Installation Guide

iPlanet Directory Server

Version 5.0

816-0798-01
April 2001

Contents

About This Guide

Welcome to iPlanet Directory Server. This manual provides a high-level overview of design and planning decisions you need to make before installing the iPlanet Directory Server, and describes the different installation methods that you can use.

Prerequisite Reading

Before you install Directory Server, we recommend that you read the *iPlanet Directory Server Deployment Guide*. The *Deployment Guide* covers key concepts on how to design and plan your directory service.

After you finish planning your directory service, follow the steps in this installation guide to install the iPlanet Directory Server and its related software components.

iPlanet Directory Server 5.0 Overview

iPlanet Directory Server 5.0 provides the following key features:

- Multi-master replication—Provides a highly available directory service for both read and write operations. Multi-master replication can be combined with simple and cascading replication scenarios to provide a highly flexible and scalable replication environment.
- Chaining and referrals—Increases the power of your directory by storing a complete logical view of your directory on a single server while maintaining data on a large number of directory servers, transparently for clients.
- Roles and Class of Service—Provides a flexible mechanism for grouping and sharing attributes between entries in a dynamic fashion.
- Improved access control mechanism—Provides support for macros that dramatically reduce the number of access control statements used in the directory, and increase the speed of access control evaluation.

- Resource-limits by bind DN—Gives you the power to control the amount of server resources allocated to search operations based on the bind DN of the client.
- Multiple databases—Provides a simple way of breaking down your directory data to simplify the implementation of replication and chaining in your directory service.
- Password Policy and Account Lockout—Allows you to define a set of rules that govern how passwords and user accounts are managed in the directory server.
- SSL—Provides secure communications over the network including ciphers with up to 168-bit encryption.

The major components of iPlanet Directory Server 5.0 include:

- An LDAP server—The core of the directory service, provided by the `slapd` daemon, and compliant with the LDAP v3 Internet standards.
- Directory Server Console—An improved management console that dramatically reduces the effort of setting up and maintaining your directory service. The directory console is part of iPlanet Console, the common management framework for iPlanet servers.
- Directory Server Gateway—A customizable HTTP to LDAP client that allows you to access directory data from a web browser.
- iPlanet Directory Express—A simple directory lookup tool that you can use right out of the box.
- SNMP Agent—Permits you to monitor your directory server in real time using the Simple Network Management Protocol (SNMP).
- Online backup and restore—Allows you to create backups and restore from backups while the server is running.

Conventions Used In This Guide

This section explains the conventions used in this book.

Monospaced font—This typeface is used for any text that appears on the computer screen or text that you should type. It is also used for filenames, functions, and examples.

NOTE	Notes and Cautions mark important information. Make sure you read the information before continuing with a task.

The greater than symbol (>) is used as a separator for successive menu selections. For example, Object > New > User means that you should pull down the Object menu, drag the mouse down to highlight New, and drag the mouse across to the New submenu in which you must select User.

Throughout this book you will see path references of the form:

`/usr/iplanet/servers/slapd-`*`serverID`*`/...`

The `/usr/iplanet/servers` directory is the default installation directory. If you have installed Directory Server in a different location, you should adapt the path accordingly. *serverID* represents the server identifier you gave the server when you installed it. For example, if you gave the server an identifier of **phonebook**, then the actual path would be:

`/usr/iplanet/servers/slapd-phonebook/. . .`

All paths specified in this manual are in UNIX format. If you are using a Windows NT-based directory server, you should assume the NT equivalent file paths whenever UNIX file paths are shown in this guide.

Related Information

The document set for iPlanet Directory Server also contains the following guides:

iPlanet Directory Server Administrator's Guide. Procedures for the day-to-day maintenance of your directory service. Includes information on configuring server-side plug-ins.

iPlanet Directory Server Deployment Guide. Procedures for the day-to-day maintenance of your directory service. Includes information on configuring server-side plug-ins.

iPlanet Directory Server Configuration, Command, and File Reference. Information about using the command-line scripts shipped with Directory Server.

iPlanet Schema Reference. Information about all the schema used in the iPlanet suite of products.

Other useful iPlanet information can be found at the following Internet locations:

- iPlanet release notes and other documentation:
  http://docs.iplanet.com/docs/manuals/
- iPlanet product status:
  http://www.iplanet.com/support/technical_resources/
- iPlanet Professional Services information:
  http://www.iplanet.com/services/pro_serv/index.html
- iPlanet developer information:
  http://developer.iplanet.com/
- iPlanet learning solutions:
  http://www.iplanet.com/learning/index.html
- iPlanet product data sheets:
  http://www.iplanet.com/products/index.html
- iPlanet product technical support
  http://www.iplanet.com/support

Chapter 1

Preparing for a Directory Server Installation

Before you begin installing iPlanet Directory Server, you should have an understanding of the various Directory Server components and the design and configuration decisions you need to make.

To help you prepare for your iPlanet Directory Server installation, you should be familiar with the concepts contained in the following sections:

- Installation Components
- Configuration Decisions
- Installation Process Overview
- Installation Privileges
- Unsetting Environment Variables (AIX only)

The *iPlanet Directory Server Deployment Guide* contains basic directory concepts as well as guidelines to help you design and successfully deploy your directory service. Be sure you understand the concepts presented in this manual before proceeding with the installation process.

Installation Components

iPlanet Directory Server contains the following software components:

- **iPlanet Console**—iPlanet Console provides the common user interface for all iPlanet server products. From it you can perform common server administration functions such as stopping and starting servers, installing new server instances, and managing user and group information. iPlanet Console can be installed as a stand-alone application on any machine. You can also install it on your network and use it to manage remote servers.
- **Administration Server**—Administration Server is a common front-end to all iPlanet servers. It receives communications from iPlanet Console and passes those communications on to the appropriate iPlanet server. Your site will have at least one Administration Server for each server root in which you have installed an iPlanet server.
- **Directory Server**—Directory Server is iPlanet's LDAP implementation. The Directory Server runs as the `ns-slapd` process (on UNIX) or `slapd` service (on Windows NT, and Windows 2000). This is the server that manages the directory databases and responds to client requests. Directory Server is a required component.
- **Directory Server Gateway**—Directory Server Gateway (DSGW) is automatically installed when you install Directory Server. Directory Server Gateway is an LDAP client that you can access from a web browser. You use LDAP clients to access or change directory information. You can access the gateway either from Administration Server or you can configure a web server to manage the gateway.
- **iPlanet Directory Express**—Directory Express is a customized version of the Directory Server Gateway. iPlanet Directory Express is intended for read-only directory access such as might be required for corporate phone book usage. iPlanet Directory Express is installed and managed in the same way as the Directory Server Gateway.

The order in which you install and configure the various components depends on whether you are performing a new installation or an upgrade. See "Installation Process Overview," on page 19 for details.

Configuration Decisions

During Directory Server installation, you are prompted for basic configuration information. Decide how you are going to configure these basic parameters before you begin the installation process. You are prompted for some or all of following information, depending on the type of installation that you decide to perform:

- Port number (see "Choosing Unique Port Numbers," on page 13).

- Server root (see “Creating a New Server Root,” on page 14).
- Users and groups to run the server as (see “Deciding the User and Group for Your iPlanet Servers (UNIX only),” on page 14).
- Your directory suffix (see “Determining Your Directory Suffix,” on page 16).
- Several different authentication user IDs (see “Defining Authentication Entities,” on page 15).
- The location of the configuration and user Directory Servers (see “Determining the Location of the Configuration Directory,” on page 17 and “Determining the Location of the User Directory”).
- The administration domain (see “Determining the Administration Domain,” on page 19).
- For security reasons, it is recommended that you turn off Directory Server Gateway if it is not going to be used.

Choosing Unique Port Numbers

Port numbers can be any number from 1 to 65535. Keep the following in mind when choosing a port number for your Directory Server:

- The standard Directory Server (LDAP) port number is 389.
- Port 636 is reserved from LDAP over SSL. Therefore, do not use port number 636 for your standard LDAP installation, even if 636 is not already in use. You can also use LDAP over TLS on the standard LDAP port.
- Port numbers between 1 and 1024 have been assigned to various services by the Internet Assigned Numbers Authority. Do not use port numbers below 1024 other than 389 or 636 for directory services as they will conflict with other services.
- On UNIX platforms, Directory Server must be run as root if will listen on either port 389 or 636.
- On Windows NT and Windows 2000, the directory service must have administrative privileges if it will use ports 389 or 636.
- Make sure the ports you choose are not already in use. Additionally, if you are using both LDAP and LDAPS communications, make sure the port numbers chosen for these two types of access are not identical.

For information on how to set up LDAP over SSL (LDAPS) for Directory Server, see the *iPlanet Directory Server Administrator's Guide*.

Creating a New Server Root

Your server root is the directory where you install your iPlanet servers. The default server root for iPlanet Directory Server is `/usr/iplanet/servers`.

The server root must meet the following requirements:

- The server root must be a directory on a local disk drive; you cannot use a networked drive for installation purposes. The file sharing protocols such as AFS, NFS and SMB do not provide file locking and performance suitable for use by the Directory Server. The server database index files may be damaged if they are not held on a local file system.
- The directory must not already exist or must be empty.
- The server root directory must not be the same as the directory from which you are running the setup program.

By default, the server root directory is one of the following:

- `/usr/iplanet/servers` (on UNIX systems)
- `c:\iplanet\servers` (on Windows NT and Windows 2000 systems)

Deciding the User and Group for Your iPlanet Servers (UNIX only)

For security reasons, it is always best to run UNIX-based production servers with normal user privileges. That is, you do not want to run Directory Server with root privileges. However, you will have to run Directory Server with root privileges if you are using the default Directory Server ports. If Directory Server is to be started by Administration Server, Administration Server must run either as root or as the same user as Directory Server.

You must therefore decide what user accounts you will use for the following purposes:

- The user and group under which you will run Directory Server.

  If you will not be running the directory server as root, it is strongly recommended that you create a user account for all iPlanet servers. You should not use any existing operating system account, and must not use the nobody account. Also you should create a common group for the directory server files; again, you must not use the nobody group.

- The user and group under which you will run Administration Server.

  For installations that use the default port numbers, this must be root. However, if you use ports over 1024, then you should create a user account for all iPlanet servers, and run Administration Server as this account.

  As a security precaution, when Administration Server is being run as root, it should be shut it down when it is not in use.

You should use a common group for all iPlanet servers, such as `gid iPlanet`, to ensure that files can be shared between servers when necessary.

Before you can install Directory Server and Administration Server, you must make sure that the user and group accounts you will use exist on your system.

Defining Authentication Entities

As you install iPlanet Directory Server and Administration Server, you will be asked for various user names, distinguished names (DN), and passwords. This list of login and bind entities will differ depending on the type of installation that you are performing:

- Directory Manager DN and password.

  The Directory Manager DN is the special directory entry to which access control does not apply. Think of the directory manager as your directory's superuser. (In former releases of Directory Server, the Directory Manager DN was known as the root DN).

  The default Directory Manager DN is `cn=Directory Manager`. Because the Directory Manager DN is a special entry, the Directory Manager DN does not have to conform to any suffix configured for your Directory Server. Therefore, you must not manually create an actual Directory Server entry that has the same DN as the directory manager DN.

  The Directory Manager password must be at least 8 characters long, and is limited to ASCII letters, digits, and symbols.

- Configuration Directory Administrator ID and password.

  The configuration directory administrator is the person responsible for managing all the iPlanet servers accessible through iPlanet Console. If you log in with this user ID, then you can administer any iPlanet server that you can see in the server topology area of iPlanet Console.

  For security, the configuration directory administrator should not be the same as the directory manager. The default configuration directory administrator ID is `admin`.

- Administration Server User and password.

  You are prompted for this only during custom installations. The Administration Server user is the special user that has all privileges for the local Administration Server. Authentication as this person allows you to administer all the iPlanet servers stored in the local server root.

  Administration Server user ID and password is used only when the Directory Server is down and you are unable to log in as the configuration directory administrator. The existence of this user ID means that you can access Administration Server and perform disaster recovery activities such as starting Directory Server, reading log files, and so forth.

  Normally, Administration Server user and password should be identical to the configuration directory administrator ID and password.

Determining Your Directory Suffix

A directory suffix is the directory entry that represents the first entry in a directory tree. You will need at least one directory suffix for the tree that will contain your enterprise's data. It is common practice to select a directory suffix that corresponds to the DNS host name used by your enterprise. For example, if your organization uses the DNS name `siroe.com`, then select a suffix of `dc=siroe,dc=com`.

For more information on planning the suffixes for your directory service, see the *iPlanet Directory Server Deployment Guide.*

Determining the Location of the Configuration Directory

Many iPlanet servers including Directory Server 5.0 use an instance of Directory Server to store configuration information. This information is stored in the `o=NetscapeRoot` directory tree. It does not need to be held on the same Directory Server as your directory data. Your *configuration directory* is the Directory Server that contains the `o=NetscapeRoot` tree used by your iPlanet servers.

If you are installing Directory Server only to support other iPlanet servers, then that Directory Server is your configuration directory. If you are installing Directory Server to use as part of a general directory service, then you will have multiple Directory Servers installed in your enterprise and you must decide which one will host the configuration directory tree, `o=NetscapeRoot`. You must make this decision before you install any iPlanet servers (including iPlanet Directory Server).

For ease of upgrades, you should use a Directory Server instance that is dedicated to supporting the `o=NetscapeRoot` tree; this server instance should perform no other function with regard to managing your enterprise's directory data. Also, do not use port 389 for this server instance because doing so could prevent you from installing a Directory Server on that host that can be used for management of your enterprise's directory data.

Because the configuration directory normally experiences very little traffic, you can allow its server instance to coexist on a machine with another more heavily loaded Directory Server instance. However, for very large sites that are installing a large number of iPlanet servers, you may want to dedicate a low-end machine to the configuration directory so as to not hurt the performance of your other production servers. iPlanet server installations result in write activities to the configuration directory. For large enough sites, this write activity could result in a short-term performance hit to your other directory activities.

Also, as with any directory installation, consider replicating the configuration directory to increase availability and reliability. See the *iPlanet Directory Server Deployment Guide* for information on using replication and DNS round robins to increase directory availability.

