdiradm -I instance_name
   ```

5. To stop the server and the administration server of an instance, run the following commands: Substitute the `instance_name` value with your instance name.

```
ibmslapd -I instance_name -k
ibmdiradm -I instance_name -k
```

Management of a directory server instance configuration

You can use Configuration Tool to verify status, manage, and modify the configuration of a directory server instance or a proxy server instance.

You can use Configuration Tool to manage and modify configuration of a directory server instance or a proxy server instance that is of same version. You cannot use Configuration Tool that is provided with a IBM Security Directory Server version to manage directory server instance or a proxy server instance of a previous or later version.

You can open Configuration Tool for an instance with one of the following options:

- Use Instance Administration tool.
- Run the **idsxcfg** command with the instance name as the parameter value.

For more information about Configuration Tool, see Chapter 19, “Instance configuration,” on page 161.

Opening Configuration Tool from Instance Administration Tool

Open IBM Security Directory Server Configuration Tool to manage or modify configuration of a directory server instance or a proxy server instance.

Before you begin

To manage an instance with Configuration Tool, you must meet the following conditions:

- An instance with the same version of Configuration Tool must exist. If an instance does not exist, create an instance. See “Creating the default directory server instance” on page 130 or “Creating a directory server instance with custom settings” on page 132.

Procedure

1. Start Instance Administration Tool. See “Starting Instance Administration Tool” on page 127.
2. From the **List of directory server instances installed on the system** list, select an instance with the same version of Instance Administration Tool.
3. To manage the instance with Configuration Tool, click **Manage**. The IBM Security Directory Server Configuration Tool window opens for the instance.
4. To close Configuration Tool, click **File** > **Exit**.
5. In the Configuration Tool confirmation window, click **Yes**.

Modify the TCP/IP settings of an instance

You can use Instance Administration Tool or command-line utilities to modify the TCP/IP settings of a directory server instance or a proxy server instance.

To modify TCP/IP settings of an instance, the version of the instance and Instance Administration Tool must be the same.

Modifying the TCP/IP settings of an instance with Instance Administration Tool

Use Instance Administration Tool to modify the TCP/IP settings for an existing instance.

Before you begin

To modify the TCP/IP settings of an instance with Instance Administration Tool, you must meet the following conditions:

1. An instance with the same version of Instance Administration Tool must exist.
2. Stop the directory server and the administration server of the instance. See "Starting or stopping a directory server and an administration server" on page 151.

Procedure

1. Start Instance Administration Tool. See "Starting Instance Administration Tool" on page 127.
2. From the **List of directory server instances installed on the system** list, select an instance with the same version of Instance Administration Tool.
3. To modify the TCP/IP settings of the instance, click **Edit TCP/IP settings**. The **Edit TCP/IP settings** window opens for the instance.
4. In the **Edit TCP/IP settings** window, select one of the following options:
   - If you want the instance to listen on all configured IP addresses of the computer, select **Listen on all configured IP addresses**.
   - If you want the instance to listen on a particular set of IP addresses that are configured on the computer, complete the following steps:
     a. Clear **Listen on all configured IP addresses**.
     b. From the **Select the specific IP addresses to listen on** list, select the IP address or addresses that you want the instance to listen on.
5. Click **Next**.
6. In the **Port details** panel, specify the following values:

   Note: You must assign a unique port numbers to the directory server ports and must not conflict with existing ports that are in use on the computer. ON AIX, Linux, and Solaris systems, port numbers in the range of 1 - 1000 can be used only by root.

   a. In the **Server port** field, enter the port number that you want the server to use as its unsecured port. The number must be in range of 1 - 65535.
   b. In the **Server secure port** field, enter the port number that you want the server to use as its secured port. The number must be in the range of 1 - 65535.
   c. In the **Administration server port** field, enter the port number that you want the administration server to use as its unsecured port. The number must be in the range of 1 - 65535.
   d. In the **Administration server secure port** field, enter the port number that you want the administration server to use as its secured port. The number must be in the range of 1 - 65535.
   e. Click **Finish**.

7. In the **Edit TCP/IP results** window, verify the log messages that are generated for the edit TCP/IP settings operation.
8. To close the **Edit TCP/IP results** window, click **Close**.
9. To close Instance Administration Tool, click **Close**.

Modifying the TCP/IP settings of an instance with command-line utilities

Use the **idssethost** and **idssetport** commands to modify the TCP/IP and port settings for an existing instance.

Before you begin

To modify the TCP/IP settings of an instance with command-line utilities, you must meet the following conditions:

1. An instance with the same version of command-line utilities must exist.
2. Stop the directory server and the administration server of the instance. See "Starting or stopping a directory server and an administration server with command-line utilities" on page 152.

Procedure

1. Log in as root user on AIX, Linux, or Solaris, and as an administrator member on Windows.
2. Change the current working directory to the `sbin` subdirectory in the IBM Security Directory Server installation location.
3. To update the IP addresses of the directory server, *instance_name*, choose one of the following options: Substitute the *instance_name* variable with your instance name.

IP address to bind	Command to run:
A specific IP address, xx.xx.xx.xx, on the computer	`idssethost -I instance_name -i xx.xx.xx.xx`
All IP addresses configured on the computer	`idssethost -I instance_name -i all`

4. To update the ports numbers of the directory server, *instance_name*, run the following command: Substitute the *instance_name* variable with your instance name.

   Note: You must assign a unique port numbers to the directory server ports and must not conflict with existing ports that are in use on the computer. ON AIX, Linux, and Solaris systems, port numbers in the range of 1 - 1000 can be used only by root.

Ports to configure	Command to run:
Server port	`idssetport -I instance_name -p port_no`
Server secure port	`idssetport -I instance_name -s secure_port`
Administration server port	`idssetport -I instance_name -a adm_port`
Administration server secure port	`idssetport -I instance_name -c adm_secure_port`

For more information about the **idssethost** and **idssetport** commands, see *Command Reference*.

5. Start the directory server and the administration server. See "Starting or stopping a directory server and an administration server with command-line utilities" on page 152.

View information about an instance

You can use Instance Administration Tool or the command-line utility to view instance details, such as instance home directory, IP addresses, and ports.

You can view information about all existing instances on the computer. The instance status can be in the stopped or started state.

The **idsilist** command also provides similar information for an instance or all available instances on the computer. For more information about the **idsilist** command, see *Command Reference*.

Viewing information about an instance with Instance Administration Tool

Use Instance Administration Tool to view details of an existing instance.

Procedure

1. Start Instance Administration Tool. See "Starting Instance Administration Tool" on page 127.
2. From the **List of directory server instances installed on the system** list, select an instance for which you want to view details.
3. Click **View**. The **View instance details** window with general and TCP/IP details for the selected instance is displayed.
4. To close the **View instance details** window, click **Close**.
5. To close Instance Administration Tool, click **Close**.

Viewing information about an instance with the command-line utility

Use the **idsilist** command to view information about an existing instance.

Procedure

1. Log in as root user on AIX, Linux, or Solaris, and as an administrator member on Windows.
2. Change the current working directory to the `sbin` subdirectory in the IBM Security Directory Server installation location.
3. To view information about the instances on a computer, run the appropriate **idsilist** command:

Task to complete	Command to run:
List all instances	`idsilist`
List all instances with complete information and description	`idsilist -a`
List all instances with complete information raw format	`idsilist -r`
List a specific instance	`idsilist -I` *instance_name*

Task to complete	Command to run:
List a specific instance with complete information and description	`idsilist -I instance_name -a`
List a specific instance with complete information in raw format	`idsilist -I instance_name -r`

For more information about the **idsilist** command, see *Command Reference*.

Directory server instance deletion

You can use Instance Administration Tool or the command-line utility to delete a directory server instance or a proxy server instance.

You might require to delete an instance from a computer, if you migrated an instance to another computer or you no longer require the instance.

If you are deleting a directory server with DB2 database, it is advisable to take backup before you delete the instance. If you are deleting a proxy server instance, it is advisable you take backup the instance.

Note: For a proxy server instance, the instance deletion is the only valid option.

With Instance Administration Tool, you can choose the following options:

- Delete a directory server instance and keep the database instance
- Delete a directory server instance and remove the associated DB2 database instance

With the **idsidrop** command, you can choose the following options:

- Delete a directory server instance and keep the database instance
- Delete a directory server instance and remove the associated DB2 database instance
- Unconfigure the directory server instance from the DB2 database instance, and do not delete the directory server instance

For more information about the **idsidrop** command, see *Command Reference*.

Deleting an instance with Instance Administration Tool

Use Instance Administration Tool to delete a directory server instance or a proxy server instance.

Before you begin

To modify the TCP/IP settings of an instance with Instance Administration Tool, you must meet the following conditions:

1. An instance with the same version of Instance Administration Tool must exist.
2. Stop the directory server and the administration server of the instance. See "Starting or stopping a directory server and an administration server" on page 151.

Procedure

1. Start Instance Administration Tool. See "Starting Instance Administration Tool" on page 127.

2. From the **List of directory server instances installed on the system** list, select an instance with the same version of Instance Administration Tool.
3. To start the deletion operation, click **Delete**.
4. In the **Delete directory server instance** window, complete the following steps:
   a. Choose one of the following deletion methods:
      - To remove the directory server instance without removing the associated DB2 database instance, click **Delete directory server instance only**.

        Note: For a proxy server instance, **Delete directory server instance only** is the only valid option available.
      - To remove the directory server instance with the associated DB2 database instance, click **Delete directory server instance and destroy associated database instance**.
   b. Click **Delete**.
   c. In the **Warning** window, click **Yes** to confirm the instance deletion.
   d. In the **Information** window, click **OK**.
   e. To close the **Delete directory server instance** window, click **Close**.
   f. To close Instance Administration Tool, click **Close**.

Deleting an instance with the command-line utility

Use the **idsidrop** command to delete an existing instance.

Before you begin

To delete an instance with the command-line utility, you must meet the following conditions:

1. An instance with the same version of the command-line utility must exist.
2. Stop the directory server and the administration server of the instance. See "Starting or stopping a directory server and an administration server with command-line utilities" on page 152.

Procedure

1. Log in as root user on AIX, Linux, or Solaris, and as an administrator member on Windows.
2. Change the current working directory to the `sbin` subdirectory in the IBM Security Directory Server installation location.
3. To delete an instance, *instance_name*, choose one of the following options: Substitute the *instance_name* variable with your instance name.

Task to complete	Command to run:
To delete a directory server instance and to retain the associated database instance	`idsidrop -I instance_name`
To delete a directory server instance and to delete the associated database instance	`idsidrop -I instance_name -r`
To unconfigure the associated database instance without deleting the directory server instance	`idsidrop -I instance_name -R`

For more information about the **idsidrop** command, see *Command Reference*.

Chapter 18. Directory structure verification

You must verify directory structure after you install IBM Security Directory Server.

Windows 32-bit and 64-bit systems

After you install IBM Security Directory Server on the Windows operating system, you can see the following directories and files in the installation location, for example: `C:\Program Files\IBM\LDAP\V6.3.1` (you can change the installation location)

appsrv
etc
java
lib
messages
bin
examples
javalib
lib64
nls
var
codeset
idstools
jre
license
properties
config
include
ldapcfg.ico
logs
sbin

Linux 64-bit systems

After you install IBM Security Directory Server on the Linux operating system, you can see the following directories and files in the installation location, for example: `/opt/ibm/ldap/V6.3.1` (you cannot change the installation location)

bin
codeset
config
etc
examples
idstools
include
javalib
LAPID
lib
lib64
nls
properties

sbin
tmp
web

Chapter 19. Instance configuration

You can use Configuration Tool or command-line utilities to configure a directory server instance or a proxy server instance as per your requirements.

IBM Security Directory Server Configuration Tool (**idsxcfg**) is a graphical user interface (GUI) that you can use to configure an instance. To use Configuration Tool , IBM Java Development Kit is required.

To start Configuration Tool , you must log in with the following credentials:

AIX, Linux, or Solaris

- Root user
- Directory server instance owner
- User ID that is in the primary group of the directory server instance owner

Windows

- User ID that is in the default administrators group

You can also use Configuration Tool to change your existing directory server configuration.

You can use Configuration Tool for the following tasks on a full directory server instance:

- Start or stop server
- Manage the primary administrator DN and password
- Configure and unconfigure DB2 database for a directory server instance
- Optimize the database that is associated with an instance
- Maintain the DB2 database with DB2 index organization or DB2 row compression
- Backup and restore the database
- Tune directory server instance performance
- Enable and disable the change log
- Add or remove suffixes
- Add or remove schema files
- Import or export LDIF data
- Configure Active Directory synchronization

You can use Configuration Tool for the following tasks on a proxy server instance:

- Start or stop server
- Manage the primary administrator DN and password
- Add or remove suffixes
- Add or remove schema files
- Backup and restore the instance

Starting Configuration Tool

Start IBM Security Directory Server Configuration Tool for an instance to configure the instance as per your directory environment requirements.

Before you begin

To manage an instance with Configuration Tool, you must meet the following conditions:

- An instance with the same version of Configuration Tool must exist. If an instance does not exist, create an instance. See "Creating a directory server instance with custom settings" on page 132 or "Creating a proxy server instance with custom settings" on page 138.
- IBM Java Development Kit must exist in the IBM Security Directory Server installation path. For the default IBM Security Directory Server installation path, see "Default installation locations" on page 25.

Procedure

1. Log in to the computer with the required permissions. See Chapter 19, "Instance configuration," on page 161.
2. Open the command prompt.
3. Change the current directory to the `sbin` sub directory in the IBM Security Directory Server installation location.
4. Run the **idsxcfg** command in the following format: Substitute the *instance_name* variable with your instance name.

   ```
   idsxcfg -I instance_name
   ```

   The IBM Security Directory Server Configuration Tool window opens for the specified instance.
5. To close the Configuration Tool window, click **File** > **Exit**.
6. In the Configuration Tool confirmation window, click **Yes**.

Start or stop a directory server and an administration server with Configuration Tool

You can use Configuration Tool to start the `ibmslapd` process and the administration server that is associated with an instance.

If you modify the configuration of a directory server, you might require to stop and start the server and the administration server to apply the changes. You can stop the directory server and the administration server only if it is running in normal or configuration mode.

You can use Configuration Tool or server utilities, such as **ibmslapd** and **ibmdiradm**, to start and stop the server and administration server. The `ibmslapd` process is associated with the directory server. You can start the directory server instance only in normal mode with Configuration Tool. To start a directory server in configuration only mode, use the command-line options.

A directory server can be in one of the following states:

- Started
- Stopped

- Started (Config only)

An administration server can be in one of the following states:

- Started
- Stopped

Starting or stopping a directory server and an administration server with Configuration Tool

Use Configuration Tool to start or stop the directory server, administration server, or both that are associated with an instance.

Procedure

1. Start Configuration Tool for an instance. See "Starting Configuration Tool" on page 162.
2. From the task list in the left navigational pane, click **Manage server state**.
3. In the **Current State** page, verify the current state of the server and administration server.
4. In the **Current State** page, take the following actions:
   - To start the directory server, administration server, or both of an instance, complete the following steps:
     - To start the directory server, click **Start server**.
     - To start the administration server, click **Start administration server**.
     - In the **Information** window, click **OK**.
   - To stop the directory server, administration server, or both, complete the following steps:
     - To stop the directory server, click **Stop server**.
     - To stop the administration server, click **Stop administration server**.
     - In the **Information** window, click **OK**.
5. To close the **Current State** page, click **Close**.
6. To close the Configuration Tool window, click **File** > **Exit**.
7. In the Configuration Tool confirmation window, click **Yes**.

Starting or stopping a directory server and an administration server with command-line utilities

Use command-line utilities to start or stop the directory server, administration server, or both that are associated with an instance.

Before you begin

To start or stop a directory server and administration server of an instance, you must meet the following conditions:

- An instance with the same version of command-line utilities must exist. If an instance does not exist, create an instance. See "Creating the default directory server instance" on page 130 or "Creating a directory server instance with custom settings" on page 132.

Procedure

1. Log in the computer with the required permission. See Chapter 19, "Instance configuration," on page 161.

2. Access the command prompt.
3. Change the current working directory to the `sbin` subdirectory in the IBM Security Directory Server installation location.
4. To start the server and the administration server of an instance, *instance_name*, run the following commands: Substitute the `instance_name` value with your instance name.

   ```
   ibmslapd -I instance_name
   ibmdiradm -I instance_name
   ```

5. To stop the server and the administration server of an instance, run the following commands: Substitute the `instance_name` value with your instance name.

   ```
   ibmslapd -I instance_name -k
   ibmdiradm -I instance_name -k
   ```

Management of primary administrator DN for an instance

To access configuration and all directory data of an instance, you must create and configure a primary administrator distinguished name (DN) for an instance.

The administrator DN is the DN used by the primary administrator of an instance. You can create only one primary administrator for an instance.

The default DN is `cn=root`. The DN value is not case-sensitive.

A DN contains `attribute:value` pairs, which are separated by commas. An example of a DN value is shown.

