Sun Java System Directory Server Enterprise Edition 6.0 Evaluation Guide

Sun™ microsystems

Contents

Preface

This *Evaluation Guide* describes the key features available in Directory Server Enterprise Edition software. Using examples, this guide provides a look at key features. To explore the features in-depth, refer to the Evaluation Toolkit.

Who Should Use This Book

This guide is intended for anyone evaluating Directory Server Enterprise Edition functionality.

The author of this guide assumes you are familiar with the following:

- LDAP and related protocols, such as DSML v2
- Internet and World Wide Web technologies
- Other services such as those provided by relational databases or Microsoft Active Directory

How This Book Is Organized

Chapter 1 provides an introduction to the Directory Server Enterprise Edition components, describes the new administration model, and summarizes the latest features.

Chapter 2 outlines where to get component products, how to install them, and where to go for the Evaluation Kit.

Chapter 3 shows you powerful features available for managing your directory service, including the through the Web-based Directory Service Control Center and the advanced command-line interface.

Chapter 4 provides a quick tour of the Directory Server Enterprise Edition features that provide high data availability and integrity.

Chapter 5 provides an introduction to the Directory Server features of DSEE that help you tune your deployment for best performance.

Chapter 6 describes the features of DSEE that secure identity to the highest degree possible

Chapter 7 describes the features of DSEE that give it the ability to support hundreds of millions and even billions of entry deployments.

Chapter 8 demonstrates DSEE virtual directory capabilities, which aggregate a single namespace from multiple heterogeneous data repositories.

Chapter 9 introduces the key features of Identity Synchronization for Windows, the software in DSEE that integrates Microsoft Active Directory and the Windows NT SAM registry into your directory service deployment.

Appendix A summarizes the standards and RFCs supported by this version of the Directory Server Enterprise Edition software.

Directory Server Enterprise Edition Documentation Set

This Directory Server Enterprise Edition documentation set explains how to use Sun Java System Directory Server Enterprise Edition to evaluate, design, deploy, and administer directory services. In addition, it shows how to develop client applications for Directory Server Enterprise Edition. The Directory Server Enterprise Edition documentation set is available at http://docs.sun.com/coll/1224.1.

For an introduction to Directory Server Enterprise Edition, review the following documents in the order in which they are listed.

TABLE P–1 Directory Server Enterprise Edition Documentation

Document Title	Contents
Sun Java System Directory Server Enterprise Edition 6.0 Release Notes	Contains the latest information about Directory Server Enterprise Edition, including known problems.
Sun Java System Directory Server Enterprise Edition 6.0 Documentation Center	Contains links to key areas of the documentation set.
Sun Java System Directory Server Enterprise Edition 6.0 Evaluation Guide	Introduces the key features of this release. Demonstrates how these features work and what they offer in the context of a fictional deployment that you can implement on a single system.
Sun Java System Directory Server Enterprise Edition 6.0 Deployment Planning Guide	Explains how to plan and design highly available, highly scalable directory services based on Directory Server Enterprise Edition. Presents the basic concepts and principles of deployment planning and design. Discusses the solution life cycle, and provides high-level examples and strategies to use when planning solutions based on Directory Server Enterprise Edition.

TABLE P–1 Directory Server Enterprise Edition Documentation   *(Continued)*

Document Title	Contents
Sun Java System Directory Server Enterprise Edition 6.0 Installation Guide	Explains how to install the Directory Server Enterprise Edition software. Shows how to select which components to install, configure those components after installation, and verify that the configured components function properly.
	For instructions on installing Directory Editor, go to http://docs.sun.com/coll/DirEdit_05q1.
	Make sure you read the information in *Sun Java System Directory Server Enterprise Edition 6.0 Release Notes* concerning Directory Editor before you install Directory Editor.
Sun Java System Directory Server Enterprise Edition 6.0 Migration Guide	Provides instructions for upgrading components from earlier versions of Directory Server, Directory Proxy Server, and Identity Synchronization for Windows.
Sun Java System Directory Server Enterprise Edition 6.0 Administration Guide	Provides command-line instructions for administering Directory Server Enterprise Edition.
	For hints and instructions on using the Directory Service Control Center, DSCC, to administer Directory Server Enterprise Edition, see the online help provided in DSCC.
	For instructions on administering Directory Editor, go to http://docs.sun.com/coll/DirEdit_05q1.
	For instructions on installing and configuring Identity Synchronization for Windows, see Part II, "Installing Identity Synchronization for Windows," in *Sun Java System Directory Server Enterprise Edition 6.0 Installation Guide*.
Sun Java System Directory Server Enterprise Edition 6.0 Developer's Guide	Shows how to develop server plug-ins with the APIs that are provided as part of Directory Server Enterprise Edition.
Sun Java System Directory Server Enterprise Edition 6.0 Reference	Introduces the technical and conceptual foundations of Directory Server Enterprise Edition. Describes its components, architecture, processes, and features. Also provides a reference to the developer APIs.
Sun Java System Directory Server Enterprise Edition 6.0 Man Page Reference	Describes the command-line tools, schema objects, and other public interfaces that are available through Directory Server Enterprise Edition. Individual sections of this document can be installed as online manual pages.
Sun Java System Identity Synchronization for Windows 6.0 Deployment Planning Guide	Provides general guidelines and best practices for planning and deploying Identity Synchronization for Windows

Related Reading

The SLAMD Distributed Load Generation Engine (SLAMD) is a Java™ application that is designed to stress test and analyze the performance of network-based applications. It was originally developed by Sun Microsystems, Inc. to benchmark and analyze the performance of LDAP directory servers. SLAMD is available as an open source application under the Sun Public License, an OSI-approved open source license. To obtain information about SLAMD, go to `http://www.slamd.com/`. SLAMD is also available as a java.net project. See `https://slamd.dev.java.net/`.

Java Naming and Directory Interface (JNDI) technology supports accessing the Directory Server using LDAP and DSML v2 from Java applications. For information about JNDI, see `http://java.sun.com/products/jndi/`. The *JNDI Tutorial* contains detailed descriptions and examples of how to use JNDI. This tutorial is at `http://java.sun.com/products/jndi/tutorial/`.

Directory Server Enterprise Edition can be licensed as a standalone product, as a component of Sun Java Enterprise System, as part of a suite of Sun products, such as the Sun Java Identity Management Suite, or as an add-on package to other software products from Sun. Java Enterprise System is a software infrastructure that supports enterprise applications distributed across a network or Internet environment. If Directory Server Enterprise Edition was licensed as a component of Java Enterprise System, you should be familiar with the system documentation at `http://docs.sun.com/coll/1286.2`.

Identity Synchronization for Windows uses Message Queue with a restricted license. Message Queue documentation is available at `http://docs.sun.com/coll/1307.2`.

Identity Synchronization for Windows works with Microsoft Windows password policies.

- Information about password policies for Windows 2003 is available in the Microsoft documentation online.
- Information about changing passwords, and about group policies in Windows 2003 is available the Microsoft documentation online.
- Information about the Microsoft Certificate Services Enterprise Root certificate authority is available in the Microsoft support documentation online.
- Information about configuring LDAP over SSL on Microsoft systems is available in the Microsoft support documentation online.

Redistributable Files

Directory Server Enterprise Edition does not provide any files that you can redistribute.

Default Paths and Command Locations

This section explains the default paths used in the documentation, and gives the locations of commands on different operating systems and deployment types.

Default Paths

The table in this section describes the default paths that are used in this document. For full descriptions of the files installed, see also Chapter 15, "Directory Server File Reference," in *Sun Java System Directory Server Enterprise Edition 6.0 Reference*, Chapter 26, "Directory Proxy Server File Reference," in *Sun Java System Directory Server Enterprise Edition 6.0 Reference*, or Appendix A, "Directory Server Resource Kit File Reference," in *Sun Java System Directory Server Enterprise Edition 6.0 Reference*.

TABLE P–2   Default Paths

Placeholder	Description	Default Value
install-path	Represents the base installation directory for Directory Server Enterprise Edition software. The software is installed in directories below this base *install-path*. For example, Directory Server software is installed in *install-path*/ds6/.	When you install from a zip distribution using dsee_deploy(1M), the default *install-path* is the current directory. You can set the *install-path* using the -i option of the dsee_deploy command. When you install from a native package distribution, such as you would using the Java Enterprise System installer, the default *install-path* is one of the following locations: ■ Solaris systems - /opt/SUNWdsee/. ■ HP-UX systems - /opt/sun/. ■ Red Hat systems - /opt/sun/. ■ Windows systems - C:\Program Files\Sun\JavaES5\DSEE.
instance-path	Represents the full path to an instance of Directory Server or Directory Proxy Server. The documentation uses /local/ds/ for Directory Server and /local/dps/ for Directory Proxy Server.	No default path exists. Instance paths must nevertheless always be found on a *local* file system. The following directories are recommended: /var on Solaris systems /global if you are using Sun Cluster

TABLE P–2 Default Paths *(Continued)*

Placeholder	Description	Default Value
serverroot	Represents the parent directory of the Identity Synchronization for Windows installation location	Depends on your installation. Note the concept of a *serverroot* no longer exists for Directory Server.
isw-*hostname*	Represents the Identity Synchronization for Windows instance directory	Depends on your installation
*/path/to/*cert8.db	Represents the default path and file name of the client's certificate database for Identity Synchronization for Windows	*current-working-dir*/cert8.db
serverroot/isw-*hostname*/logs/	Represents the default path to the Identity Synchronization for Windows local logs for the System Manager, each connector, and the Central Logger	Depends on your installation
serverroot/isw-*hostname*/logs/central/	Represents the default path to the Identity Synchronization for Windows central logs	Depends on your installation

Command Locations

The table in this section provides locations for commands that are used in Directory Server Enterprise Edition documentation. To learn more about each of the commands, see the relevant man pages.

TABLE P–3 Command Locations

Command	Java ES, Native Package Distribution	Zip Distribution
cacaoadm	Solaris - /usr/sbin/cacaoadm	Solaris - *install-path*/dsee6/cacao_2.0/usr/lib/cacao/bin/cacaoadm
	Red Hat, HP-UX - /opt/sun/cacao/bin/cacaoadm	Red Hat, HP-UX - *install-path*/dsee6/cacao_2.0/cacao/bin/cacaoadm
	Windows - *install-path*\share\cacao_2.0\bin\cacaoadm.bat	Windows - *install-path*\dsee6\cacao_2.0\bin\cacaoadm.bat

TABLE P–3 Command Locations *(Continued)*

Command	Java ES, Native Package Distribution	Zip Distribution
certutil	Solaris - /usr/sfw/bin/certutil Red Hat, HP-UX - /opt/sun/private/bin/certutil	*install-path*/dsee6/bin/certutil
dpadm(1M)	*install-path*/dps6/bin/dpadm	*install-path*/dps6/bin/dpadm
dpconf(1M)	*install-path*/dps6/bin/dpconf	*install-path*/dps6/bin/dpconf
dsadm(1M)	*install-path*/ds6/bin/dsadm	*install-path*/ds6/bin/dsadm
dsccmon(1M)	*install-path*/dscc6/bin/dsccmon	*install-path*/dscc6/bin/dsccmon
dsccreg(1M)	*install-path*/dscc6/bin/dsccreg	*install-path*/dscc6/bin/dsccreg
dsccsetup(1M)	*install-path*/dscc6/bin/dsccsetup	*install-path*/dscc6/bin/dsccsetup
dsconf(1M)	*install-path*/ds6/bin/dsconf	*install-path*/ds6/bin/dsconf
dsee_deploy(1M)	Not provided	*install-path*/dsee6/bin/dsee_deploy
dsmig(1M)	*install-path*/ds6/bin/dsmig	*install-path*/ds6/bin/dsmig
entrycmp(1)	*install-path*/ds6/bin/entrycmp	*install-path*/ds6/bin/entrycmp
fildif(1)	*install-path*/ds6/bin/fildif	*install-path*/ds6/bin/fildif
idsktune(1M)	*install-path*/dsrk6/bin/idsktune	*install-path*/dsrk6/bin/idsktune
insync(1)	*install-path*/ds6/bin/insync	*install-path*/ds6/bin/insync
ns-accountstatus(1M)	*install-path*/ds6/bin/ns-accountstatus	*install-path*/ds6/bin/ns-accountstatus
ns-activate(1M)	*install-path*/ds6/bin/ns-activate	*install-path*/ds6/bin/ns-activate
ns-inactivate(1M)	*install-path*/ds6/bin/ns-inactivate	*install-path*/ds6/bin/ns-inactivate
repldisc(1)	*install-path*/ds6/bin/repldisc	*install-path*/ds6/bin/repldisc
schema_push(1M)	*install-path*/ds6/bin/schema_push	*install-path*/ds6/bin/schema_push
smcwebserver	Solaris, Linux, HP-UX - /usr/sbin/smcwebserver Windows - *install-path*\share\ webconsole\bin\smcwebserver	This command pertains only to Directory Service Control Center, which is not available in the zip distribution.

TABLE P–3   Command Locations   *(Continued)*

Command	Java ES, Native Package Distribution	Zip Distribution

wcadmin	Solaris, Linux, HP-UX -
	
	`/usr/sbin/wcadmin`
	
	Windows -
	
	install-path`\share\`
	`webconsole\bin\wcadmin`
		This command pertains only to Directory Service Control Center, which is not available in the zip distribution.

Typographic Conventions

The following table describes the typographic changes that are used in this book.

TABLE P–4   Typographic Conventions

Typeface	Meaning	Example
AaBbCc123	The names of commands, files, and directories, and onscreen computer output	Edit your `.login` file. Use `ls -a` to list all files. `machine_name% you have mail.`
AaBbCc123	What you type, contrasted with onscreen computer output	`machine_name%` **su** `Password:`
AaBbCc123	A placeholder to be replaced with a real name or value	The command to remove a file is `rm` *filename*.
AaBbCc123	Book titles, new terms, and terms to be emphasized (note that some emphasized items appear bold online)	Read Chapter 6 in the *User's Guide*. A *cache* is a copy that is stored locally. Do *not* save the file.