CAUTION Corrupting the configuration directory tree can result in the necessity of reinstalling all other iPlanet servers that are registered in that configuration directory. Remember the following guidelines when dealing with the configuration directory:

- Always back up your configuration directory after you install a new iPlanet server.
- Never change the host name or port number used by the configuration directory.
- Never directly modify the configuration directory tree. Only the setup program for the various iPlanet servers should ever modify the configuration.

Determining the Location of the User Directory

Just as the configuration directory is the Directory Server that is used for iPlanet server administration, the *user directory* is the Directory Server that contains the entries for users and groups in your enterprise.

For most directory installations, the user directory and the configuration directory should be two separate server instances. These server instances can be installed on the same machine, but for best results you should consider placing the configuration directory on a separate machine.

Between your user directory and your configuration directory, it is your user directory that will receive the overwhelming percentage of the directory traffic. For this reason, you should give the user directory the greatest computing resources. Because the configuration directory should receive very little traffic, it can be installed on a machine with very low-end resources (such as a minimally-equipped Pentium).

Also, you should use the default directory ports (389 and 636) for the user directory. If your configuration directory is managed by a server instance dedicated to that purpose, you should use some non-standard port for the configuration directory.

You cannot install a user directory until you have installed a configuration directory somewhere on your network.

Determining the Administration Domain

The administration domain allows you to logically group iPlanet servers together so that you can more easily distribute server administrative tasks. A common scenario is for two divisions in a company to each want control of their individual iPlanet servers. However, you may still want some centralized control of all the servers in your enterprise. Administration domains allow you to meet these conflicting goals.

Administration domains have the following qualities:

- All servers share the same configuration directory, regardless of the domain they belong to.
- Servers in two different domains may use two different user directories for authentication and user management.
- The configuration directory administrator has complete access to all installed iPlanet servers, regardless of the domain that they belong to.
- Each administration domain can be configured with an administration domain owner. This owner has complete access to all the servers in the domain but does not have access to the servers in any other administration domain.
- The administration domain owner can grant individual users administrative access on a server by server basis within the domain.

For many installations, you can have just one administration domain. In this case, choose a name that is representative of your organization. For other installations, you may want different domains because of the demands at your site. In the latter case, try to name your administration domains after the organizations that will control the servers in that domain.

For example, if you are an ISP and you have three customers for whom you are installing and managing iPlanet servers, create three administration domains each named after a different customer.

Installation Process Overview

You can use one of several installation processes to install Directory Server. Each one guides you through the installation process and ensures that you install the various components in the correct order.

The following sections outline the installation processes available, how to upgrade from an earlier release of iPlanet Directory Server, and how to unpack the software to prepare for installation.

Selecting an Installation Process

You can install Directory Server software using one of the four different installation methods provided in the setup program:

- **Express Installation**. Use this if you are installing for the purposes of evaluating or testing iPlanet Directory Server. Express installation is described in "Using Express Installation," on page 45.
- **Typical Installation**. Use this if you are performing a normal install of Directory Server. Typical installation is described in "Using Typical Installation," on page 47.
- **Custom Installation.** In iPlanet Directory Server 5.0, the custom installation process is very similar to the typical installation process. The main difference is that the custom installation process will allow you to import an LDIF file to initialize the user directory database that is created by default.
- **Silent Installation**. Use this if you want to script your installation process. This is especially useful for installing multiple consumer servers around your enterprise. Silent install is described in Chapter 4, "Silent Installation."

Beyond determining which type of installation process you will use, the process for installing iPlanet Directory Server is as follows:

1. Plan your directory service. By planning your directory tree in advance, you can design a service that is easy to manage and easy to scale as your organization grows. For guidance on planning your directory service, refer to the *iPlanet Directory Server Deployment Guide*.
2. Install your Directory Server as described in this manual.
3. Create the directory suffixes and databases. You do not have to populate your directory now; however, you should create the basic structure for your tree, including all major roots and branch points. For information about the different methods of creating a directory entry, refer to the *iPlanet Directory Server Administrator's Guide*.
4. Create additional Directory Server instances and set up replication agreements between your directory servers to ensure availability of your data.

Upgrade Process

iPlanet Directory Server 5.0 supports migration from Directory Server 4.1, 4.11, and 4.12 releases. The migration process is described in Chapter 6, “Migrating From Previous Versions.”

For information on migrating servers involved in replication agreements, refer to the *iPlanet Directory Server Administrator’s Guide.*

Unpacking the Software

If you have obtained iPlanet Directory Server 5.0 software from the iPlanet web site, you will need to unpack it before beginning installation.

1. Create a new directory for the installation:

   ```
   # mkdir ds5.0
   # cd ds5.0
   ```

2. Download the product binaries file to the installation directory.
3. On UNIX, unpack the product binaries file using the following command:

   ```
   # gzip -dc file_name.tar.gz | tar -xvof -
   ```

   where *file_name* corresponds to the product binaries that you want to unpack.

   On Windows NT and Windows 2000, unzip the product binaries.

Installation Privileges

On UNIX you must install as root if you choose to run the server on a port below 1024, such as the default ldap ports: 389, and 636 (ldap over SSL). If you choose port numbers higher than 1024, you can install using any valid UNIX login.

On Windows NT or Windows 2000 you must run the installation as administrator.

Unsetting Environment Variables (AIX only)

If you are installing Directory Server on an AIX machine, the installer will execute the following files (depending upon the shell you use):

Shell name	File
sh (bourne shell)	$HOME/.profile
csh and tcsh shell	$HOME/.login $HOME/.cshrc
ksh (korn shell)	$HOME/.profile $HOME/.kshrc
bash (bourne again shell)	$HOME/.profile $HOME/.bashrc

The installation program does not unset the environment variables in each shell. So, if the file contains printouts or other information, it may affect installation by causing unexpected error message and behaviors.

For example, to unset the .profile and .kshrc files in the korn shell, you issue the following command

```
unset ENV
```

Computer System Requirements

Before you can install iPlanet Directory Server 5.0, you must make sure that the systems on which you plan to install the software meet the minimum hardware and operating system requirements.

These requirements are described in detail for each platform in the following sections:

- Supported Platforms
- Operating System Requirements
- Hardware Requirements

Supported Platforms

iPlanet Directory Server 5.0 is supported on the following platforms:

- Sun Solaris 2.6 for SPARC operating environment
- Sun Solaris 8 for SPARC (32 and 64 bit) operating environment
- Microsoft Windows NT 4.0 Server (x86 only)
- Microsoft Windows 2000 Server
- Hewlett-Packard HP-UX 11.0 (PA-RISC 1.1 or 2.0).
- IBM AIX 4.3.3 (Power PC)

This release of the Directory Server is not supported on any version of Linux, Tru64 UNIX or OpenVMS.

NOTE For each platform, check the required patches and kernel parameter settings, as described in the following sections.

Hardware Requirements

On all platforms, you will need:

- Roughly 2 GB of disk space for a minimal installation. For production systems, you should plan at least 2GB to support the product binaries, databases, and log files (log files require 1 GB by default); 4GB and greater may be required for very large directories.
- 256 MB of RAM. However, you should plan from 256 MB to 1 GB of RAM for best performance on large production systems.

The following table contains some guidelines for disk space and memory requirements depending on the number of entries managed by your Directory Server. This assumes entries in the LDIF file are approximately 100 bytes in size, and only the recommended indexes are configured. If you are using larger entries, make sure that at least four times the size of the LDIF file is available on disk.

Number of Entries	Disk Space and Memory Required
10,000 - 250,000 entries	Free disk space: 2 GB Free memory: 256 MB
250,000 - 1,000,000 entries	Free disk space: 4 GB Free memory: 512 MB
Over 1,000,000 entries	Free disk space: 8GB Free memory: 1 GB

Operating System Requirements

This section covers the required operating system versions and patches.

idsktune Utility

For UNIX platforms, iPlanet Directory Server provides a utility that can help you check that you have the appropriate patches installed on your system. It also provides useful information and advice on how to tune your kernel parameters for best performance. This utility is called `idsktune` and is located in the `/usr/iplanet/servers/bin/slapd/server` directory. For information on running `idsktune`, refer to Chapter 7, "Troubleshooting."

NOTE Before you install iPlanet Directory Server, you must check that DNS is properly configured on your system, and that the system has a static IP address.

Solaris 2.6 and Solaris 8 Operating Systems

If you run iPlanet Directory Server on a Solaris operating system, you must ensure that the recommended patch cluster is installed. Solaris patches are identified by two numbers, for example 106125-10. The first number (106125) identifies the patch itself. The second number identifies the version of the patch, in the example above the patch is version number 10. We recommend installing the latest version of the patch in order to benefit from the latest fixes.

See the Solaris Operating Environment Security Sun Blueprint at http://www.sun.com/blueprints/0100/security.pdf for advice on guarding against potential security threats.

Disk Space Requirements

Ensure that you have sufficient disk space before downloading the software.

current working directory: 120 MB
partition containing `/usr/iplanet`: 2 GB

Required System Modules

iPlanet Directory Server is optimized for systems with the UltraSPARC chipsets. It will not run on SPARC v8 or earlier chipsets.

Patches

Use of Solaris 2.6 or 8 with the Sun recommended patches is required.

The following Sun patches should be installed on your system before installing this iPlanet product. The command "`showrev -p`" will list the patches which have been installed. If you need to get a patch, see the web page `sunsolve.sun.com` or FTP to `ftp://sunsolve.sun.com/pub/patches`.

You will need to reboot your machine after installing these patches.

In addition to the patches listed here, you may want to install the latest patch cluster for your version of Solaris, which includes additional recommended and security patches. The Sun recommended patch clusters can be obtained from your Solaris support representative, or from `http://sunsolve.sun.com`.

Table 2-1 Solaris 2.6 Patch List

105181-22	105552-3	107774-1
105210-32	105562-3	107991-1
105216-4	105568-18	108307-2
105284	105580-15	108346-3
105356-16	105591-9	108468-2
105357-4	105600-19	108492-1
105375-24	106828-1	108499-1
105379-6	106834-1	108660-1
105395-6	106894-1	108804-1
105401-28	107565-2	108890-1
105403-3	107618-1	108893-1
105407-1	107733-8	108895-1
105472-7	107758-1	109266-1
105529-9	107766-1	109339-1
		109388-1

Table 2-2 Solaris 8 Patch List

108528-01
108652-13
108875-07
108968-02
108974-02
108975-02
108977-01
109137-01
109320-01

This release of iPlanet Directory Server is not supported on Solaris 2.5.1 or earlier, Solaris 7, or any version of Solaris x86.

This release of iPlanet Directory Server may be used on a 64 bit Solaris 8 environment, but will run as a 32 bit process, and is limited to 3.7 GB of process memory.

Verify System Tuning

Basic Solaris tuning guidelines are available from several books, including *Sun Performance and Tuning: Java and the Internet (ISBN 0-13-095249-4) and Solaris Performance Administration* (ISBN 0-07-011768-3). Advanced tuning information is available from the Web site: `http://www.rvs.uni-hannover.de/people/voeckler/tune/EN/tune.html`.

File Descriptors

The system-wide maximum file descriptor table size setting will limit the number of concurrent connections that can be established to iPlanet Directory Server. The governing parameter, `rlim_fd_max`, is set in the `/etc/system` file. By default if this parameter is not present the maximum is 1024. It can be raised to 4096 by adding to `/etc/system` a line

```
set rlim_fd_max=4096
```

and rebooting the system. This parameter should not be raised above 4096 without first consulting your Sun Solaris support representative as it may affect the stability of the system.

TCP Tuning

By default, the TCP/IP implementation in a Solaris kernel is not correctly tuned for Internet or Intranet services. The following `/dev/tcp` tuning parameters should be inspected, and if necessary changed to fit the network topology of the installation environment.

The `tcp_time_wait_interval` in Solaris 7 and 8 and `tcp_close_wait_interval` in Solaris 2.6 specify the number of milliseconds that a TCP connection will be held in the kernel's table after it has been closed. If its value is above 30000 (30 seconds) and the directory is being used in a LAN, MAN or under a single network administration, it should be reduced by adding a line similar to the following to the `/etc/init.d/inetinit` file:

```
ndd -set /dev/tcp tcp_close_wait_interval 30000
```

The `tcp_conn_req_max_q0` and `tcp_conn_req_max_q` parameters control the maximum backlog of connections that the kernel will accept on behalf of the iPlanet Directory Server process. If the directory is expected to be used by a large number of client hosts simultaneously, these values should be raised to at least 1024 by adding a line similar to the following to the `/etc/init.d/inetinit` file:

```
ndd -set /dev/tcp tcp_conn_req_max_q0 1024
ndd -set /dev/tcp tcp_conn_req_max_q 1024
```

The `tcp_keepalive_interval` specifies the interval in seconds between keepalive packets sent by Solaris for each open TCP connection. This can be used to remove connections to clients that have become disconnected from the network.

The `tcp_rexmit_interval_initial` value should be inspected when performing server performance testing on a LAN or high speed MAN or WAN. For operations on the wide area Internet, its value need not be changed.

The `tcp_smallest_anon_port` controls the number of simultaneous connections that can be made to the server. When `rlim_fd_max` has been increased to above 4096, this value should be decreased, by adding a line similar to the following to the `/etc/init.d/inetinit` file:

```
ndd -set /dev/tcp tcp_smallest_anon_port 8192
```

The `tcp_slow_start_initial` parameter should be inspected if clients will predominately be using the Windows TCP/IP stack.

Windows NT 4.0 Server

This section describes how to install iPlanet Directory Server on Windows NT.

Configuring a Machine to Run iPlanet Directory Server

iPlanet Directory Server should be installed on a computer which is isolated from the public Internet by a network-level firewall. This is necessary to protect the NT operating system from IP-based attacks.

No other network functions should be provided by this computer. The computer should not be dual-booting or run other operating systems. At a minimum, the computer system should have at least 256 MB of RAM, 2 GB of disk, a Pentium II or later processor, and a 100MBps Ethernet connection.

Ensure that you have sufficient disk space before downloading the software.

Download drive: 120 MB
Installation drive: 200 MB

Required System Modules

iPlanet Directory Server 5.0 is not supported on Windows NT 3.5.1 or earlier releases, or Windows NT for the Alpha architecture. Neither is it supported on Windows NT Workstation, because this form of the operating system is not suitable for scalable Internet or Intranet server deployments. Windows NT Workstation is limited in its allowable setting for connection backlog. Windows NT Server allows a connection backlog setting of more than 10, which is necessary for TCP/IP servers under heavy load.