```
cn=Ben Gray,ou=dept_audit,o=sample
```

You can use Configuration Tool or the command-line utility, **idsdnpw**, to set or change the primary administrator DN. To set or change the primary administrator DN, you must stop the `ibmslapd` process that is associated with the instance.

Managing the primary administrator DN with Configuration Tool

Use Configuration Tool to configure the primary administrator DN for an instance.

Before you begin

To configure the primary administrator DN for an instance, you must complete the following requirements:

- Stop the directory server. See "Starting or stopping a directory server and an administration server with Configuration Tool" on page 163.

Procedure

1. Start Configuration Tool for an instance. See "Starting Configuration Tool" on page 162.
2. From the task list in the left navigational pane, click **Manage administrator DN**.
3. In the **Administrator DN** field, enter the DN for the primary administrator or accept the default DN, `cn=root`.
4. Click **OK**.
5. To confirm your action, click **OK**.

6. To close the Configuration Tool window, click **File** > **Exit**.
7. To confirm your action, click **Yes**.

What to do next

Start the directory server. See "Starting or stopping a directory server and an administration server with Configuration Tool" on page 163.

Managing the primary administrator DN with the command-line utility

Use the command-line utility, **idsdnpw**, to manage the primary administrator DN for an instance.

Before you begin

To configure the primary administrator DN for an instance, you must complete the following requirements:

- Stop the directory server. See "Starting or stopping a directory server and an administration server with command-line utilities" on page 152.

About this task

If you do not specify the administrator DN value, the default value, `cn=root`, is set in the `ibmslapd.conf` file for the directory server instance. You must specify the primary administrator password for an instance.

If you do not specify the password, the **idsdnpw** command prompts for the password. The password is not shown at the command prompt when you type it.

Procedure

1. Log in as directory server instance owner.
2. Access the command prompt.
3. Change the current working directory to the `sbin` subdirectory in the IBM Security Directory Server installation location.
4. To set the administrator DN for an instance, run the following command: Substitute the `instance_name`, `adminDN`, and `adminPWD` values as per your requirements.

   ```
   idsdnpw -I instance_name -u adminDN -p adminPWD
   ```

   For more information about the **idsdnpw** command, see *Command Reference*.

What to do next

Start the directory server. See "Starting or stopping a directory server and an administration server with command-line utilities" on page 152.

Management of primary administrator password for an instance

To authenticate against an instance and to access configuration and all directory data, you must create and configure a primary administrator password for an instance.

The administrator password is case-sensitive. You must not use Double byte character set (DBCS) characters in the password since it is not supported. You must save the administrator password for future reference.

You can use Configuration Tool or the command-line utility, **idsdnpw**, to configure the primary administrator password. To configure the administrator password, you must stop the `ibmslapd` process that is associated with the instance.

If you enable the administration password policy, the primary administrator password must conform to the administration password policy requirements. For information about the password policy, see *Administration Guide*.

Managing the primary administrator password with Configuration Tool

Use Configuration Tool to configure the password for primary administrator of an instance.

Before you begin

To configure password for the primary administrator DN of an instance, you must complete the following requirements:

- Stop the directory server. See "Starting or stopping a directory server and an administration server with Configuration Tool" on page 163.

Procedure

1. Start Configuration Tool for an instance. See "Starting Configuration Tool" on page 162.
2. From the task list in the left navigational pane, click **Manage administrator password**.
3. In the **Administrator password** field, enter the password for the primary administrator.
4. In the **Confirm password** field, enter the password for the primary administrator.
5. Click **OK**.
6. To confirm your action, click **OK**.
7. To close the **Manage administrator password** page, click **OK**.
8. To close the Configuration Tool window, click **File** > **Exit**.
9. To confirm your action, click **Yes**.

What to do next

Start the directory server. See "Starting or stopping a directory server and an administration server with Configuration Tool" on page 163.

Managing the primary administrator password with the command-line utility

Use the command-line utility, **idsdnpw**, to manage the primary administrator password for an instance.

Before you begin

To configure the primary administrator password for an instance, you must complete the following requirements:

- Stop the directory server. See "Starting or stopping a directory server and an administration server with command-line utilities" on page 152.

Procedure

1. Log in as directory server instance owner.
2. Access the command prompt.
3. Change the current working directory to the `sbin` subdirectory in the IBM Security Directory Server installation location.
4. To set the administrator password for an instance, run the following command: Substitute the `instance_name`, `adminDN`, and `adminPWD` values as per your requirements.

   ```
   idsdnpw -I instance_name -u adminDN -p adminPWD
   ```

   For more information about the **idsdnpw** command, see *Command Reference*.

What to do next

Start the directory server. See "Starting or stopping a directory server and an administration server with command-line utilities" on page 152.

Database configuration for a directory server instance

To use an instance as a directory server and store directory data, you must configure a DB2 database for the instance.

You can use Instance Administration Tool, Configuration Tool, or the **idscfgdb** command, to create and configure a DB2 database. You must stop the directory server before you configure or unconfigure the database. For more information about the **idscfgdb** command, see *Command Reference*.

If you choose to create the default instance with Instance Administration Tool, the DB2 database instance is also created and configured for the instance. For a proxy server instance, you do not require to configure a DB2 database.

When you configure a DB2 database for an instance, the configuration file of the instance is updated with the DB2 database information. The tool also creates database and local loopback settings.

The database and local loopback settings are created, if they do not exist. You can specify whether to create the database as a local code page database or as a UTF-8 database. The default code page that is used for DB2 database creation is UTF-8.

Configuring a database for an instance with Configuration Tool

Use Configuration Tool to configure a DB2 database for a directory server instance.

Before you begin

To configure a DB2 database for a directory server instance, you must complete the following tasks:

- Stop the directory server. See "Starting or stopping a directory server and an administration server with Configuration Tool" on page 163.
- A system user ID must exist to own the DB2 database instance. For more information about system user ID requirements, see "Users and groups that are associated with a directory server instance" on page 117.

Procedure

1. Start Configuration Tool for an instance. See "Starting Configuration Tool" on page 162.
2. From the task list in the left navigational pane, click **Database tasks** > **Configure database**.
3. In the **Configure database** page, select one of the following options:
   - To configure a database for an instance, complete the following steps:
     a. In the **Database user name** field, enter the system user ID who must own the database. The directory server instance uses this system user ID to connect to the database.
     b. In the **Password** field, enter the password for the database administrator.
     c. In the **Database name** field, enter the database name.
     d. If you want to set any of the following DB2 configuration settings, select **Show advanced tablespace options**.
        – You want the database to use the System Managed Storage (SMS) data storage for the DB2 table spaces. When SMS is used, the file system manager of the operating system allocates and manages the table space where DB2 tables are stored.
        – You want the database to use the Database Managed Storage (DMS) data storage for the DB2 table spaces. Also, you want to configure the database for the `USERSPACE1` and `LDAPSPACE` table spaces, size, and location. When DMS is used, the table spaces are managed by the database manager. The database administrator decides which devices and files to use, and DB2 manages the space on those devices and files.

        If you do not select **Show advanced tablespace options**, a DB2 database with the `USERSPACE1` and `LDAPSPACE` table spaces is created by using DMS with default sizes and locations. If you configure an instance with an existing database, **Show advanced tablespace options** is disabled when you enter the name of an existing database in the **Database name** field.
     e. Click **Next**.
   - To configure the database administrator password again, complete the following steps:
     a. Click **Reset password**.
     b. In the **Password** field, enter the password for the database administrator.
     c. In the **Confirm password** field, enter the password for the database administrator.
     d. Click **Next**.
4. If you create and configure a DB2 database, complete the following steps:
   a. In the **Database install location** field, enter the database location path. You can click **Browse** to specify a directory. On Windows, you must provide a

disk drive location, such as `C:`. On AIX, Linux, and Solaris, the location must be a directory name, such as `/home/ldapdb`.

Note: The minimum disk space that is required for a DMS database is 1 GB. For an SMS database, a minimum of 150 MB of disk space is required. These requirements are for an empty database. When you store data in the database, more disk space is required.

b. To configure the directory server with database for online backup, complete the following steps:
   1) Select **Configure for online backup**.
   2) In the **Database backup location** field, enter the location where you want to store the backup image. You can click **Browse** to specify the location.

   Note: Do not exit Configuration Tool or cancel operation when the backup operation is running.
   When you configure the database for online backup after the database configuration is complete an initial, offline backup of the database is run. After the offline backup operation is complete, the administration server is restarted. You can also configure online backup for a directory server instance with the **idscfgdb** command. However, you cannot unconfigure online backup with the **idscfgdb** command and the **-c** parameter. If you configure online backup for an instance with Instance Administration Tool or Configuration Tool, you can unconfigure it with Configuration Tool or the **idscfgdb** command.

c. In the **Character-set option** area, choose one of the following options to create a database type:

   Note: Create a universal DB2 database if you plan to store data in multiple languages in the directory server. A DB2 Universal Database is also most efficient because less data translation is needed. If you want to use language tags, the database must be a UTF-8 database. For more information about UTF-8, see "UTF-8 support" on page 121.
   - To create an UCS Transformation Format (UTF-8) database in which LDAP clients can store UTF-8 character data, click **Create a universal DB2 database** .
   - To create a database in the local code page, click **Create a local codepage DB2 database**.

d. Click **Next**.

5. If you selected **Show advanced tablespace options**, you must complete the following steps:
   a. From the **Select database tablespace type** list, select a database type. The DMS database table space type is the default. If you select SMS database table space type, all other fields are disabled. DMS table space support is used only for the `USERSPACE1` and `LDAPSPACE` table spaces. All other table spaces, such as catalog and temporary table spaces, are of type SMS.
   a. Under the **USERSPACE1 tablespace details** area, specify the following details:
      1) From the **Tablespace container** list, select the container type. If you want the `USERSPACE1` table space location on the file system, select **File**. If the database table space container location is in a file system, a DMS `cooked` table space is created. You can specify the initial size for the table space and an extendable unit size, and the table space is

automatically expanded when required. If you want to create the USERSPACE1 table space on a raw device, select **Raw device**. A raw device is a device where no file system is installed, such as a hard disk that does not contain a file system. If the database table space container location is in a raw device, a DMS raw table space is created. In this case, the size of the database table space container is fixed and cannot be expanded. If you select **Raw device**, specify the size along with the container location instead of accepting the default values.

2) If you selected **File** in the **Tablespace container** list, specify the following details:
   a) In the **Directory path** field, specify the directory path where you want create the USERSPACE1 table space. You can click **Browse** to select the directory.
   b) In the **File name** field, enter the file name of the table space that you want to create, or accept the default file name, USPACE.
   c) In the **Initial size** field, enter the initial size for the USERSPACE1 table space in pages or accept the default value. For the **File** type table space container, the USERSPACE1 table space container is of auto-incremental type. You can provide the initial size in the **Initial size** field, and an extendable unit size in the **Extendable size** field. The default value for the initial size is 16 K pages, and the default extendable unit size is 8 K pages. The page size for the USERSPACE1 table space container is 4 KB per page.
3) If you selected **Raw device** in the **Tablespace container** list, specify the following details:
   a) In the **Device path** field, enter the location of the raw device. On Windows, the path must start with \\.\. An example that shows the path with device name, \\.*device_name*. On AIX, Linux, and Solaris, the device path must be a valid path.
   b) In the **Initial size** field, enter the initial size for the USERSPACE1 table space or accept the default value. For the **Raw Device** type table space container, the size of the USERSPACE1 table space container is fixed. The default size is 16 K pages. For better results, specify the size you want.

b. Under the **LDAPSPACE tablespace details** area, specify the following details:
   1) From the **Tablespace container** list, select the container type. If you want the LDAPSPACE table space location on a file system, select **File**. If you want to create the LDAPSPACE table space on a raw device, select **Raw device**. A raw device is a device where no file system is installed, such as a hard disk that does not contain a file system.
   2) If you selected **File** in the **Tablespace container** list, specify the following details:
      a) In the **Directory path** field, specify the directory path where you want create the LDAPSPACE table space. You can click **Browse** to select the directory.
      b) In the **File name** field, enter the file name of the table space that you want to create, or accept the default file name, ldapspace.
      c) In the **Initial size** field, enter the initial size for the LDAPSPACE table space in pages or accept the default value. For the **File** type table space container, the LDAPSPACE table space container is of auto-incremental type. You can provide the initial size in the **Initial size** field, and an extendable unit size in the **Extendable size** field.

The default value for the initial size is 16 K pages, and the default extendable unit size is 8 K pages. The page size for the LDAPSPACE table space container is 32 KB per page.

3) If you selected **Raw device** in the **Tablespace container** list, specify the following details:

a) In the **Device path** field, enter the location of the raw device. On Windows, the path must start with \\.\. An example that shows the path with device name, \\.*device_name*. On AIX, Linux, and Solaris, the device path must be a valid path.

b) In the **Initial size** field, enter the initial size for the LDAPSPACE table space or accept the default value. For the **Raw Device** type table space container, the size of the LDAPSPACE table space container is fixed. The default size is 16 K pages. For better results, specify the size you want.

c. If you selected **File** in one or both of the **Tablespace container** fields, specify the number of pages by which to expand the table space containers in the **Extendable size** field.

6. Click **Finish**.
7. To accept task completion, click **OK**.
8. Verify the logs that are generated for the database configuration operation.
9. To close the **Configure database** page, click **Close**.
10. To close the Configuration Tool window, click **File** > **Exit**.
11. To confirm your action, click **Yes**.

What to do next

After you configure a database, you must complete the following configurations for an instance:

- Configure primary administrator DN and password. See "Managing the primary administrator DN with Configuration Tool" on page 164 and "Managing the primary administrator password with Configuration Tool" on page 166.
- Configure the required suffixes. See "Suffix configuration" on page 193.

Configuring a database for an instance with the command-line utility

Use the command-line utility, **idscfgdb**, to configure a DB2 database for a directory server instance.

Before you begin

To configure a DB2 database for a directory server instance, you must complete the following tasks:

- Do not set the *DB2COMM* environment variable when you configure a database.
- Stop the directory server. See "Starting or stopping a directory server and an administration server with command-line utilities" on page 152.
- A system user ID must exist to own the DB2 database instance. For more information about system user ID requirements, see "Users and groups that are associated with a directory server instance" on page 117.

About this task

You can run the **idscfgdb** command to complete the following operations:

- Creates and configures database to a directory server instance. Creates local loopback settings, if they do not exist.
- Adds information about the database to the `ibmslapd.conf` file of the directory server instance

You can specify whether to create the database as a local code page database or as a UTF-8 database, which is the default.

Procedure

1. Log in as directory server instance owner.
2. Access the command prompt.
3. Change the current working directory to the `sbin` subdirectory in the IBM Security Directory Server installation location.
4. To configure a DB2 database to a directory server instance with the following values, run the following command:
   - Instance name: `ldapdb`
   - Database name: `ldapdb`
   - DB2 database administrator ID: `ldapdb`
   - DB2 database administrator password: `ldapdb123`
   - Database location: `/home/ldapdb`

   ```
   idscfgdb -I ldapdb -a ldapdb -w ldapdb123 -t ldapdb
   -l /home/ldapdb
   ```

   On Windows, specify the disk drive name for database location. On Solaris, specify an appropriate database location. For more information about the **idscfgdb** command, see *Command Reference*. The command configures a database with DMS table spaces with default sizes.

Examples

Example 1:

To configure a database with a DMS table space on a file system and with a specific size for the table space, run the **idscfgdb** command with the following values:

- Instance name: `ldapdb`
- Database name: `ldapdb`
- DB2 database administrator ID: `dbadmin`
- DB2 database administrator password: `ldapdb123`
- Database location: `c:\dblocation`
- Location of the `USERSPACE1` table space: `c:\dblocation\ldapinst\tablespaceloc\USPACE`
- Container size of the `USERSPACE1` table spaces: 10000 pages
- Extension size: 16 pages

```
idscfgdb -I ldapdb -a dbadmin -t ldapdb
-w ldapdb123 -n -l c:\dblocation
-u c:\dblocation\ldapinst\tablespaceloc\USPACE -U 10000 -z 16
```

Example 2:

To configure the same database with SMS table spaces, run the **idscfgdb** command with the following values:

- Instance name: `ldapdb`
- Database name: `ldapdb`
- DB2 database administrator ID: `dbadmin`
- DB2 database administrator password: `ldapdb123`
- Database location: `c:\dblocation`