Shell Prompts in Command Examples

The following table shows default system prompts and superuser prompts.

TABLE P–5   Shell Prompts

Shell	Prompt
C shell on UNIX and Linux systems	`machine_name%`
C shell superuser on UNIX and Linux systems	`machine_name#`

TABLE P–5 Shell Prompts *(Continued)*

Shell	Prompt
Bourne shell and Korn shell on UNIX and Linux systems	`$`
Bourne shell and Korn shell superuser on UNIX and Linux systems	`#`
Microsoft Windows command line	`C:\`

Symbol Conventions

The following table explains symbols that might be used in this book.

TABLE P–6 Symbol Conventions

Symbol	Description	Example	Meaning
`[ ]`	Contains optional arguments and command options.	`ls [-l]`	The `-l` option is not required.
`{	}`	Contains a set of choices for a required command option.	`-d {y|n}`	The `-d` option requires that you use either the `y` argument or the `n` argument.
`${ }`	Indicates a variable reference.	`${com.sun.javaRoot}`	References the value of the `com.sun.javaRoot` variable.
`-`	Joins simultaneous multiple keystrokes.	Control-A	Press the Control key while you press the A key.
`+`	Joins consecutive multiple keystrokes.	Ctrl+A+N	Press the Control key, release it, and then press the subsequent keys.
$\rightarrow$	Indicates menu item selection in a graphical user interface.	File $\rightarrow$ New $\rightarrow$ Templates	From the File menu, choose New. From the New submenu, choose Templates.

Documentation, Support, and Training

The Sun web site provides information about the following additional resources:

- Documentation (http://www.sun.com/documentation/)
- Support (http://www.sun.com/support/)
- Training (http://www.sun.com/training/)

15

Third-Party Web Site References

Third-party URLs are referenced in this document and provide additional, related information.

Note – Sun is not responsible for the availability of third-party web sites mentioned in this document. Sun does not endorse and is not responsible or liable for any content, advertising, products, or other materials that are available on or through such sites or resources. Sun will not be responsible or liable for any actual or alleged damage or loss caused or alleged to be caused by or in connection with use of or reliance on any such content, goods, or services that are available on or through such sites or resources.

Searching Sun Product Documentation

Besides searching for Sun product documentation from the docs.sun.com web site, you can use a search engine of your choice by typing the following syntax in the search field:

search-term `site:docs.sun.com`

For example, to search for `Directory Server`, type the following:

`"Directory Server" site:docs.sun.com`

To include other Sun web sites in your search, such as java.sun.com, www.sun.com, and developers.sun.com, use `sun.com` in place of `docs.sun.com` in the search field.

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions. To share your comments, go to `http://docs.sun.com` and click Send Comments. In the online form, provide the full document title and part number. The part number is a 7-digit or 9-digit number that can be found on the book's title page or in the document's URL. For example, the part number of this book is 819-0998.

1

Overview of Directory Server Enterprise Edition and the Latest Features

This chapter provides an introduction to the Sun Java™ System Directory Server Enterprise Edition6.0 components, describes the new administration model, and summarizes the latest features. This chapter covers the following topics:

DSEE Components

Directory Server Enterprise Edition (DSEE) serves as the backbone to an enterprise identity infrastructure. DSEE includes the following components:

- **Directory Service Control Center (DSCC)**. Provides a browser-based administration interface to handle the configuration of directory and directory proxy services.

- **Directory Server**. Provides the highly scalable, secure, flexible means to store and manage identity data.

- **Directory Proxy Server**. Enhances security, offers virtual directory capabilities, and further increases directory service availability and scalability.

- **Identity Synchronization for Windows**. Brings bidirectional, on-demand synchronization with Microsoft Active Directory and with Microsoft Windows NT SAM Registry.

- **Directory Editor**. Offers a configurable, browser-based user interface to manage directory content.

- **Directory Server Resource Kit (DSRK)**. Includes a set of utilities to access and tune directory services. The DSRK supports the Lightweight Directory Access Protocol (LDAP) v2 and v3, and the Directory Services Markup Language (DSML) v2. You can use the DSRK to create custom applications to access your directory data.

New Administration Model

DSEE includes a completely new administration architecture. Before you can evaluate the features of DSEE, you need to understand the basics of this new architecture.

In DSEE 6.0, all previous administrative interfaces (the Java console and the `ldapmodify` and `ldapsearch` commands) are replaced by two new administrative interfaces:

- A web-based console
- A command-line interface

As an administrator, you can perform most administrative tasks with either interface. The following figure illustrates the DSEE administration framework.
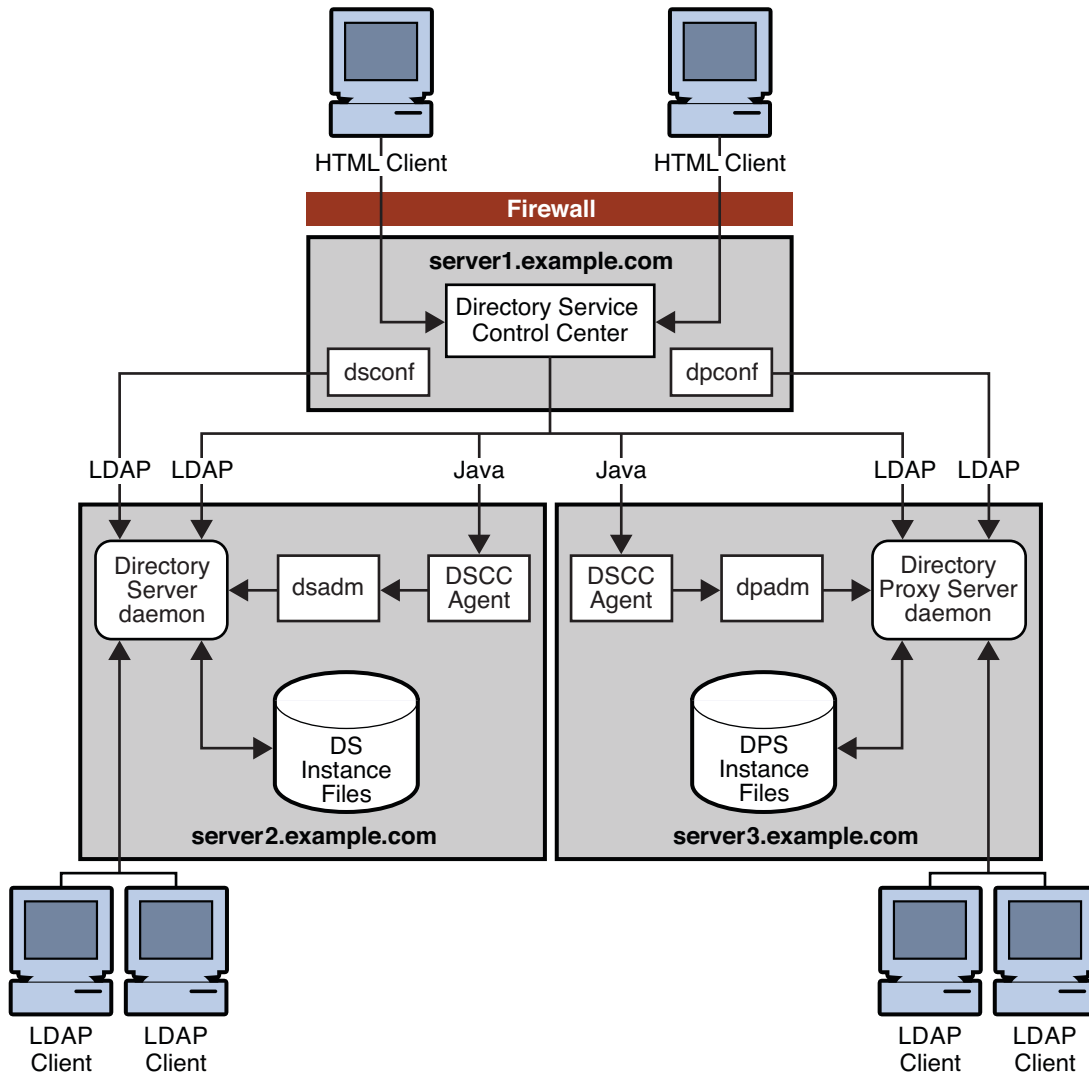
FIGURE 1–1   Directory Server Enterprise Edition 6.0 Administration Framework

This administration framework supports Directory Server and Directory Proxy Server and consists of the following components:

- **Directory Service Control Center (DSCC).** The graphical user interface used to administer Directory Server and Directory Proxy Server instances. The DSCC plugs into the Sun Java Web Console. The DSCC registry maintains a list of registered Directory Servers and Directory Proxy Servers and enables you to group multiple server instances into a single directory service.

Chapter 1 • Overview of Directory Server Enterprise Edition and the Latest Features

19

- **DSCC agents**. One DSCC agent runs on each server through which you remotely administer Directory Server or Directory Proxy Server. The DSCC agent runs the local Directory Server and Directory Proxy Server commands for administering local instances of Directory Server.

- Directory Server and Directory Proxy Server product installation on local or remote servers.

- Directory Server and Directory Proxy Server instances created on local or remote servers.

Although this guide provides information about both the console and the command-line interface (CLI), the console is usually shown when illustrating a feature. However, the Evaluation Kit provides numerous CLI examples to demonstrate the features of the CLI.

For a more in-depth description of the new administration model, see "Directory Server Enterprise Edition Administration Model" in *Sun Java System Directory Server Enterprise Edition 6.0 Deployment Planning Guide*.

What's New at a Glance

This section describes the main new features and enhancements in all of the component products of DSEEand includes the following information:

General DSEE Enhancements

General DSEE enhancements include the following:

- **Web-based administration interface (Directory Service Control Center)**. The DSCC provides a graphical user interface for managing individual Directory Server and Directory Proxy Server instances, as well as groups of servers. The DSCC therefore enables a unified view of an entire directory service topology.

- **Global account lockout**. You can configure global account lockout for a directory service topology so that a user account is locked, due to consecutive failures to bind, across the entire collection of servers.

New Features in Directory Server 6.0

Directory Server 6.0 includes the following new features and enhancements:

- **Service manageability command-line tools.** Directory Server includes new tools to facilitate command-line management of the server.

- **Replication enhancements.** These enhancements include: no fixed limit to the number of replication masters, the ability to prioritize replication, a global retro changelog, replicated account lockout data, fast replication restart for recovery (minutes or less), and a fast count of pending replication changes so that you can get accurate status on replication convergence.

- **Security enhancements.** These enhancements include: additional connection-based access control files, rejection of binds with no password, forced password change after reset, multiple directory superusers, changes to passwords using the LDAP Password Modify Extended Operation specified in RFC 3062, last login time tracking, enhanced auditing for updates performed using proxy authorization, and improved ACI processing performance.

- **Enhanced password policy.** The new password policy provides a grace login limit, safe password modifications, as well as two new controls, `passwordPolicyRequest` and `passwordPolicyResponse`. These controls enable LDAP clients to obtain account status information on LDAP `add`, `delete`, `modrdn`, `compare`, and `search` operations. The password policy can now be applied to proxy authentication to prevent client operations when an account is locked.

- **New operational attribute for group membership**. Entries that are members of static groups now have the operational attribute `isMemberOf`, which holds the DNs of the static groups to which the members belong.

- **Enhancements to static group management.** These enhancements include performance improvements for large, multi-valued attributes and membership testing for group entries.

- **More configuration changes while the server is online.** You can change the configuration of suffixes, indexes, schema, and the replication topology while the server is running.

- **Attribute syntax validation on update.** When syntax checking is on, all import and update operations are checked to ensure that updated attributes adhere to the syntax definitions.

- **Threshold on heap memory.** When the threshold is reached, Directory Server attempts to free memory from the entry caches.

- **Frozen mode for database backup.** You can stop database updates on disk so that a file system snapshot can be taken safely

- **Log management improvements.** This version of Directory Server brings improvements to time-based log rotation, rotate now functionality for access, error, and audit logs, and configurable permissions for log files. It also provides more flexible logging of users involved in proxy authorization.

- **Fine-grained all IDs threshold configuration.** You can configure the all IDs threshold individually for each index, saving you disk space.

- **Plug-in call ordering.** For further information, see "Ordering Plug-In Calls" in *Sun Java System Directory Server Enterprise Edition 6.0 Developer's Guide.*

- **SNMP monitoring support.** Directory Server now supports the Mail and Directory Management Information Base (MADMAN MIB) for use with Simple Network Management Protocol (SNMP) monitoring agents as described in RFC 2605 (`http://www.ietf.org/rfc/rfc2605.txt`).

- **Monitoring using the Sun Java Enterprise System Monitoring Console.** Directory Server supports the use of the Monitoring Console to view monitored data and to produce threshold alarms.

- **LDAP utilities and character sets for passwords.** The LDAP command-line utilities now convert passwords entered on the command line to UTF8 by default.

  In LDAP, `userPassword` values are binary. The server therefore sees a password as a string of bytes, which is often not the way that the user sees a password. By converting passwords that a user enters to UTF8, the utilities make it possible for passwords entered on one system to be entered on another system.

- **More LDAP controls and extended operations.** Directory Server now supports additional LDAP controls and extended operations.

  For a complete list of LDAP controls, see the `controls`(5dsconf) man page.

  For a complete list of extended operations, see the `extended-operations`(5dsconf) man page.

New Features in Directory Proxy Server 6.0

Directory Proxy Server 6.0 includes the following new features and enhancements:

- **Virtual directory.** The virtual directory enables you to define how data is displayed to LDAP client applications, define virtual domains that aggregate data from multiple data sources, map attribute names and values to suit LDAP application and multiple disparate data sources, access data repositories that are compliant with the JDBC™ technology, and access flat LDAP Data Interchange Format (LDIF) file resources.

- **New, richer architecture.** To make new functionality possible, the Directory Proxy Server architecture has changed significantly.

- **Directory data distribution.** You can distribute directory data using the proxy, enabling much higher scalability for write operations.