Installing Windows NT Server

During the installation of Windows NT, please observe the following:

- If there is already an operating system present on the computer, choose to perform a fresh install rather than an upgrade.
- Format the drives with NTFS rather than FAT, as NTFS allows access controls to be set on files and directories.
- Specify that the computer will be a stand-alone server and will not be a member of any existing domain or workgroup. This will reduce dependencies on the network security services.
- Choose an administrator password of at least 9 characters. Use punctuation or other non-alphabetic characters in the first 7 characters.
- Do not install Internet Information Server.
- Specify only TCP/IP as network protocol, and do not install any other network services.

Installing Third-Party Utilities

You need an UNZIP utility to unpack the directory server software. There are many commercially licensed, free and shareware tools available, such as PKZIP or Winzip. Note that shareware unregistered versions of PKZIP 2.70 maintain a TCP/IP connection to an Internet advertising service, and so may not be suitable for installation on this system.

You need to install Adobe Acrobat Reader to read the documentation. It can be downloaded from `ftp://ftp.adobe.com/pub/adobe/acrobatreader/win/4.x`.

To edit the server configuration file, you will need a text editor that is capable of handling large text files (Notepad and Wordpad are not suitable). If you are already familiar with Emacs on UNIX, a port to Windows can be downloaded from `ftp://ftp.cs.washington.edu/pub/ntemacs/`. There are many other shareware and commercial text editors available.

Installing Microsoft Utilities

The following additional utilities are recommended to improve the security of the Windows NT Operating System. They are not required for the operation of the iPlanet Directory Server.

If you have the Resource Kit CD-ROM produced by Microsoft Press, then copy the utility '`passprop.exe`' from the Windows NT Server Resource Kit onto the system. The utility is located on the CD in the `i386\netadmin` directory. You will need this later to enable Administrator account lockout.

At this point you will need to install Service Pack 4 or later, if not already installed. This is needed for the installation of Microsoft Internet Explorer 5. Service packs can be obtained from `http://www.microsoft.com/windows/servicepacks/`.

You will need to install Microsoft Internet Explorer 5 or later, as this is needed by the Security Configuration Manager.

The Microsoft Security Configuration Manager is located on the Service Pack 4 CD-ROM, or can be downloaded from `ftp://ftp.microsoft.com/bussys/winnt/winnt-public/tools/scm/`. This tool is described in Microsoft Knowledge Base article Q195227.

Ensure That the System Clock is Correct and Kept Accurate

So that date and time stamps in log files can be correlated with those of other computer systems, the system clock should be kept reasonably in sync. As the NET TIME command requires NetBIOS, which will be disabled during post-installation system configuration, either a TCP/IP based NTP client should be installed (such as the shareware program Tardis), or a time radio receiver attached. See `http://www.ntp.org/` for more information on NTP clients for Windows NT.

Install Windows Service Packs and Hotfixes

Windows NT Service Packs include key fixes that are necessary to maintain the security and reliability of the operating system. The hotfix series contains important changes for problems that were found after the service pack was released.

Install Windows NT 4.0 Service Pack 6a or Later

It can be obtained from `http://www.microsoft.com/windows/servicepacks/`. The system will reboot after the service pack is installed.

Install Hotfixes

Download and install any Windows NT 4.0 Hotfixes that are for the service pack that is installed on the system, such as `post-sp6a` for Service Pack 6a. They can be obtained from `ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/`. It will probably be necessary to reboot the system after each hotfix is installed.

Install TCP ISN Patch

If you will be authenticating users to the directory, then TCP connection hijacking is a vulnerability. Microsoft has released a patch to improve the serial numbers, `q243835i.exe`. For more information please see `http://www.microsoft.com/security/bulletins/ms99-046.asp`

Additional Post-Installation System Configuration

The Windows environment will require tuning to provide optimum performance for iPlanet Directory Server in an operational environment. Consult the Windows system administrator's documentation or support channel for information on NT tuning for multi-threaded internet services. The following sections provide some guidelines.

Restrict Network Services

Network file sharing is not required by iPlanet Directory Server and should be disabled. Go to the Control Panel and open the Network icon. Remove the Workstation, Computer Browser, NetBIOS Interface, Remote Access Service and Server Services from Network Services tab. Leave RPC Configuration.

The SNMP service may be left if SNMP monitoring will be used.

From then on, each time the Network Control Panel is used, Windows NT will prompt to install Windows NT Networking. Always answer No to the prompt.

Remove NETBIOS

The server uses only TCP/IP and does not require any Microsoft network services. On the Bindings tab of the Network window, select All Protocols. Disable the WINS Client. This unbinds NETBIOS from TCP/IP.

Enable Port Filtering

The RPC services are not removed, as it may be necessary for Microsoft software to make RPC connections on the loopback interface. However, the RPC ports must not be accessible to other systems.

Open the Network window; select the Protocols tab, then select TCP/IP and click Properties...; select Advanced and Enable Security. On the TCP/IP Filtering window, permit only TCP ports 389 and 636 and the administration port number, permit no UDP ports, and permit only IP protocol 6 (TCP). If you have multiple interfaces, it may be necessary to repeat this for each interface.

Note that after this change has been made, the Microsoft command-line FTP client will no longer operate. This is because the Microsoft client requires the FTP server to establish a connection in the reverse direction, and all non-LDAP ports are blocked.

Disable IP Routing

On the TCP/IP protocol window, disable IP Routing.

Disable WINS Client

On the Devices window of the Control Panel, disable the WINS Client.

Remove the OS/2 and POSIX Subsystem Keys From the Registry

iPlanet Directory Server does not require OS/2 and POSIX subsystems. Remove them by performing the following registry actions with regedit.

Delete all subkeys of:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OS/2 Subsystem for NT
```

There is another key under CurrentControlSet\Control named SessionManager, without a space in its name. Do not alter anything below that key.

Delete the value of Os2LibPath in this key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Environment
```

Change the value of the Optional item in the following key to the two bytes "`00 00`":

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\SubSystems
```

Delete the Posix and OS/2values from the following key:

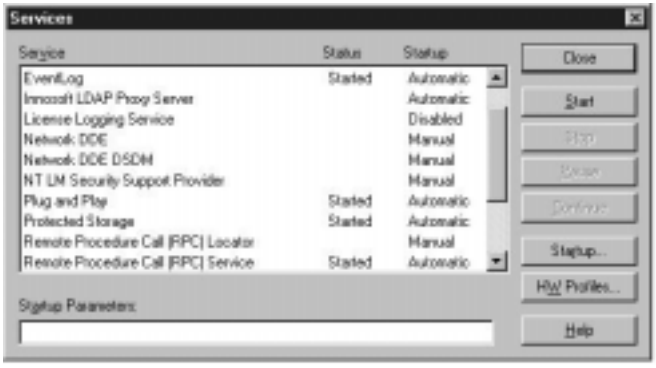
```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\SubSystems
```

Remove the OS/2 DLLs

Delete all files in the `%SystemRoot%\system32\os2` directory and all subdirectories.

Stop Unneeded Services

Open the Control Panel, and the Services panel. Stop and disable any running services except for the following: EventLog, iPlanet Directory Server, iPlanet Administration Server, NT LM Security Support Provider, Plug and Play, Protected Storage, Remote Procedure Call (RPC) Service, and SNMP. Services that are listed as Manual start do not need to be disabled.



Ensure System Will Automatically Reboot on Error

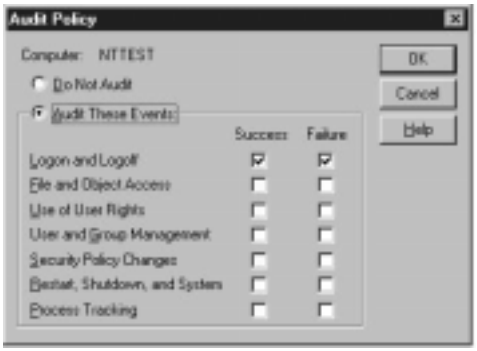
Open the Control Panel System panel. Under the Startup/Shutdown tab, set the show list time to `0` seconds, and select the Automatic reboot checkbox.

Configure User Accounts

Open the Administrative tools. (Start>Programs>Administrative Tools>User Manager.) Under Policies, choose Account... On the Account Policies window, allow accounts to be locked out.

Next, under Policies, choose User Rights... Select Access this computer from the network, remove Everyone and add Authenticated Users.

Next, under Policies, choose Audit, select Audit These Events, and check the boxes for both Success and Failure for the Logon and Logoff Events.



You may wish also to rename the administrator account to something else, making it harder to guess.

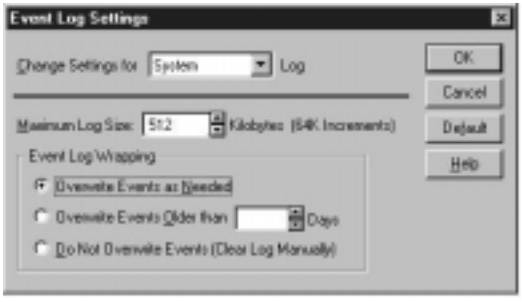
If you have copied the passprop utility from the NT Server Resource Kit, it can be used to allow lockout of the administrator's account by running it on the command line as `passprop/adminlockout`.

Encrypt Account Database

Protect the NT user account database, SAM, by running the `syskey` program. This encrypts the Administrator's password so that registry-extracting hacker tools cannot use it.

Event Log Configuration

Open the Event Viewer (Start>Programs>Administrative Tools>Event Viewer); set the log overwrite intervals (located under Log>Log Settings...) to a value appropriate to your deployment.



Set Tuning Parameters

The transmission control blocks (TCBs) store data for each TCP connection. A control block is attached to the TCB hash table for each active connection. If there are not enough control blocks available when an LDAP connection arrives at the server via TCP/IP, there is added delay while it waits for additional control blocks to be created. By increasing the TCB timewait table size, you reduce latency overhead by allowing more client connections to be serviced faster. To adjust this value, add to the following registry key:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters
```

the `MaxFreeTcbs` value of 0xFA0.

This example increases the TCB timewait table to 4,000 entries from the default of 2,000. Now that the overhead time introduced by TCP has been lowered for iPlanet Directory Server, adjust the corresponding hash table that stores the TCBs. Adjust the hash table by adding to the following registry value:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters
```

the value of `MaxHashTableSize` to 0x400.

This increases the TCB hash table size from 512 to 1,024, allowing more room for connection information. TCB information is stored in the nonpaged memory pool. If iPlanet Directory Server is experiencing memory bottlenecks and more memory cannot be allotted to the server, lower the above values.

On a multiprocessor system, we recommend optimizing the NIC and CPU relationship. Each LDAP request received over the network generates an interrupt to the processor requesting service. If the processor does not consider the request to be sufficiently urgent, (i.e., with a sufficiently high interrupt level), it defers the request. This deferred interrupt request becomes a Deferred Procedure Call (DPC). As more and more requests come into the server, the number of interrupts and DPCs increases.

When an interrupt is sent to a particular CPU and is subsequently deferred, additional server overhead is incurred if this DPC is shipped off to another CPU in the server (if the server is an SMP capable machine). This is NTs default behavior and can be costly from a performance perspective. To stop this transfer from happening, add to the following registry value:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NDIS\Parameters
```

the value of `ProcessorAffinityMask` to 0.

This forces the CPU that handled the interrupt to also handle any associated DPCs. This also insures that the network interface card or cards are not to associated with a specific CPU. This improves the CPUs servicing of interrupts and DPCs generated by the network interface card(s).

Windows NT ships with a variety of transport drivers such as TCP/IP, NBF (NetBEUI), and NWLink. All of these transports export a TDI interface on top and an NDIS (Network Driver Interface Specification) on the bottom. (Windows NT also ships with AppleTalk and DLC, however, these do not have a TDI interface.) If the TCP/IP protocol is first in the bindings list, average connection setup time decreases.

Windows NT can implement the Van Jacobson TCP fast retransmit and recovery algorithm to quickly retransmit missing segments upon the receipt of n ACKS, without waiting for the retransmission timer to expire. To implement the Van Jacobson algorithm, edit:

`HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/Tcpip/Parameters`

Add a value named `TcpMaxDupAcks`, with type `REG_DWORD`, and set the value to the number of ACKs. The range is 1-3, and the default is 2.

Windows 2000 Server and Advanced Server

Configuring a Machine to Run iPlanet Directory Server

iPlanet Directory Server should be installed on a computer that is isolated from the public Internet by a network-level firewall. This is necessary to protect the operating system from IP-based attacks.

No other network functions should be provided by this computer. The computer should not be dual-booting or run other operating systems. At a minimum, the computer system should have at least 256 MB of RAM, 16 B of disk, a Pentium II or later processor, and a 100 MBps Ethernet connection.

Ensure that you have sufficient disk space before downloading the software.

download drive: 120 MB
installation drive: 200 MB

Required System Modules

iPlanet Directory Server 5.0 is not supported on Windows 2000 Pro or Windows 2000 DataCenter Server.

Installing Windows 2000 Server

During the installation of Windows 2000, please observe the following:

- If there is already an operating system present on the computer, choose to perform a fresh install rather than an upgrade.
- Format the drives with NTFS rather than FAT, as NTFS allows access controls to be set on files and directories.
- Specify that the computer will be a stand-alone server and will not be a member of any existing domain or workgroup. This will reduce dependencies on the network security services.
- Choose an administrator password of at least 9 characters. Use punctuation or other non-alphabetic characters in the first 7 characters.
- Do not install Internet Information Server.
- Specify only TCP/IP as network protocol, and do not install any other network services.

Installing Third-Party Utilities

You need an UNZIP utility to unpack the directory server software. There are many commercially licensed, free and shareware tools available, such as PKZIP or Winzip. Please note that shareware unregistered versions of PKZIP 2.70 maintain a TCP/IP connection to an Internet advertising service, and so may not be suitable for installation on this system.

You need Adobe Acrobat Reader to read the documentation. If you do not have it installed, you can download it from:

`ftp://ftp.adobe.com/pub/adobe/acrobatreader/win/4.x.`

To edit the server configuration file, you will need a text editor that is capable of handling large text files (Notepad and Wordpad are not suitable). If you are already familiar with Emacs text editor on UNIX, a port to Windows can be downloaded from `ftp://ftp.cs.washington.edu/pub/ntemacs/`. There are many other shareware and commercial text editors available.