```
idscfgdb -I ldapdb -a dbadmin -t ldapdb
-w ldapdb123 -n -l c:\dblocation
-m SMS
```

What to do next

After you configure a database, you must complete the following configurations for an instance:

- Configure primary administrator DN and password. See "Managing the primary administrator DN with the command-line utility" on page 165 and "Managing the primary administrator password with the command-line utility" on page 166.
- Configure the required suffixes. See "Suffix configuration" on page 193.

Management of the DB2 database administrator password

If you change the system password for the DB2 instance owner, you must update the directory server instance configuration file with the password.

When you change the system password for the DB2 instance owner of a database that is configured with an instance, the password is not updated in the instance configuration file. If the database administrator password in the configuration file of an instance does not match with the system password of the DB2 instance owner that is associated with the database, the instance might not start in normal mode. You must update the instance configuration file with the latest DB2 instance owner password.

You can use Configuration Tool, the **idscfgdb** command, or the **idsldapmodify** command to update the DB2 database administrator password.

When you use Configuration Tool or the **idscfgdb** command to change the database administrator password, you must stop the directory server before you change the password. To change the database administrator password with the **idsldapmodify** command, you must start the directory server in configuration mode. Run the **idsldapmodify** command with the primary directory server administrator or as a local administrator group member with the `dirdata` role.

For more information about the **idscfgdb** and **idsldapmodify** commands, see *Command Reference*.

Modifying the DB2 database administrator password with Configuration Tool

Use Configuration Tool to update the DB2 database administrator password in the directory server instance configuration file.

Before you begin

To update the DB2 database administrator password in the instance configuration file, you must complete the following tasks:

- A directory server instance that is configured with a DB2 database must exist. See "Configuring a database for an instance with Configuration Tool" on page 167.
- Stop the directory server. See "Starting or stopping a directory server and an administration server with Configuration Tool" on page 163.

About this task

Configuration Tool updates the DB2 database administrator password in the directory server instance configuration file. If the change log is configured for the instance, the tool also updates the password for the change log database owner in the configuration file.

Procedure

1. Start Configuration Tool for an instance. See "Starting Configuration Tool" on page 162.
2. From the task list in the left navigational pane, click **Database tasks** > **Configure database**.
3. In the **Configure database** page, complete the following steps:
   a. Select **Reset password**.
   b. In the **Password** field, enter the password for the database administrator.
   c. In the **Confirm password** field, enter the password for the database administrator.
   d. Click **Next**.
4. Click **Finish**.
5. To accept task completion, click **OK**.
6. Verify the logs that are generated for the database password configuration operation.
7. To close the **Configure database** page, click **Close**.
8. To close the Configuration Tool window, click **File** > **Exit**.
9. To confirm your action, click **Yes**.

What to do next

Start the directory server. See "Starting or stopping a directory server and an administration server with Configuration Tool" on page 163.

Modifying the DB2 database administrator password with the command-line utility

Use the **idscfgdb** or **idsldapmodify** command-line utility to update the DB2 database administrator password in the directory server instance configuration file.

Before you begin

To update the DB2 database administrator password in the instance configuration file, you must complete the following tasks:

- A directory server instance that is configured with a DB2 database must exist. See "Configuring a database for an instance with the command-line utility" on page 171.

About this task

You can run the **idscfgdb** command to update the configuration file of an instance with the DB2 database administrator password. You must stop the directory server before you run the **idscfgdb** command.

You can use the **idsldapmodify** command to change the password when the directory server instance is running. Run the **idsldapmodify** command with the primary directory server administrator or as a local administrator group member with the `dirdata` role.

For more information about the **idscfgdb** and **idsldapmodify** commands, see *Command Reference*.

Procedure

1. Log in as directory server instance owner.
2. Access the command prompt.
3. To change the DB2 database administrator password, choose one of the following methods:
   - To change the DB2 database administrator password with the **idscfgdb** command, complete the following steps:
     a. Change the current working directory to the `sbin` subdirectory in the IBM Security Directory Server installation location.
     b. Stop the directory server. See "Starting or stopping a directory server and an administration server with command-line utilities" on page 152.
     c. Run the **idscfgdb** command in the following format:
        ```
        idscfgdb -I instance_name -w db2adminPWD
        ```
     d. Start the directory server. See "Starting or stopping a directory server and an administration server with command-line utilities" on page 152.
   - To change the DB2 database administrator password with the **idsldapmodify** command, complete the following steps:
     a. Change the current working directory to the `bin` subdirectory in the IBM Security Directory Server installation location.
     b. Run the **idsldapmodify** command in the following format:
        ```
        idscfgdb -h IP_address -p port -D adminDN -w adminPWD -i file1.ldif
        ```
        The `file1.ldif` contains the following entries:
        ```
        dn: cn=Directory, cn=RDBM Backends, cn=IBM Directory, cn=Schemas,
         cn=Configuration
        changetpye: modify
        replace: ibm-slapdDbUserPW
        ibm-slapdDbUserPW: db2adminPWD
        ```
     c. Restart the directory server. See "Starting or stopping a directory server and an administration server with command-line utilities" on page 152.

Database unconfiguration from a directory server instance

To use an existing directory server instance with another DB2 database, you must unconfigure the existing DB2 database from an instance.

For a directory server instance, you can unconfigure a database only if you configured DB2 database for the instance.

With Configuration Tool or the **idsucfgdb** command, you can choose to run the following operations:

- Remove the DB2 database information from the configuration file of a directory server instance. In this operation, the utility unconfigures the DB2 database from an instance and does not delete the DB2 database.
- Remove the DB2 database information from the configuration file of a directory server instance and delete the DB2 database. In this operation, the DB2 database is deleted and all data is lost.

After you unconfigure the DB2 database from a directory server instance, the database is inaccessible to the instance.

For a proxy server instance, the database unconfiguration operation is not supported.

For more information about the **idsucfgdb** command, see *Command Reference*.

Unconfiguring the DB2 database from an instance with Configuration Tool

Use Configuration Tool to unconfigure the DB2 database from a directory server instance.

Before you begin

To unconfigure the DB2 database from an instance, the instance must meet the following requirements:

- A directory server instance that is configured with a DB2 database must exist. See "Configuring a database for an instance with Configuration Tool" on page 167.
- Stop the directory server. See "Starting or stopping a directory server and an administration server with Configuration Tool" on page 163.

Procedure

1. Start Configuration Tool for an instance. See "Starting Configuration Tool" on page 162.
2. From the task list in the left navigational pane, click **Database tasks** > **Unconfigure database**.
3. In the **Unconfigure database** page, complete the following steps:
   a. From the Options area, select one of the following options:
      - To unconfigure the DB2 database from an instance without deleting the DB2 database, click **Unconfigure database**.
      - To unconfigure the DB2 database from an instance and to delete the DB2 database, click **Unconfigure and destroy database**.
   b. To remove the database backup copy for the instance if the database is configured for online backup, select **Remove the backup copy of the database**.
   c. To start the unconfiguration, click **Unconfigure**.
   d. In the confirmation window, click **Yes**.
4. To accept task completion, click **OK**.

5. Verify the logs that are generated for the database unconfiguration operation.
6. To close the **Unconfigure database** page, click **Cancel**.
7. To close the Configuration Tool window, click **File** > **Exit**.
8. To confirm your action, click **Yes**.

Unconfiguring the DB2 database from an instance with the command-line utility

Use the command-line utility, **idsucfgdb**, to unconfigure the DB2 database from a directory server instance.

Before you begin

To unconfigure the DB2 database from an instance, the instance must meet the following requirements:

- A directory server instance that is configured with a DB2 database must exist. See "Configuring a database for an instance with the command-line utility" on page 171.
- Stop the directory server. See "Starting or stopping a directory server and an administration server with command-line utilities" on page 152.

Procedure

1. Log in as directory server instance owner.
2. Access the command prompt.
3. Change the current working directory to the `sbin` subdirectory in the IBM Security Directory Server installation location.
4. To unconfigure the DB2 database from an instance, choose one of the following options:
   - To unconfigure the database from a directory server instance, run the **idsucfgdb** command in the following format:
     ```
     idsucfgdb -I instance_name
     ```
   - To unconfigure and delete the database from a directory server instance, run the **idsucfgdb** command in the following format:
     ```
     idsucfgdb -I instance_name -r
     ```

Database optimization

To improve the DB2 database search performance, you can optimize the database and update DB2 statistics for the database tables.

You can use Configuration Tool or the **idsrunstats** command to optimize DB2 database. You must run the DB2 optimization operation periodically or after the database updates, such as after data import operations.

When you run database optimization, the tool collects statistics on all indexes that are defined on tables and updates it. The DB2 query optimizer uses these statistics to determine the optimum path to access the data.

You cannot run DB2 optimization, if the instance is a proxy server or the instance is not configured with a DB2 database.

For more information about the **idsrunstats** command, see *Command Reference*.

Optimizing database with Configuration Tool

Use Configuration Tool to optimize the DB2 database that is associated with an instance.

Before you begin

To optimize the DB2 database for an instance, the instance must meet the following requirements:

- A directory server instance that is configured with a DB2 database must exist. See "Configuring a database for an instance with Configuration Tool" on page 167.

Procedure

1. Start Configuration Tool for an instance. See "Starting Configuration Tool" on page 162.
2. From the task list in the left navigational pane, click **Database tasks** > **Optimize database**.
3. In the **Optimize database** page, complete the following steps:
   a. To start the database optimization operation, click **Optimize**.
   b. To accept task completion, click **OK**.
   c. Verify the logs that are generated for the database optimization operation.
   d. To clear the logs, click **Clear results**.
4. To close the **Optimize database** page, click **Close**.
5. To close the Configuration Tool window, click **File** > **Exit**.
6. To confirm your action, click **Yes**.

Optimizing database with the command-line utility

Use the command-line utility, **idsrunstats**, to optimize the DB2 database that is associated with an instance.

Before you begin

To optimize the DB2 database of an instance, the instance must meet the following requirements:

- A directory server instance that is configured with a DB2 database must exist. See "Configuring a database for an instance with the command-line utility" on page 171.

Procedure

1. Log in as directory server instance owner.
2. Access the command prompt.
3. Change the current working directory to the `sbin` subdirectory in the IBM Security Directory Server installation location.
4. To optimize the DB2 database, run the **idsrunstats** command in the following format:

   ```
   idsrunstats -I instance_name
   ```

   For more information about the **idsrunstats** command, see *Command Reference*.

Database maintenance

To improve search or update operations against an instance, you can run DB2 index reorganization or DB2 row compression.

You can use Configuration Tool or the **idsdbmaint** command to run DB2 index reorganization or DB2 row compression.

When the DB2 tables of a database are updated with many insertions and deletions, search and update operations against the database become slower. If you reorganize the DB2 index, the performance of the search and update operations improves.

When you run DB2 row compression, the tool searches for repeating patterns and replaces them with shorter symbol strings. The tool analyzes and then runs the row compression only if the compression results in an improvement of greater than 30 percent.

You can also use the **idsdbmaint** command to convert an SMS table space to a DMS table space or a DMS table space to an SMS table space. Table space conversion is not supported by Configuration Tool. For more information about the **idsdbmaint** command, see *Command Reference*.

Running database maintenance with Configuration Tool

Use Configuration Tool to maintain the DB2 database that is associated with an instance.

Before you begin

To maintain the DB2 database for an instance, the instance must meet the following requirements:

- A directory server instance that is configured with a DB2 database must exist. See "Configuring a database for an instance with Configuration Tool" on page 167.
- Stop the directory server. See "Starting or stopping a directory server and an administration server with Configuration Tool" on page 163.

Procedure

1. Start Configuration Tool for an instance. See "Starting Configuration Tool" on page 162.
2. From the task list in the left navigational pane, click **Database tasks** > **Maintenance** .
3. In the **Maintenance** page, complete the following steps:
   a. Select the DB2 database maintenance operation that you want to run:
      - To run DB2 index reorganization, click **Perform index reorganization**.
      - To run DB2 row compression, click **Inspect the tables and perform row compression**.
   b. Click **OK**.
   c. In the task completion window, click **OK**.
   d. Verify the logs that are generated for the database maintenance operation.
   e. To clear the logs, click **Clear results**.
4. To close the **Maintenance** page, click **Close**.

5. To close the Configuration Tool window, click **File** > **Exit**.
6. To confirm your action, click **Yes**.

What to do next

Start the directory server. See "Starting or stopping a directory server and an administration server with Configuration Tool" on page 163.

Running database maintenance with the command-line utility

Use the command-line utility, **idsdbmaint**, to run maintenance operation on the DB2 database that is associated with an instance.

Before you begin

To run the DB2 database maintenance operation, the instance must meet the following requirements:

- A directory server instance that is configured with a DB2 database must exist. See "Configuring a database for an instance with the command-line utility" on page 171.
- Stop the directory server. See "Starting or stopping a directory server and an administration server with command-line utilities" on page 152.

Procedure

1. Log in as directory server instance owner.
2. Access the command prompt.
3. Change the current working directory to the `sbin` subdirectory in the IBM Security Directory Server installation location.
4. To run DB2 index reorganization, run the **idsdbmaint** command in the following format:

   ```
   idsdbmaint -I instance_name -i
   ```

   For more information about the **idsdbmaint** command, see *Command Reference*.
5. To run DB2 row compression, run the **idsdbmaint** command in the following format:

   ```
   idsdbmaint -I instance_name -r
   ```

What to do next

Start the directory server. See "Starting or stopping a directory server and an administration server with command-line utilities" on page 152.

Directory server backup

To recover from a directory server instance failure, you must back up the directory server instance frequently.

You can use Configuration Tool or the **idsdbback** command to back up an instance. You cannot use the **idsdbback** command to back up a proxy server instance because no database is associated with a proxy server.

You can configure a database that is associated with an instance for online backup by using the **idscfgdb** command. However, you cannot unconfigure online backup by using the **idscfgdb** command with the **-c** parameter. If you configure online

backup for an instance by using Instance Administration Tool or Configuration Tool, you can unconfigure it with Configuration Tool or the **idscfgdb** command. For the most reliable results, use Instance Administration Tool or Configuration Tool to configure online backup for an instance with database.

You can also use the **idsdb2ldif** command to export the entries in a directory server to an LDIF file. You can use the **migbkup** command to back up schema and configuration files for a directory server instance and a proxy server instance. For more information about the **idsdbback**, **idsdb2ldif**, or **migbkup** command, see *Command Reference*. For more information about the appropriate command to use in your environment, see the *Performance Tuning and Capacity Planning Guide*.

With Configuration Tool, you can take the following actions:

- Back up the configuration settings for a directory server instance or a proxy server instance.
- Back up the directory server instance with its database.
- Back up the directory server instance and the change log database if it is configured for an instance.

For more information about the backup and restore operations, see the *Administration Guide*.

Backing up the database of a directory server instance with Configuration Tool

Use Configuration Tool to back up a directory server instance with its database to recover from any failure.

Before you begin

To back up a directory server instance with its database, the instance must meet the following requirements:

- A directory server instance that is configured with a DB2 database must exist. See "Configuring a database for an instance with Configuration Tool" on page 167.

Procedure

1. Start Configuration Tool for an instance. See "Starting Configuration Tool" on page 162.
2. From the task list in the left navigational pane, click **Backup/Restore** > **Backup database**.
3. In the **Backup database** page, complete the following steps:
   a. In the **Backup directory** field, enter the directory path in which you want to back up all directory data and configuration files. You can also click **Browse** to specify the directory path.
   b. For online backup, choose one of the following options:
      - To configure the directory server and its database for online backup if it not already configured for online backup, select **Update database configuration to support online backup**.
      - To run online backup for the directory server instance if online backup is configured on the server, select **Perform online backup**.
   c. To back up the change log database for the instance if the change log is configured, select **Include change log data in backup**.

d. To exclude the database files from backup, select **Do not backup database files**. If you select**Do not backup database files**, the database and change log database files for the directory server instance are not backed up. The tool backs up the directory server instance files, such as key stash files, schema, and configuration files.

e. To decide whether to continue with backup if the backup directory exists or otherwise, choose one of the following options:

- To create the backup directory if it does not exist, click **Create backup directory as needed**.
- If the backup directory does not exist, and you do not want to create the directory, click **Halt if backup directory is not found**. If a backup directory does not exist and you select this option, the database is not backed up.