- **Operation-based routing.** Directory Proxy Server can route different LDAP operations on the same client connection to different servers and enable successive requests on the same client connection to be sent to the same LDAP servers.

- **Full command-line and web-based administrative capabilities.** Directory Proxy Server now provides complete administrative capabilities both on the command line and through the Directory Service Control Center.

- **Administrative alerts.** You can configure what Directory Proxy Server does when an alert occurs, such as sending emailor running a script.

  For further information, see Chapter 28, "Directory Proxy Server Monitoring and Alerts," in *Sun Java System Directory Server Enterprise Edition 6.0 Administration Guide.*

- **DN and attribute rewriting.** You can configure Directory Proxy Server to automatically modify the DN, attribute types, and attribute values of entries such that a client application view of an entry can be significantly different that what is stored in the directory.

- **Fewer server restarts.** Directory Proxy Server now requires fewer configuration-related restarts than ever before, making it easier to respond automatically to the need for changes in how the server behaves.

- **Logging aligned with Directory Server.** Directory Proxy Server log files now fit more effectively with those of Directory Server. Their formats are very similar, and they allow you to trace requests through Directory Proxy Server to Directory Server and back to client applications.

- **Improved resource management.** Directory Proxy Server now pools connections to data sources such as Directory Server and can use proxy authentication to further reduce resources used to establish connections, and to authenticate repeatedly.

- **Schema management.** Directory Proxy Server generates a single schema from multiple heterogeneous data sources, performs schema checking, and performs attribute value syntax checking.

- **Access controls.** Directory Proxy Server supports access control instructions (ACIs) that determine which permissions are granted to users.

New Features in Identity Synchronization for Windows

Identity Synchronization for Windows includes the following new features and enhancements:

- **Group synchronization with Active Directory.** Identity synchronization between Directory Server and Active Directory is simpflied because you can map a group on Directory Server to Microsoft Active Directory domain global distribution groups and domain global security groups.

- **Failover support for multiple master replicas.** For more information about failover support, see Appendix E, "Identity Synchronization for Windows Installation Notes for Replicated Environments," in *Sun Java System Directory Server Enterprise Edition 6.0 Installation Guide.*

- **Account lockout synchronization with Active Directory.** Identity Synchronization for Windows synchronizes account lockout information between Directory Server and Active Directory, improving security coherency between the two directories.

- **No need for a local Directory Server.** A Directory Server instance does not need to be installed on the system that is running Identity Synchronization for Windows. When the installer does not find a local Administration Server, the installer adds the Administration Server at the specified server root location, so you do not have to install the Directory Serversoftware.

- **Integrated Directory Server Plug-in.** The Identity Synchronization for Windows plug-in for Directory Server is now installed with Directory Server rather than Identity Synchronization for Windows. The installer provides an option to configure the plug-in while installing the Directory Server Connector. The same option is available through the command line interface.

- **Support for Red Hat Linux.** Identity Synchronization for Windows now supports Red Hat Linux.

2

Getting Started

This chapter describes how to get started evaluating Directory Server Enterprise Edition (DSEE)with the Evaluation Kit. It outlines where to get component products, how to install them, and where to obtain the Evaluation Kit.

Note – The Evaluation Kit is provided as is. It is not part of DSEE and is not covered by the support contract. It is intended for evaluation purposes only and is not supported in a production environment.

This chapter contains the following topics:

Obtaining and Installing the Evaluation Kit

The Evaluation Kit provides a collection of automated demonstration scripts that help you evaluate the features of DSEE through the command line. In addition to the scripts, the Evaluation Kit contains sample data and the configuration files required to run the evaluation.

You can download the Evaluation Kit from `http://www.sun.com/bigadmin/scripts/indexSjs.html`. Click the link to the Directory Server Enterprise Edition 6.0 Evaluation Kit.

Note – The Evaluation Kit is not supported on Windows.

The Evaluation Kit is delivered in a compressed archive (ZIP) file named `dsee6-kit.tar.gz`. Once installed, the Evaluation Kit sets up the following files and directories:

- A global configuration file, env.cfgin the main *install-base* directory. Do not modify this file.
- A directory, *install-base*/kit/, that contains the evaluation scripts.
- A unique configuration file, dsee6-env.cfg in the *install-base*/kit/ directory, that contains configurable variables.
- A command-line utility, *install-base*/tools/zonemgr, which allows you to set up and manage Solaris™ 10 zones, if you want to use them in this evaluation.

Installing DSEE

This section outlines how to install the DSEE software. It provides a brief overview of the packaging formats required if you plan to use the Evaluation Kit, describes what component products are installed by the packages, and provides pointers to information about installing DSEE manually or automatically.

DSEE Packaging Formats

DSEE 6.0 is available in two packaging formats:

- Java Enterprise System distribution, the native package distribution that is provided as part of Sun Java Enterprise System. The Java Enterprise System distribution does not include the Directory Server Resource Kit.

  You install software from the Java Enterprise System distribution with the Java Enterprise System installer.
- Zip distribution, which supports non-root installations. The zip distribution does not include the Directory Service Control Center.

If you plan to use the Evaluation Kit, which requires both the Directory Server Resource Kit and the Directory Service Control Center, you need to install both packaging formats.

Component Products Installed With DSEE

The DSEE 6.0 distribution includes the following component products:

- Directory Service Control Center
- Directory Server
- Directory Proxy Server
- Identity Synchronization for Windows
- Directory Editor
- Directory Server Resource Kit

Directory Server has no component product prerequisites.

Directory Proxy Server depends on Directory Server to route LDAP requests to backend Directory Servers.

Installing the DSEE Software for the Evaluation Kit

For a production environment, install DSEE using the Java Enterprise System installer. For more information about installing DSEE, see Part I, "Installing Directory Service Control Center, Directory Proxy Server, Directory Server, and Directory Server Resource Kit," in *Sun Java System Directory Server Enterprise Edition 6.0 Installation Guide*. For detailed instructions on using all features of the Java Enterprise System installer, see the Java Enterprise System documentation at `http://docs.sun.com/coll/1286.2`.

To evaluate DSEE in a *non-production* environment using the Evaluation Kit, you can install DSEE automatically by using a demonstration script from the Evaluation Kit, or you can install DSEE manually.

To automate the installation of DSEE, run the `Install_DSEE6.sh` script as root. This script installs Directory Server and Directory Proxy Server using both the zip distribution and the Java Enterprise System distribution. The script describes each step of the installation as it proceeds. For more information about how to download and run this script, refer to the README file provided with the Evaluation Kit.

If you do not want to use the demonstration script, you can install each component product manually.

For information about installing Directory Server manually, see "To Install Only Directory Server From the Zip Distribution" in *Sun Java System Directory Server Enterprise Edition 6.0 Installation Guide*.

For information about installing Directory Proxy Server manually, see "To Install Only Directory Proxy Server From the Zip Distribution" in *Sun Java System Directory Server Enterprise Edition 6.0 Installation Guide*.

Uninstalling the DSEE Software

To uninstall the software automatically, run the `Uninstall_DSEE6.sh` script. This script shuts down all instances, removes any instance data, and cleanly uninstalls the DSEE packages. For more information about this script, refer to the README file provided with the Evaluation Kit.

For information about uninstalling the software manually, see Chapter 2, "Uninstallation," in *Sun Java System Directory Server Enterprise Edition 6.0 Installation Guide*.

3

Service Manageability

This chapter describes the Directory Server Enterprise Edition service manageability features. This chapter covers the following topics:

Web-Based Directory Service Management With the DSCC

The primary interface for DSEE is the Directory Service Control Center (DSCC). The DSCC enables you to perform almost all administrative tasks.

When you initiate an action through the DSCC, the operation is passed to the appropriate console agents or through LDAP. The console agents run the corresponding Directory Server or Directory Proxy Server command to perform the administrative action.

The DSCC plugs in to Sun Java Web Console. For information about starting and using the DSCC, see "Directory Service Control Center Interface" in *Sun Java System Directory Server Enterprise Edition 6.0 Administration Guide*.

Diverse Views to Simplify Service Management

The DSCC provides various data views to help you manage your services most effectively. For example, the DSCC provides a topology view, where you can see all of the servers involved in a

replication topology and the relationship between them. The following figure demonstrates the topology view of a simple two-master, two-consumer replication topology.
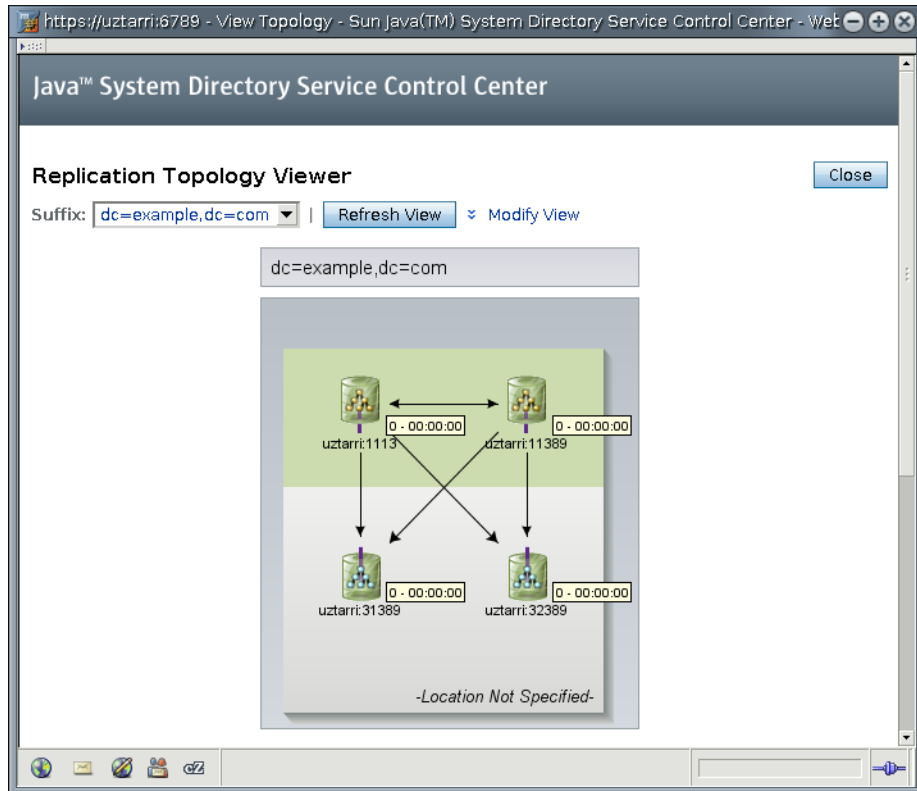
The arrows show the direction in which information is propagated. The servers are listed hierarchically, with the master servers appearing at the top and the read-only consumer replicas appearing at the bottom. If hub servers were used, they would be displayed in the middle. The DSCC allows you to modify the view by applying filters so that you can display only a particular suffix.

The DSCC provides tools for viewing the replication status of suffixes. This view summarizes for each server the number of changes currently missing and the age of the latest change that needs to be applied, as illustrated in the following figure.

You can also use the DSCC to view the Directory Server and Directory Proxy Serverlogs, which show the timestamp, log level, messages, and message sort. You can modify the log view to show only entries that contain a string you specify.

Configuration and Suffix Cloning

A production environment usually includes multiple instances for redundancy and load balancing. In most cases, each of these servers has the same configuration. The DSCC simplifies service management by allowing you to install an instance of the server once and to copy that server's configuration and replication configuration to another instance.

The DSCC enables you to clone an instance or suffix configuration by selecting an existing instance and then cloning either the instance or the suffix configuration to other directory instances.

For example, to simplify the deployment of your replicated topology, you can create a master replication configuration and then propagate it to the other masters in your topology. You can also choose to clone only parts of the configuration, such as the indexes.

The following figure illustrates how you can copy configuration settings from one Directory Server to other servers by using the Copy Directory Server Configuration wizard.
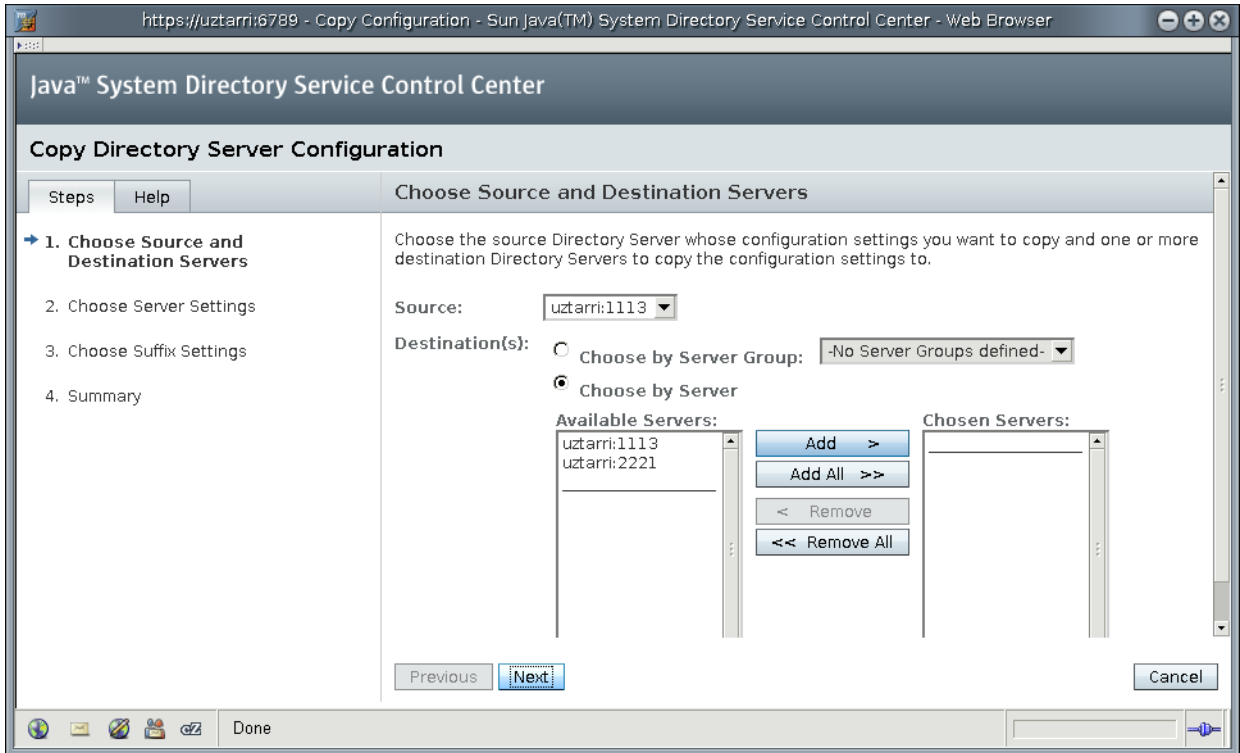
The DSCC provides similar wizards for copying suffix configuration or cloning a Directory Proxy Server configuration.