Ensure That the System Clock is Correct and Kept Accurate

To facilitate the correlation of date and time stamps in log files with those of other computer systems, keep your system clock reasonably in sync. As the NET TIME command requires NetBIOS, which will be disabled during post-installation system configuration, either a TCP/IP based NTP client should be installed (such as the shareware program Tardis), or a time radio receiver attached. See `http://www.ntp.org/` for more information on NTP clients for Windows.

Install Windows Service Packs and Hotfixes

Windows 2000 Service Packs include key fixes which are needed to maintain the security and reliability of the operating system. The hotfix series contains important changes for problems discovered after the service pack had been released.

Additional Post-Installation System Configuration

The Windows 2000 environment requires tuning to provide optimum performance for iPlanet Directory Server in an operational environment. Consult the Windows 2000 system administrator's documentation or support channel for information on Windows 2000 tuning for multi-threaded internet services.

HP-UX 11 Operating System

Disk Space Requirements

Ensure that you have sufficient disk space before downloading the software.

download drive: 120 MB
installation drive: 2 GB

Required System Modules

iPlanet Directory Server 5.0 is not supported on HP-UX 10 or earlier. The minimum system module required is HP-UX 11. iPlanet Directory Server may be used on a 64 bit HP-UX 11 environment, but will run as a 32 bit process, and is limited to 1 GB of process memory.

For best results, iPlanet Directory Server 5.0 requires an HP 9000 architecture with a PA-RISC 1.1 or PA-RISC 2.0 CPU.

NOTE Future versions of iPlanet Directory Server may not be supported on HP systems with PA-RISC 1.1 CPUs. These include the 9000/7xx series, C100, C110, C160L, J200, J210, J210XC, B132L, B132L+, B160L and B180L systems.

Patches

You should install patches before you install Directory Server. Use the following patches when running iPlanet Directory Server on HP-UX 11.0:

- PHCO_19491
- PHKL_14750
- PHCO_19666
- PHKL_20016
- PHKL_18543
- PHCO_17556
- The following patches are dependencies of patch PHKL_18543: PHKL_17038, PHCO_17792, PHKL_20079, and PHKL_20674.
- For applications that use AWT, use the following patches: PHSS_20141, PHSS_17535, PHSS_20140 PHSS_19964. The following patches are dependencies of patch PHSS_20140: PHNE_20094 and PHSS_20145.
- Ensure the HP C++ runtime libraries are installed on your system. The latest version is available as patch PHSS_16587.

You can also check the following website for information about patch requirements: `http://www.unix.hp.com/java/`.

Verify System Tuning

Set your kernel parameters as follows:

- Make sure the `maxdsize` kernel parameter is at least equal to

  cachesize * entrysize + 4096

  That is, if your directory server cachesize is 1000 (this is the default), your average directory entry size is 20 KB, then make sure your `maxdsize` kernel parameter is at least (1000*20000) + 4096, or at least 21 MB.

- Set `max_thread_proc` (max number of threads per process) to 128

- Set `ncallout` (max number of pending timeouts) to `128+NPROC`.
- Set `maxfiles` to at least 120.

On HP-UX machines, administrators need to turn on large file support in order for iPlanet Directory Server to work properly.

To change an existing file system from one that has no large files to one that accepts large files:

1. Unmount the system using the umount command. For example:

```
umount  /export
```

2. Create the large file system. For example:

```
fsadm -F vxfs -o largefiles /dev/vg01/rexport
```

3. Remount the file system. For example:

```
/usr/sbin/mount -F vxfs -o largefiles /dev/vg01/export
```

For additional information and recommendations about setting these parameters, consult the HP documentation for your system.

Installing Third-Party Utilities

You will need the gunzip utility to unpack the directory server software. The GNU gzip and gunzip programs are described in more detail at `http://www.gnu.org/software/gzip/gzip.html` and can be obtained from many software distribution sites.

You need Adobe Acrobat Reader to read the documentation. If you do not have it installed, you can download it from:
`http://www.adobe.com/products/acrobat/readstep2.html`

IBM AIX 4.3.3 Operating System

Disk Space Requirements

Ensure that you have sufficient disk space before downloading the software.

current working directory: 120 MB
partition containing `/usr`: 2 GB

Required System Modules

You need to use of AIX 4.3.3 or later versions. iPlanet Directory Server 5.0 is not supported on AIX 4.3.2 or earlier releases. It is also not supported on AIX 5.0L.

Patches

To determine which patches, or APARs, are required for your system, refer to

`http://server.software.ibm.com/cgi-bin/support/rs6000.support/downloads`

Installing Third-Party Utilities

You will need the gunzip utility to unpack the directory server software. The GNU gzip and gunzip programs are described in more detail at:
`http://www.gnu.org/software/gzip/gzip.html`
and can be obtained from many software distribution sites.

Install Adobe Acrobat Reader to read the documentation. If you do not have it installed, you can download it from:
`http://www.adobe.com/products/acrobat/readstep2.html`

DNS and NIS Requirements (UNIX only)

Prior to installation, it is necessary to have configured the DNS resolver and NIS domain name.

The DNS resolver is typically set by the file `/etc/resolv.conf`. However, also check the file `/etc/nsswitch.conf`, and on Solaris `/etc/netconfig`, to ensure that the DNS resolver will be used for name resolution.

If you are not already using NIS, you will also need to set the default NIS domain name. Typically this is done by placing the NIS domain name in the file `/etc/defaultdomain` and rebooting, or by using the `domainname` command.

Chapter 3

Using Express and Typical Installation

This chapter describes how to perform basic installation activities. This chapter contains the following sections:

- Using Express Installation
- Using Typical Installation

Using Express Installation

Use express installation if you are installing Directory Server to evaluate or test the product. Because express installation does not offer you the choice of selecting your server port number or your directory suffix, you should not use it for production installations.

To perform an express installation, do the following:

1. On UNIX machines, log in as root (root login is required for express installation). On Windows NT and Windows 2000 machines, log in with administrator privileges.
2. Create a new directory:

   ```
   # mkdir directory
   ```

   ```
   # cd ds5.0
   ```
3. If you have not already done so, download the product binaries file to the installation directory.
4. On UNIX, unpack the product binaries file using the following command:

   ```
   # gunzip -dc file_name.tar.gz | tar -xvof -
   ```

where *file_name* corresponds to the product binaries you want to unpack.

On Windows NT and Windows 2000, unzip the product binaries.

5. Run the setup program. You can find it in the directory in which you untarred or unzipped the binary files. On a UNIX system, issue the following command:

   ```
   ./setup
   ```

   Select “yes” to continue with installation, then select “yes” to agree to the license.

6. When you are asked what you would like to install, select the default, iPlanet Servers.

7. When you are asked what type of installation you would like to perform, select Express Installation.

8. For server root or destination directory, enter a full path to the location where you want to install your server.

   The location that you enter must be some directory other than the directory from which you are running the setup program. If the directory that you specify does not exist, the setup program creates it for you.

9. UNIX only. For the user and group to run the servers as, enter the identity that you want this server to run as. For more information on the user and groups that you should use when running iPlanet servers, see “Deciding the User and Group for Your iPlanet Servers (UNIX only),” on page 14.

10. For Configuration Directory Administrator ID and password, enter the name and password that you will log in as when you want to authenticate to the console with full privileges (think of this as the root or superuser identity for the iPlanet Console).

The server is then unpackaged, minimally configured, and started. You are told what host and port number on which the Administration Server is listening.

Note the following about your new Directory Server installation:

- The Directory Server is listening on port 389.
- The server is configured to use the following suffixes:

  `dc=your_machine's_DNS_domain_name`. That is, if your machine is named `test.siroe.com`, then you will have the suffix `dc=siroe,dc=com` configured for this server.

  `o=NetscapeRoot`

Do not modify the contents of the directory under the `o=NetscapeRoot` suffix. Either create data under the first suffix, or create a new suffix to be used for this purpose. For details on how to create new suffixes for your Directory Server, see the *iPlanet Directory Server Administrator's Guide*.

Using Typical Installation

Most first time installations of Directory Server 5.0 can be performed using the Typical Installation option of the setup program. Typical installation differs slightly depending on whether you are installing on UNIX or Windows NT and Windows 2000. The following sections outline the different procedures.

Using Typical Installation on UNIX

To perform a typical installation on UNIX:

1. Log in as root.
2. Create a new directory:

   ```
   # mkdir directory
   ```

   ```
   # cd ds5.0
   ```
3. If you have not already done so, download the product binaries file to the installation directory.
4. Unpack the product binaries file using the following command:

   # gunzip -dc *file_name*.tar.gz | tar -xvof -

   where *file_name* corresponds to the product binaries that you want to unpack.
5. Run the setup program. You can find it in the directory where you untarred binary files. Issue the following command from the installation directory:

   ```
   ./setup
   ```
6. The setup program asks if you would like to proceed with the setup. Press Enter to respond with the default (the default for this prompt is Yes) or press n if you would like to exit the setup program.

   If you want to log in as root or superuser (su), you will need to exit the setup program.

7. Next, the setup program asks you if you agree to the license terms. Press “y” to agree with the license terms.
8. When you are asked what you would like to install, press Enter to select the default, iPlanet Servers (this is item 1).
9. When you are asked what type of installation you would like to perform, press Enter to select the default, Typical Installation.
10. For server root, enter a full path to the location where you want to install your server.

    The location that you enter must be some directory other than the directory from which you are running setup. If the directory that you specify does not exist, setup creates it for you.

    By default, the setup program provides the following path:

    `/usr/iplanet/servers`

    If you want to install the software into this directory tree, press Enter; otherwise, supply your own path.
11. For the Server Products Core Components, Directory Suite, Administration Services, nsPerl, and PerLDAP, press Enter to select the default (all components).
12. Press Enter to select all of the Server Products Core Components.
13. Press Enter to select all the Directory Suite components.
14. Press Enter to select all of the Administration Services components (iPlanet Administration Server and the Administration Server Console).
15. Press Enter to install nsPerl.
16. Press Enter to install PerLDAP.
17. For the hostname, enter a fully qualified hostname or select the default (which is the local host).

CAUTION Note that the default hostname may be incorrect if the installer cannot locate a DNS name in your system. For example, you might not have a DNS name if your system uses NIS.

The hostname must be a fully qualified host and domain name. If the default hostname is not a fully qualified host and domain name, installation will fail. Refer to “Common Installation Problems,” on page 83 for more information about entering a fully qualified domain name.

18. The setup program then asks you for the System User and the System Group names. Enter the identity under which you want the servers to run.

    For more information on the user and group names that you should use when running iPlanet servers, see “Deciding the User and Group for Your iPlanet Servers (UNIX only),” on page 14.

19. For the configuration directory, select the default if this directory will host your `o=NetscapeRoot` tree. Otherwise, enter `Yes`. You will then be asked for the contact information for the configuration directory.

    If the server you are currently installing is not the configuration directory, then the configuration directory must exist before you can continue this installation.

20. The setup program then asks if the server you are currently installing will be the one for your user data. For most cases, you can select the default. However, if you intend this server instance to be used as a configuration directory only, then you should enter `Yes`.

21. For the Directory Server port, select the default (389) unless you already have another application using that port.

22. For the Directory Server Identifier, enter a unique value (normally the default is sufficient).

    This value is used as part of the name of the directory in which the Directory Server instance is installed. For example, if your machine's host name is `phonebook`, then this name is the default and selecting it will cause the Directory Server instance to be installed into a directory labeled `slapd-phonebook`.

CAUTION The directory server identifier must not contain a period. For example, siroe.server.com is not a valid server identifier name.

---

23. For Configuration Directory Administrator ID and password, enter the name and password that you will log in as when you want to authenticate to the console with full privileges.

24. For a directory suffix, enter a distinguished name meaningful to your enterprise.

    This string is used to form the name of all your organization's directory entries. Therefore, pick a name that is representative of your organization. It is recommended that you pick a suffix that corresponds to your internet DNS name.

    For example, if your organization uses the DNS name `siroe.com`, then enter `dc=siroe,dc=com` here.

25. For Directory Manager DN, enter the distinguished name that you will use when managing the contents of your directory with unlimited privileges.

NOTE Any Distinguished Names must be entered in the UTF-8 character set encoding. Older encodings such as ISO-8859-1 are not supported.

    In former releases of Directory Server, the Directory Manager was known as the root DN. This is the entry that you bind to the directory as when you want access control to be ignored. This distinguished name can be short and does not have to conform to any suffix configured for your directory. However, it should not correspond to an actual entry stored in your directory.

26. For the Directory Manager password, enter a value that is at least 8 characters long.

27. For Administration Domain, enter the domain that you want this server to belong to.

    The name you enter should be a unique string that is descriptive of the organization responsible for administering the domain. For information on administration domains, see "Determining the Administration Domain," on page 19.

28. For the administration port number, enter a value that is not in use (for example, you might want to use the value 5000 to indicate a 5.0 Directory Server). Be sure to record this value.

29. For the user you want to run Administration Server as, enter `root`. This is the default.

    For information on why you should run Administration Server as root, see "Deciding the User and Group for Your iPlanet Servers (UNIX only)," on page 14.

The server is then unpackaged, minimally configured, and started. You are told what host and port number Administration Server is listening on.

The server is configured to use the following suffixes:

- The suffix that you configured.
- `o=NetscapeRoot`

Do not modify the contents of the directory under the `o=NetscapeRoot` suffix. Either create data under the first suffix, or create a new suffix to be used for this purpose. For details on how to create new suffixes for your Directory Server, see the *iPlanet Directory Server Administrator's Guide*.

Using Typical Installation on Windows NT and Windows 2000

To perform a typical installation on Windows NT and Windows 2000:

1. Log in as a user with administrator privileges.
2. If you have not already done so, download the product binaries file to the installation directory.
3. Unzip the product binaries files and run the setup program.
4. When you are asked what you would like to install, select the default, iPlanet Servers.
5. When you are asked what type of installation you would like to perform, select the default, Typical.
6. For server installation root, enter a full path to the location where you want to install your server.