Note: Do not exit Configuration Tool when the backup operation is running.

f. To start the backup operation, click **Backup**.

g. If the backup operation requires to stop the directory server, click **Yes**.

h. To confirm task completion, click **OK**.

i. Verify the logs that are generated for the backup operation.

j. To clear the logs, click **Clear results**.

k. To close the **Backup database** page, click **Close**.

4. To close the Configuration Tool window, click **File** > **Exit**.
5. To confirm your action, click **Yes**.

Backing up a proxy server instance with Configuration Tool

Use Configuration Tool to back up a proxy server instance to recover from any failure.

Before you begin

To back up a proxy server instance, a proxy server instance must exist. See "Creating a proxy server instance with custom settings" on page 138.

Procedure

1. Start Configuration Tool for an instance. See "Starting Configuration Tool" on page 162.
2. From the task list in the left navigational pane, click **Backup/Restore** > **Backup instance**.
3. In the **Backup instance** page, complete the following steps:
   a. In the **Backup directory** field, enter the directory path in which you want to back up the schema and configuration files. You can also click **Browse** to specify the directory path.
   b. For a proxy server instance, the **Do not backup database files** check box is selected.
   c. To decide whether to continue with backup if the backup directory exists or otherwise, choose one of the following options:
      - To create the backup directory if it does not exist, click **Create backup directory as needed**.

- If the backup directory does not exist, and you do not want to create the directory, click **Halt if backup directory is not found**. If a backup directory does not exist and you select this option, the proxy instance is not backed up.

Note: Do not exit Configuration Tool when the backup operation is running.

d. To start the backup operation, click **Backup**.
e. If the operation requires to stop the instance, click **Yes**.
f. To confirm task completion, click **OK**.
g. Verify the logs that are generated for the backup operation.
h. To clear the logs, click **Clear results**.
i. To close the **Backup instance** page, click **Close**.

4. To close the Configuration Tool window, click **File** > **Exit**.
5. To confirm your action, click **Yes**.

Restore a directory server

If your directory server instance fails, you can restore your instance to the most recent backup image.

You can use Configuration Tool or the **idsdbestore** command to restore directory data and, optionally, configuration settings that were previously backed up. You must stop the directory server before you can restore the database, configuration settings, or both.

For a proxy server, you can restore the configuration settings. For a proxy server, you must run the **idsdbrestore** command with the **-x** parameter.

For an instance with a DB2 database, you can restore the database into a database and database instance with the same name that was used for the database backup. For a directory server with a DB2 database, you can restore only if a database is configured for the directory server instance. The **idsdbestore** command restores the backup database into the currently configured database. The command fails if the backed up database instance and database do not match the configured database instance and database. To restore the database, location of the backed up database and the database that the command is restoring must be the same.

For more information about the **idsdbrestore** command, see *Command Reference*.

Restoring the database of a directory server with Configuration Tool

Use Configuration Tool to restore a directory server instance and its database from a backed up image.

Before you begin

To restore a directory server instance and its database, the instance must meet the following requirements:

- A directory server instance that is configured with a DB2 database must exist. See “Configuring a database for an instance with Configuration Tool” on page 167.

- A backup image of the directory server instance must exist. See “Backing up the database of a directory server instance with Configuration Tool” on page 181.
- Stop the directory server. See “Starting or stopping a directory server and an administration server with Configuration Tool” on page 163.

Procedure

1. Start Configuration Tool for an instance. See “Starting Configuration Tool” on page 162.
2. From the task list in the left navigational pane, click **Backup/Restore** > **Restore database**.
3. In the **Restore database** page, complete the following steps:
   a. In the **Restore directory** field, enter the directory path that contains the backup image of the instance. You can also click **Browse** to specify the directory path.
   b. If you want to restore only the directory data and not the configuration settings from the backed up image, select **Preserve current configuration settings**. If you want to restore both the database and configuration settings, you must clear **Preserve current configuration settings**.
   c. If the change log is configured for the instance and you want to restore the change log data, select **Include change log data in restore**.
   d. To start the restore operation, click **Restore**.
   e. If the operation requires to stop the directory server, click **Yes**.
   f. To confirm task completion, click **OK**.
   g. Verify the logs that are generated for the restore operation.
   h. To clear the logs, click **Clear results**.
   i. To close the **Restore database** page, click **Close**.
4. To close the Configuration Tool window, click **File** > **Exit**.
5. To confirm your action, click **Yes**.

Restoring a proxy server instance with Configuration Tool

Use Configuration Tool to restore a proxy server instance to recover from any failure.

Before you begin

To restore a proxy server instance, the proxy server instance must meet the following requirements:

- The proxy server instance must exist. See “Creating a proxy server instance with custom settings” on page 138.
- A backup image of the proxy server instance must exist. See “Backing up a proxy server instance with Configuration Tool” on page 182.
- Stop the directory server. See “Starting or stopping a directory server and an administration server with Configuration Tool” on page 163.

Procedure

1. Start Configuration Tool for an instance. See “Starting Configuration Tool” on page 162.
2. From the task list in the left navigational pane, click **Backup/Restore** > **Restore instance**.
3. In the **Restore instance** page, complete the following steps:

a. In the **Restore directory** field, enter the directory path that contains the backup image of the instance. You can also click **Browse** to specify the directory path.
b. If you do want to restore the configuration settings from the backed up image, select **Preserve current configuration settings**.
c. To start the restore operation, click **Restore**.
d. If the operation requires to stop the directory server, click **Yes**.
e. To confirm task completion, click **OK**.
f. Verify the logs that are generated for the restore operation.
g. To clear the logs, click **Clear results**.
h. To close the **Restore instance** page, click **Close**.

4. To close the Configuration Tool window, click **File** > **Exit**.
5. To confirm your action, click **Yes**.

Tuning a directory server for performance

You must tune a directory server instance to improve the search and update performance.

You can run Configuration Tool or the **idsperftune** command to tune a directory server instance. The tool generates performance tuning setting values for the directory server caches and DB2 buffer pools. The tool generates the tuning settings that are based on the values that you provide about the directory server instance. The tool can also update the tuning settings for an instance. The tool backs up the `ibmslapd.conf` file and saves it in the `logs/ibmslapd.conf.save` file in the home directory for a directory server instance.

The tool saves the information that you provide in the `logs/perftune_input.conf` file in the home directory for a directory server instance.

Configuration Tool or the **idsperftune** command uses the values that you provide to calculate the following tuning settings for the instance:

- Entry cache size
- Filter cache size
- Group Member Cache size
- Group Member Cache Bypass Limit
- `DB2 LDAPDB` buffer pool size
- `DB2 IBMDEFAULTDB` buffer pool size

If your directory server instance is running, the tool monitors the performance of the instance and provides the database health check information. The database health check information includes the following DB2 parameters:

- `DB2 NUM_IOSERVERS`
- `DB2 NUM_IOCLEANERS`
- `CATALOGCACHE_SZ`
- `PCKCACHESZ`
- `LOGFILSIZ`
- `LOCKLIST`

If you run advanced tuning on an instance, the tool collects and analyzes data about the directory server instance. You must run the instance for some time to

collect DB2 tuning data during the database health check analysis. The tool generates the tuning values for the following DB2 parameters and saves them in the `logs/perftune_stat.log` file for the instance.

- `SORTHEAP`
- `MAXFILOP`
- `DBHEAP`
- `CHNGPGS_THRESH`
- `NUM_IOSERVERS`
- `NUM_IOCLEANERS`

The health status suggestions for the DB2 parameters can be one of the following values:

- `OK`
- `Increase`
- `Decrease`
- `Not Collected`

The health status of DB2 parameters that are not analyzed is assigned the `Not Collected` value. You can use the suggested values to decide the DB2 parameters that you can tune to obtain better performance.

For better performance, you must run the tool on an instance as soon as you load the initial directory data. After the initial tuning, run the tool periodically especially after you add many entries or modify the content of entries.For more information about tuning a directory server instance, see the *Performance Tuning and Capacity Planning Guide*.

You cannot use Configuration Tool or the **idsperftune** command to tune a proxy server instance or an instance that is not configured with a database.

Configuring a directory server for performance tuning with Configuration Tool

Use Configuration Tool to tune a directory server to improve the performance of the search and update operations.

Before you begin

To tune a directory server instance, the instance must meet the following requirements:

- A directory server instance that is configured with a DB2 database must exist. See "Configuring a database for an instance with Configuration Tool" on page 167.

Procedure

1. Start Configuration Tool for an instance. See "Starting Configuration Tool" on page 162.
2. From the task list in the left navigational pane, click **Database tasks** > **Performance tuning**.
3. In the **Performance tuning** page, complete the following steps:
   a. In the **Percentage of available system memory to be allocated to this directory instance** field, enter the percentage of system memory you want

allocated to the instance. The available system memory is divided between multiple directory server instances, or between instances and other servers that you plan to run on the system. The tool uses the value that you provide to calculate the sizes of the entry and filter caches.

b. In the **Planned number of groups** field, enter the number of groups that you expect to add in the instance. The tool uses the value that you provide to calculate the sizes for the directory server caches.

c. In the **Maximum number of members in a group that will be referenced frequently** field, enter the average number of members for groups that are referenced frequently.

d. Under the **Number of entries and average entry size** area, choose one of the following options:

- If you want to estimate the number of entries in the directory and the average size of an entry, complete the following steps:
  1) In the **Planned number of entries** field, enter the total number of entries that are planned for the instance. The tool attempts to determine the number of entries in the directory server instance. If it cannot, it uses the default of 10,000 entries. The tool uses this value to calculate the sizes for the directory server caches.
  2) In the **Average size of an entry**field, enter the average size in bytes of an entry that is in the instance. The tool attempts to compute the size of an entry in the directory server instance. If it cannot, it uses the default of 2650 bytes. The tool uses this value to calculate the sizes for the directory server caches.
- If you want the tool to determine the total number of entries and average entry size, click **Load from server instance database**. The tool populates the **Planned number of entries** and **Average size of an entry** fields.

e. Under the **Update frequency** area, choose one of the following options:

- If you expect frequent updates to the instance, click **Frequent updates**. (As a guideline, an average of more than one update for every 500 searches can be considered frequent updates.)
- If you expect less frequent updates or if updates are grouped and made during certain durations in a day, click **Batch updates**.

The tool uses this information to set the filter cache size. The filter cache is useful only when there are infrequent updates to the instance and the same searches are run multiple times. If frequent updates are expected, the filter cache is set to 0. If infrequent or batch updates are expected, the filter cache is set to 1024 filter cache entries.

f. If you want the tool to provide performance analysis values, select **Enable collection of additional system data for extended tuning**.

- When you select the check box, the DB2 monitor switches `BUFFERPOOL` and `SORTHEAP` are enabled. The performance of the directory server instance might degrade when the tool enables the DB2 monitor switches to collect the data.
- To obtain accurate data for optimal tuning of your directory server instance, select the check box when directory activity is typical for your environment. If you run the database health check when the server is not busy, then the usual does not provide optimum performance values.

g. Click **Next**. The **Performance tuning: verification** page opens.

4. In the **Performance tuning: verification** page, complete the following steps:

a. In the **Database health status** list, verify the performance tuning settings that the tool generates. If there are no database activities for the instance, the **Database health status** list might not be populated. The list is populated if the tool collects information about at least one DB2 related parameter. The tuning settings are also logged in the `perftune_stat.log` file.

b. To modify the database parameter values, click **Tune database parameters**. The **Database parameters** window opens.

c. In the **Database parameters** window, specify values for the following database parameters:

1) In the **Database heap** field, enter the maximum memory in pages to set for database heap. The database heap contains control block information for tables, indexes, table spaces, and buffer pools. It also contains memory for the log buffer and temporary memory that is used by utilities.

2) In the **Package cache size** field, enter the size in pages to cache the sections for static and dynamic SQL and XQuery statements on a database.

3) In the **Log buffer size** field, enter the size in pages for the buffer that must be allocated for log records. You must specify the amount of the database heap to use as a buffer for log records.

4) In the **Maximum database files open per application** field, enter the maximum number of file handles that can be open for each database agent.

5) In the **Changed pages threshold** field, enter the percentage of changed pages.

6) In the **Sort heap size** field, enter the maximum size for sort heap in pages. The sort heap can be used as private memory pages for private sorts or as shared memory pages for shared sorts.

7) In the **Log file size** field, enter the size in KB for the log files. This parameter defines the size of each primary and secondary log file.

8) In the **Database log path** field, enter the location where you want to store the log files. You can click **Browse** to specify the location.

9) To save the set values and to update the database parameters with the values, click **OK**. If you do not specify values for parameters, the default values are set.

5. To confirm whether to update the directory and database settings with the tuning values, choose one of the following options:
   - To update the tuning settings for your directory server instance, click **Yes, use the recommended values to update the directory and database configuration settings**.
   - If you do not want to use the tuning settings, click **No, keep the current settings. No configuration settings will be updated**.
6. To apply the changes, click **Finish**.
7. To confirm the task completion, click **OK**.
8. Verify the logs that are generated when the tuning settings are updated.
9. To clear the logs, click **Clear results**.
10. To close the **Performance tuning** page, click **Close**.
11. To close the Configuration Tool window, click **File** > **Exit**.
12. To confirm your action, click **Yes**.

Configuring a directory server for performance tuning with the command-line utility

Use the command-line utility, **idsperftune**, to tune a directory server to improve the performance of the search and update operations.

Before you begin

To tune a directory server instance, the instance must meet the following requirements:

- A directory server instance that is configured with a DB2 database must exist. See "Configuring a database for an instance with the command-line utility" on page 171.

Procedure

1. Log in as directory server instance owner.
2. Access the command prompt.
3. Change the current working directory to the `sbin` subdirectory in the IBM Security Directory Server installation location.
4. To tune a directory server and its database, run the **idsperftune** command.
   - To run basic tuning of the directory server, run the **idsperftune** command in the following format:

     ```
     idsperftune -I instance_name -i property_file -B -u
     ```

     When you specify the **-u** parameter, the LDAP cache and DB2 buffer pool settings are updated in the server and the database. If you do not specify the **-u** parameter, the tuning settings are logged only in the `perftune_stat.log` file.
   - To obtain the number of entries and average entry size from an instance and its database, run the **idsperftune** command in the following format:

     ```
     idsperftune -I instance_name -s
     ```
   - To run advanced tuning of the directory server, run the **idsperftune** command in the following format:

     ```
     idsperftune -I instance_name -i property_file -A -m
     ```

     When you specify the **-m** parameter, the monitor switches for `BUFFERPOOL` and `SORT` are turned on. To obtain accurate data for optimal tuning of your instance, run the command when directory activity is typical for your environment.

   For more information about the **idsperftune** command, see *Command Reference*.

Change log management for a directory server instance

You can configure the change log database to record changes to the schema or directory entries of an instance.

The change log records all update operations, such as `add`, `delete`, `modify`, and `modrdn`, against a directory server instance. You can use client utilities to retrieve the change log data that is recorded when changes are made to a directory server database.

You can use Configuration Tool or the command-line utilities to enable or disable the change log database. You must stop the directory server before you configure or unconfigure the change log database.

To configure the change log for a directory server, use the **idscfgchglg** command. To unconfigure the change log for a directory server, use the **idsucfgchglg** command. You cannot configure a change log database for a proxy server instance.

To configure the change log for a directory server instance, you must meet the following criteria:

1. A DB2 instance with the same name as the directory server instance must exist.
2. You must configure a database for the directory server instance.
3. On AIX, Linux, and Solaris, the local loopback service must be registered in the `/etc/services` file.

When you configure a change log database, it is created in the same database instance as the directory server instance database. For the change log database, an additional 30 MB of hard disk space is required. When you configure the change log, the change log entry is added to the configuration file of the directory server instance.

Configuring the change log with Configuration Tool

Use Configuration Tool to configure the change log database for a directory server instance.

Before you begin

To configure the change log for an instance, the instance must meet the following requirements:

- A directory server instance that is configured with a DB2 database must exist. See "Configuring a database for an instance with Configuration Tool" on page 167.
- Stop the directory server. See "Starting or stopping a directory server and an administration server with Configuration Tool" on page 163.

Procedure

1. Start Configuration Tool for an instance. See "Starting Configuration Tool" on page 162.