Advanced Command-Line Interface

The DSEE CLI is designed to reduce all administrative tasks to a few commands. The look, feel, and use of these commands is similar across the DSEE administrative framework. For example, administrative tasks for Directory Server and Directory Proxy Server are performed with the `dsadm` and `dpadm` commands, respectively. The usage and syntax of these two commands is similar.

The command-line tools wrap much of the complexity of LDIF-based configuration, enabling you to write more succinct, readable scripts. The Evaluation Kit demonstrates the major features of DSEE with a series of such command-line scripts. These scripts provide comments to explain how each command is being used before it is run.

Overview of the Commands

The DSEE includes the following new tools to facilitate command-line management of the server:

- dsadm – Handles local Directory Server instance files, creating instances and managing the server process running on the local host.

  For more information, see the dsadm(1M) man page.

- dpadm – Handles local Directory Proxy Server instance files, creating instances and managing the server process running on the local host. .

  For more information, see the dpadm(1M) man page.

- dsconf – Connects to a Directory Server instance over LDAP to manage the server configuration: imports, backups, replication agreements and more.

  For more information, see the dsconf(1M) man page.

- dpconf – Connects to a Directory Proxy Server instance over LDAP to manage the server configuration.

  For more information, see the dpconf(1M) man page.

On a Solaris package installation, these commands are located in /opt/SUNWdsee/ds6/bin and /opt/SUNWdsee/dps6/bin by default.

Some administrative operations, such as starting and stopping a server instance, require a local agent. For the command line, the local agent is the command itself. The dsadm and dpadm commands run locally because they require the server to be offline or they require specific system rights. For example, if you use the dsadm command to change a certificate, the server can be running but the operation needs to be executed by a privileged user.

You can use the DSEE CLI to administer and configure your directory remotely. You can run the dsconf and dpconf commands remotely to create suffixes, server instances, and indexes. These commands use LDAP authentication, so you do not need a local user on your machine, although the server instance itself must be running.

Simplified Installation

DSEE includes several features that improve the way in which the component products can be installed.

Automated Installation From the Command Line

DSEE provides flexible commands for each step of the installation process so that you can write custom scripts to install and minimally configure a DSEE instance. You can then use your scripts to standardize your deployment so that each server is automatically configured the same.

To see an example of an automatic installation, run the `Install_DSEE6.sh` and `Setup_DS_Service.sh` scripts from the Evaluation Kit on any Solaris 10 server. These scripts install and configure an entire directory service from the command line.

Non-Root Installation

Directory Server allows you to install the DSEE components as a non-root user. This non-root installation is possible with the zip distribution as well as the Java Enterprise System installer. Operating system-specific packaging formats, such as `SVR4` for Solaris and `rpm` for Linux, require installation as a privileged user.

Note – You must be the root user to install the Directory Service Control Center.

User-Specified Installation Path

Both the zip distribution and Java Enterprise System distribution provide the ability to install DSEE components into a user-specified installation directory.

Multiple Separate Installations

With the zip distribution, you can install multiple distinct installations of the component products within a single operating system instance. You can even install the zip distribution on a system with an existing directory server installation. The following constraints apply when installing multiple installations on a single system:

- Each instance must be configured so that the total resources (RAM, CPU, and disk) that areconsumed by the sum of all instances on the server do not exceed the available resources.
- Each installation must have its own distinct installation path.
- Each installation must have its own agent port.

With the introduction of Solaris 10 zones, you can also install different versions and installations of the package version of DSEE. In this case, each installation must be contained within its own unique Solaris 10 whole root zone.

To make managing zones easier, the `zonemgr` tool is included with the Evaluation Kit. For the correct usage and examples of `zonemgr`, go to:

> http://mydataexchange.net/zonemgr

Online Configuration Changes

Directory Server allows you to change the configuration of the following while the server is running:

- **Suffixes.** After Directory Server has been installed and brought online, you can continue to add new suffixes dynamically while the server keeps running.

- **Indexes.** After you have defined the suffixes, you can add new indexes to accelerate search performance. You can customize your index according to function, such as indexes that list entries that have a particular attribute, that approximate a particular attribute, that contain a substring, or that match a particular locale. Indexes can be updated dynamically without interrupting the normal functions of the directory server itself.

- **Schema.** You can change the directory schema dynamically. If the schema needs to be extended to meet the needs of an application, you can add new object classes and attributes while the server is running, without affecting operations.

- **Replication topology.** You can set up and modify the replication topology while the server is runningl.

Availability Across Your Entire Network

Directory Server can be configured to listen on multiple specific IP addresses. This feature allows Directory Server to be available simultaneously on several networks, including intranets and secure or restricted networks, such as demilitarized zones (DMZs).

Grouping Entries for Simplified Management

You can simplify entry management by associating related entries in groups. The group mechanism makes it easy to retrieve a list of entries that are members of a given group and set access permissions for a whole group.

Entries can be managed as members of dynamic and static groups. Static groups are suitable for groups with few members, such as a group of directory administrators. A dynamic group specifies one or more URL search filters, so the dynamic group membership is defined each time these search filters are evaluated.

You can retrieve a list of all the static groups a given user is a member of by using the dynamic `isMemberOf` attribute. This attribute is located in the user entry and in nested group entries and holds the DNs of the static groups to which the member belongs. For example, Kirsten Vaughan is a new system administrator in the human resources department. Her entry shows that she is a member of both the System Administrators group and the HR Managers group.

```
$ ldapsearch -b "dc=example,dc=com" uid=kvaughan isMemberOf
```

```
uid=kvaughan, ou=People, dc=example,dc=com
isMemberOf: cn=System Administrators, ou=Groups, dc=example,dc=com
isMemberOf: cn=HR Managers,ou=groups,dc=example,dc=com
```

Membership testing for group entries has been improved. These improvements remove some of the previous restrictions on static groups, specifically the restriction on group size. This performance improvement is only effective after the group entry has been loaded into the entry cache.

Tunable Index Limits

Directory Server supports configuring the all IDs threshold individually for each index, saving disk space. You can change the global default all IDs threshold value and index-specific values by using the CLI or the DSCC.

See the all-ids-threshold(5dsconf) man page for details on this property.

For example, the *server* level all IDs threshold setting is inherited for *any* indexes on suffixes that do not have a defined value.

The following command shows the default value of the global all IDs threshold:

```
# dsconf get-server-prop -w /tmp/.pwd-file -p 20390 all-ids-threshold : 4000
```

You can change the global default all IDs threshold value by using the following command:

```
# dsconf set-server-prop -w /tmp/.pwd-file -p 20390 -i all-ids-threshold:2000
```

To view the current value of the global all IDs threshold, run the following command:

```
# dsconf get-server-prop -w /tmp/.pwd-file -p 20390 all-ids-threshold
all-ids-threshold  :  4000
```

Where to Go From Here

To read more about the features presented in this chapter, refer to the following documentation.

Feature	Documentation
Directory Service Control Center	"Directory Service Control Center Interface" in *Sun Java System Directory Server Enterprise Edition 6.0 Administration Guide*

Feature	Documentation
Installing DSEE	Part I, "Installing Directory Service Control Center, Directory Proxy Server, Directory Server, and Directory Server Resource Kit," in *Sun Java System Directory Server Enterprise Edition 6.0 Installation Guide*
Indexing	Chapter 12, "Directory Server Indexing," in *Sun Java System Directory Server Enterprise Edition 6.0 Administration Guide*
Directory schema	Chapter 11, "Directory Server Schema," in *Sun Java System Directory Server Enterprise Edition 6.0 Administration Guide*
Replication configuration	Chapter 10, "Directory Server Replication," in *Sun Java System Directory Server Enterprise Edition 6.0 Administration Guide*
Static and dynamic groups	"Managing Groups" in *Sun Java System Directory Server Enterprise Edition 6.0 Administration Guide*
Tuning the all IDs threshold property	`all-ids-threshold(5dsconf)` man page

For a hands-on demonstration of the features described in this chapter, use the scripts provided with the Evaluation Kit. The following table lists the scripts available to demonstrate each feature.

Feature	Evaluation Script
Installing DSEE from the command line	`Install_DSEE6.sh`
Setting up Directory Server instances from the command line	`Setup_DS_Service.sh`
Setting up Directory Proxy Server instances from the command line	`Setup_DPS_Service.sh`
Using static groups and retrieving all groups that a user is a member of by using the `isMemberOf` attribute	`Demo_Static_Groups.sh`
Listening on multiple IP addresses	`Demo_Multiple_IP_Listeners.sh`
Tuning the directory server IDs threshold	`Demo_AllIDsThreshold.sh`

4

High Data Availability and Integrity

This chapter describes the Directory Server Enterprise Edition features that provide high data availability and integrity. This chapter covers the following topics:

Robust Replication

Directory Server provides a robust replication mechanism, including the following features:

- Unlimited masters for replication
- Prioritized replication
- Globally synchronized replication using the retro changelog
- Replicated account lockout attributes
- Monitoring replication convergence

Unlimited Masters for Replication

In a multimaster replication environment, data is updated on multiple masters. Each master maintains a change log, and the changes made on each master are replicated to the other servers. Each master plays the role of supplier and consumer. Directory Server removes previous limits on the number of masters, allowing your multimaster replication topology to include an unlimited number of masters in multiple data centers.

You can also configure your replication topology to contain only masters, eliminating the need to route operations to consumers and simplifying your overall deployment.

Prioritized Replication

Directory Server allows you to prioritize updates for replication. Priority is a boolean feature and is on or off. You can prioritize replication according to the following parameters:

- Attribute name

  For example, a password attribute can be configured to replicate immediately.

- Operation type .

  For example, you can set up add operations to have a higher priority than modification operations.

- Client identity.

  For example, you can specify that modifications made by administrative users have a higher priority than modifications made by regular users.

- Entry or subtree.

  For example, you can specify that a particular group has a higher priority than other groups.

The priority rules are configured on each master replica. The master can replicate an update to one or more hubs or consumer replicas. The priority of the update is then cascaded across all of the hubs and consumer replicas. If one parameter is configured for prioritized replication, all updates that have that parameter are prioritized for replication. If multiple parameters are configured for prioritized replication, only updates that match *all* parameters are prioritized for replication.

See "Replication Priority" in *Sun Java System Directory Server Enterprise Edition 6.0 Administration Guide* for instructions on configuring prioritized replication using command-line tools.

Globally Synchronized Replication Using the Retro Changelog

The retro changelog receives updates from all master replicas in the topology. The updates from each master replica are combined in the retro changelog. The retro changelog provides a way for applications to track changes so that they can be synchronized. Directory Server enables you to access a coherent version of the retro changelog on any master in a multimaster topology. You can also update your application to manage its state according to change numbers. This makes it possible to fail over between retro changelogs on different servers.

The global retro changelog contains all of the changes. If two changes occur on the same entry in two different locations, the retro changelog provides an ordered change description. If you query the retro changelog from any server, it will contain similar information.

See "Replication and the Retro Change Log Plug-In" in *Sun Java System Directory Server Enterprise Edition 6.0 Reference* for background information about the retro changelog.

Replicated Account Lockout Attributes

Directory Server replicates account lockout data that is stored when a client application fails to authenticate to the server. You can use this feature with the Directory Proxy Server capability to route binds appropriately. Together, these features provide global account lockout. Global account lockout prevents a client application from gaining more than a specified number of login attempts across an entire directory service topology.

See "Preventing Authentication by Using Global Account Lockout" in *Sun Java System Directory Server Enterprise Edition 6.0 Deployment Planning Guide* for an overview of the topic.

Monitoring Replication Convergence

Directory Server quickly calculates the number of pending replication changes using the ds5ReplicaPendingChangesCount attribute. Directory Server finds the oldest change that the consumer is aware of and can compare it with the other servers, making it possible to calculate the replication delay. From this change, the consumer can also browse the list of changes until the most recent change, and count the number of changes that need to be applied.

Moreover, this attribute can be queried with virtually no impact to Directory Server performance, regardless of how large the change log grows.