   The location that you enter must be some directory other than the directory from which you are running setup. If the directory that you specify does not exist, setup creates it for you.
7. For configuration directory, select the default if this directory will host your `o=NetscapeRoot` tree. Otherwise, enter the appropriate contact information for the configuration directory.

   If this Directory Server instance is not the configuration directory, then the configuration directory must exist and be running before you can continue this installation.

8. For the directory to store data in, you must decide if this Directory Server instance will store your enterprise's data. For most cases, you can select the default, "Store data in this Directory Server." However, if this Directory Server instance is intended to be a configuration directory only, then you should select "Store data in an existing Directory Server."

9. For server identifier, enter a unique value (normally the default is sufficient).

   This value is used as part of the name of the directory in which the Directory Server instance is installed. For example, if your machine's hostname is `phonebook` then this name is the default and selecting it will cause the Directory Server instance to be installed into a directory labeled `slapd-phonebook`.

10. For a directory suffix, enter a distinguished name that is meaningful to your enterprise.

    This string is used to form the name of all your organization's directory entries. Therefore, pick some name that is representative of your organization. It is recommended that you pick a suffix that corresponds to your Internet DNS name. For example, if your organization uses the DNS name `siroe.com`, then enter `dc=siroe,dc=com` here.

11. For the Directory Server port, select the default (389) unless you already have another application using that port.

12. For Configuration Directory Administrator ID and password, enter the name and password that you will log in as when you want to authenticate to the console with full privileges.

13. For Administration Domain, enter the domain to which you want this server to belong.

    The name that you enter should be a unique string that is descriptive of the organization responsible for administering the domain. For information on administration domains, see "Determining the Administration Domain," on page 19.

14. For Directory Manager DN, enter the distinguished name that you will use when managing the contents of your directory with unlimited privileges.

NOTE Any Distinguished Names must be entered in the UTF-8 character set encoding. Older encodings such as ISO-8859-1 are not supported.

In former releases of Directory Server, the Directory Manager was known as the root DN. This is the entry that you bind to the directory as when you want access control to be ignored. This distinguished name can be short and does not have to conform to any suffix configured for your directory. However, it should not correspond to an actual entry stored in your directory.

15. For Directory Manager password, enter a value that is at least 8 characters long.
16. For administration port number, enter a value that is not in use. Be sure to record this value.

The server is then unpackaged, minimally configured, and started. You are told which host and port number the Administration Server is listening on.

The server is configured to use the following suffixes:

- The suffix that you configured.
- `o=NetscapeRoot`

Do not modify the contents of the directory under the `o=NetscapeRoot` suffix. Either create data under the first suffix, or create a new suffix to be used for this purpose. For details on how to create new suffixes for your Directory Server, see the *iPlanet Directory Server Administrator's Guide*.

Chapter 4

Silent Installation

Silent installation allows you to use a file to predefine all the answers that you would normally supply to the setup program interactively. This provides you with the ability to script the installation of your Directory Servers.

This chapter includes the following sections:

- Using Silent Installation
- Preparing Silent Installation Files
- Installation Directives

Using Silent Installation

To use silent installation, you call the setup program with the `-s` and `-f` command line options. That is, to use silent installation:

1. On UNIX machines, log in as `root`. On Windows NT and Windows 2000 machines, log in with Administrator privileges.
2. Create a new directory:

   ```
   # mkdir directory
   ```

   ```
   # cd ds5.0
   ```
3. If you have not already done so, download the product binaries file to the installation directory.
4. On UNIX, unpack the product binaries file using the following command:

   ```
   # gunzip -dc file_name.tar.gz | tar -xvof-
   ```

   where *file_name* corresponds to the product binaries that you want to unpack.

5. On Windows NT and Windows 2000, unzip the product binaries.
6. Prepare the file that will contain your installation directives.
7. Run the setup program with the `-s` and `-f` command line options:

   ```
   setup -s -f file_name
   ```

   where *file_name* is the name of the file that contains your installation directives.

The next section in this chapter provides some examples of the silent install files. A section describing all of the silent installation directives that you can use when installing Directory Server then follows.

Preparing Silent Installation Files

Silent installation is intended for use at sites where many server instances must be created. For Directory Server, it is especially useful for heavily replicated sites that will create a large number of consumer servers.

This section first describes how to create silent installation files. It then provides examples of using silent installation to support the following common installation scenarios:

- A Typical Installation
- Using an Existing Configuration Directory
- Installing the Stand-Alone iPlanet Console

You find a definition of the individual installation directives in “Installation Directives,” on page 60.

NOTE Any Distinguished Names in the files must be in the UTF-8 character set encoding.

Creating Silent Installation Files

The best way to create a file for use with silent installation is to use the setup program to interactively create a server instance of the type that you want to duplicate around your enterprise.

To do this run setup with the `-k` flag. The setup program will create the following file:

`/<ServerRoot>/setup/install.inf`

This file contains all the directives that you would use with silent installation to create the server instance. You can then use this file to create other server instances of that type.

You will have to make some modifications to this file before you use it on other machines. Specifically, ensure that you:

- Set the `FullMachineName` directive to a value that is appropriate for the machine on which iPlanet Directory Server will be installed, if it's not to be the local machine. In most circumstances, it is best not to use this directive because `FullMachineName` will then default to the local host name. However, if you use custom installation to generate your initial server instance, then this directive will appear in the `install.inf` file.
- Set the `ServerIPAddress` directive appropriate for the local machine. The same usage rules apply for `ServerIPAddress` as for `FullMachineName`. Specifically, try to not include ServerIPAddress in your `install.inf` file unless you absolutely have to (as may be necessary for multi-homed systems).
- Verify the installation path on the `ServerRoot` directive. If you are installing on both Windows NT or Windows 2000 and UNIX machines, make sure the appropriate path delimiter is used. Add or remove the Windows NT or Windows 2000 drive letter designation as is appropriate for the host you are installing on.
- If you are installing more than one Directory Server on the same host, make sure the `ServerIdentifier` directive contains a unique value for each server instance.
- If you create your `install.inf` file on a Windows NT or Windows 2000 machine, then the `SuiteSpotUserID` and `SuiteSpotGroup` directives are both set to `nobody`. If you subsequently use this file on a UNIX machine, ensure the user and group specified by these directives are appropriate for the machine. The `SuiteSpotUserID` and `SuiteSpotGroup` directives determine what user and group a server will run under when installed on a UNIX system.

Be sure to protect `install.inf` files since they contain passwords in clear.

For complete information on the directives you can use in a silent installation file, see "Installation Directives," on page 60.

A Typical Installation

The following is the `install.inf` file that is generated for a typical installation:

```
[General]
FullMachineName=   dir.siroe.com
SuiteSpotUserID=   nobody
SuiteSpotGroup=   nobody
ServerRoot=   /usr/iplanet/servers
AdminDomain=   siroe.com
ConfigDirectoryAdminID=   admin
ConfigDirectoryAdminPwd=   admin
ConfigDirectoryLdapURL=   ldap://dir.siroe.com:389/o=NetscapeRoot
UserDirectoryAdminID=   admin
UserDirectoryAdminPwd=   admin
UserDirectoryLdapURL= ldap://dir.siroe.com:389/o=siroe.com
Components=   svrcore,base,slapd,admin

[slapd]
SlapdConfigForMC=   Yes
SecurityOn=   No
UseExistingMC=   No
UseExistingUG=   No
ServerPort= 389
ServerIdentifier=   dir
Suffix=   o=mcom.com
RootDN=   cn=Directory Manager
UseReplication=   No
SetupSupplier=   No
SetupConsumer=   No
AddSampleEntries=   No
InstallLdifFile=   suggest
AddOrgEntries=   Yes
DisableSchemaChecking=   No
RootDNPwd=   admin123
Components=   slapd,slapd-client

[admin]
SysUser=   root
Port=   23611
ServerIpAddress=   111.11.11.11
ServerAdminID=   admin
ServerAdminPwd=   admin
Components=   admin,admin-client,base-jre

[base]
Components=   base,base-client
```

Using an Existing Configuration Directory

The following is the `install.inf` file that is generated when you perform a typical installation and you choose to use an existing Directory Server as the configuration directory:

```
[General]
FullMachineName=   dir.siroe.com
SuiteSpotUserID=   nobody
SuiteSpotGroup=   nobody
ServerRoot=   /usr/netscape/server4
AdminDomain=   siroe.com
ConfigDirectoryAdminID=   admin
ConfigDirectoryAdminPwd=   admin
ConfigDirectoryLdapURL=
ldap://dir.siroe.com:25389/o=NetscapeRoot
UserDirectoryLdapURL= ldap://dir.siroe.com:18257/dc=siroe,dc=com
UserDirectoryAdminID=   cn=Directory Manager
UserDirectoryAdminPwd=   admin123
Components=   svrcore,base,slapd,admin

[slapd]
SlapdConfigForMC=   No
SecurityOn=   No
UseExistingMC=   y
UseExistingUG=   No
ServerPort=   18257
ServerIdentifier=   directory
Suffix=   o=siroe.com
RootDN=   cn=Directory Manager
UseReplication=   No
SetupSupplier=   No
SetupConsumer=   No
AddSampleEntries=   No
InstallLdifFile=   suggest
AddOrgEntries=   Yes
DisableSchemaChecking=   No
RootDNPwd=   admin123
Components=   slapd,slapd-client

[admin]
SysUser=   root
Port=   33646
ServerIpAddress=   111.11.11.11
ServerAdminID=   admin
ServerAdminPwd=   admin
Components= admin,admin-client,base-jre

[base]
Components=   base,base-client, base-jre

[nsperl]
Components=   nsperl553

[perldap]
Components=   perldap14
```

Installing the Stand-Alone iPlanet Console

The following is the `install.inf` file that is generated when you install just iPlanet Console:

```
[General]
FullMachineName=   dir.siroe.com
ConfigDirectoryLdapURL=   ldap://dir.siroe.com:389/o=NetscapeRoot
SuiteSpotUserID=   nobody
SuiteSpotGroup=   nobody
ConfigDirectoryAdminID=   admin
ConfigDirectoryAdminPwd=   admin
ServerRoot=   /usr/netscape/server4
Components=   svrcore,base,slapd,admin

[base]
Components=   base-client

[slapd]
Components=   slapd-client

[admin]
Components= admin-client,base-jre
```

Installation Directives

This section describes the basic format of the file used for silent installation. It then describes the directives that are available for each area of the silent installation file. Specifically, the following sections are provided here:

- Silent Installation File Format
- [General] Installation Directives
- [Base] Installation Directives
- [slapd] Installation Directives
- [admin] Installation Directives

Silent Installation File Format

When you use silent installation, you provide all the installation information in a file. This file is formatted as follows:

```
[General]
directive=value
directive=value
directive=value
...
[Base]

directive=value
directive=value
directive=value
...
[slapd]
directive=value
directive=value
directive=value
...
[admin]
directive=value
directive=value
directive=value
....
```

The keywords [General], [slapd], and [admin] are required. They indicate that the directives that follow are meant for a specific aspect of the installation. They must be provided in the file in the order indicated above.

[General] Installation Directives

[General] installation directives specify information of global interest to the iPlanet servers installed at your site. That is, the information you provide here will be common to all your iPlanet servers.

The [General] installation directives are:

Table 4-1 [General] Installation Directives

Directive	Description
Components	Specifies components to be installed. The list of available components will differ depending on the iPlanet servers available on your installation media. For stand-alone directory installation, the list of components is: • `srvrcore`—uninstallation binaries • `base`—the base installation package • `admin`—the Administration Server binaries • `slapd`—the Directory Server binaries This directive is required. At a minimum, you should always provide: `components = srvrcore, base, admin`
ServerRoot	Specifies the full path to the directory where the iPlanet server binaries are installed. This directive is required.
FullMachineName	Specifies the fully qualified domain name of the machine on which you are installing the server. The default is the local host name.
SuiteSpotUserID	UNIX only. Specifies the username that iPlanet servers will run as. This parameter does not apply to the user that the Administration Server runs as. See the SysUser directive in Table 4-5 for more information. The default is user `nobody` but this should be changed for most deployments.
SuiteSpotGroup	UNIX only. Specifies the group that iPlanet servers will run as. The default is group `nobody` but this should be changed for most deployments.
ConfigDirectoryLdapURL	Specifies the LDAP URL that is used to connect to your configuration directory. LDAP URLs are described in the *iPlanet Directory Server Administrator's Guide*. This directive is required.
AdminDomain	Specifies the administration domain under which this server will be registered. See "Determining the Administration Domain," on page 19 for more information about administration domains.
ConfigDirectoryAdminID	Specifies the user ID of the entry that has administration privileges to the configuration directory. This directive is required.

Table 4-1 [General] Installation Directives *(Continued)*

Directive	Description
ConfigDirectoryAdminPwd	Specifies the password for the ConfigDirectoryAdminID. This directive is required.
UserDirectoryLdapURL	Specifies the LDAP URL that is used to connect to the directory where your user and group data is stored. If this directive is not supplied, the configuration directory is used for this purpose. LDAP URLs are described in the *iPlanet Directory Server Administrator's Guide*.
UserDirectoryAdminID	Specifies the user ID of the entry that has administration privileges to the user directory.
UserDirectoryAdminPwd	Specifies the password for the UserDirectoryAdminID.

[Base] Installation Directives

There is only one [Base] installation directive and it allows you to determine whether iPlanet Console is installed:

Table 4-2 [Base] Installation Directive

Directive	Description
Components	Specifies the base components to be installed. The base components are: • `base`—install the shared libraries used by all Server Consoles. You must install this package if you are also installing some other iPlanet server. • `base-client`—install the Java run time environment used by the Server Consoles. • `base-jre`—causes the Java run time environment to be installed. This directive is required if you are installing an iPlanet server (versus, for example, just iPlanet Console). You must install both packages when you are installing an iPlanet server.