2. From the task list in the left navigational pane, click **Manage changelog**.
3. In the **Manage changelog** page, complete the following steps:
   a. To configure the change log, select **Enable change log database**.
   b. Under the **Maximum number of log entries** area, specify the maximum number of entries that you want to record in the change log database.
      - To record unlimited number of entries in the change log, click **Unlimited**.
      - To record a specific number of entries, click **Entries** and enter the number of entries. The default number of entries is 1,000,000.
   c. Under the **Maximum age** area, specify the maximum number of durations for which you want to store entries in the change log database.
      - To store the entries in the change log indefinitely, click **Unlimited**.
      - To store entries for a specific duration, click **Age** and enter the number of days and hours.

d. To apply the changes, click **Update**.
e. To confirm task completion, click **OK**.
f. Verify the logs that are generated for the change log database configuration.
g. To clear the logs, click **Clear results**.
h. To close the **Manage changelog** page, click **Close**.

4. To close the Configuration Tool window, click **File** > **Exit**.
5. To confirm your action, click **Yes**.

What to do next

Start the directory server. See "Starting or stopping a directory server and an administration server with Configuration Tool" on page 163.

Configuring the change log with the command-line utility

Use the command-line utility, **idscfgchglg**, to configure the change log database for a directory server instance.

Before you begin

To configure the change log for an instance, the instance must meet the following requirements:

- A directory server instance that is configured with a DB2 database must exist. See "Configuring a database for an instance with the command-line utility" on page 171.
- Stop the directory server. See "Starting or stopping a directory server and an administration server with command-line utilities" on page 152.

Procedure

1. Log in as directory server instance owner.
2. Access the command prompt.
3. Change the current working directory to the `sbin` subdirectory in the IBM Security Directory Server installation location.
4. To configure the change log for directory server instance, run the **idscfgchglg** command.
   - To configure the change log for an instance with no age limit or size limit, run the **idscfgchglg** command:

     ```
     idscfgchglg -I instance_name -m 0
     ```

   - To configure the change log for an instance with a size limit of 1,000,000 and an age of 25 hours, run the **idscfgchglg** command:

     ```
     idscfgchglg -I instance_name -m 1000000 -y 1 -h 1
     ```

   For more information about the **idscfgchglg** command, see *Command Reference*.

What to do next

Start the directory server. See "Starting or stopping a directory server and an administration server with command-line utilities" on page 152.

Unconfiguring the change log with Configuration Tool

Use Configuration Tool to unconfigure the change log database from a directory server instance.

Before you begin

To unconfigure the change log from an instance, the instance must meet the following requirements:

- The change log for an instance must be configured. See "Configuring the change log with Configuration Tool" on page 190.
- Stop the directory server. See "Starting or stopping a directory server and an administration server with Configuration Tool" on page 163.

Procedure

1. Start Configuration Tool for an instance. See "Starting Configuration Tool" on page 162.
2. From the task list in the left navigational pane, click **Manage changelog**.
3. In the **Manage changelog** page, complete the following steps:
   a. To unconfigure the change log, clear **Enable change log database**.
   b. To apply the changes, click **Update**.
   c. In the **Manage changelog** window, click **Yes** to confirm your action.
   d. Verify the logs that are generated when you unconfigure the change log database.
   e. To clear the logs, click **Clear results**.
   f. To close the **Manage changelog** page, click **Close**.
4. To close the Configuration Tool window, click **File** > **Exit**.
5. To confirm your action, click **Yes**.

What to do next

Start the directory server. See "Starting or stopping a directory server and an administration server with Configuration Tool" on page 163.

Unconfiguring the change log with the command-line utility

Use the command-line utility, **idsucfgchglg**, to unconfigure the change log database from a directory server instance.

Before you begin

To unconfigure the change log from an instance, the instance must meet the following requirements:

- The change log for an instance must be configured. See "Configuring the change log with the command-line utility" on page 191.
- Stop the directory server. See "Starting or stopping a directory server and an administration server with command-line utilities" on page 152.

Procedure

1. Log in as directory server instance owner.
2. Access the command prompt.
3. Change the current working directory to the `sbin` subdirectory in the IBM Security Directory Server installation location.
4. To unconfigure the change log for directory server instance, run the **idsucfgchglg** command in the following format:

   ```
   idsucfgchglg -I instance_name
   ```

For more information about the **idsucfgchglg** command, see *Command Reference*.

What to do next

Start the directory server. See "Starting or stopping a directory server and an administration server with command-line utilities" on page 152.

Suffix configuration

To create a directory hierarchy, you must configure the required suffix for your directory server instance.

A suffix is known as a naming context. It is a distinguished name (DN) that identifies the top entry in a directory hierarchy. LDAP uses the relative naming scheme. Therefore, a DN is also the suffix for all entries in a directory hierarchy. In a directory server, you can add multiple suffixes, each identifying a directory hierarchy. When you add a suffix, the entry is added in the configuration file of a directory server instance. The following example shows a suffix entry, `o=sample`.

You can use Configuration Tool to add or remove suffixes. You can also use the **idscfgsuf** command to add suffixes and the **idsucfgsuf** command to remove suffixes. You must stop the directory server before you add or remove a suffix. For more information about the **idscfgsuf** or **idsucfgsuf** command, see *Command Reference*.

You cannot remove the system defined suffixes from a directory server instance. These suffixes are not available in a proxy server instances. The following suffixes are defined by system:

- `cn=localhost`
- `cn=configuration`
- `cn=ibmpolicies`
- `cn=Deleted Objects`

When you add entries to a directory server, you must consider the following points:

- You must add a suffix entry in a directory server for a suffix DN.
- An entry DN that you add to a directory server must contain a suffix that match the suffix DN value. The following example shows an entry with a suffix DN, `ou=Marketing,o=sample`.
- You cannot add an entry on a proxy server instance or a directory server that is not configured with a DB2 database.

If a query contains a suffix that does not match any suffix that are configured for the local database, the query is referred to the LDAP server that is identified by the default referral. If no LDAP default referral is specified, the following message is generated: `Object does not exist`.

Adding a suffix with Configuration Tool

Use Configuration Tool to add a suffix for an instance.

Before you begin

To add a suffix for an instance, you must complete the following steps:

- Stop the directory server. See "Starting or stopping a directory server and an administration server with Configuration Tool" on page 163.

About this task

When you add a suffix to an instance, the suffix entry is added to the configuration file of an instance.

Procedure

1. Start Configuration Tool for an instance. See "Starting Configuration Tool" on page 162.
2. From the task list in the left navigational pane, click **Manage suffixes**.
3. In the **Manage suffixes** page, complete the following steps:
   a. In the Suffix DN field, enter the suffix that you want to add to the instance.
   b. Click **Add**.
   c. To apply the changes, click **OK**.
4. To close the Configuration Tool window, click **File** > **Exit**.
5. To confirm your action, click **Yes**.

What to do next

Start the directory server. See "Starting or stopping a directory server and an administration server with Configuration Tool" on page 163.

Adding a suffix with the command-line utility

Use the command-line utility, **idscfgsuf**, to add a suffix for an instance.

Before you begin

To add a suffix for an instance, you must complete the following steps:

- Stop the directory server. See "Starting or stopping a directory server and an administration server with command-line utilities" on page 152.

About this task

When you add a suffix to an instance, the suffix entry is added to the configuration file of an instance.

Procedure

1. Log in as directory server instance owner.
2. Access the command prompt.
3. Change the current working directory to the `sbin` subdirectory in the IBM Security Directory Server installation location.
4. To add the `o=sample` suffix to an instance, run the **idscfgsuf** command in the following format:

   ```
   idscfgsuf -I instance_name -s "o=sample"
   ```

   For more information about the **idscfgsuf** command, see *Command Reference*.

What to do next

Start the directory server. See “Starting or stopping a directory server and an administration server with command-line utilities” on page 152.

Removing a suffix with Configuration Tool

Use Configuration Tool to remove a suffix from a directory server instance.

Before you begin

To remove a suffix from a directory server instance, you must complete the following steps:

- Stop the directory server. See “Starting or stopping a directory server and an administration server with Configuration Tool” on page 163.

About this task

When you remove a suffix to an instance, the suffix entry is removed from the configuration file of an instance.

Procedure

1. Start Configuration Tool for an instance. See “Starting Configuration Tool” on page 162.
2. From the task list in the left navigational pane, click **Manage suffixes**.
3. In the **Manage suffixes** page, complete the following steps:
   a. From the **Current suffix DNs** list, select the suffix that you want to remove. For a full directory server, you cannot remove the following system defined suffixes:
      - `cn=localhost`
      - `cn=configuration`
      - `cn=ibmpolicies`
      - `cn=Deleted Objects`
   b. Click **Remove**.
   c. In the **Manage suffixes** confirmation window, click **OK**
   d. To apply the changes, click **OK**.
4. To close the Configuration Tool window, click **File** > **Exit**.
5. To confirm your action, click **Yes**.

What to do next

Start the directory server. See “Starting or stopping a directory server and an administration server with Configuration Tool” on page 163.

Removing a suffix with the command-line utility

Use the command-line utility, **`idsucfgsuf`**, to remove a suffix from an instance.

Before you begin

To remove a suffix from an instance, you must complete the following steps:

- Stop the directory server. See “Starting or stopping a directory server and an administration server with Configuration Tool” on page 163.

About this task

When you remove a suffix to an instance, the suffix entry is removed from the configuration file of an instance. For a full directory server, you cannot remove the following system defined suffixes:

- `cn=localhost`
- `cn=configuration`
- `cn=ibmpolicies`
- `cn=Deleted Objects`

Procedure

1. Log in as directory server instance owner.
2. Access the command prompt.
3. Change the current working directory to the `sbin` subdirectory in the IBM Security Directory Server installation location.
4. To remove the `o=sample` suffix from an instance, run the **idsucfgsuf** command:

   ```
   idsucfgsuf -I instance_name -s "o=sample"
   ```

   For more information about the **idsucfgsuf** command, see *Command Reference*.

What to do next

Start the directory server. See "Starting or stopping a directory server and an administration server with command-line utilities" on page 152.

Schema management

If you want an instance to support custom object classes and attributes, you must add a schema file that defines the custom object classes and attributes.

You can use Configuration Tool or the command-line utilities, such as **idscfgsch** or **idsucfgsch**, to manage the schema files. The schema file must exist on the computer. For more information about the **idscfgsch** command or the **idsucfgsch** command, see *Command Reference*.

You must stop the directory server before you add or remove schema files.

When you add or remove schema files, the configuration file of the instance is updated. You can run the following schema management operations:

- Add a schema file to the list of schema files that is loaded at the server startup.
- Remove a schema file from the list of schema files that gets updated at the server startup.
- Change the type of validation checking that is done for schema files.

You cannot remove the following system-defined schema files:

- `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

You can also use Configuration Tool to specify the schema validation rule to check whether the entries meet the schema rules. The default schema validation rule is Version 3 (Lenient). The following schema validation rules are supported by a directory server:

Version 3 (Strict)
The server runs LDAP version 3 strict validation check against the entries. With this type of validation, all parent object classes must be present when you add entries.

Version 3 (Lenient)
The server runs LDAP version 3 lenient validation check against the entries. With this type of validation, all parent object classes do not require to be present when you add entries. LDAP version 3 lenient is the default schema validation rule.

Version 2
The server runs LDAP version 2 check against the entries.

None The server does not run validation check.

Managing a schema file with Configuration Tool

Use Configuration Tool to manage schema files for an instance.

Before you begin

To manage schema files for an instance, you must complete the following steps:

- Stop the directory server. See "Starting or stopping a directory server and an administration server with Configuration Tool" on page 163.

About this task

When you add or remove a schema file, the configuration file of an instance is updated with the schema entry.

Procedure

1. Start Configuration Tool for an instance. See "Starting Configuration Tool" on page 162.
2. From the task list in the left navigational pane, click **Manage schema files**.
3. In the **Manage schema files** page, choose the operation that you want to run.
   - To add a schema file in the configuration file of an instance, complete the following steps:
     a. In the **Path and file name** field, enter the schema file name with path. You can click **Browse** and specify the schema file name and location.
     b. Click **Add**.
   - To remove a schema file in the configuration file of an instance, complete the following steps:

a. From the **Current schema files** list, select the schema file name that you want to remove.
b. Click **Remove**.
c. In the **Manage schema files** confirmation window, click **OK**.

4. To apply the changes, click **OK**.
5. To close the Configuration Tool window, click **File** > **Exit**.
6. To confirm your action, click **Yes**.

What to do next

Start the directory server. See "Starting or stopping a directory server and an administration server with Configuration Tool" on page 163.

Managing a schema file with the command-line utility

Use the command-line utilities to manage schema files for a directory server instance.

Before you begin

To manage schema files for an instance, you must complete the following steps:

- Stop the directory server. See "Starting or stopping a directory server and an administration server with command-line utilities" on page 152.

About this task

When you add or remove a schema file, the configuration file of an instance is updated with the schema entry.

Procedure

1. Log in as directory server instance owner.
2. Access the command prompt.
3. Change the current working directory to the `sbin` subdirectory in the IBM Security Directory Server installation location.
4. To manage a schema file for an instance, choose the operation that you want to run.
   - To add a schema file for an instance, run the **idscfgsch** command in the following format:

     ```
     idscfgsch -I instance_name -s schema_file.oc
     ```

   - To remove a schema file from an instance, run the **idsucfgsch** command in the following format:

     ```
     idsucfgsch -I instance_name -s schema_file.oc
     ```

   For more information about the **idscfgsch** or **idsucfgsch** command, see *Command Reference*.

What to do next

Start the directory server. See "Starting or stopping a directory server and an administration server with command-line utilities" on page 152.

Configuring schema validation check with Configuration Tool

Use Configuration Tool to configure schema validation check for an instance.

Before you begin

To configure a schema validation rule for an instance, you must complete the following steps:

- Stop the directory server. See "Starting or stopping a directory server and an administration server with Configuration Tool" on page 163.

About this task

When you configure the schema validation check, the configuration file of an instance is updated with the value.

Procedure

1. Start Configuration Tool for an instance. See "Starting Configuration Tool" on page 162.
2. From the task list in the left navigational pane, click **Manage schema files**.
3. Under the **Schema validation rules** area in the **Manage schema files** page, choose one of the following schema validation rules to configure:
   - To configure LDAP version 3 strict validation check, click **Version 3 (Strict)**.
   - To configure LDAP version 3 lenient validation check, click **Version 3 (Lenient)**.
   - To configure LDAP version 2 check, click **Version 2**.
   - To configure LDAP version 2 check, click **None**.
4. To apply the changes, click **OK**.
5. To close the Configuration Tool window, click **File** > **Exit**.
6. To confirm your action, click **Yes**.

What to do next

Start the directory server. See "Starting or stopping a directory server and an administration server with Configuration Tool" on page 163.

LDIF data management

To use directory data, you must add data to a directory server instance from an existing instance or from an LDAP Data Interchange Format (LDIF) file.

You can use Configuration Tool to import data from an LDIF file or to export data from a database to an LDIF file. LDIF is used to represent LDAP entries in text form. When you import data, you can add entries to an empty directory database or to a database that contains entries. You can also use Configuration Tool to validate the data in the LDIF file without adding the data to the directory.

You can add data to an instance that is configured with DB2 database. You must not add directory data to a proxy server instance, as it is not supported.

If you want to import LDIF data from another server instance, you must cryptographically synchronize the server instances. You must synchronize two-way cryptography between directory server instances to reduce the time that is required to encrypt and decrypt data during server communications. When you import an LDIF data that is not cryptographically synchronized, AES encrypted entries in the file are not imported. For more information about synchronize two-way cryptography, see *Command Reference*.

If the server instances are not cryptographically synchronized, provide the encryption seed and encryption salt of the target server when you export an LDIF file from a source server. The AES-encrypted data is decrypted by using the AES keys of the source server and then it is encrypted with the encryption seed and salt values of target server. This encrypted data is stored in the LDIF file.

To import data, you must meet the following requirements before you start the process:

- Import or export of LDIF data is not supported for a proxy server instance or an instance that is not configured with a DB2 database.
- Add the required suffixes on the target server to which you want to import the data. See "Suffix configuration" on page 193.
- You must stop the target server to which you want to import data.

After you load large amounts of data, such as populating the database with **idsbulkload**, you must optimize the database. This operation can improve the performance of the database.

You can also use the following command-line utilities to import, export, or validate LDIF data:

- To import data from an LDIF file, use the **idsldif2db** or the **idsbulkload** utility.
- To export data to an LDIF file, use the **idsdb2ldif** utility.
- To validate the data in the LDIF file, use the **idsbulkload** utility

For more information about the command-line utilities, see *Command Reference*.

Examples

To retrieve the encryption salt value of a server, run the **idsldapsearch** command of the following format:

```
idsldapsearch -h host_name -p port -D adminDN -w adminPWD \
 -b "cn=crypto,cn=localhost" objectclass=* ibm-slapdCryptoSalt

ibm-slapdCryptoSalt=:SxaQ+.qdKor
```

The string after equals sign (=) in the `ibm-slapdCryptoSalt` attribute is the encryption salt. In the example, `:SxaQ+.qdKor` is the encryption salt.

Importing LDIF data with Configuration Tool

Use Configuration Tool to import data to a directory server instance from an LDIF file.

Before you begin

To import data from an LDIF file to an instance, the instance must meet the following requirements:

- A directory server instance that is configured with a DB2 database must exist. See "Configuring a database for an instance with Configuration Tool" on page 167.
- The required suffix entries must be configured. See "Adding a suffix with Configuration Tool" on page 193.
- Stop the directory server. See "Starting or stopping a directory server and an administration server with Configuration Tool" on page 163.

Procedure

1. Start Configuration Tool for an instance. See "Starting Configuration Tool" on page 162.
2. From the task list in the left navigational pane, click **LDIF tasks** > **Import LDIF data**.
3. In the **Import LDIF data** page, complete the following steps:
   a. In the **Path and LDIF file name** field, enter the path and file name of the LDIF file from which you want to import data. You can also click **Browse** and specify the LDIF file name with path.
   b. If you want to remove trailing spaces from the data, select **Remove trailing spaces in Standard import or Bulkload**.
   c. Based on the number of entries that you want to import, select an appropriate option:
      - To import the data by using the **idsldif2db** utility, click **Standard import**. Use this option if the LDIF file contains fewer number of entries.
      - To import the data by using the **idsbulkload** utility, click **Bulkload**. For LDIF files with large number of entries, the **idsbulkload** utility is faster than the **idsldif2db** utility to import data.
   d. If you selected the **Bulkload** option to import data, specify the types of validation you want to run of the LDIF data:
      1) To verify whether the LDIF data conforms to schema, select **Enable schema checking**.
      2) To verify whether the LDIF data contains appropriate ACLs, select **Enable ACL checking**.
   e. To start the import operation, click **Import**.
   f. To confirm the task completion, click **OK**.
   g. Verify the logs that are generated for the LDIF file import operation.
   h. To clear the logs, click **Clear results**.
   i. To close the **Import LDIF data** page, click **Close**.
4. To close the Configuration Tool window, click **File** > **Exit**.
5. To confirm your action, click **Yes**.

What to do next

Start the directory server. See "Starting or stopping a directory server and an administration server with Configuration Tool" on page 163. After you load large amounts of data, such as populating the database with **idsbulkload**, you must optimize the database. For more information about optimizing database, see "Optimizing database with Configuration Tool" on page 178.

Validating LDIF data with Configuration Tool

Use Configuration Tool to validate an LDIF file against the directory server schema without adding the data to the database.

Before you begin

To validate data in an LDIF file with the directory server schema, the instance must meet the following requirements:

- A directory server instance that is configured with a DB2 database must exist. See "Configuring a database for an instance with Configuration Tool" on page 167.

- Stop the directory server. See “Starting or stopping a directory server and an administration server with Configuration Tool” on page 163.

Procedure

1. Start Configuration Tool for an instance. See “Starting Configuration Tool” on page 162.
2. From the task list in the left navigational pane, click **LDIF tasks** > **Import LDIF data**.
3. In the **Import LDIF data** page, complete the following steps:
   a. In the **Path and LDIF file name** field, enter the path and file name of the LDIF file from which you want to import data. You can also click **Browse** and specify the LDIF file name with path.
   b. Click **Data validation only**.
   c. To start the data validation operation, click **Import**.
   d. To confirm the task completion, click **OK**.
   e. Verify the logs that are generated for the data validation operation.
   f. To clear the logs, click **Clear results**.
   g. To close the **Import LDIF data** page, click **Close**.
4. To close the Configuration Tool window, click **File** > **Exit**.
5. To confirm your action, click **Yes**.

What to do next

Start the directory server. See “Starting or stopping a directory server and an administration server with Configuration Tool” on page 163.

Exporting LDIF data with Configuration Tool

Use Configuration Tool to export directory data from an instance to an LDIF file.

Before you begin

To export data from an instance to an LDIF file, the instance must meet the following requirements:

- A directory server instance that is configured with a DB2 database must exist. See “Configuring a database for an instance with Configuration Tool” on page 167.
- The instance must contain directory entries.

Procedure

1. Start Configuration Tool for an instance. See “Starting Configuration Tool” on page 162.
2. From the task list in the left navigational pane, click **LDIF tasks** > **Export LDIF data**.
3. In the **Export LDIF data** page, complete the following steps:
   a. In the **Path and LDIF file name** field, enter the path and file name of the LDIF file to which you want to export data. You can also click **Browse** and specify the LDIF file name with path.
   b. If the file exists and you want to overwrite the file with data, select **Overwrite if file exists**.

c. If you want to export the operation attributes, such as `creatorsName`, `createTimestamp`, `modifiersName`, and `modifyTimestamp`, select **Export operational attributes**. The operational attributes are created and modified by the server when a directory entry is created or modified. The attributes contain information about the user who created or modified the entry and the time the entry was created or modified. These entries are stored as a base-64-encoded control in the LDIF file.

d. To import data to an Advanced Encryption Standard (AES)-enabled destination server and if the server is not cryptographically synchronized with the source server, select **Export data for AES-enabled destination server**.

e. To export entries that are deleted but are still stored in the tombstone subtree, select **Export deleted entries**. For more information about the tombstone subtree, see the *IBM Security Directory Server 6.3.1 Administration Guide*.

f. If you selected **Export data for AES-enabled destination server**, specify the following values:
   - In the **Encryption seed** field, enter the encryption seed of the destination server.
   - In the **Encryption seed** filed, enter the encryption salt of the destination server. For more information about how to retrieve the encryption salt, see "LDIF data management" on page 199.

g. To specify a filter for entries that are exported to the LDIF file, enter the DN of a valid replication filter in the **Filter entry DN** field. The filter exports specific database entries that meet the criteria to the LDIF file. For more information about the replication filters, see the *IBM Security Directory Server 6.3.1 Administration Guide*.

h. If you want to add comments to the LDIF file, enter comments in the **Comments** field.

i. If you want to export entries under a specific subtree, enter the DN of the subtree in the **Subtree DN** field. The subtree DN identifies the top entry of the subtree to write to the LDIF file. The subtree and all entries under it in the directory hierarchy, are written to the file. If you do not specify a subtree DN, all directory entries that are stored in the database are written to the output file. The entries are identified based on the suffixes that are specified in the configuration file of the directory server instance.

j. To start the export operation, click **Export**.

k. To confirm the task completion, click **OK**.

l. Verify the logs that are generated for the export LDIF data operation.

m. To clear the logs, click **Clear results**.

n. To close the **Export LDIF data** page, click **Close**.

4. To close the Configuration Tool window, click **File** > **Exit**.

5. To confirm your action, click **Yes**.

Active Directory synchronization

You can synchronize the entries in the users and groups container that are in Microsoft Active Directory with an IBM Security Directory Server instance. The data synchronization is one way from Active Directory to a directory server instance.

Note: From IBM Security Directory Server, version 6.3.1, the Active Directory synchronization solution is deprecated.

You can use Configuration Tool or the command-line utilities, such as **idsadscfg** and **idsadsrun**, to configure and run Active Directory synchronization.

Note: The synchronization of users and groups from Active Directory to an IBM Security Directory Server instance through IBM Security Directory Proxy Server is not supported.

Active Directory synchronization uses IBM Tivoli Directory Integrator for synchronizing the users and groups containers. You must install IBM Tivoli Directory Integrator before you use Active Directory synchronization.

IBM Tivoli Directory Integrator is required for the following actions:

- Run the configuration
- Start, stop, restart, and monitor operations

You must consider the following points when you configure Active Directory synchronization:

- The Active Directory synchronization application and IBM Tivoli Directory Integrator must be on the same computer as the directory server instance.
- Active Directory synchronization synchronizes only the users and groups container. The tool does not synchronize other objects or containers to a directory server instance.
- The solution also checks the group memberships of the user entry and the user entry is added to any groups in the instance that are synchronized with Active Directory. When an existing user entry is moved out of user container, the user entry is deleted from the instance. The user entry is also deleted from all groups in the instance.
- Active Directory synchronization does not synchronize nested organizational units (`ou`).
- Multiple attributes from Active Directory cannot be mapped to a single attribute in a directory server instance.
- The `userpassword` attribute from Active Directory cannot be mapped to a directory server instance. User password is not synchronized by this solution.
- Active Directory synchronization can synchronize users and groups from one or more user containers of Active Directory to a single organizational unit (`ou`) of a directory server. However, the tool does not synchronize multiple user and group containers of Active Directory to multiple organizational units (`ou`) of a directory server.
- You can specify multiple user containers to synchronize with a single organizational unit (`ou`) in a directory server with the semicolon (`;`) as a separator. Use of other characters as separators are not supported. If you use the semicolon (`;`) as a separator, enclose the argument in quotation marks (`"`). The following example shows semicolon (`;`) as a separator: `"ou=SWUGroups,dc=adsync,dc=com;ou=STGGroups,dc=adsync,dc=com"`.
- The `SAMAccountName` attribute from Active Directory is used to compose the `$dn` attribute in IBM Security Directory Server. The `SAMAccountName` attribute is unique in a domain, there are no conflicts when you synchronize multiple Active Directory user containers to a single organizational unit of a directory server.
- The solution supports a secure connection with Active Directory, but does not support a secure connection to a directory server instance.

- If you change the administrator DN, password, or both for a directory server instance after you configure Active Directory synchronization, you must reconfigure Active Directory synchronization.
- If user or group containers from Active Directory are changed when Active Directory synchronization is running, you must reconfigure Active Directory synchronization with the changed names. Otherwise, the Active Directory synchronization program might not run.
- If you modify IBM Security Directory Server users and groups from any other tool other than Active Directory synchronization, Active Directory synchronization might not work correctly.

Configuring and running Active Directory synchronization

To synchronize user and group containers of Active Directory to an IBM Security Directory Server instance, configure and run Active Directory synchronization.

Before you begin

To configure and run Active Directory synchronization, you must install the following software:

- IBM Security Directory Server
- IBM Tivoli Directory Integrator

Procedure

1. If you installedIBM Tivoli Directory Integrator in a custom path, set the *IDS_LDAP_TDI_HOME* environment variable with the installation path.

   Note: On Windows system, set the environment variable with an installation path that does not contain spaces and quotation marks. Use the short name when you specify the path.
   The following path is the default installation path of IBM Tivoli Directory Integrator:

   AIX and Solaris
   `/opt/IBM/TDI/V7.1`

   Linux `/opt/ibm/TDI/V7.1`

   Windows
   `C:\Program Files\IBM\TDI\V7.1`
2. Optional: Load the sample `users.ldif` and `groups.ldif` files in Active Directory.
3. Run the **idsadscfg** command to configure Active Directory synchronization. You can also run Configuration Tool to configure Active Directory synchronization. The command creates the `adsync_private.prop` and `adsync_public.prop` files.
4. Modify the `adsync_public.prop` file to customize optional attributes and SSL parameters. For information about the files, see *IBM Security Directory Server Administration Guide*. For more information about secure communication, see *IBM Security Directory Server Administration Guide*.
5. Run the **idsadsrun** command to start Active Directory synchronization. The command prompts if you want to fully synchronize, followed by real-time synchronization, or start real-time synchronization. The Active Directory synchronization tool identifies the changes to the Active Directory entries and synchronizes them with the entries in IBM Security Directory Server.

6. Optional: Run IBM Tivoli Directory Integrator Administration and Monitoring Console to administer and monitor the synchronization.

Configuring Active Directory synchronization with Configuration Tool

Use Configuration Tool to configure Active Directory synchronization with a directory server instance.

Before you begin

To configure Active Directory synchronization, you must meet the following requirements:

- Install IBM Tivoli Directory Integrator.
- Stop the directory server. See "Starting or stopping a directory server and an administration server with Configuration Tool" on page 163.

Procedure

1. Start Configuration Tool for an instance. See "Starting Configuration Tool" on page 162.
2. From the task list in the left navigational pane, click **Active directory synchronization**.
3. In the **Active Directory synchronization: Instance Details** page, provide the configuration details for the IBM Security Directory Server instance. The information that you provide are saved in the `adsync_private.properties` and `adsync_public.properties` files. The files are stored in the `etc/tdisoldir` subdirectory of the instance home directory.
4. In the **Directory suffix** field, enter the directory server suffix that you want to use for Active Directory synchronization. The **LDAP URL** field is populated with the URL for the directory server instance. You cannot edit this field.
5. In the **Group container entry DN** field, enter the DN of an existing container to which you want to copy groups from Active Directory. Groups and the memberships of users in groups are synchronized between Active Directory and IBM Security Directory Server. When you add or remove a user from a group in Active Directory, the entry is added or removed from the corresponding group in the IBM Security Directory Server instance.
6. In the **User container entry DN** field, enter the DN of an existing container to which you want to copy users from Active Directory.
7. If you want to use an SSL connection to Active Directory, select **Use SSL connection to Active directory**. SSL connection to IBM Security Directory Server is not supported. For information about steps to configure an SSL connection to Active Directory, see the *IBM Security Directory Server Administration Guide*.
8. Click **Next**. The **Active Directory synchronization: Active Directory details** page opens.
9. In the **Host address** field, enter the host name or IP address of the Active Directory domain controller.
10. In the **Host port** field, enter the port that is used by Active Directory.
11. In the **Login name** field, enter the login name thatIBM Tivoli Directory Integrator must use to bind to Active Directory. The login ID must contain the required permission to read the Active Directory entries that are to be propagated to the directory server instance.

12. In the Login password field, enter the password that IBM Tivoli Directory Integrator must use to bind to Active Directory.
13. In the **Search base** field, enter the subtree in Active Directory from which you want to propagate the changes to the instance. The changes to user entries from the subtree are propagated to the directory server instance. To propagate all users in Active Directory groups to the instance, set the search base to the top of hierarchy in Active Directory.
14. In the **Group container entry DN** field, enter the Active Directory container DN from which you want to synchronize the groups to the instance.
15. In the **User container entry DN** field, enter the Active Directory container DN from which you want to synchronize the user entries to the instance.
16. Click **Finish**. The **Active Directory synchronization: Results** window opens.
17. Verify the log messages that are generated for Active Directory synchronization configuration.
18. To clear the logs, click **Clear results**.
19. To close the **Active Directory synchronization** page, click **Close**.
20. To close the Configuration Tool window, click **File** > **Exit**.
21. To confirm your action, click **Yes**.

Configuring Active Directory synchronization with the command-line utility

Use the command-line utility, **idsadscfg**, to configure Active Directory synchronization with a directory server instance.

Before you begin

To configure Active Directory synchronization, you must meet the following requirements:

- Install IBM Tivoli Directory Integrator.
- Stop the directory server. See "Starting or stopping a directory server and an administration server with command-line utilities" on page 152.

Procedure

1. Log in as root on AIX, Linux, or Solaris, and as an administrator group member on Windows.
2. Access the command prompt.
3. Change the current working directory to the `sbin` subdirectory in the IBM Security Directory Server installation location.
4. To configure Active Directory synchronization with an instance, run the **idsadscfg** command in the following format:

```
idsadscfg -I instance_name -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
```

   For more information about the **idsadscfg** command, see *Command Reference*.

What to do next

Run the **idsadsrun** command to start Active Directory synchronization. For more information about the **idsadsrun** command, see *Command Reference*.

Chapter 20. Autostart of directory server instances at operating system startup

You can configure directory server instances to start automatically when a computer restarts after it is shut down for maintenance or upgrade.

When you create a directory server instance, the administration server starts if the instance creation is successful. To start a directory server with DB2 database, you must start the `ibmslapd` or `idsslapd` process for the instance.

When you restart a computer, you must start both the administration server and `ibmslapd` process that are associated with the instance. However, you can configure services and processes that are associated with an instance to start automatically on your operating system.

To start the directory server instance on AIX, Linux, or Solaris at operating system startup, you must update the `/etc/inittab` file with the server information. The `inittab` file specifies the processes that must be started at system startup and during normal operation. You must add an entry for directory server in the `inittab` file in the following format:

```
id:runlevels:action:process
```

The attributes in the file require`inittab` the following values:

`id` This attribute specifies a 1-4 digit unique ID in the file.

`runlevels`
The `runlevels` attribute indicates the `runlevel` mode of the operating system in which the process starts automatically. It refers to the mode of operation of an AIX, Linux, or Solaris operating system. The `runlevels` attribute configuration differs between operating systems. See your operating system manual for a specific `runlevel` configuration details.

`action` The `action` specifies the action type.

`process`
The `process` attribute specifies the process to start.

Configuring autostart for a directory server instance on Windows

Use the **Services** window to configure autostart of a directory server instance on Windows.

Before you begin

To configure a directory server instance for starting automatically after you start the operating system, your computer must meet the following requirements:

- The computer must contain a directory server instance that can be run in normal mode.

About this task

On Windows, you can start a directory server, the `idsslapd` process, from the **Services** window or with the **`idsslapd`** command. For a directory server instance

with DB2 database, you must set the service that is associated with directory server depend on the DB2 instance service. For a directory server instance with DB2 database, DB2 must start before the idsslapd process can start. If you do not set the dependency and configure the **Startup Type** field to Automatic for the service that is associated with the server, error might occur when you restart the computer. For a proxy server instance, you do not require to configure the dependency on the service that is associated with the DB2 instance.

For a proxy server instance, use the 1, 2, 4, 5, and 6 steps.

Procedure

1. Log in as an administrator group member.
2. To open the **Services** window, complete the following steps:
   a. Click **Start** > **Run**.
   b. In the **Open** field, enter services.msc.
   c. Click **OK**.
3. Find the DB2 service name that is associated with your directory server instance that you want to autostart. The service name starts with DB2 - SDSV631DB2 -. If your DB2 instance name is DSRDBM01, the entry is DB2 - SDSV631DB2 - DSRDBM01. Double-click the service and record the value that comes after DB2 - SDSV631DB2 - in the **Display name** field. In the example, the value is DSRDBM01.
4. Find the service for the directory server instance that you want to autostart. The service name starts with IBM Security Directory Server Instance 6.3.1. If your instance name is dsrdbm01, the entry is IBM Security Directory Server Instance 6.3.1 - dsrdbm01. Double-click the service and record the value that comes after IBM Security Directory Server Instance 6.3.1 - in the **Display name** field. In the example, for the instance, dsrdbm01, the value is idsslapd-dsrdbm01.
5. In the IBM Security Directory Server Instance 6.3.1 - dsrdbm01 Properties window, from the **Startup type** list select Automatic.
6. Click **OK**.
7. To close the **Services** window, click **File** > **Exit**.
8. To open the Windows registry, complete the following steps:
   a. Click **Start** > **Run**.
   b. In the **Open** field, enter regedit.
   c. Click **OK**.
9. On the left navigation pane, go to **My Computer** > **HKEY_LOCAL_MACHINE** > **SYSTEM** > **CurrentControlSet** > **Services**.
10. Find the service that is associated with your directory server instance. In the example, it is idsslapd-dsrdbm01.
11. Click the service that is associated with your instance.
12. On the right pane of the window, double-click the DependOnService attribute.
13. In the **Edit Multi-String** window, add the DB2 service name that is associated with the instance under **LanmanServer**. In the example, it is DSRDBM01.
14. Click **OK**. It creates a dependency on the DB2 service.
15. To close the Windows registry, click **File** > **Exit**.

Results

When you restart the computer, the directory server instance starts automatically.

Configuring autostart for a directory server instance on UNIX

Update the /etc/inittab file with directory server entries to configure autostart of a directory server instance on AIX, Linux, or Solaris.

Before you begin

To configure a directory server instance for starting automatically after you start the operating system, your computer must meet the following requirements:

- The computer must contain a directory server instance that can be run in normal mode.

Procedure

1. Log in as a root user.
2. To configure a directory server instance or a proxy server instance for autostart, add the following entries in the /etc/inittab file:
   a. To add the idsslapd process and administration server that is associated with a directory server instance, add the following entries:

      AIX
      ```
      srv1:2:once:/opt/IBM/ldap/V6.3.1/sbin/idsslapd -I instance_name > /dev/null 2>&1 #Autostart IBM Directory Server Instance

      adm1:2:once:/opt/IBM/ldap/V6.3.1/sbin/ibmdiradm -I instance_name > /dev/null 2>&1 #Autostart IBM Directory Administartion Server
      ```

      Linux
      ```
      srv1:2345:once:/opt/ibm/ldap/V6.3.1/sbin/ibmslapd -I instance_name > /dev/null 2>&1 #Autostart IBM Directory Server Instance

      adm1:2345:once:/opt/ibm/ldap/V6.3.1/sbin/ibmdiradm -I instance_name > /dev/null 2>&1 #Autostart IBM Directory Administartion Server
      ```

      Solaris
      ```
      srv1:234:once:/opt/IBM/ldap/V6.3.1/sbin/ibmslapd -I instance_name > /dev/null 2>&1 #Autostart IBM Directory Server Instance

      adm1:234:once:/opt/IBM/ldap/V6.3.1/sbin/ibmdiradm -I instance_name > /dev/null 2>&1 #Autostart IBM Directory Administartion Server
      ```

      Substitute the *instance_name* variable with your instance name.

   b. To add the idsslapd process and administration server that is associated with a proxy server instance, you must first start the directory server instances. You must start all the directory servers with DB2 database before you start the proxy server. If your computer contains full directory servers and a proxy server, add a delay between the full directory server and the proxy server startup. In the following example, the delay is introduced by adding an entry of the following format, id:2345:wait, the /etc/inittab file.

      AIX
      ```
      srv1:2345:once:/opt/IBM/ldap/V6.3.1/sbin/idsslapd -I instance_name1 > /dev/null 2>&1 #Autostart IBM Directory Server Instance
      ```

```
adm1:2345:once:/opt/IBM/ldap/V6.3.1/sbin/ibmdiradm -I
instance_name1 > /dev/null 2>&1 #Autostart IBM Directory
Administartion Server

srv2:2345:once:/opt/IBM/ldap/V6.3.1/sbin/idsslapd -I
instance_name2 > /dev/null 2>&1 #Autostart IBM Directory
Server Instance

adm2:2345:once:/opt/IBM/ldap/V6.3.1/sbin/ibmdiradm -I
instance_name2 > /dev/null 2>&1 #Autostart IBM Directory
Administartion Server

srv3:2345:wait:/opt/IBM/ldap/V6.3.1/sbin/idsslapd -I
proxy_instance1 -k > /dev/null 2>&1 #Autostart IBM Directory
Proxy Server Instance

adm3:2345:wait:/opt/IBM/ldap/V6.3.1/sbin/ibmdiradm -I
proxy_instance1 -k > /dev/null 2>&1 #Autostart IBM Directory
Administartion Server

srv4:2345:wait:/opt/IBM/ldap/V6.3.1/sbin/idsslapd -I
proxy_instance1 > /dev/null 2>&1 #Autostart IBM Directory
Proxy Server Instance

adm4:2345:wait:/opt/IBM/ldap/V6.3.1/sbin/ibmdiradm -I
proxy_instance1 > /dev/null 2>&1 #Autostart IBM Directory
Administartion Server
```

Substitute the *instance_name1* and *instance_name2* variables with your directory server instance names. Substitute the *proxy_instance1* variable with your proxy server instance name.

Results

After the entries are added to the `/etc/inittab` file, the directory server instance (full or proxy) can autostart after system restart.

Chapter 21. Fix pack strategy

Find information about fix packs and patches for IBM Security Directory Server.

For Windows, IBM Installation Manager-based patches and fix packs will be available.

For Linux 64 and AIX, patches or fix packs will be available in the native method only.

IBM Installation Manager-based patches or fixpacks can be installed in the GUI and in silent installation mode. Script-based installation of fix packs will be available for UNIX systems.

You can identify the version of a patch or fix pack using IBM Installation Manager. You can check the version of the installed fix pack or patch using two ways:

- Select File->View Installed Packages
- Use the imcl command from tools directory of the installation directory of IBM Installation Manager.

On UNIX systems, check the versions of native packages to determine the version of the installed patch or fix pack.

Note: After the native-based fix pack is applied on the base version, no modification or uninstallation should be done by IBM Installation Manager. After you apply the native fix pack, use only the native method for further operations.

Chapter 22. Uninstallation of IBM Security Directory Server and corequisite software

You might want to remove IBM Security Directory Server and its corequisite software if you plan use the computer for a different purpose or plan to retire your computer.

You can use IBM Installation Manager or operating system utilities for uninstallation of IBM Security Directory Server. You must use the same mode for uninstallation that you used for installation. You must use IBM Installation Manager for both installation and uninstallation, or operating system utilities for both installation and uninstallation. You must not use a mix both modes for installation and uninstallation.

If you want to remove IBM Security Directory Server from your computer, consider the following conditions before uninstallation:

1. You must stop all IBM Security Directory Server client and server processes.
   - Directory server
   - Administration server
   - LDAP traces
   - Web Administration Tool and the application server that is associated with it
   - Custom LDAP applications
2. If you plan to run IBM Security Directory Server installation again on the computer, you do not require to delete directory server instance or unconfigure DB2 database from the instance. If you remove IBM Security Directory Server from your computer, the directory server instances are left intact unless you manually remove or unconfigure them.
3. The `idsldap` user and group that were created during the installation of IBM Security Directory Server are left on the system after uninstallation. You must consider the additional conditions before the uninstallation of IBM Security Directory Server form AIX, Linux, or Solaris.
   - If you do not want the `idsldap` user and group that is defined, use the operating system utilities to remove them. The `idsldap` user and group are required by both the proxy server and the full directory server and they must exist on your computer if you contain IBM Security Directory Server installed.
   - If you remove the `idsldap` user and do not remove the home directory of the user, problems can occur when the `idsldap` user is created during installation of IBM Security Directory Server. Therefore, be sure to remove the home directory of the `idsldap` user if you remove the `idsldap` user. If you use the **`userdel`** command to remove the `idsldap` user, be sure to use the **`-r`** parameter to remove the home directory, `userdel -r idsldap`.
4. On Windows, the administration server and directory server services are removed during the uninstallation of IBM Security Directory Server. The services are not replaced during the installation of IBM Security Directory Server. You can use the **`idsslapd`** command to add the server service, and the **`idsdiradm`** command to add the administration server service. For more information about the **`idsslapd`** and **`idsdiradm`** commands, see *IBM Security Directory Server Command Reference*.

Uninstallation with IBM Installation Manager

If you used IBM Installation Manager for the installation of IBM Security Directory Server, use IBM Installation Manager for the uninstallation of IBM Security Directory Server and its components.

When you use IBM Installation Manager for uninstallation of IBM Security Directory Server, the program removes IBM Security Directory Server and all its corequisite software that were installed. You cannot selectively remove features of IBM Security Directory Server during uninstallation with IBM Installation Manager.

If you installed IBM DB2 that is provided with IBM Security Directory Server, you must remove all the DB2 instances that were created with the DB2 copy for successful uninstallation of IBM DB2. If a DB2 instance that was created with the DB2 copy remains on your computer, then during uninstallation of IBM Security Directory Server DB2 is not removed. IBM Installation Manager logs error messages in its log file.

You must either use IBM Installation Manager or operating system utilities for the installation, modification, or uninstallation of IBM Security Directory Server and its components. You must not use both IBM Installation Manager and operating system utilities the installation, modification, or uninstallation of IBM Security Directory Server and its components.

Uninstalling with IBM Installation Manager

Use IBM Installation Manager for uninstallation of IBM Security Directory Server, if you used IBM Installation Manager for installation of IBM Security Directory Server.

Before you begin

You must stop all IBM Security Directory Server client and server processes.

- Directory server
- Administration server
- LDAP traces
- Custom LDAP applications

If any processes are in use, the programs and libraries cannot be removed.

Procedure

1. Start IBM Installation Manager.
   - AIX and Linux:
     a. Open a command-line window and change to the directory that contains IBM Installation Manager. The following directory is the default IBM Installation Manager installation location:
        `opt/IBM/InstallationManager/eclipse`
     b. Run the following command:
        `./IBMIM`
   - Microsoft Windows:
     a. Click **Start** > **All Programs** > **IBM Installation Manager** > **IBM Installation Manager**.
2. Click **Uninstall**.

3. Select **IBM Security Directory Server** with the appropriate version, and then click **Next**.
4. In the **Uninstall Packages** window, review the packages that are selected for uninstall.

   Important: If you choose to continue with an existing version of a DB2 or GSKit during the installation, IBM Installation Manager updates its registry with the feature entry. If you remove a feature that was installed with the **Continue with the existing** option, Installation Manager takes the following actions:

   - Removes the feature entry from the IBM Installation Manager registry.
   - Does not uninstall the feature from the computer.

   If DB2 instances exist that you created with the DB2 copy installed with IBM Installation Manager, you cannot uninstall IBM Security Directory Server. In such situation, you must manually remove the DB2 instances and then try again. It is advisable to take database backup before you remove DB2 instances.
5. Click **Uninstall**. When the uninstallation finishes, IBM Installation Manager indicates whether the uninstallation is a success or failure.
6. Optional: If an error occurs during uninstallation, click **View Log File** to read the details. For more information, see Chapter 5, "IBM Installation Manager log files," on page 41.
7. Click **Finish**.
8. Click **File** > **Exit**.

Results

IBM Installation Manager uninstalls IBM Security Directory Server and its components.

Uninstalling silently with a response file

Complete the steps to uninstall IBM Security Directory Server components silently with a response file.

Before you begin

IBM Installation Manager, version 1.7.0 or later is required for the silent installation of IBM Security Directory Server packages.

About this task

You can use the default response file or record a customized response file and use it as the input file for silent uninstallation.

Procedure

1. Log in to the system as an administrator.
2. Access the **IBMIM** command in the IBM Installation Manager installation location.

Operating system	Default location of the IBMIM command:
Microsoft Windows	`C:\Program Files\IBM\InstallationManager\eclipse`
AIX and Linux	`/opt/IBM/InstallationManager/eclipse`

3. Optional: Run the **IBMIM** command to record a response file for silent uninstallation.
   a. Run the following commands on various operating systems:

      Microsoft Windows

      ```
      IBMIM.exe -record path_name\uninstall_responseFile.xml
      -skipInstall agentDataLocation
      ```

      AIX and Linux

      ```
      ./IBMIM -record path_name/uninstall_responseFile.xml
      -skipInstall agentDataLocation
      ```

      The command opens IBM Installation Manager.
   b. Complete the IBM Security Directory Server uninstallation recording. For more information, see 2 on page 216
4. Run the **IBMIM** command to start silent uninstallation with the response file as input.

Operating system	Command to run:
Microsoft Windows	`IBMIM.exe -silent -input path_name\uninstsll_responseFile.xml -noSplash`
AIX and Linux	`./IBMIM -silent -input path_name/uninstall_responseFile.xml -noSplash`

5. Verify the uninstallation summary and the log files.

Operating system	Default log path:
Microsoft Windows	`C:\ProgramData\IBM\InstallationManager\logs`
AIX and Linux	`/var/ibm/InstallationManager/logs/`

6. Verify whether the IBM Security Directory Server packages are uninstalled.

Operating system	Verifying packages:
Microsoft Windows	See “Verifying IBM Security Directory Server features on Windows” on page 81.
AIX and Linux	See “Verifying IBM Security Directory Server packages” on page 83.

Results

IBM Installation Manager uninstalls IBM Security Directory Server components silently.

Uninstalling silently with the imcl uninstall command

Complete the steps to uninstall IBM Security Directory Server components silently with the **imcl** uninstall command.

Before you begin

IBM Installation Manager, version 1.7.0 or later is required for the silent installation of IBM Security Directory Server packages.

About this task

You can use the **imcl** uninstall command to uninstall IBM Security Directory Server in silent mode.

Procedure

1. Log in to the system as an administrator.
2.
3. Run the **imcl listInstalledPackages** command from the <*IBM_Installation_Manager_install_dir*>/eclipse/tools directory.

Operating system	Command to run
Microsoft Windows	`imcl.exe listInstalledPackages`
AIX and Linux	`./imcl listInstalledPackages`

   This command lists all packages that are installed by IBM Installation Manager.
4. Run **imcl uninstall com.ibm.security.directoryserver.v631_6.3.1.0**. Use the Security Directory Server entry, which will come as output of the above-mentioned command **imcl listInstalledPackages**.

Operating system	Command to run:
Microsoft Windows	`imcl.exe uninstall com.ibm.security.directoryserver.v631_6.3.1.0`
AIX and Linux	`./imcl uninstall com.ibm.security.directoryserver.v631_6.3.1.0`

Results

IBM Installation Manager uninstalls IBM Security Directory Server components silently.

Uninstallation of IBM Security Directory Server with operating system utilities

If you used operating system utilities for the installation of IBM Security Directory Server, use operating system utilities for the uninstallation of IBM Security Directory Server.

You can use operating system utilities for uninstallation of IBM Security Directory Server on computers with AIX, Linux, Solaris, and HP-UX operating systems. On Windows, you must use IBM Installation Manager for installation and uninstallation of IBM Security Directory Server. See “Uninstalling with IBM Installation Manager” on page 216.

When you use operating system utilities for uninstallation of IBM Security Directory Server, the program removes IBM Security Directory Server. You can selectively remove features of IBM Security Directory Server during uninstallation with operating system utilities.

You must stop all IBM Security Directory Server client and server processes before the uninstallation of IBM Security Directory Server.

- Directory server
- Administration server
- LDAP traces
- Web Administration Tool and the application server that is associated with it
- Custom LDAP applications

If you created and configured a directory server instance with DB2 database, they are not removed when you use operating system utilities for uninstallation of IBM Security Directory Server.

Uninstallation with AIX utilities

You can use AIX command-line utilities for uninstallation of IBM Security Directory Server from an AIX system.

You can use one of the following utilities for IBM Security Directory Server uninstallation:

SMIT The preferred uninstallation method is to use the utility. For more information, see "Uninstalling with SMIT."

installp
For more information, see "Uninstalling with **installp**" on page 221.

Uninstalling with SMIT

Use the **smit** command to complete the uninstallation of IBM Security Directory Server from an AIX system.

Before you begin

You must stop all IBM Security Directory Server client and server processes.

- Directory server
- Administration server
- LDAP traces
- Web Administration Tool and the application server that is associated with it
- Custom LDAP applications

Procedure

1. Log in as the root user.
2. Access the command prompt.
3. Run the **smit** command. The **Software Installation and Maintenance** window opens.
4. Select **Software Installation and Maintenance** > **Software Maintenance and Utilities**.
5. Select **Remove Installed Software**.
6. In the **Software Name** field, press **F4** to show the list of installed software. You can provide the `idsldap` value in the field to list all the IBM Security Directory Server packages.
7. Select the packages that you want to remove and press Enter.

Results

The SMIT utility removes IBM Security Directory Server from the AIX system. If you selected to remove all IBM Security Directory Server packages, the utility also removes theIBM Security Directory Server installation directory, `/opt/IBM/ldap/V6.3.1`, from the AIX system.

What to do next

Verify whether the IBM Security Directory Server uninstallation is successful. For more information, see "Verifying IBM Security Directory Server packages" on page 83.

Uninstalling with `installp`

Use the **`installp`** command to complete the uninstallation of IBM Security Directory Server from an AIX system.

Before you begin

You must stop all IBM Security Directory Server client and server processes.

- Directory server
- Administration server
- LDAP traces
- Web Administration Tool and the application server that is associated with it
- Custom LDAP applications

Procedure

1. Log in as the root user.
2. Access the command prompt.
3. Run the following command to determine the IBM Security Directory Server packages that you want to remove:

   ```
   lslpp -l 'idsldap*'
   ```
4. To remove a IBM Security Directory Server package, run the following command:

   ```
   installp -u package_name
   ```

   To remove IBM Security Directory Server completely, remove all the IBM Security Directory Server packages. For uninstallation of IBM Security Directory Server, you must provide packages in reverse order of installation. For more information about the sequence, see "Packages for installation on an AIX system" on page 65. To remove the `idsldap.ent631` package, run the following command:

   ```
   installp -u idsldap.ent631
   ```

What to do next

Verify whether the IBM Security Directory Server uninstallation is successful. For more information, see "Verifying IBM Security Directory Server packages" on page 83.

Uninstallation with Linux utilities

You can use Linux command-line utilities for the uninstallation of IBM Security Directory Server from a Linux system.

IBM Security Directory Server package names are different for computers with different operating systems and architecture. You must verify the installed IBM Security Directory Server packages before uninstallation.

Uninstalling with Linux utilities

Use the **rpm** command to complete the uninstallation of IBM Security Directory Server from a Linux system.

Before you begin

You must stop all IBM Security Directory Server client and server processes.

- Directory server
- Administration server
- LDAP traces
- Web Administration Tool and the application server that is associated with it
- Custom LDAP applications

About this task

The following example shows the uninstallation of IBM Security Directory Server packages from an AMD64 Opteron/EM64T Linux system. For System z, System i or System p, or System x Linux, you must substitute with the appropriate package names.

Procedure

1. Log in as the root user.
2. Access the command prompt.
3. Run the following command to determine the IBM Security Directory Server packages that you want to remove:

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

4. To remove a IBM Security Directory Server package, run the following command:

   ```
   rpm -ev package_name
   ```

   To remove IBM Security Directory Server completely, remove all the IBM Security Directory Server packages. For uninstallation of IBM Security Directory Server, you must provide packages in reverse order of installation sequence. For more information about the sequence, see "Packages for installation on a Linux system" on page 71. To remove the `idsldap-srv64bit631-6.3.1-0.x86_64.rpm` package, run the following command:

   ```
   rpm -ev idsldap-srv64bit631-6.3.1-0.x86_64.rpm
   ```

What to do next

Verify whether the IBM Security Directory Server uninstallation is successful. For more information, see "Verifying IBM Security Directory Server packages" on page 83.

Uninstallation with Solaris utilities

You can use Solaris command-line utilities for the uninstallation of IBM Security Directory Server from a Solaris system.

IBM Security Directory Server package names are same for Solaris SPARC and Solaris X64 systems.

Uninstalling with Solaris utilities

Use the **pkgrm** command to complete the uninstallation of IBM Security Directory Server from a Solaris system.

Before you begin

You must stop all IBM Security Directory Server client and server processes.

- Directory server
- Administration server
- LDAP traces
- Web Administration Tool and the application server that is associated with it
- Custom LDAP applications

Procedure

1. Log in as the root user.
2. Access the command prompt.
3. Run the following command to determine the IBM Security Directory Server packages that you want to remove:

   ```
   pkginfo | grep -i IDSl
   ```

4. To remove a IBM Security Directory Server package, run the following command:

   ```
   pkgrm package_name
   ```

   To remove IBM Security Directory Server completely, remove all the IBM Security Directory Server packages. For uninstallation of IBM Security Directory Server, you must provide packages in reverse order of installation sequence. For more information about the sequence, see "Packages for installation on a Solaris system" on page 74. To remove the `IDSlent631` package, run the following command:

   ```
   pkgrm IDSlent631
   ```

What to do next

Verify whether the IBM Security Directory Server uninstallation is successful. For more information, see "Verifying IBM Security Directory Server packages" on page 83.

Uninstallation with HP-UX utilities

You can use HP-UX command-line utilities for the uninstallation of IBM Security Directory Server from an HP-UX system.

On HP-UX (Itanium) computers, only IBM Security Directory Server client packages are supported.

Uninstalling with HP-UX utilities

Use the **swremove** command to complete the uninstallation of IBM Security Directory Server from an HP-UX system.

Before you begin

You must stop all IBM Security Directory Server client processes.

- LDAP traces
- Custom LDAP applications

Procedure

1. Log in as the root user.
2. Access the command prompt.
3. Run the following command to determine the IBM Security Directory Server packages that you want to remove:

   ```
   swlist | grep -i idsldap
   ```
4. To remove a IBM Security Directory Server package, run the following command:

   ```
   swremove package_name
   ```

   To remove IBM Security Directory Server completely, remove all the IBM Security Directory Server packages. For uninstallation of IBM Security Directory Server, you must provide packages in reverse order of installation sequence. For more information about the sequence, see "Packages for installation on an HP-UX Itanium system" on page 78. To remove the `idsldap.cltjava631.depot` package, run the following command:

   ```
   swremove idsldap.cltjava631.depot
   ```

What to do next

Verify whether the IBM Security Directory Server uninstallation is successful. For more information, see "Verifying IBM Security Directory Server packages" on page 83.

Uninstallation of IBM DB2 with DB2 commands

If you installed the IBM DB2 copy that is provided with IBM Security Directory Server manually, use the DB2 commands to remove IBM DB2 from the computer.

If you installed the IBM DB2 copy with IBM Installation Manager during the installation of IBM Security Directory Server, IBM DB2 is installed in a predefined location. For more information about the default location, see "Default installation locations" on page 25. If you installed the IBM DB2 copy with IBM Installation Manager, you must use IBM Installation Manager for uninstallation of IBM DB2.

If your computer contains DB2 instances for the IBM DB2 copy, you must manually drop the DB2 instances before the uninstallation of IBM DB2. It is advisable to back up DB2 databases and data before the uninstallation.

If you manually installed IBM DB2 in a custom location with DB2 commands, use DB2 commands for uninstallation of IBM DB2. On AIX, Linux, and Solaris, run the **db2_deinstall** command in the *DB2_instalaton_location*`/install/` directory for uninstallation of IBM DB2. On Windows, run the **db2unins** command in the *DB2_instalaton_location*`\bin` directory for uninstallation of IBM DB2. For more information about the uninstallation of IBM DB2, see the IBM DB2 documentation at http://pic.dhe.ibm.com/infocenter/db2luw/v9r7/topic/com.ibm.db2.luw.doc/welcome.html.

Uninstallation of IBM Global Security Kit with operating system utilities

If you used operating system utilities for the installation of IBM Global Security Kit (GSKit), use operating system utilities for the uninstallation of GSKit.

You can use operating system utilities for uninstallation of GSKit from computers with AIX, Linux, Solaris, and HP-UX operating systems.

On Windows, you can run GSKit uninstallation manually only if you selected to use an installed GSKit version with IBM Installation Manager during the installation. If IBM Security Directory Server is installed on your computer, you must not remove GSKit if it is in use. If you want to use the latest GSKit version, you must use IBM Installation Manager to modify the GSKit feature to remove it from its registry. You can then run GSKit uninstallation.

Uninstalling IBM Global Security Kit with SMIT

Use the **smit** command to complete the uninstallation of IBM Global Security Kit (GSKit) from an AIX system.

Procedure

1. Log in as the root user.
2. Access the command prompt.
3. Run the **smit** command. The **Software Installation and Maintenance** window opens.
4. Select **Software Installation and Maintenance** > **Software Maintenance and Utilities**.
5. Select **Remove Installed Software**.
6. In the **Software Name** field, press **F4** to show the list of installed software. You can provide the `GSKit` value in the field to list all the GSKit packages.
7. Set the value for **REMOVE dependent software** to `YES` to remove software products and updates that are dependent upon the product you are removing.
8. Select the packages that you want to remove and press Enter.
9. Verify whether the GSKit uninstallation is successful.

   ```
   lslpp -l 'GSK*'
   ```

Uninstalling IBM Global Security Kit with `installp`

Use the **installp** command to complete the uninstallation of IBM Global Security Kit (GSKit) from an AIX system.

Procedure

1. Log in as the root user.
2. Access the command prompt.
3. Run the following command to determine the GSKit packages that you want to remove:

   ```
   lslpp -l 'GSK*'
   ```
4. To remove a GSKit package, run the following command:

   ```
   installp -u package_name
   ```

   To remove GSKit completely, remove all the GSKit packages of the same version. For uninstallation of GSKit, you must first remove the GSKit SSL

package and then the GSKit crypt package. To remove the GSKit8.gskssl64.ppc.rte and GSKit8.gskcrypt64.ppc.rte packages, run the following command:

```
installp -u GSKit8.gskssl64.ppc.rte
installp -u GSKit8.gskcrypt64.ppc.rte
```

5. Verify whether the GSKit uninstallation is successful.

```
lslpp -l 'GSK*'
```

Uninstalling IBM Global Security Kit with Linux utilities

Use the **rpm** command to complete the uninstallation of IBM Global Security Kit (GSKit) from a Linux system.

About this task

The following example shows the uninstallation of GSKit packages from an AMD64 Opteron/EM64T Linux system. For System z, System i or System p, or System x Linux, you must substitute with the appropriate package names.

Procedure

1. Log in as the root user.
2. Access the command prompt.
3. Run the following command to determine the GSKit packages that you want to remove:

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

4. To remove a GSKit package, run the following command:

```
rpm -ev package_name
```

To remove GSKit completely, remove all the GSKit packages of the same version. For uninstallation of GSKit, you must first remove the GSKit SSL package and then the GSKit crypt package. To remove the gskssl64-8.0-14.26.x86_64 and gskcrypt64-8.0-14.26.x86_64 packages, run the following command:

```
rpm -ev gskssl64-8.0-14.26.x86_64
rpm -ev gskcrypt64-8.0-14.26.x86_64
```

5. Verify whether the GSKit uninstallation is successful.

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

Uninstalling IBM Global Security Kit with Solaris utilities

Use the **pkgrm** command to complete the uninstallation of IBM Global Security Kit (GSKit) from a Solaris system.

Procedure

1. Log in as the root user.
2. Access the command prompt.
3. Run the following command to determine the GSKit packages that you want to remove:

```
pkginfo | grep -i gsk
```

4. To remove a GSKit package, run the following command:

```
pkgrm package_name
```

To remove GSKit completely, remove all the GSKit packages of the same version. For uninstallation of GSKit, you must first remove the GSKit SSL package and then the GSKit crypt package. To remove the `gsk8ssl64` and `gsk8cry64` packages, run the following command:

```
pkgrm gsk8ssl64
pkgrm gsk8cry64
```

5. Verify whether the GSKit uninstallation is successful.

```
pkginfo | grep -i gsk
```

Uninstalling IBM Global Security Kit with HP-UX utilities

Use the **swremove** command to complete the uninstallation of IBM Global Security Kit (GSKit) from an HP-UX system.

Procedure

1. Log in as the root user.
2. Access the command prompt.
3. Run the following command to determine the GSKit packages that you want to remove:

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

4. To remove a GSKit package, run the following command:

```
swremove package_name
```

To remove GSKit completely, remove all the GSKit packages of the same version. For uninstallation of GSKit, you must first remove the GSKit SSL package and then the GSKit crypt package. To remove the `gskssl64` and `gskcrypt64` packages, run the following command:

```
swremove gskssl64
swremove gskcrypt64
```

5. Verify whether the GSKit uninstallation is successful.

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

Uninstalling IBM Global Security Kit on Windows

Use the IBM Global Security Kit (GSKit) commands to complete the uninstallation of GSKit from a Windows system.

About this task

In the example, silent uninstallation of the GSKit SSL 64-bit and GSKit crypt 64-bit packages from a Windows system on an AMD64/EM64T architecture is shown. For a Windows operating system on an IA32/x86 architecture the GSKit package names are different. For information about GSKit package names, see Chapter 9, “Installation of IBM Global Security Kit,” on page 53.

Note: You can also use **Start** > **Control Panel** > **Add or Remove Programs** to remove the GSKit packages.

Procedure

1. Log in as a member of the administrator group.
2. Access the command prompt.
3. Change the current working directory to the `gskit` directory where the IBM Global Security Kit installable is stored.

4. To remove GSKit 64-bit packages silently, run the following commands: To remove GSKit completely, remove all the GSKit packages of the same version. For uninstallation of GSKit, you must first remove the GSKit SSL package and then the GSKit crypt package.

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

Uninstallation of language packs

To complete the uninstallation of IBM Security Directory Server, you must uninstall language packs that you installed on your computer.

If you installed IBM Security Directory Server and language packs on your computer with IBM Installation Manager, you must use IBM Installation Manager for uninstallation of language packs.

If you used operating system utilities for installation of language packs, use the operating system utilities for uninstallation of language packs.

All the language packs are uninstalled from your system, if you do not select the Proxy Server or Server feature for the installation.

Uninstalling language packs with operating system utilities

Use the operating system utilities to complete the uninstallation of a language pack if you installed language pack with the operating system utilities.

Before you begin

You must stop all IBM Security Directory Server client and server processes before the uninstallation of IBM Security Directory Server language packs.

- Directory server
- Administration server
- LDAP traces
- Custom LDAP applications

Procedure

1. Log in as the root user.
2. Access the command prompt.
3. Determine the language packs on your computer that you want to remove:

Operating system	Command to run:
AIX	`lslpp -l 'idsldap.msg631*'`
Linux	`rpm -qa | grep -i idsldap-msg631`
Solaris	`pkginfo | grep IDSl`

4. To uninstall the language pack for a language, run the package uninstallation commands. In the following example, the uninstallation of language pack for the French language is shown. You can uninstall any language pack by replacing with the appropriate package names for the operating system.

Operating system	Command to run:
AIX	`installp -u idsldap.msg631.fr_FR`

Operating system	Command to run:
Linux	`rpm -ev idsldap-msg631-fr-6.3.1-0.noarch.rpm`
Solaris	`pkgrm IDSlfr631`

5. Verify whether the language pack installation is successful. For more information, see "Verifying IBM Security Directory Server packages" on page 83.

Appendix A. Directory Services Markup Language

You can use Directory Services Markup Language to represent the directory structure information, directory queries and updates, and results of directory operations in XML format.

When you complete the installation of IBM Security Directory Server Web Administration Tool, an archive file of Directory Services Markup Language (DSML) files, `DSML.zip`, are stored on your computer. The `DSML.zip` is stored in the `idstools` subdirectory in IBM Security Directory Server installation location. For more information about the default IBM Security Directory Server installation location, see "Default installation locations" on page 25.

The `DSML.zip` file contains DSML installable and documentation that guides you with DSML installation, configuration, usage. The `DSML.zip` file contains the following files:

`DSMLReadme.txt`
The `DSMLReadme.txt` files lists the files in the package and instruction for the installation and configuration of DSML.

`dsml.pdf`
The `dsml.pdf` file is in PDF format and describes how to use DSML.

`dsml.htm`
The `dsml.htm` file is in HTML format and describes how to use DSML.

Appendix B. Accessibility features for Security Directory Server

Accessibility features help a user who has a physical disability, such as restricted mobility or limited vision, to use information technology products successfully.

The major accessibility features in this product enable users to do the following:

- Use assistive technologies, such as screen-reader software, to hear what is displayed on the screen. Consult the product documentation of the assistive technology for details on using those technologies with this product.
- Operate specific or equivalent features using only the keyboard.
- Magnify what is displayed on the screen.

In addition, the product documentation was modified to include the following features to aid accessibility:

- All documentation is available in HTML formats to give the maximum opportunity for users to apply screen-reader software.
- All images in the documentation are provided with alternative text so that users with vision impairments can understand the contents of the images.

Accessibility

The following list includes the major accessibility features in IBM Security Directory Server.

- Supports keyboard-only operation
- Supports interfaces commonly used by screen readers
- Keys are tactilely discernible and do not activate just by touching them

The IBM Security Directory Server documentation is accessibility-enabled. The accessibility features of the documentation are described in the online documentation set.

Keyboard navigation

Standard shortcut and accelerator keys are used by the product and are documented by the operating system. Refer to the documentation provided by your operating system for more information.

This product uses standard Microsoft Windows navigation keys.

Magnifying what is displayed on the screen

You can enlarge information on the product windows using facilities provided by the operating systems on which the product is run. For example, in a Microsoft Windows environment, you can lower the resolution of the screen to enlarge the font sizes of the text on the screen. Refer to the documentation provided by your operating system for more information.

IBM and accessibility

See the IBM Human Ability and Accessibility Center for more information about the commitment that IBM has to accessibility: `http://www.ibm.com/able`

Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law :

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to

IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Index

E

F

G

H

I

L

T

U

V

W

Printed in USA

SC27-2747-01