In the Directory Service Control Center, you can view a summary of all the pending changes for a given suffix .In the Suffixes tab, the pending changes are in the Missing Changes column, as shown in the following figure.
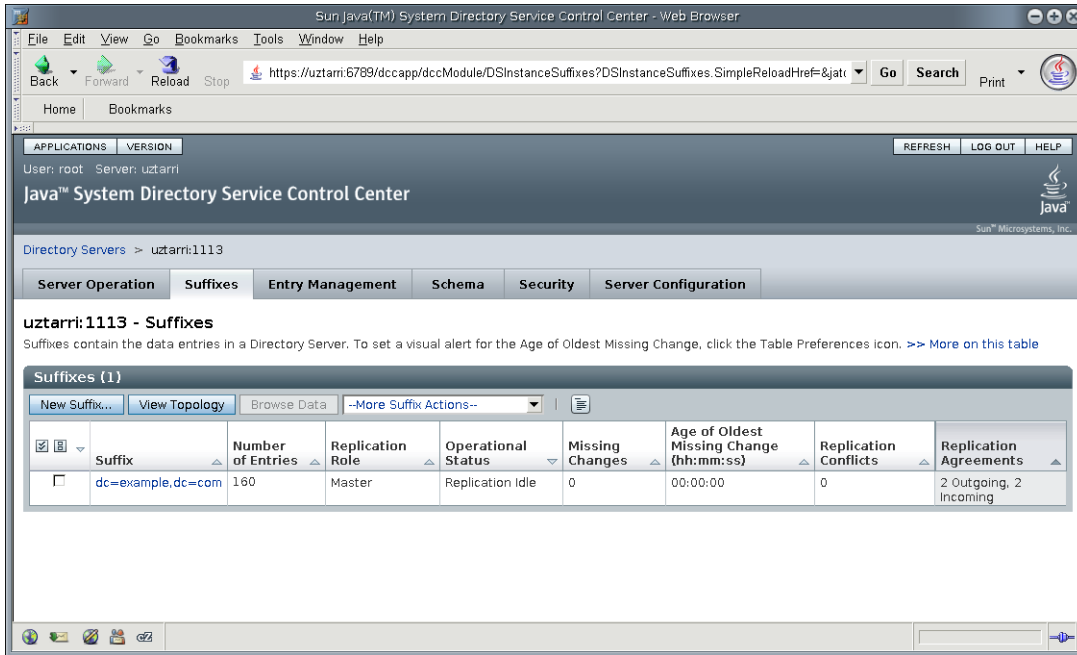
Importing Many Entries to Large Replicated Suffixes

Directory Server provides a mechanism for adding new entries to an existing database. This import process checks if a given entry already exists so that data is not overwritten. This feature allows you to import an LDIF file in multiple passes at different times. Successive imports do not delete what already exists in the database.

For more information about importing entries to large replicated suffixes, see "Incrementally Adding Many Entries to Large Replicated Suffixes" in *Sun Java System Directory Server Enterprise Edition 6.0 Administration Guide*.

Synchronized Backup and Export

All offline and online backup methods can be invoked in the CLI by using `dsadm` or `dsconf`. The default behavior for these commands is to operate in synchronous mode. The commands do not return a completion code until the task is complete. The commands also offer an asynchronous mode, by setting the `-a` flag.

Online Binary Backup

You can perform an online binary backup with `dsconf` or by using the Directory Service Control Center (DSCC).

For example, to back up master `sA1` and store the resulting binary backup in the `/install-path/sA1-bak` directory, run the following command:

```
$ dsconf backup -p 20390 /install-path/sA1-bak
```

Use the `-a` or `--async` option to start a backup task that returns immediately.

Online LDIF Export

You can perform an online LDIF export using the command line or using the DSCC. For example, use the following command to export to a file called `export.ldif`:

```
$ dsconf export -p 20390 "dc=example,dc=com" /install-path/export.ldif
Beginning export of 'example'
example: Processed 8 entries (100%).
Export finished.

Task completed (slapd exit code: 0).
```

Offline Binary Backup

The following command performs an offline binary backup:

```
$ dsadm backup  /install-path/sA1 /install-path/sA1-bak
[28/Oct/2006:23:38:13 -0500] - Backup starting (/install-path/sA1-bak)
[28/Oct/2006:23:38:13 -0500] - WARNING<20509> - Backend Database - conn=-1 op=-1 msgId=-1 -
  Cannot create new directory /install-path/sA1-bak/dsA1 (-5943) Cannot create or rename a filename that already
[28/Oct/2006:23:38:13 -0500] - Backing up file 1 (/install-path/sA1-bak/dsA1/dsA1_objectclass.db3)
[28/Oct/2006:23:38:13 -0500] - Backing up file 2 (/install-path/sA1-bak/dsA1/dsA1_id2entry.db3)
  [28/Oct/2005:23:38:13 -0500] - Backup completed (/install-path/sA1-bak)
```

Offline LDIF Export

The following command performs an offline LDIF export:

```
$ dsadm export /install-path/sA1 "dc=example,dc=com" /install-path/export.ldif
Exporting data...
[28/Oct/2005:23:37:46 -0500] - DEBUG - conn=-1 op=-1 msgId=-1 -  Backend Instance: dsA1
```

```
ldiffile: /install-path/export.ldif
[28/Oct/2005:23:37:46 -0500] - export dsA1: Processed 8 entries (100%).
```

Binary Restore Methods

The dsadm and dsconf commands can also be used to restore data. The commands are used the same way as for backups except that the commands passed are dsadm restore and dsconf restore.

File System Snapshot of Frozen Database

Directory Server provides a configurable feature that enables you to stop database updates on disk so that a file system snapshot can be taken safely.

When frozen mode is set, all configured databases are taken offline. Any internal operations in progress are notified of the database going offline. LDAP operations in progress are completed, and the database environment is flushed. Subsequent incoming operations are refused until the server property is reset to read-write or read-only. In a single server topology, operations received when frozen mode is on result in an LDAP error being returned.

The standard error message for database offline is logged. In a replicated topology, a referral is returned. For this feature to work correctly, no other tasks should be running on the databases. When the operation to turn frozen mode on has returned LDAP_SUCCESS (0), it is safe to take the file system snapshot.

See "Backing Up a File System" in *Sun Java System Directory Server Enterprise Edition 6.0 Administration Guide* for instructions on configuring frozen mode using command-line tools.

Changing Attributes While the Server Is Online

In previous versions of Directory Server, attributes such as the all IDs threshold required the server to be offline when the attribute value was changed. You can now change the values of such attributes while the instance is online.

Although the value can be changed online, changes for some attributes might not take effect until after the instance has been restarted. In addition, some changes require manual intervention before restarting. For example, you can change the path to the data directory with the server online, but before the change takes effect, you need to do the following:

1. Stop the instance.
2. Ensure that the new directory exists and has the correct permissions.
3. Move the data from its present location to the new location.

4. Restart the instance.

The following sections describe the changes that can now be made with the server online.

Changing the All IDs Threshold

You can change the global and index-specific values of the all IDs threshold with the server online. The change does not take effect until the affected indexes are re-indexed or the data is re-initialized.

For example, on the command line, you can change the global all IDs threshold by running the following command:

```
# dsconf set-server-prop -p 20390 all-ids-threshold:2000
```

Changing the Database Path

You can change the database path attribute while the server is online. After you have changed the path, you then need to stop the server, move the database files, and start the server.

The database path attributes include `nsslapd-db-home-directory`, `nsslapd-db-logdirectory`, and `nsslapd-directory`. These attributes correspond to the `dsconf` command properties `db-env-path`, `db-log-path`, and `db-path`, respectively.

For example, to change the location of the `example` backend database, do the following:

```
# /opt/sun/install-path/bin/dsconf set-suffix-prop -p 20390 "dc=example,dc=com" \
db-path:/install-path/dbtst
Changing "db-path" does not move the database file automatically.
You will have to stop the server, move the database files and restart the server.
Do you want to continue [y/n] ? y
Directory Server needs to be restarted for changes to take effect
# mv /install-path/sA1/db/example /install-path/dbtst
# /opt/sun/install-path/bin/dsadm start /install-path/sA1
Server started: pid=29050
```

Attribute Syntax Validation on Update

Every attribute defined in the server's schema has a syntax associated with it. The syntax defines the kind of information that is expected to be held in the attribute so that the server can perform the appropriate kinds of matching against it. The syntax definition also allows the server to properly index the values so that searches against it can be processed quickly.

Chapter 4 • High Data Availability and Integrity

Directory Server Enterprise Edition introduces a configurable option, `check-syntax-enabled`, set by using the `dsconf` command, to ensure that updated attributes adhere to the syntax definitions. Attribute values are rejected when they violate the syntax definitions. For example, when syntax checking is on, if a user tries to update an attribute with an integer syntax to include a non-numeric value, the update will be rejected.

By default, syntax checking is off. When syntax checking is on, all import and update operations are checked.

Schema Validation by Directory Proxy Server

Directory Proxy Server provides schema validation to ensure that only the allowed data is permitted on write operations. For example, when entries are aggregated using the virtual directory functionality, the aggregate entries might not match the schema of any of the backend servers participating in the entry aggregation. In this case, schema checking can occur on the Directory Proxy Server using a virtual schema.

When schema checking is enabled, Directory Proxy Server retrieves schema available in the `cn=schema` suffix and uses it to do schema checking. You can define the LDIF data view holding the `cn=schema` suffix. The content of the `cn=schema` suffix can point to an LDAP server or to a schema stored in an LDIF file local to the Directory Proxy Server.

Where to Go From Here

To read more about the features presented in this chapter, refer to the following documentation.

Feature	Documentation
Designing a highly available deployment	Chapter 12, "Designing a Highly Available Deployment," in *Sun Java System Directory Server Enterprise Edition 6.0 Deployment Planning Guide*
Backing up and restoring directory data	Chapter 8, "Directory Server Backup and Restore," in *Sun Java System Directory Server Enterprise Edition 6.0 Administration Guide*
Using a global retro changelog	"Replication and the Retro Change Log Plug-In" in *Sun Java System Directory Server Enterprise Edition 6.0 Reference*
Using global account lockout	"Preventing Authentication by Using Global Account Lockout" in *Sun Java System Directory Server Enterprise Edition 6.0 Deployment Planning Guide*

Feature	Documentation
Making a file system snapshot when the database is in frozen mode	"Backing Up a File System" in *Sun Java System Directory Server Enterprise Edition 6.0 Administration Guide*
Checking valid attribute syntax on update	"Checking Valid Attribute Syntax" in *Sun Java System Directory Server Enterprise Edition 6.0 Administration Guide*

For a hands-on demonstration of the features described in this chapter, use the scripts provided with the Evaluation Kit. The following table lists the scripts available to demonstrate each feature.

Feature	Evaluation Script
Synchronizing replicas in a multimaster environment, even under a heavy load	`Demo_Replication_Sync.sh`
Backing up, recovering, exporting, and importing data	`Demo_Backup_Strategies.sh`
Creating a file system snapshot when the database is in frozen mode	`Demo_Frozen_Mode.sh`
Changing the all IDs threshold while the server is online	`Demo_AllIDsThreshold.sh`
Changing the backend database of a directory server instance while the server is online	`Demo_Changing_DB_Dir.sh`
Enabling and using Directory Proxy Server schema checking	`Demo_DPS_Schema_Checking.sh`

5

Tuned for Performance

This chapter describes the Directory Server features that help you tune your deployment for best performance. This chapter covers the following topics:

- "Cache Optimizations" on page 49
- "Log Management Improvements" on page 50
- "Where to Go From Here" on page 54

Cache Optimizations

For fast response time to client requests, Directory Server caches directory information in memory. For top performance, you can tune your suffix entry cache settings to optimize performance. Directory Server provides easier control of cache sizing, and once tuned, the server adheres strictly to the cache setting.

This section describes the main features of the Directory Server cache:

- Setting thresholds on dynamic memory use
- Optimizing cache memory allocation
- Grouping entries for simplified management

Setting Thresholds on Dynamic Memory Use

Directory Server allows you to strictly control the use of memory for cache purposes so that less memory is used. You specify a low and high threshold for dynamic memory use. When this threshold is reached, Directory Server attempts to free memory from the suffix entry caches and to keep memory use under control. If the server reaches the high threshold, the server goes into aggressive mode to free memory. Performance is only effected when the high threshold is reached.

This feature provides two configurable thresholds: a *soft threshold* and a *hard threshold*. When the soft threshold is reached, Directory Server attempts to free memory concurrently with other operations. When the hard threshold is reached, operations on the cache are prevented while memory is being freed. These two thresholds are defined by two server properties:

- `heap-high-threshold-size` specifies the hard threshold.
- `heap-low-threshold-size` specifies the soft threshold.

See the `server(5dsconf)` man page for details on the two server properties.

Optimizing Cache Memory Allocation

The size of the cache determines how the memory is allocated. For example, if the cache is less than two Gbytes, the server uses one memory pool. If the cache size is larger than two Gbytes, the server optimizes cache memory allocation by using as many pools as necessary, with each pool dedicated to a particular size.

Log Management Improvements

This version of Directory Server brings improvements to time-based log rotation, rotate on-demand functionality for access, error, and audit logs, and configurable permissions for log files. It also provides more flexible logging of users involved in proxy authorization.

The following sections describe changes that have been made in the logging functionality of Directory Server.

Time-Based Log Rotation and Deletion

Directory Server supports rotating and deleting logs not only after a specified interval, but also at a specified time. This feature lets you more easily perform operations such as log analysis and trending, as each rotated log file covers the same length of time. This feature can also be used to meet auditing and security requirements because it makes it easier to determine the specific period of time covered by a given log file.

You can specify whether to rotate the log according to a time interval or according to the size of the log file. The following figure illustrates using the DSCC to configure log rotation to occur once a week at midnight, as well as to rotate the log files when the size limit exceeds 100 Mbytes:
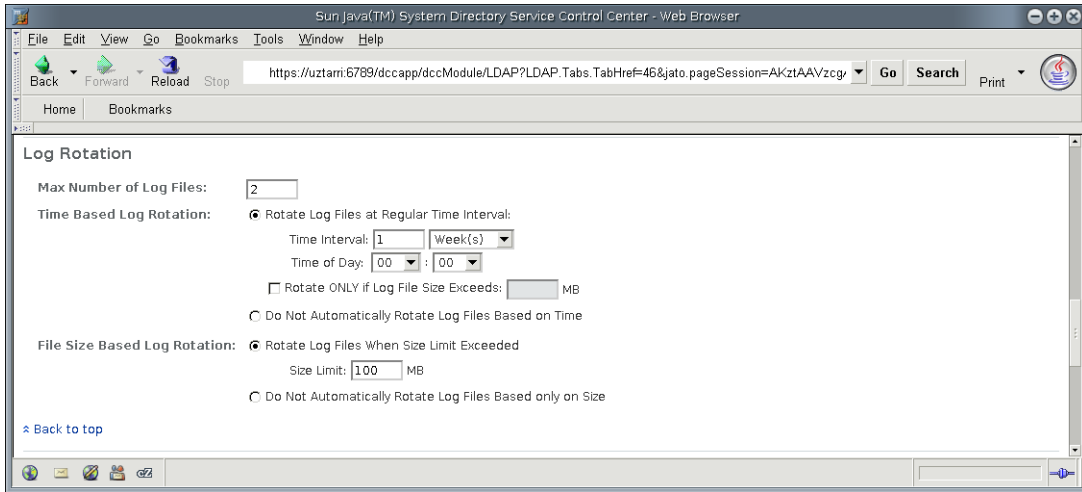
See the log(5dsconf) man page for details on the rotation-time log property.