[slapd] Installation Directives

[slapd] installation directives specify information of interest only to the Directory Server instance that you are currently installing. These directives are described in the following sections:

- Required [slapd] Installation Directives
- Optional [slapd] Installation Directives

Required [slapd] Installation Directives

You must provide the following directives when you use silent installation with Directory Server:

Table 4-3 Required [slapd] Installation Directives

Directive	Description
Components	Specifies the slapd components to be installed. The slapd components are: • `slapd`—install the Directory Server. • `slapd-client`—install the Directory Server Console. This directive is required. It is recommended that you always install both components any time you install the Directory Server.
ServerPort	Specifies the port the server will use for LDAP connections. For information on selecting server port numbers, see “Choosing Unique Port Numbers,” on page 13. This directive is required.
ServerIdentifier	Specifies the server identifier. This directive is required. This value is used as part of the name of the directory in which the Directory Server instance is installed. For example, if your machine's hostname is phonebook then this name is the default and selecting it will cause the Directory Server instance to be installed into a directory labeled `slapd-phonebook`.
Suffix	Specifies the suffix under which you will store your directory data. For information on suffixes, see “Determining Your Directory Suffix,” on page 16. This directive is required.

Table 4-3 Required [slapd] Installation Directives *(Continued)*

Directive	Description
RootDN	Specifies the distinguished name used by the directory manager. For information on the directory manager, see “Defining Authentication Entities,” on page 15. This directive is required.
RootDNPwd	Specifies the directory manager’s password. This directive is required.

Optional [slapd] Installation Directives

You may provide the following directives when you use silent installation with Directory Server:

Table 4-4 Optional [slapd] Installation Directives

Directive	Description
AddSampleEntries	If set to `Yes`, this directive causes the `siroe.ldif` sample directory to be loaded. Use this directive if you are installing the Directory Server for evaluation purposes and you do not already have an LDIF file to populate your directory with. Default is `no`.
AddOrgEntries	If set to `Yes`, this directive causes the new Directory Server instance to be created with a suggested directory structure and access control. If this directive is used and `InstallLdifFile` is also used, then this directive has no effect. Default is `no`.
InstallLdifFile	Causes the contents of the LDIF file to be used to populate your directory.

[admin] Installation Directives

[admin] installation directives specify information of interest only to your Directory Server’s Administration Server. That is, this is the installation information required for the Administration Server that is used to manage the Directory Server instance that you are currently installing.

The [admin] installation directives are:

Table 4-5 [admin] Installation Directives

Directive	Description
Components	Specifies the admin components to be installed. The base components are: • `admin`—install the Administration Server. You must install the Administration Server if you are also installing some other iPlanet server. • `admin-client`—install iPlanet Console. Specify just this component if you are installing iPlanet Console as stand-alone. Do not install this component if you will remotely manage your servers and iPlanet Console will be installed somewhere else on your network.
SysUser	UNIX only. Specifies the user that the Administration Server will run as. For default installations that use the default iPlanet port numbers, this user must be root. Root is the default. For information on what users your servers should run as, see “Deciding the User and Group for Your iPlanet Servers (UNIX only),” on page 14
Port	Specifies the port that the Administration Server will use. Note that the Administration Server’s host name is given by the `FullMachineName` directive. For more information on `FullMachineName`, see Table 4-1.
ServerAdminID	Specifies the administration ID that can be used to access this Administration Server if the configuration directory is not responding. The default is to use the value specified by the `ConfigDirectoryAdminID` directive. See “Defining Authentication Entities,” on page 15 for information on this directive.
ServerAdminPwd	Specifies the password for ServerAdminID.
ServerIPAddress	Specifies the IP address that the Administration Server will listen to. Use this directive if you are installing on a multi-homed system and you do not want to use the first IP address for your Administration Server.

Chapter 5

Post Installation

This chapter describes the post-installation procedures for launching the online help and populating the directory tree.

Launching the Help System

The help system for iPlanet Directory Server is dependent upon iPlanet Administration Server. If you are running iPlanet Directory Server Console on a machine remote to Administration Server, you will need to confirm the following:

Client IP address authorized on Administration Server. The machine running iPlanet Directory Server Console needs access to Administration Server. To configure Administration Server to accept the client machine's IP address, do the following in Administration Server:

1. Launch iPlanet Administration Server Console. The console should be running on the same machine as Administration Server.
2. Click the Configuration tab, then click the Network tab.
3. In the Connection Restrictions Settings, select "IP Addresses to Allow" from the pull down menu. Click Edit.
4. Edit the IP Addresses field to the following: *.*.*.*

   This allows all clients access to Administration Server.
5. Restart Administration Server. You can now launch the online help by clicking any of the Help buttons in the Directory Server Console.

Proxy authorized on Administration Server. If you use proxies for your HTTP connections on the client machine running Directory Server Console, you need to do one of the following:

- Remove proxies on the machine running Directory Server Console. This allows the client machine to access Administration Server directly.

  To remove the proxies on the machine running Directory Server Console, you need to alter the proxy configuration of the browser you will use to run the help. In Netscape Communicator, select Preferences from the Edit menu. Select Advanced then Proxies to access the proxy configuration. In Internet Explorer, select Internet Options from the Tools menu.

- Add the client machine proxy IP address to Administration Server list of acceptable IP addresses.

CAUTION Adding the client machine proxy IP address to Administration Server creates a potential security hole in your system.

Populating the Directory Tree

During installation, a simple directory database was created for you. In addition, a simple directory structure was placed in the database for you to use. This directory structure contained basic access control and the major branch points for the recommended directory structure.

Now you need to populate your database with user entries. There are several ways you can create and populate your directory suffixes. These are explained in detail in the *iPlanet Directory Server Administrator's Guide*.

The main methods are:

- Create a database from LDIF—Use this method if you want to use the sample directory data shipped with Directory Server, if you are importing entries from another directory via LDIF, or if you have more than a few entries to add at once. For more information about LDIF, refer to the *iPlanet Directory Server Administrator's Guide*.

- Start your Directory Server with an empty database and import data over LDAP—This method requires you to populate your directory using an LDAP client such as Directory Server Gateway or the `ldapmodify` command-line utility. Use this method if you have just a few entries to add at a time. For information on setting up the Directory Server Gateway, see the *iPlanet Directory Server Gateway Customization Guide.*

As you are populating your directory, consider your access control needs and set access control accordingly. For more information on access control, see the *iPlanet Directory Server Deployment Guide* and the *iPlanet Directory Server Administrator's Guide*.

Chapter 6

Migrating From Previous Versions

You can upgrade to iPlanet Directory Server 5.0 from Netscape Directory Server 4.0, 4.1, 4.11, or 4.12. This chapter describes how in the following sections:

- Migration Overview
- Migration Prerequisites
- Identifying Custom Schema
- Migration Procedure
- Migrating a Replicated Site

This chapter does not explain how to upgrade from Innosoft Distributed Directory Server 4.5.1. That process is described in the Innosoft Distributed Directory Server Transition Guide.

Migration Overview

Before you migrate your directory service to iPlanet Directory Server 5.0, you should become familiar with the new features offered in this release of the Directory Server.

The migration process is performed by running the `migrateInstance5` script on the system where your legacy Directory Server is installed. You must shut down your directory service before running the migration script.

The migration script performs the following tasks in sequence:

- Checks the schema configuration files, and notifies you of any changes between the standard configuration files and the ones present on your system.

- Creates a database for each suffix stored in the legacy Directory Server. (In Directory Server 5.0 you can have multiple databases, but just one suffix per database).
- Migrates the server parameters and database parameters. (In Directory Server 5.0, these are stored as LDAP entries in the `dse.ldif` file.)
- Migrates user-defined schema objects.
- Migrates indexes.
- Migrates standard server plug-ins.
- Migrates the certificate database, and SSL parameters

The migration script shuts down your legacy Directory Server before performing the migration process. The migration script also backs up your current configuration.

Migration Prerequisites

This section lists the prerequisites that your system must meet before you can consider beginning the migration process.

- You must be using Directory Server 4.0, 4.1, 4.11, or 4.12. When you run the migration script, the legacy server process `ns-slapd` should be stopped.
- Your legacy Directory Server and your new Directory Server 5.0 must be installed on the same host; migration cannot occur over networked drives.
- If you want to continue to run your legacy Directory Server, when you install iPlanet Directory Server 5.0 choose different ports for LDAP traffic and for secured connections from the ones used by your legacy Directory Server.

  If you will not be running your legacy Directory Server, use the same port numbers to ensure that any directory clients that have static configuration information (including directory server port numbers) will continue to work.
- Your iPlanet Directory Server 5.0 must be running when you execute the migration script.
- Any custom schema that you created in your legacy Directory Server must be stored in the `slapd.user_oc.conf` and `slapd.user_at.conf files`. If it is not, refer to the procedure described in “Identifying Custom Schema” to move it to those files.
- On UNIX, set the following environment variables:

```
PERL5LIB=/usr/iplanet/servers/bin/slapd/admin/bin
PATH=/usr/iplanet/servers/bin/slapd/admin/bin:$PATH
```

- On NT, set the following environment variable:

  ```
  PERL5LIB=server5root\bin\slapd\admin\bin
  ```

  and add `server5root/bin/slapd/admin/bin` to the `PATH` environment variable. Replace `server5root` with the directory under which you installed the Directory Server.

Identifying Custom Schema

If you customized the schema in your legacy Directory Server by modifying `slapd.at.conf` or `slapd.oc.conf` directly, then the server migration process cannot migrate your custom schema for you. Instead, you are notified during migration that you have modified the standard schema and that you need to manually fix the problem. The migration process then saves a copy of your schema files and uses standard legacy schema files in their place.

While the migration will complete in this situation, you will probably find that you cannot modify your data in Directory Server 5.0. Therefore, you are strongly recommended to copy your custom schema into separate files before you perform the migration. You can use the standard `slapd.user_oc.conf` and `slapd.user_at.conf` files or any files declared in `slapd.conf` with the `useroc` and `userat` keywords respectively.

To separate your custom schema from your standard schema:

1. Examine your old `slapd.at.conf` and `slapd.oc.conf` files to discover all the schema additions that you made there.

   To ensure that you have properly identified all your changes to standard files, you can compare them with the standard files provided in the `/bin/slapd/install/version4` directory. Alternatively, if you have already tried to run the `migrateInstance5` script, use the notifications that it issues.

2. Move your custom schema elements to the following files:

/usr/iplanet/servers/slapd-*serverID*/config/slapd.user_at.conf and /usr/iplanet/servers/slapd-*serverID*/config/slapd.user_oc.conf

These file names are recommended because the 4.x schema configuration editor writes to them. However, you can use any file name you like.

Note that if there are inheritance relationships between custom defined object classes, you must ensure that in the order in which they appear in the schema configuration file, the superior object class is defined before the others.

3. Include these files into your slapd.conf file using the userat and useroc directives. Place your new directives at the same place in the file as the include statements for other configuration files.

   The order in which the various configuration files are included is not important.

Then, if you added custom attributes to standard object classes in slapd.oc.conf, you must do the following:

4. In the slapd.user_oc.conf file (or your equivalent), create a new object class that includes your custom attributes.
5. Add this new object class to every entry in your directory that uses the custom attributes.

Migration Procedure

Before you migrate your server, copy your configuration files to a safe place. The following files contain important configuration information:

- slapd.conf
- dsgw.conf
- Custom schema files, if any.

Once you have backed up your critical configuration information, do the following to migrate a server to 5.0:

1. Stop your legacy Directory Server.

NOTE	If you do not stop the legacy Directory Server, the migration script does it for you.

2. On the machine where your legacy Directory Server is installed, install a new 5.0 Directory Server.

   The installation process is described in Chapter 3, “Using Express and Typical Installation,” or Chapter 4, “Silent Installation.”

   Use a different port number from your legacy production server if you plan to continue to run your legacy Directory Server. Use the same port numbers as your legacy production server if you want to ensure that any directory clients that have static configuration information (including directory server port numbers) will continue to work.

3. Run the migration script. As root user (UNIX), or administrator (on NT), change directory to `/usr/iplanet/servers/bin/slapd/admin/bin`. Then enter the following command:

   On UNIX:

```
migrateInstance5 -D rootDN -w passwd -p port -o server4ID -n server5ID
```

   ON NT:

```
perl migrateInstance5 -D rootDN -w passwd -p port -o server4ID -n server5ID
```

   where:

   - *rootDN* is the DN for Directory Manager in Directory Server 5.0
   - *passwd* is the password for Directory Manager in Directory Server 5.0
   - *port* is the LDAP port number in Directory Server 5.0
   - *server4ID* is the path to the legacy Directory Server directory (for example, `/usr/netscape/server4/slapd-`*serverID*)
   - *server5ID* is the path to the Directory Server 5.0 directory (for example, `/usr/iplanet/servers/slapd-`*serverID*)

   The following is an example of an actual command on UNIX:

```
migrateInstance5 -D "cn=Directory Manager" -w secret -p 1389 -o
/usr/netscape/server4/slapd-coolwave -n /usr/iplanet/servers/slapd-coolwave
```

   The following is an example of an actual command on NT:

```
perl migrateInstance5 -D "cn=Directory Manager" -w secret -p 1389 -o
/usr/netscape/server4/slapd-coolwave -n /usr/iplanet/servers/slapd-coolwave
```

4. Provide a path and filename for your backup directory, or accept the default.

   The following is an extract of the script’s output:

```
Parse the configuration file:
/space/iPlanet/server4_11/slapd-coolwave/config/slapd.conf...

Suffix o=France.Sun.COM doesn't exist

Backend: MigratedDB_0 has been created !!!

Suffix dc=coolwave,dc=France,dc=Sun,dc=COM doesn't exist

Backend: MigratedDB_1 has been created !!!

For the suffix o=NetscapeRoot, we do nothing

Suffix dc=radius.fr doesn't exist

Backend: MigratedDB_2 has been created !!!

Update general server parameters...

Update successfully passwordHistory

Update global LDBM parameters...

Update successfully nsslapd-mode

Update specific backend parameters...

Migrate DSE entries...

Migrate attributes...

Migrate objectclasses...

Migrate indexes...

Migrate plugin's...
```

Your legacy Directory Server is then migrated. As a result of this migration, a new Directory Server 5.0 instance is installed using the configuration information obtained from your legacy Directory Server. In addition, the data from your old server is migrated to the new server and the new server is started.

Migrating a Replicated Site

This section describes the migration path that you can follow to migrate a replication topology of 4.x servers to a replication topology of 5.0 directory servers.

You can migrate instances of Directory Server 4.0, 4.1, 4.11, and 4.12 because these releases of the Directory Server can replicate to a Directory Server 5.0 configured as a consumer.

The constraints, approach, and a summary of the steps involved in migrating a replicated environment are provided below.

Constraints

The following constraints must be observed in order to successfully complete the migration of a replicated environment:

- The replication topology of legacy servers must be a valid topology.
- The new 5.0 Directory Server must be a consumer of a 4.x Directory Server.
- The 5.0 Directory Server must be configured as a legacy consumer.
- The replication agreement between the 4.x supplier server and the 5.0 consumer server must be a 4.x supplier-initiated replication agreement.

Approach

Given the constraints, the approach to migrating a replication topology of 4.x servers is to:

1. Install the 5.0 Directory Server, configure it both:
    - As a read-write replica that logs changes (the role the server will fulfill once the migration process is completed)
    - As a legacy consumer, (the role the server must play during the migration process)
2. Configure the 4.x supplier to send updates to the 5.0 Directory Server.
3. Upgrade 4.x consumer servers to Directory Server 5.0, and change their supplier server to be the Directory Server 5.0 that you configured in Step 1.

    This Directory Server now acts as a hub supplier.
4. Retire the 4.x supplier.

    The Directory Server 5.0 that you configured in Step 1 is now the only supplier in the topology.

Example: Detail of Steps

Consider a fairly simple replication topology:

- One supplier Server A
- Two consumer servers Server B and Server C

- Server A has a supplier-initiated replication agreement to Server B and to Server C
- Servers A, B, and C are 4.0, 4.1, 4.11, or 4.12 directory servers.

NOTE You can migrate a topology where Server B and Server C have CIR replication agreements with Server A. However, you cannot have CIR agreements in the new replication environment because Directory Server 5.0 does not support consumer-initiated replication.

To migrate this topology, follow these steps:

1. Install iPlanet Directory Server 5.0 on a new server, Server D.
2. Configure Server D for the role it will fulfill in the migrated replication topology, that is as a read-write replica that logs changes.

   This procedure is explained in the Replication chapter in the *iPlanet Directory Server Administrator's Guide.*
3. Then configure Server D to be a legacy consumer.

   This procedure is explained in the Replication chapter in the *iPlanet Directory Server Administrator's Guide.*
4. Upgrade Server B to iPlanet Directory Server 5.0, following the instructions given in the *iPlanet Directory Server Installation Guide.*
5. Make Server B a read-only replica of Server D.

   This means that Server D is now a hub supplier: it receives updates from Server A, and in turn updates Server B.
6. Upgrade Server C to iPlanet Directory Server 5.0, and make it a read-only replica of Server D.
7. Retire Server A. Disable legacy consumer settings on server D.

   This leaves Server D as the single supplier for consumer servers B and C.

When you have completed the migration of your replication topology, you can evolve it to use multi-master replication. To do this, you must add a new iPlanet Directory Server 5.0 that acts as a master to your replication topology. You cannot change one of the read-only replicas to become a read-write replica.

For more information on multi-master replication topologies, refer to the *iPlanet Directory Server Administrator's Guide*.

Chapter 7

Troubleshooting

This chapter describes the most common installation problems and how to solve them. It also provides some tips on checking patch levels and kernel parameter settings for your system.

Running idsktune

The `idsktune` utility provides an easy and reliable way of checking the patch levels and kernel parameter settings for your system. You must install the Directory Server before you can run `idsktune`. `idsktune` is not available for Windows NT or Windows 2000.

To run `idsktune`:

1. Change to the installation directory for your Directory Server.

   By default, this directory is `/usr/iplanet/servers`.

2. Change to the `bin/slapd/server` subdirectory.

3. As root, enter the following command:

   ```
   # ./idsktune
   ```

The following is an example of output that idsktune generates. Note that idsktune does not itself make any changes to the system.

```
iPlanet Directory Server system tuning analysis version 30-OCT-2000.
Copyright 2000 Sun Microsystems, Inc.
NOTICE : System is usparc-sun-solaris5.8 (SUNW,Ultra-5_10) (1 processor).
NOTICE : Patch 109320-01 is not installed.
```

```
NOTICE : Patch 108875-04 is present, but 108875-07 is a more recent version.

NOTICE : Patch 108652-04 is present, but 108652-13 is a more recent version.

NOTICE : Solaris patches can be obtained from http://sunsolve.sun.com or your
Solaris support representative.

WARNING: The tcp_close_wait_interval is set to 240000 milliseconds (240 seconds).
This value should be reduced to allow for more simultaneous connections to the
server. A line similar to the following should be added to the
/etc/init.d/inetinit file:

ndd -set /dev/tcp tcp_time_wait_interval 30000

NOTICE : The tcp_conn_req_max_q value is currently 128, which will limit the value
of listen backlog which can be configured.  It can be raised by adding to
/etc/init.d/inetinit, after any adb command, a line similar to:

ndd -set /dev/tcp tcp_conn_req_max_q 1024

NOTICE : The tcp_keepalive_interval is set to 7200000 milliseconds (120 minutes).
This may cause temporary server congestion from lost client connections.

NOTICE : The tcp_keepalive_interval can be reduced by adding the following line to
/etc/init.d/inetinit:

ndd -set /dev/tcp tcp_keepalive_interval 600000

NOTICE : The NDD tcp_rexmit_interval_initial is currently set to 3000 milliseconds
(3 seconds).  This may cause packet loss for clients on Solaris 2.5.1 due to a bug
in that version of Solaris.  If the clients are not using Solaris 2.5.1, no
problems should occur.

NOTICE : If the directory is service is intended only for LAN or private
high-speed WAN environment, this interval can be reduced by adding to
/etc/init.d/inetinit:

ndd -set /dev/tcp tcp_rexmit_interval_initial 500

NOTICE : The NDD tcp_smallest_anon_port is currently 32768.  This allows a maximum
of 32768 simultaneous connections.  More ports can be made available by adding a
line to /etc/init.d/inetinit:

ndd -set /dev/tcp tcp_smallest_anon_port 8192

WARNING: tcp_deferred_ack_interval is currently 100 milliseconds. This will cause
Solaris to insert artificial delays in the LDAP protocol. It should be reduced
during load testing.

This line can be added to the /etc/init.d/inetinit file:

ndd -set /dev/tcp tcp_deferred_ack_interval 5
```

```
WARNING: There are only 1024 file descriptors available, which limit the number of
simultaneous connections.  Additional file descriptors, up to 65536, are available
by adding to /etc/system a line like set rlim_fd_max=4096

NOTICE : / partition has less space available, 245MB, than the largest allowable
core file size of 460MB.  A daemon process which dumps core could cause the root
partition to be filled.

#
```

Common Installation Problems

Clients cannot locate the server.
First, try using the host name. If that does not work, use the fully qualified name (such as `www.domain.com`), and make sure the server is listed in the DNS. If that does not work, use the IP address.

The port is in use.
You probably did not shut down a server before you upgraded it. Shut down the old server, then manually start the upgraded one.

Another installed server might be using the port. Make sure the port you have chosen is not already being used by another server.

LDAP authentication error causes install to fail.
If you are installing Directory Server in a network which uses NIS naming rather than DNS naming, you may get the following error:

```
ERROR: Ldap authentication failed for url ldap://incorrect.DNS.address
user id admin (151:Unknown error.)

Fatal Slapd Did not add Directory Server information to
Configuration Server.

ERROR. Failure installing iPlanet Directory Server. Do you want to
continue [n]?
```

This error occurs when a machine is not correctly configured to use DNS naming. The default fully qualified host and domain name presented during installation is not correct. If you accept the defaults, you receive the LDAP authentication error.

To successfully install, you need to provide a fully qualified domain name that consists of a local host name along with its domain name. A host name is the logical name assigned to a computer. For example, `mycomputer` is a host name and `siroe.com` is a fully qualified domain name.

A fully qualified domain name should be sufficient to determine a unique Internet address for any host on the Internet. The same naming scheme is also used for some hosts that are not on the Internet, but share the same namespace for electronic mail addressing.

I have forgotten the Directory manager DN and password.
You can find out what the Directory Manager DN is by examining `/usr/iplanet/servers/slapd-`*server ID*`/config/dse.ldif` and looking for the `nsslapd-rootdn` attribute.

If you have forgotten the Directory Manager DN password, you can reset it by doing the following:

1. Find the `nsslapd-rootpw` attribute in slapd.conf. If the attribute value is not encrypted in any way (that is, it does not start with `{SHA}` or `{CRYPT}`) then the password is exactly what is shown on the parameter.
2. If the attribute is encrypted, then delete the attribute value and replace it with some clear text value. For example, if you change the `nsslapd-rootpw` attribute so that it is:

   ```
   nsslapd-rootpw: my_password
   ```

   then your Directory Manager DN password will be `my_password`.
3. Restart your Directory Server.
4. Once your server has restarted, login as the Directory Manager and change the password. Make sure you select an encryption scheme when you do so.

For information on changing a Directory Manager password, see the *iPlanet Directory Server Administrator's Guide*.

Glossary

access control instruction *See ACI.*

ACI Access Control Instruction. An instruction that grants or denies permissions to entries in the directory.

access control list *See ACL.*

ACL Access control list. The mechanism for controlling access to your directory.

access rights In the context of access control, specify the level of access granted or denied. Access rights are related to the type of operation that can be performed on the directory. The following rights can be granted or denied: read, write, add, delete, search, compare, self-write, proxy and all.

account inactivation Disables a user account, group of accounts, or an entire domain so that all authentication attempts are automatically rejected.

All IDs Threshold A size limit which is globally applied to every index key managed by the server. When the size of an individual ID list reaches this limit, the server replaces that ID list with an All IDs token.

All IDs token A mechanism which causes the server to assume that all directory entries match the index key. In effect, the All IDs token causes the server to behave as if no index was available for the search request.

anonymous access When granted, allows anyone to access directory information without providing credentials, and regardless of the conditions of the bind.

approximate index Allows for efficient approximate or “sounds-like” searches.

attribute Holds descriptive information about an entry. Attributes have a label and a value. Each attribute also follows a standard syntax for the type of information that can be stored as the attribute value.

attribute list A list of required and optional attributes for a given entry type or object class.

authenticating directory server In pass-through authentication (PTA), the authenticating directory server is the directory server that contains the authentication credentials of the requesting client. The PTA-enabled host sends PTA requests it receives from clients to the bind host.

authentication (1) Process of proving the identity of the client user to the Directory Server. Users must provide a bind DN and either the corresponding password or certificate in order to be granted access to the directory. Directory Server allows the user to perform functions or access files and directories based on the permissions granted to that user by the directory administrator.

(2) Allows a client to make sure they are connected to a secure server, preventing another computer from impersonating the server or attempting to appear secure when it is not.

authentication certificate Digital file that is not transferable and not forgeable and is issued by a third party. Authentication certificates are sent from server to client or client to server in order to verify and authenticate the other party.

base DN Base distinguished name. A search operation is performed on the base DN, the DN of the entry and all entries below it in the directory tree.

base distinguished name *See base DN*.

bind DN Distinguished name used to authenticate to Directory Server when performing an operation.

bind distinguished name *See bind DN*.

bind rule In the context of access control, the bind rule specifies the credentials and conditions that a particular user or client must satisfy in order to get access to directory information.

branch entry An entry that represents the top of a subtree in the directory.

browser Software, such as Netscape Navigator, used to request and view World Wide Web material stored as HTML files. The browser uses the HTTP protocol to communicate with the host server.

browsing index Otherwise known as the virtual view index, speeds up the display of entries in the Directory Server Console. Browsing indexes can be created on any branchpoint in the directory tree to improve display performance.

CA *See Certificate Authority.*

cascading replication In a cascading replication scenario, one server, often called the hub supplier acts both as a consumer and a supplier for a particular replica. It holds a read-only replica and maintains a change log. It receives updates from the supplier server that holds the master copy of the data, and in turn supplies those updates to the consumer.

certificate A collection of data that associates the public keys of a network user with their DN in the directory. The certificate is stored in within the directory as user object attributes.

Certificate Authority Company or organization that sells and issues authentication certificates. You may purchase an authentication certificate from a Certification Authority that you trust. Also known as a CA.

CGI Common Gateway Interface. An interface for external programs to communicate with the HTTP server. Programs written to use CGI are called CGI programs or CGI scripts, and can be written in many of the common programming languages. CGI programs handle forms or perform output parsing that is not done by the server itself.

chaining A method for relaying requests to another server. Results for the request are collected, compiled and then returned to the client.

change log A change log is record that describes the modifications that have occurred on a replica. The supplier server then replays these modifications on the replicas stored on consumer servers, or on other masters, in the case of multi-master replication.

character type Distinguishes alphabetic characters from numeric or other characters and the mapping of upper-case to lower-case letters.

ciphertext Encrypted information that cannot be read by anyone without the proper key to decrypt the information.

CIR *See consumer-initiated replication.*

class definition Specifies the information needed to create an instance of a particular object and determines how the object works in relation to other objects in the directory.

class of service *See CoS.*

classic CoS A classic CoS identifies the template entry by both its DN and the value of one of the target entry's attributes.

client *See LDAP client.*

code page An internal table used by a locale in the context of the internationalization plug-in that the operating system uses to relate keyboard keys to character font screen displays.

collation order Provides language and cultural-specific information about how the characters of a given language are to be sorted. This information might include the sequence of letters in the alphabet or how to compare letters with accents to letters without accents.

consumer Server containing replicated directory trees or subtrees from a supplier server.

consumer-initiated replication Replication configuration where consumer servers pull directory data from supplier servers.

consumer server In the context of replication, a server that holds a replica that is copied from a different server is called a consumer for that replica.

CoS A method for sharing attributes between entries in a way that is invisible to applications.

CoS definition entry Identifies the type of CoS you are using. It is stored as an LDAP subentry below the branch it affects.

CoS template entry Contains a list of the shared attribute values.

daemon A background process on a Unix machine that is responsible for a particular system task. Daemon processes do not need human intervention to continue functioning.

DAP Directory Access Protocol. The ISO X.500 standard protocol that provides client access to the directory.

Data Master The server that is the master source of a particular piece of data.

database link An implementation of chaining. The database link behaves like a database but has no persistent storage. Instead, it points to data stored remotely.

default index One of a set of default indexes created per database instance. Default indexes can be modified, although care should be taken before removing them, as certain plug-ins may depend on them.

definition entry *See CoS definition entry.*

Directory Access Protocol *See DAP.*

directory tree The logical representation of the information stored in the directory. It mirrors the tree model used by most file systems, with the tree's root point appearing at the top of the hierarchy. Also known as DIT.