For example, from the command line, you can display the current configuration for the access log as follows:

```
$ dsconf get-log-prop -p 20390
enabled                  :  on
level                    :  default
max-age                  :  1M
max-disk-space-size      :  500M
max-file-count           :  10
max-size                 :  100M
min-free-disk-space-size :  5M
path                     :  /install-path/sA1/logs/access
perm                     :  600
rotation-interval        :  1d
rotation-min-file-size   :  unlimited
rotation-time            :  undefined
verbose-enabled          :  N/A
```

You can change the rotation interval for the access log through the command line as follows:

```
$ dsconf set-log-prop -p 20390 rotation-interval:2d
```

Now, to display the new log file rotation interval, type the following:

```
$ dsconf get-log-prop -p 20390 rotation-interval
rotation-interval  :  2d
```

On-Demand Log Rotation

You can manually rotate Directory Server access, error, and audit logs. This feature is useful when you want the server to stop writing to the current log file while you examine the file. You might also choose to use this feature with system scheduler utilities in addition to time-based log rotation.

You can rotate the access log by using the DSCC. The following figure illustrates the logging configuration screen and the Rotate Log File Now button. Clicking this button allows you to close the current log file and start a new one.

To rotate the access log from the command line, type the following:

```
$ dsconf rotate-log-now -p 20390
```

See the dsconf(1M) man page for details on the rotate-log-now subcommand.

Configurable Log File Permissions Settings

Directory Server provides the ability to configure the permissions with which the log file is created, allowing you to change permissions to logs from the default value. This feature lets you tightly control what the user who starts the server can do. At the same time, you can permit specific applications and other users to access key, time-dependent information contained in the logs.

Directory Server enables you to specify the permissions with which a log file will be created.

Log file creation permissions can be set using the dsconf command or using the DSCC as illustrated in the following figure.
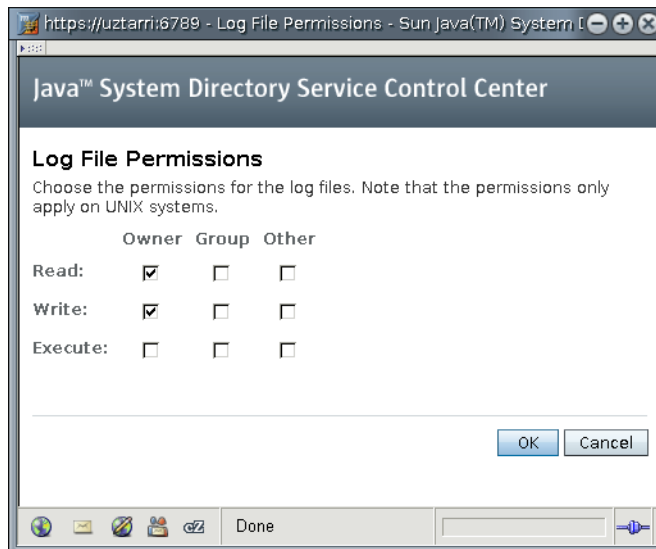
See the log(5dsconf) man page for details on the perm log property.

Monitoring and Managing Persistent Searches

You can now monitor the number of persistent searches that are running on the server, and set a maximum number of persistent searches. To monitor the number of persistent searches, view the value for the currentpsearches attribute, which is stored under cn=monitor. To set a maximum number of persistent searches, use the command dsconf set-server-prop max-psearch-count:*number*. This feature is useful for troubleshooting and preventing performance issues related to persistent searches.

Where to Go From Here

To read more about the features presented in this chapter, refer to the following documentation.

Feature	Documentation
Defining your Directory Server performance requirements	"Defining Performance Requirements" in *Sun Java System Directory Server Enterprise Edition 6.0 Deployment Planning Guide*
Introduction to caches and how Directory Server uses them	"Caches and How Directory Server Uses Them" in *Sun Java System Directory Server Enterprise Edition 6.0 Reference*
Tuning cache settings for better performance	"Tuning Cache Settings" in *Sun Java System Directory Server Enterprise Edition 6.0 Reference*
Introduction to Directory Server logging	Chapter 7, "Directory Server Logging," in *Sun Java System Directory Server Enterprise Edition 6.0 Reference*
Managing Directory Server logs	Chapter 14, "Directory Server Logging," in *Sun Java System Directory Server Enterprise Edition 6.0 Administration Guide*

For a hands-on demonstration of the features described in this chapter, use the scripts provided with the Evaluation Kit. The following table lists the scripts available to demonstrate each feature.

Feature	Evaluation Script
Forcing immediate log file rotation	`Demo_Rotate_Log_Now.sh`
Configuring log file permissions	`Demo_Log_File_Creation_Permissions.sh`

6 CHAPTER 6

Enhanced Security

This chapter describes the features of DSEE that secure identity to the highest degree possible. This chapter covers the following topics:

- "Connection-Based Access Control" on page 55
- "New Password Policy" on page 56
- "Preventing Binds With No Password" on page 59
- "Forced Password Change After Reset" on page 60
- "Global Account Lockout" on page 61
- "Directory Manager Enhancements" on page 62
- "Simplified Password Updates With LDAP Extended Operations" on page 62
- "Tracking of Last Login Time" on page 62
- "Enhanced Auditing for Updates Performed Using Proxy Authorization" on page 62
- "ACI Performance Enhancements" on page 63
- "Where to Go From Here" on page 63

Connection-Based Access Control

Directory Server enables you to use the host access control file `hosts.allow` and `hosts.deny` to specify the connection conditions to access the server. You can enable connection-based access control by using the `dsconf` command. Set the server property `host-access-dir-path` to the absolute path of the file system directory where the `hosts.allow` and `hosts.deny` files are located. See the `server(5dsconf)` and `hosts_access(4)` man pages for more information.

Connection-based access control can also be configured using ACIs. See "ACI Bind Rules" in *Sun Java System Directory Server Enterprise Edition 6.0 Reference* for background on ACI bind rules.

New Password Policy

Directory Server Enterprise Edition implements a new password policy that provides the following new features:

- A grace login limit, specified by the `pwdGraceLoginLimit` attribute. This attribute specifies the number of times that an expired password can be used to authenticate. If the attribute is not present or if it is set to 0, authentication will fail.

- Safe password modification, specified by the `pwdSafeModify` attribute. This attribute specifies whether the existing password must be sent when changing a password. If the attribute is not present, the existing password does not need to be sent.

In addition, the new password policy provides two new controls, `passwordPolicyRequest` and `passwordPolicyResponse`. These controls enable LDAP clients to obtain the account status information on LDAP `add`, `delete`, `modrdn`, `compare`, and `search` operations. The following information is available, using the OID `1.3.6.1.4.1.42.2.27.8.5.1` in the search:

- Period of time before the password expires
- Number of grace login attempts remaining
- The password has expired
- The account is locked
- The password must be changed after being reset
- Password modifications are allowed
- The user must supply his/her old password
- The password quality (syntax) is insufficient
- The password is too short
- The password is too young
- The password already exists in history

Managing the Password Policy Using the DSCC

The DSCC provides a tab for managing the password policies. You can use this tab to add new policies, assign a policy to Directory Server users, delete password policies, and change the password policy compatibility mode. The following figure illustrates this tab.

When you define a new password policy, you use the New Password Policy wizard. It allows you to specify password change settings, expiration settings, and content settings. It also allows you to specify account lockout settings. The following figure illustrates step 2 of the New Password Policy wizard.
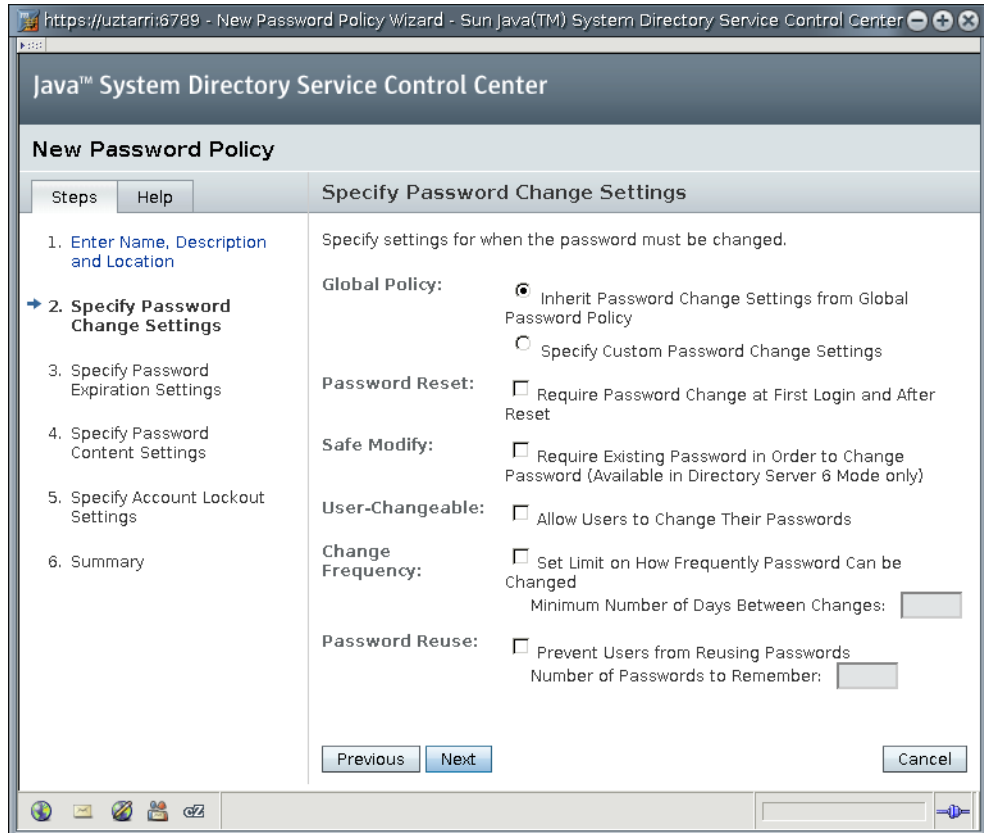
Migrating to the New Password Policy

For migration purposes, the new password policy maintains compatibility with previous Directory Server versions by identifying a compatibility mode. The compatibility mode determines whether password policy attributes are handled as *old* attributes or *new* attributes, where *old* refers to any Directory Server 5 password policy attributes.

See "New Password Policy" in *Sun Java System Directory Server Enterprise Edition 6.0 Migration Guide* for details on migrating to the new password policy.

Preventing Binds With No Password

Directory Server prevents authentication with a null password. All non-anonymous binds must therefore specify a password to bind to the directory. Otherwise, Directory Server returns an authentication error, LDAP_INAPPROPRIATE_AUTH.

You can disable this feature by setting the server property require-bind-pwd-enabled to off using the dsconf set-server-prop command.

The following command-line sequence walks you through a demonstration of this feature.

The default value of the Require Bind on Authentication feature is on. Check this by using the following command:

```
# dsconf get-server-prop -p 20390 -w /tmp/.pwd-file require-bind-pwd-enabled
require-bind-pwd-enabled  :  on
```

Authenticating with a null password results in the following error message:

```
# ldapsearch -D cn=altrootdn -w '' -p 20390 -b cn=config 'objectclass=*' dn
ldap_simple_bind: Inappropriate authentication
ldap_simple_bind: additional info: binds with a dn require a password
```

Note that this feature does not block anonymous binds:

```
# ldapsearch -p 20390 -b cn=config 'objectclass=*' dn
version: 1
dn: cn=SNMP,cn=config
```

Disable this feature by setting it to off:

```
# dsconf set-server-prop -p 20390 -w /tmp/.pwd-file require-bind-pwd-enabled:off
# dsconf get-server-prop -p 20390 -w /tmp/.pwd-file require-bind-pwd-enabled
require-bind-pwd-enabled  :  off
```

This time authenticating with a null password succeeds:

```
# ldapsearch -D cn=altrootdn -w '' -p 20390 -b cn=config 'objectclass=*' dn
version: 1
dn: cn=SNMP,cn=config
```

For instructions on using the Directory Service Control Center to configure password policy, see the DSCC online help.

Forced Password Change After Reset

This new feature of Directory Server enables administrators to force *regular* system users to change their passwords after a password reset.

This feature is enabled by the `pwd-must-change-enabled` property. This property specifies whether a user must change the password when he first binds or after the password has been set or reset. The feature is disabled by default.

You can enable this feature by selecting the Password Reset checkbox in the DSCC as illustrated in the following figure.