Directory Manager The privileged database administrator, comparable to the root user in UNIX. Access control does not apply to the directory manager.

Directory Server Gateway (DSGW) A collection of CGI forms that allows a browser to perform LDAP client functions, such as querying and accessing a Directory Server, from a web browser.

directory service A database application designed to manage descriptive, attribute-based information about people and resources within an organization.

distinguished name String representation of an entry's name and location in an LDAP directory.

DIT *See directory tree.*

DM *See Directory Manager.*

DNS Domain Name System. The system used by machines on a network to associate standard IP addresses (such as 198.93.93.10) with hostnames (such as `www.iPlanet.com`). Machines normally get the IP address for a hostname from a DNS server, or they look it up in tables maintained on their systems.

DNS alias A DNS alias is a hostname that the DNS server knows points to a different host—specifically a DNS CNAME record. Machines always have one real name, but they can have one or more aliases. For example, an alias such as `www.[yourdomain].[domain]` might point to a real machine called `realthing.[yourdomain].[domain]` where the server currently exists.

DSGW *See Directory Server Gateway (DSGW).*

entry A group of lines in the LDIF file that contains information about an object.

entry distribution Method of distributing directory entries across more than one server in order to scale to support large numbers of entries.

entry ID list Each index that the directory uses is composed of a table of index keys and matching entry ID lists. The entry ID list is used by the directory to build a list of candidate entries that may match the client application's search request.

equality index Allows you to search efficiently for entries containing a specific attribute value.

file extension The section of a filename after the period or dot (.) that typically defines the type of file (for example, .GIF and .HTML). In the filename `index.html` the file extension is `html`.

file type The format of a given file. For example, graphics files are often saved in GIF format, while a text file is usually saved as ASCII text format. File types are usually identified by the file extension (for example, .GIF or .HTML).

filter A constraint applied to a directory query that restricts the information returned.

filtered role Allows you to assign entries to the role depending upon the attribute contained by each entry. You do this by specifying an LDAP filter. Entries that match the filter are said to possess the role.

gateway *See Directory Server Gateway (DSGW).*

general access When granted, indicates that all authenticated users can access directory information.

hostname A name for a machine in the form machine.domain.dom, which is translated into an IP address. For example, `www.iPlanet.com` is the machine www in the subdomain iPlanet and com domain.

HTML Hypertext Markup Language. The formatting language used for documents on the World Wide Web. HTML files are plain text files with formatting codes that tell browsers such as the Netscape Navigator how to display text, position graphics and form items, and display links to other pages.

HTTP Hypertext Transfer Protocol. The method for exchanging information between HTTP servers and clients.

HTTPD An abbreviation for the HTTP daemon or service, a program that serves information using the HTTP protocol. The daemon or service is often called an httpd.

HTTP-NG The next generation of Hypertext Transfer Protocol.

HTTPS A secure version of HTTP, implemented using the Secure Sockets Layer, SSL.

hub supplier In the context of replication, a server that holds a replica that is copied from a different server, and in turn replicates it to a third server. See also cascading replication.

index key Each index that the directory uses is composed of a table of index keys and matching entry ID lists.

indirect CoS An indirect CoS identifies the template entry using the value of one of the target entry's attributes.

international index Speeds up searches for information in international directories.

International Standards Organization *See ISO.*

IP address Internet Protocol address. A set of numbers, separated by dots, that specifies the actual location of a machine on the Internet (for example, 198.93.93.10).

ISO International Standards Organization

knowledge reference Pointers to directory information stored in different databases.

LDAP Lightweight Directory Access Protocol. Directory service protocol designed to run over TCP/IP and across multiple platforms.

LDAPv3 Version 3 of the LDAP protocol, upon which Directory Server bases its schema format

LDAP client Software used to request and view LDAP entries from an LDAP Directory Server. See also *browser*.

LDAP Data Interchange Format *See LDAP Data Interchange Format.*

LDAP URL Provides the means of locating directory servers using DNS and then completing the query via LDAP. A sample LDAP URL is `ldap://ldap.iplanet.com`

LDBM database A high-performance, disk-based database consisting of a set of large files that contain all of the data assigned to it. The primary data store in Directory Server.

LDIF LDAP Data Interchange Format. Format used to represent Directory Server entries in text form.

leaf entry An entry under which there are no other entries. A leaf entry cannot be a branch point in a directory tree.

Lightweight Directory Access Protocol *See LDAP.*

locale Identifies the collation order, character type, monetary format and time / date format used to present data for users of a specific region, culture, and / or custom. This includes information on how data of a given language is interpreted, stored, or collated. The locale also indicates which code page should be used to represent a given language.

managed object A standard value which the SNMP agent can access and send to the NMS. Each managed object is identified with an official name and a numeric identifier expressed in dot-notation.

managed role Allow you to create an explicit enumerated list of members.

management information base *See MIB.*

mapping tree A data structure that associates the names of suffixes (subtrees) with databases.

master agent *See SNMP master agent.*

matching rule Provides guidelines for how the server compares strings during a search operation. In an international search, the matching rule tells the server what collation order and operator to use.

MD5 A message digest algorithm by RSA Data Security, Inc., which can be used to produce a short digest of data, that is unique with high probability, and is mathematically extremely hard to produce a piece of data that will produce the same message digest.

MD5 signature A message digest produced by the MD5 algorithm.

MIB Management Information Base. All data, or any portion thereof, associated with the SNMP network. We can think of the MIB as a database which contains the definitions of all SNMP managed objects. The MIB has a tree like hierarchy, where the top level contains the most general information about the network and lower levels deal with specific, separate network areas.

MIB namespace Management Information Namespace. The means for directory data to be named and referenced. Also called the directory tree.

monetary format Specifies the monetary symbol used by specific region, whether the symbol goes before or after its value, and how monetary units are represented.

multi-master replication An advanced replication scenario in which two servers each hold a copy of the same read-write replica. Each server maintains a change log for the replica. Modifications made on one server are automatically replicated to the other server. In case of conflict, a time stamp is used to determine which server holds the most recent version.

multiplexor The server containing the database link that communicates with the remote server.

n + 1 directory problem The problem of managing multiple instances of the same information in different directories, resulting in increased hardware and personnel costs.

name collisions Multiple entries with the same distinguished name.

nested role Allow you to create roles that contain other roles.

network management application Network Management Station component that graphically displays information about SNMP managed devices (which device is up or down, which and how many error messages were received, etc.).

network management station *See NMS.*

NIS Network Information Service. A system of programs and data files that Unix machines use to collect, collate, and share specific information about machines, users, file systems, and network parameters throughout a network of computers.

NMS Network Management Station. Powerful workstation with one or more network management applications installed.

ns-slapd iPlanet's LDAP Directory Server daemon or service that is responsible for all actions of the Directory Server. See also slapd.

object class Defines an entry type in the directory by defining which attributes are contained in the entry.

object identifier A string, usually of decimal numbers, that uniquely identifies a schema element, such as an object class or an attribute, in an object-oriented system. Object identifiers are assigned by ANSI, IETF or similar organizations.

OID *See object identifier.*

operational attributes Operational attributes contain information used internally by the directory to keep track of modifications and subtree properties. They are not returned in response to a search unless explicitly requested.

parent access When granted, indicates that users have access to entries below their own in the directory tree, that is, if the bind DN is the parent of the targeted entry.

pass-through authentication *See PTA.*

pass-through subtree In pass-through authentication, the PTA directory server will pass through bind requests to the authenticating directory server from all clients whose DN is contained in this subtree.

password file A file on Unix machines that stores Unix user login names, passwords, and user ID numbers. It is also known as `/etc/passwd`, because of where it is kept.

password policy A set of rules that govern how passwords are used in a given directory.

permission In the context of access control, the permission states whether access to the directory information is granted or denied, and the level of access that is granted or denied. See access rights.

PDU Protocol Data Unit. Encoded messages which form the basis of data exchanges between SNMP devices.

pointer CoS A pointer CoS identifies the template entry using the template DN only.

presence index Allows you to search for entries that contain a specific indexed attribute.

protocol A set of rules that describes how devices on a network exchange information.

protocol data unit *See PDU.*

proxy authentication A special form of authentication where the user requesting access to the directory does not bind with its own DN but with a proxy DN.

proxy DN Used with proxied authorization. The proxy DN is the DN of an entry that has access permissions to the target on which the client-application is attempting to perform an operation.

PTA Pass-through authentication. Mechanism by which one directory server consults another to check bind credentials.

PTA directory server In pass-through authentication (PTA), the PTA directory server is the server that sends (passes through) bind requests it receives to the authenticating directory server.

PTA LDAP URL In pass-through authentication, the URL that defines the authenticating directory server, pass-through subtree(s) and optional parameters.

RAM Random access memory. The physical semiconductor-based memory in a computer. Information stored in RAM is lost when the computer is shut down.

rc.local A file on Unix machines that describes programs that are run when the machine starts. It is also called `/etc/rc.local` because of its location.

RDN Relative distinguished name. The name of the actual entry itself, before the entry's ancestors have been appended to the string to form the full distinguished name.

referential integrity Mechanism that ensures that relationships between related entries are maintained within the directory.

referral (1) When a server receives a search or update request from an LDAP client that it cannot process, it usually sends back to the client a pointer to the LDAP sever that can process the request.

(2) In the context of replication, when a read-only replica receives an update request, it forwards it to the server that holds the corresponding read-write replica. This forwarding process is called a referral.

replica A database that participates in replication

read-only replica A replica that refers all update operations to read-write replicas. A server can hold any number of read-only replicas.

read-write replica A replica that contains a master copy of directory information and can be updated. A server can hold any number of read-write replicas.

relative distinguished name *See RDN*.

replication Act of copying directory trees or subtrees from supplier servers to consumer servers.

replication agreement Set of configuration parameters that are stored on the supplier server and identify the databases to replicate, the consumer servers to which the data is pushed, the times during which replication can occur, the DN and credentials used by the supplier to bind to the consumer, and how the connection is secured.

RFC Request For Comments. Procedures or standards documents submitted to the Internet community. People can send comments on the technologies before they become accepted standards.

role An entry grouping mechanism. Each role has *members*, which are the entries that possess the role.

role-based attributes Attributes that appear on an entry because it possesses a particular role within an associated CoS template.

root The most privileged user available on Unix machines. The root user has complete access privileges to all files on the machine.

root suffix The parent of one or more sub suffixes. A directory tree can contain more than one root suffix.

schema Definitions describing what types of information can be stored as entries in the directory. When information that does not match the schema is stored in the directory, clients attempting to access the directory may be unable to display the proper results.

schema checking Ensures that entries added or modified in the directory conform to the defined schema. Schema checking is on by default and users will receive an error if they try to save an entry that does not conform to the schema.

Secure Sockets Layer *See SSL.*

self access When granted, indicates that users have access to their own entries, that is, if the bind DN matches the targeted entry.

Server Console Java-based application that allows you to perform administrative management of your Directory Server from a GUI.

server daemon The server daemon is a process that, once running, listens for and accepts requests from clients.

server service The server service is a process on Windows NT that, once running, listens for and accepts requests from clients. It is the SMB server on Windows NT.

server root A directory on the server machine dedicated to holding the server program and configuration, maintenance, and information files.

Server Selector Interface that allows you select and configure servers using a browser.

service A background process on a Windows NT machine that is responsible for a particular system task. Service processes do not need human intervention to continue functioning.

SIE Server Instance Entry.

Simple Network Management Protocol *See SNMP.*

single-master replication The most basic replication scenario in which two servers each hold a copy of the same read-write replicas to consumer servers. In a single-master replication scenario, the supplier server maintains a change log.

SIR *See supplier-initiated replication.*

slapd LDAP Directory Server daemon or service that is responsible for most functions of a directory except replication. See also *ns-slapd*.

SNMP Simple Network Management Protocol. Used to monitor and manage application processes running on the servers, by exchanging data about network activity.

SNMP master agent Software that exchanges information between the various subagents and the NMS.

SNMP subagent Software that gathers information about the managed device and passes the information to the master agent.

SSL Secure Sockets Layer. A software library establishing a secure connection between two parties (client and server) used to implement HTTPS, the secure version of HTTP.

standard index Indexes that are maintained by default.

sub suffix A branch underneath a root suffix.

subagent *See SNMP subagent*.

substring index Allows for efficient searching against substrings within entries. Substring indexes are limited to a minimum of two characters for each entry.

suffix The name of the entry at the top of the directory tree, below which data is stored. Multiple suffixes are possible within the same directory. Each database only has one suffix.

superuser The most privileged user available on Unix machines (also called root). The superuser has complete access privileges to all files on the machine.

supplier Server containing the master copy of directory trees or subtrees that are replicated to consumer servers.

supplier server In the context of replication, a server that holds a replica that is copied to a different server is called a supplier for that replica.

supplier-initiated replication Replication configuration where supplier servers replicate directory data to consumer servers.

symmetric encryption Encryption that uses the same key for both encrypting and decrypting. DES is an example of a symmetric encryption algorithm.

system index Cannot be deleted or modified as it is essential to Directory Server operations.

target In the context of access control, the target identifies the directory information to which a particular ACI applies.

target entry The entries within the scope of a CoS.

TCP/IP Transmission Control Protocol / Internet Protocol. The main network protocol for the Internet and for enterprise (company) networks.

template entry *See CoS template entry*.

time / date format Indicates the customary formatting for times and dates in a specific region.

TLS Transport Layer Security. The new standard for secure socket layers, a public key based protocol.

topology The way a directory tree is divided among physical servers and how these servers link with one another.

Transport Layer Security *See TLS*.

uid A unique number associated with each user on a Unix system.

URL Uniform Resource Locator. The addressing system used by the server and the client to request documents. It is often called a location. The format of a URL is `[protocol]://[machine:port]/[document]`. The port number is necessary only on selected servers, and it is often assigned by the server, freeing the user of having to place it in the URL.

virtual list view index Otherwise known as a browsing index, speeds up the display of entries in the Directory Server Console. Virtual list view indexes can be created on any branchpoint in the directory tree to improve display performance.

X.500 standard The set of ISO / ITU-T documents outlining the recommended information model, object classes and attributes used by directory server implementations.

Index

I

L

M

N

P

R

S

T

U