To view the current policy for requiring password change after password reset, use the following command:

```
# dsconf get-server-prop -p 20390 pwd-must-change-enabled
pwd-must-change-enabled  :  off
```

Enable the policy that requires changing the password after a reset as follows:

```
# dsconf set-server-prop  -p 20390 pwd-must-change-enabled:on
```

See Chapter 7, "Directory Server Password Policy," in *Sun Java System Directory Server Enterprise Edition 6.0 Administra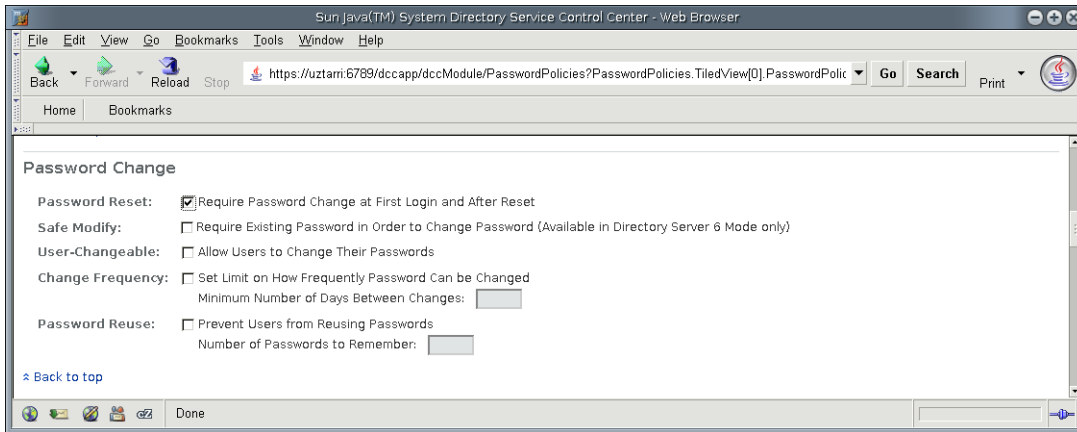tion Guide* for instructions on configuring password policy using command-line tools. For instructions on using the Directory Service Control Center to configure password policy, open the DSCC online help.

Global Account Lockout

This version of DSEE enables global account lockout. When a user account is locked due to consecutive failures to bind, the user account is effectively locked across the entire collection of servers.

You can configure user account lockout using the DSCC as illustrated in the following figure.
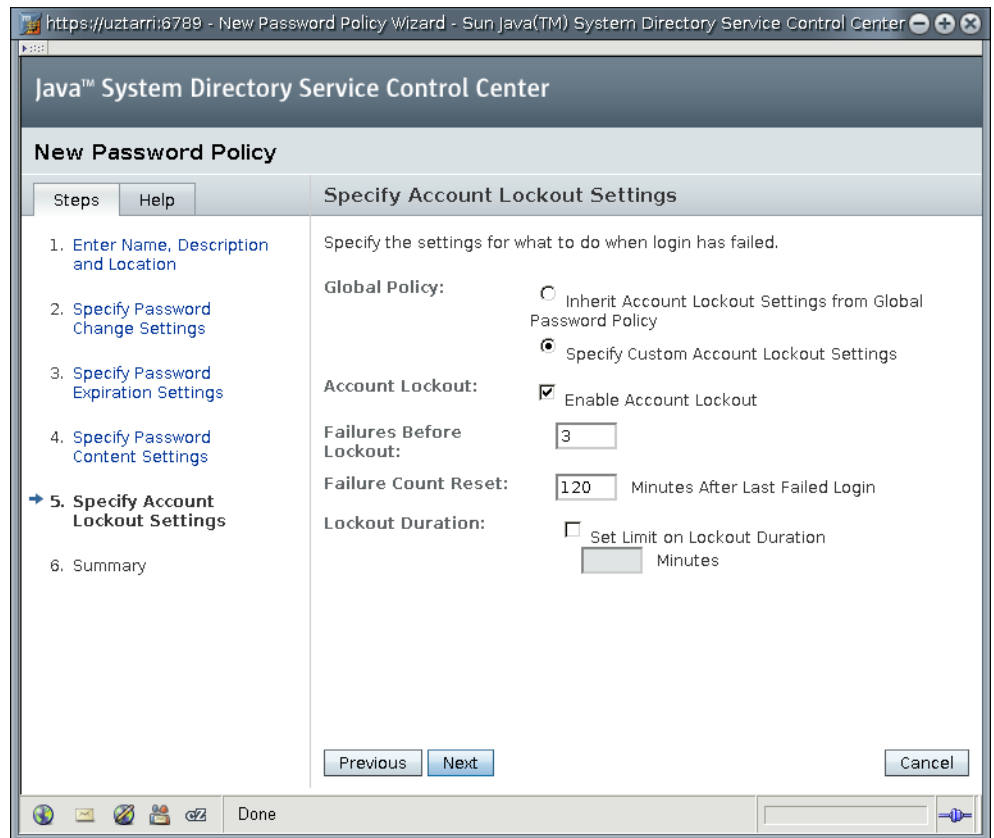
Directory Server now replicates account lockout data stored when a client application fails to authenticate to the server. When used together with the Directory Proxy Server capability to route binds appropriately, global account lockout can prevent a client application from gaining more than the number of tries you specify before being locked out across an entire directory service topology.

For more information, see "Preventing Authentication by Using Global Account Lockout" in *Sun Java System Directory Server Enterprise Edition 6.0 Deployment Planning Guide.*

Directory Manager Enhancements

Directory Server can be managed by directory administrators, who belong to the group cn=Administrators,cn=config. These users are subject to a special global ACI that gives them complete access to the directory. The default administrator created with each instance is cn=admin,cn=Administrators,cn=config.

Because these users have real entries, you can add certificates to their entries. This means that the administrator entry you create can bind using an SSL certificate. Furthermore, the server locks the administrative user out after too many failed bind attempts.

Simplified Password Updates With LDAP Extended Operations

Directory Server allows you to change expired passwords using the LDAP Password Modify Extended Operation specified in RFC 3062. The ldappasswd(1) command can be used to change expired passwords from the command line.

Tracking of Last Login Time

When you enable last login time tracking using the password policy attribute pwdKeepLastAuthTime(5dsat), Directory Server records the time of the last successful authentication in the operation attribute pwdLastAuthTime(5dsat) on the user entry.

Enhanced Auditing for Updates Performed Using Proxy Authorization

Directory Server now supports enhanced auditing for updates performed using proxy authorization. The server can log the identity authorized to perform an operation, rather than the identity that authenticated to Directory Server. When you set useAuthzIdForAuditAttrs on cn=config to on, the server records the authorization ID in the creatorsName or modifiersName attribute during a write operation on an entry. By default, Directory Server records the authentication ID.

ACI Performance Enhancements

Directory Server ACI processing has been enhanced to improve performance when one or both of the following are true:

- Numerous ACIs apply to regular user searches that retrieve all attributes on entries with large number of attributes
- Access control processing involves DNs that the server must normalize

Where to Go From Here

To read more about the features presented in this chapter, refer to the following documentation.

Feature	Documentation
Configuring a password policy using the command line	Chapter 7, "Directory Server Password Policy," in *Sun Java System Directory Server Enterprise Edition 6.0 Administration Guide*
Enabling global account lockout	"Preventing Authentication by Using Global Account Lockout" in *Sun Java System Directory Server Enterprise Edition 6.0 Deployment Planning Guide*
Overview of the new password policy architecture	"New Password Policy" in *Sun Java System Directory Server Enterprise Edition 6.0 Migration Guide*
Migrating to the new password policy	"Password Policy Configuration Attributes" in *Sun Java System Directory Server Enterprise Edition 6.0 Migration Guide*
Configuring connection-based access control with ACIs	"ACI Bind Rules" in *Sun Java System Directory Server Enterprise Edition 6.0 Reference*

For a hands-on demonstration of the features described in this chapter, use the scripts provided with the Evaluation Kit. The following table lists the scripts available to demonstrate each feature.

Feature	Evaluation Script
Preventing binds with no password	`Demo_Required_Bind_DN.sh`
Changing the root DN password from the command line	`Demo_RootPW_Change.sh`
Adding access controls to a JDBC data view	`Demo_JDBC_RW_Control.sh`

Feature	Evaluation Script
Setting up a secure administrative account	`Demo_Secure_root_DN.sh`
Forcing a password reset for non-root users	`Demo_non-root-PW-reset.sh`

Managed Scalability

This chapter describes the features of DSEE that give it the ability to support hundreds of millions and even billions of entry deployments. DSEE allows a flat namespace, such as ou=people, to be split up across multiple sets of servers configured for multimaster replication. This chapter covers the following topics:

Load Balancing and Operation-Based Routing

Directory Proxy Server now makes it possible both to route different LDAP operations on the same client connection to different servers and to enable successive requests on the same client connection to be sent to the same LDAP server. In addition, Directory Proxy Server offers a wider range of load balancing policies.

Furthermore, you can configure Directory Proxy Server to load balance LDAP traffic across different LDAP servers depending on the LDAP operation requested.

You can select your load balancing algorithms using the DSCC New Data Source Pool wizard, as illustrated in the following figure.
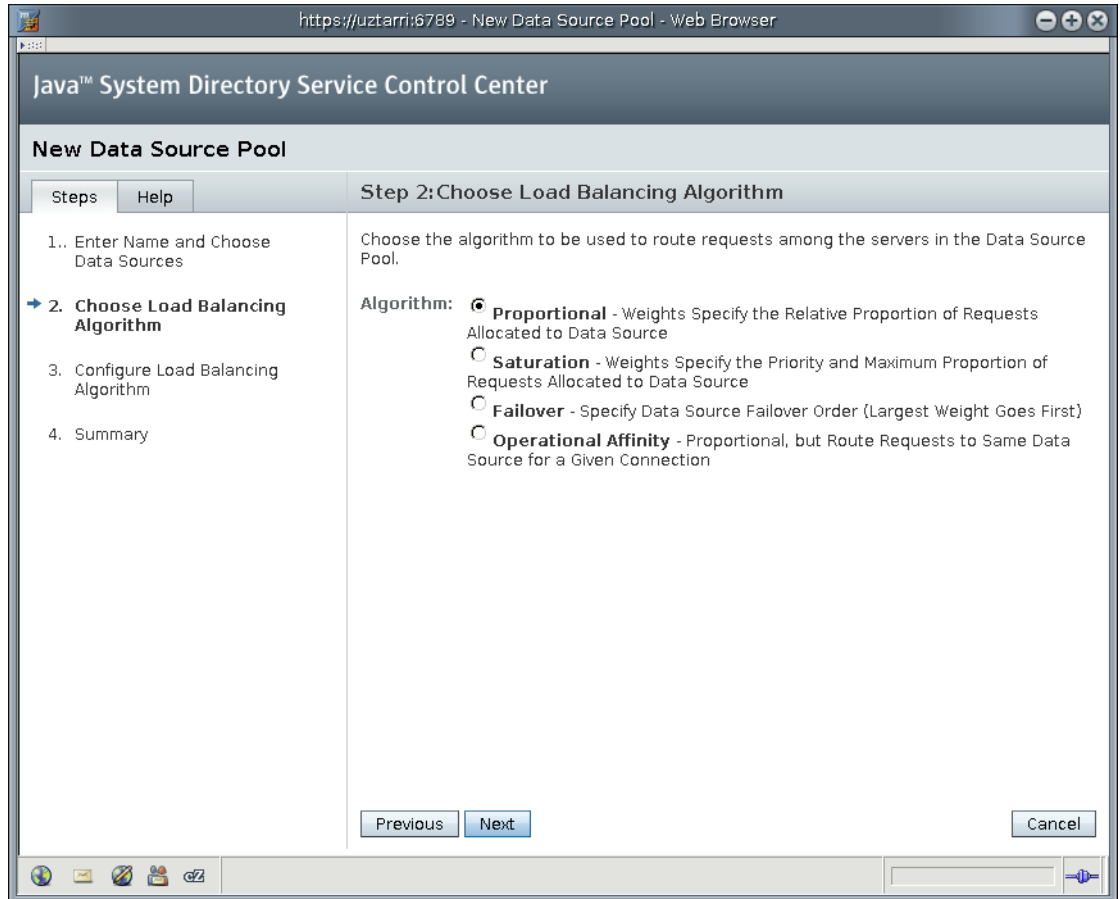
You can also use the DSCC New Data Source Pool wizard to configure the load balancing algorithm. The following figure illustrates how you define the percentage of read and write operations that are routed to each data source with the DSCC.

Step 3: Configure Load Balancing Algorithm

Set the read and write operation load balancing weights for each data source. You can set separate weights for each operation type after you complete the wizard by editing the data source pool properties.

Proportional: Specify relative proportion of requests to be allocated to each data source

Data Sources and Load Balancing Weights (4)

Data Source	Read/Bind Operations		Write Operations	
sA2	0	0%	50	49%
sA1	0	0%	50	49%
cA1	50	50%	1	0%
cA2	50	50%	1	0%

After you have configured the data source and its load balancing algorithm, you associate the data source with a data view by using the New Data View wizard, as illustrated in the following figure.
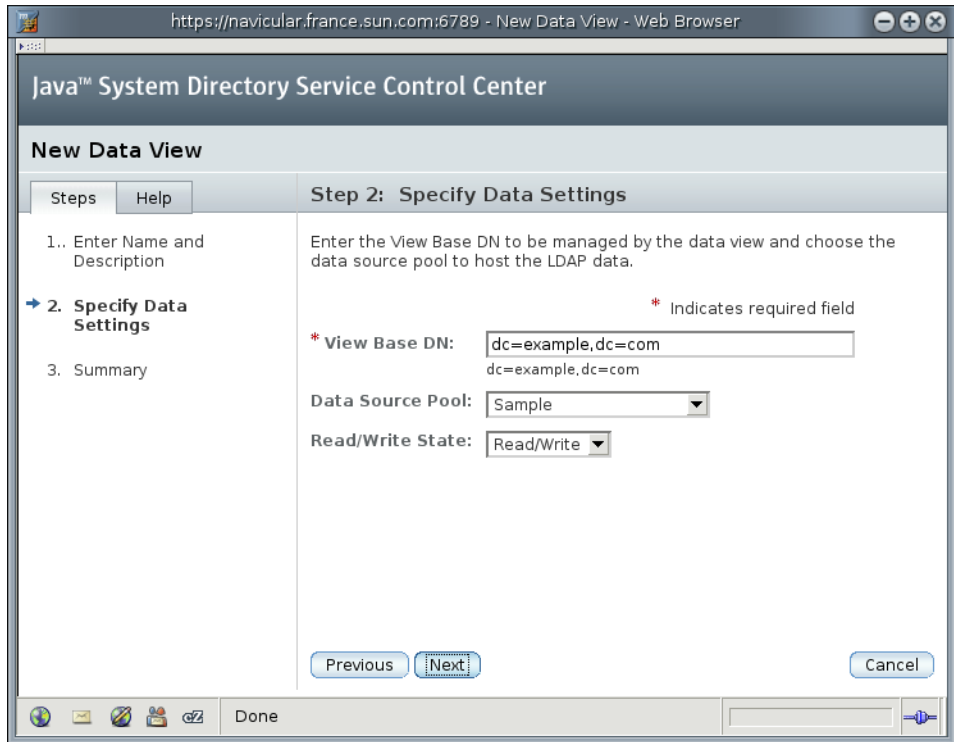
https://navicular.france.sun.com:6789 - New Data View - Web Browser

Java™ System Directory Service Control Center

New Data View

| Steps | Help |

Step 2: Specify Data Settings

1.. Enter Name and Description

➔ 2. **Specify Data Settings**

3. Summary

Enter the View Base DN to be managed by the data view and choose the data source pool to host the LDAP data.

* Indicates required field

* View Base DN: `dc=example,dc=com`
dc=example,dc=com

Data Source Pool: Sample

Read/Write State: Read/Write

Previous Next Cancel

Done

DN and Attribute Rewriting

You can configure Directory Proxy Server to automatically modify the DN, attribute types, and attribute values of entries. A client application view of an entry can thus be significantly different from what is stored in the directory.

DN rewriting is supported for the following operations on one DN:

- Add
- Bind
- Compare
- Delete
- Modify
- Modify DN

DN rewriting is also supported for the search operation base and the result entry DNs. The following figure illustrates how you can configure DN mapping using the Directory Service Control Center.
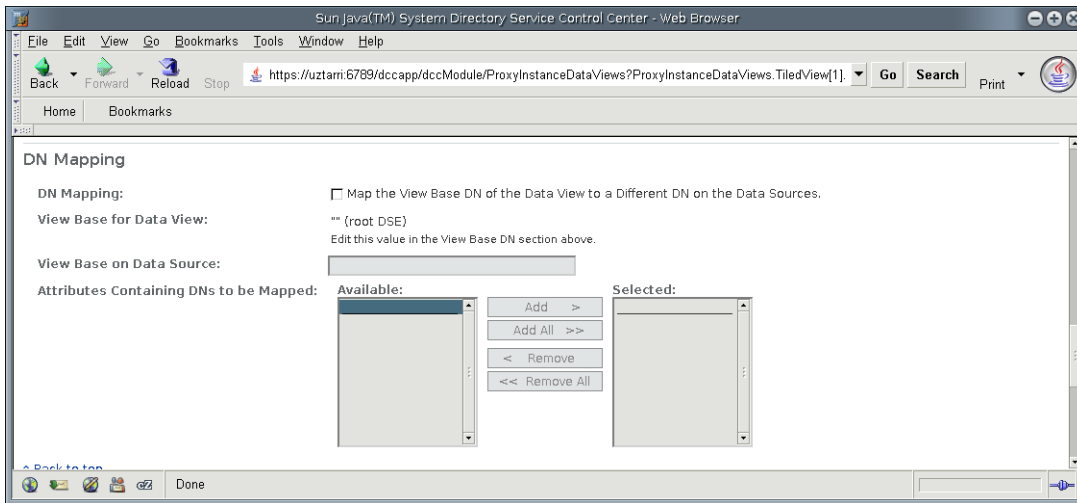
You can also use the Directory Service Control Center to map attributes, as illustrated in the following figure.
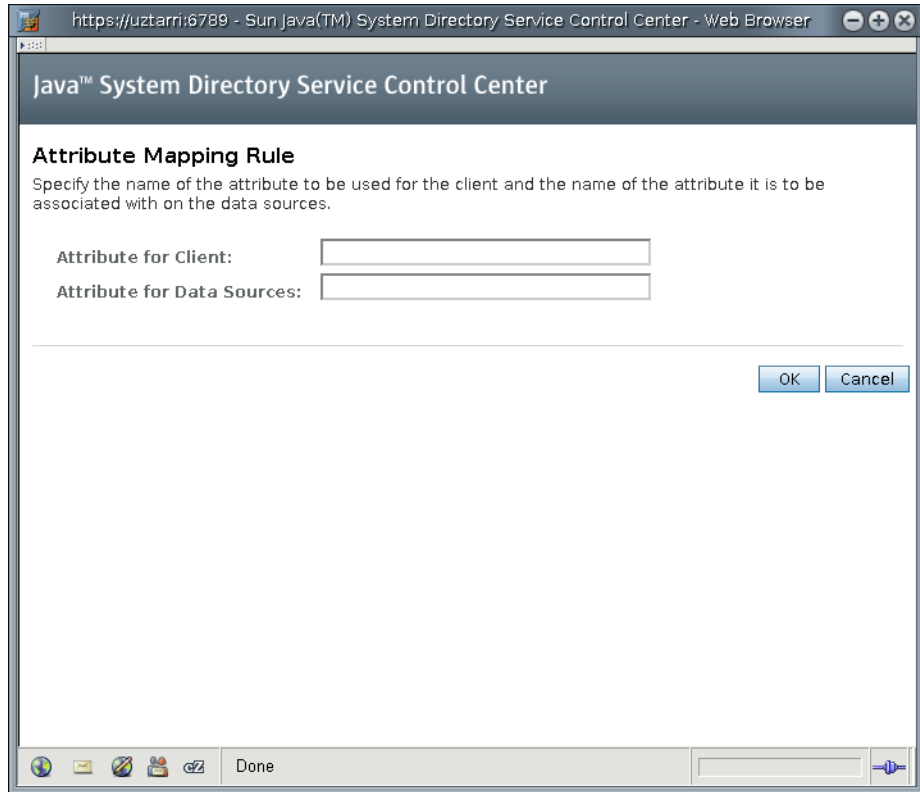
See "Creating and Configuring Data Views for Example Use Cases" in *Sun Java System Directory Server Enterprise Edition 6.0 Administration Guide* for example configurations using command-line tools.

Customizable Data Distribution for Faster Writes

You can design your deployment of DSEE to distribute your directory across servers to help you achieve the best possible performance for your directory-enabled applications. Customized distribution also increases the availability of your directory and improves the ease of managing your directory. The workload for each server is reduced because the contents of the databases have been distributed among a number of servers. Yet, from a clients perspective, the directory appears to be a single directory tree.

Distributing your data allows you to scale your directory across multiple servers without physically containing those directory entries on each server in your enterprise. A distributed directory can thus hold a much larger number of entries than would be possible with a single

server. In addition, you can configure your directory to hide the distribution details from the user. As far as users and applications are concerned, a single directory answers their directory queries.

For further information, see "Using Distribution for Write Scalability" in *Sun Java System Directory Server Enterprise Edition 6.0 Deployment Planning Guide*.

Where to Go From Here

To read more about the features presented in this chapter, refer to the following documentation.

Feature	Documentation
Designing a scaled deployment	Chapter 10, "Designing a Scaled Deployment," in *Sun Java System Directory Server Enterprise Edition 6.0 Deployment Planning Guide*
Administering Directory Proxy Server	Part II, "Directory Proxy Server Administration," in *Sun Java System Directory Server Enterprise Edition 6.0 Administration Guide*
Designing a global deployment	Chapter 11, "Designing a Global Deployment," in *Sun Java System Directory Server Enterprise Edition 6.0 Deployment Planning Guide*
Overview of the Directory Proxy Server architecture	Part II, "Directory Proxy Server Reference," in *Sun Java System Directory Server Enterprise Edition 6.0 Reference*
About Directory Proxy Server load balancing and client affinity	Chapter 25, "Directory Proxy Server Load Balancing and Client Affinity," in *Sun Java System Directory Server Enterprise Edition 6.0 Reference*
Configuring load balancing	Chapter 22, "Directory Proxy Server Load Balancing and Client Affinity," in *Sun Java System Directory Server Enterprise Edition 6.0 Administration Guide*

For a hands-on demonstration of the features described in this chapter, use the scripts provided with the Evaluation Kit. The following table lists the scripts available to demonstrate each feature.

Feature	Evaluation Script
Load balancing and operation routing	`Setup_DPS_Service.sh`
Mapping DNs	`Setup_DPS_Add_DN_ReMapping.sh`

8

Virtual Directory

The virtual directory functionality provided by Directory Proxy Server enables you to aggregate different data into an LDAP view displayed to LDAP client applications. Data can be filtered or even changed, based on what the client application requires. Different applications can therefore have different virtual views of the same data. By providing a logical layer that presents the data in custom views, you can avoid changes to your underlying infrastructure and existing applications and can deploy more quickly.

This chapter provides an overview of the virtual directory features and covers the following topics:

Defining a Virtual Namespace Made Up of Multiple Sources

The virtual directory consolidates data from multiple directories, databases, and other data sources into a logical view that you can customize for each application's specifications. These virtual namespaces are created when source data is transformed into the proper format, joined from several sources, and restructured according to the needs of your client applications. Different applications can therefore have different *virtual views* of exactly the same data. Because the virtual namespace is created without changes to the underlying data, implementation is simplified.

For example, an enterprise has deployed a directory server with information about its employees. A separate directory server contains additional employee information to support Access Manager. The enterprise sets up Directory Proxy Server to provide the Access Manager environment a single view of the user data in both directories. The enterprise also uses

Directory Proxy Server to distribute updates made to the user entries to the appropriate repository. For example, when a bind is made, updates made by Access Manager to user entries are limited to the Access Manager directory.

For information about creating multiple virtual data views, see "Construction of Virtual Data Views" in *Sun Java System Directory Server Enterprise Edition 6.0 Reference*.

The following sections describe the various data views supported by the virtual directory.

Access to JDBC Compliant Data Repositories

The virtual directory provides a JDBC data view that enables you to make relational databases accessible to LDAP client applications. For example, JDBC data views enable you to map LDAP attributes to columns in an RDBMS table or in a SQL database. For information about accessing data repositories that are compliant with the JDBC technology, see "JDBC Data Views" in *Sun Java System Directory Server Enterprise Edition 6.0 Reference*

Access to Flat LDIF File Resources

The virtual directory provides an LDIF data view that enables LDAP client access to flat LDIF files. For information about accessing LDIF files, see "LDIF Data Views" in *Sun Java System Directory Server Enterprise Edition 6.0 Reference*.

Access to LDAP Resources

For a demonstration of adding an LDAP virtual view to an existing DPS configuration, run the `Setup_DPS-LDAP_Data_View.sh` script.

Aggregating Data Views to Create Virtual Entries

The virtual directory can create purely virtual entries that are built from multiple entries in multiple data views. You define virtual domains that aggregate data from multiple data sources. These sources can be LDAP directories, JDBC compliant data repositories, or flat LDIF files. Data aggregation includes joining data sources with dissimilar attribute names and different DNs.

For example, a directory contains an entry for Adam Brown, `cn=Adam Brown`. A human resource application requests the salary information for this user, but this information is stored in a separate Oracle database. Directory Proxy Server accesses the Oracle® database for the salary information and uses entry aggregation to add this information dynamically to the entry when it is retrieved by the human resources application. However, for other applications, such as a company address book, this information is not displayed as part of the user entry.

For more information about aggregating data sources, see "Join Data Views" in *Sun Java System Directory Server Enterprise Edition 6.0 Reference*.

Mapping Attribute Names and Values

The virtual data transformation feature enables you to map attribute names and values to suit LDAP client applications and multiple disparate data sources. For example, an attribute used by a client application can be mapped to any attribute name in an LDAP directory, LDIF file, or RDBMS database. This feature includes the dynamic creation, deletion, and renaming of virtual attributes, and of attribute values. Multivalued attributes are supported. A facility for defining default attribute values is also provided.

For more information about virtual data transformations, see "Virtual Data Transformations" in *Sun Java System Directory Server Enterprise Edition 6.0 Reference*.

Where to Go From Here

To read more about the features presented in this chapter, refer to the following documentation.

Feature	Documentation
Sample virtual directory deployment	Chapter 14, "Deploying a Virtual Directory," in *Sun Java System Directory Server Enterprise Edition 6.0 Deployment Planning Guide*
Creating virtual data views	Chapter 24, "Directory Proxy Server Virtual Data Views," in *Sun Java System Directory Server Enterprise Edition 6.0 Administration Guide*
Overview of JDBC virtual views	"JDBC Data Views" in *Sun Java System Directory Server Enterprise Edition 6.0 Reference*
Overview of LDIF virtual views	"LDIF Data Views" in *Sun Java System Directory Server Enterprise Edition 6.0 Reference*
Overview of join data views	"Join Data Views" in *Sun Java System Directory Server Enterprise Edition 6.0 Reference*
Overview of transforming virtual data	"Virtual Data Transformations" in *Sun Java System Directory Server Enterprise Edition 6.0 Reference*

For a hands-on demonstration of the features described in this chapter, use the scripts provided with the Evaluation Kit. The following table lists the scripts available to demonstrate each feature.

Feature	Evaluation Script
Adding a JDBC virtual view	`Setup_DPS-JDBC_Data_View.sh`
Adding an LDIF file virtual view	`Setup_DPS-LDIF_Data_View.sh`
Adding an LDAP virtual view	`Setup_DPS-LDAP_Data_View.sh`
Joining several virtual views	`Setup_DPS-Join_Views.sh`
Mapping DNs	`Setup_DPS_Add_DN_ReMapping.sh`

Synchronizing Directory Server With Windows Users and Groups

Identity Synchronization for Windows provide bidirectional password and user attribute synchronization between Directory Server and the Windows Active Directory or NT SAM registry. This chapter describes the key features of Identity Synchronization for Windows and covers the following topics:

- "Account Synchronization" on page 75
- "Group Synchronization With Active Directory" on page 76
- "Failover Support for Multimaster Replicas" on page 76
- "Integrated Administration Server Support for Windows Synchronization" on page 76
- "Where to Go From Here" on page 76

Account Synchronization

Identity Synchronization for Windows synchronizes account creation, modification, inactivation, and deletion between Active Directory and Directory Server, or Windows NT and Directory Server. Using Identity Synchronization for Windows you can create, modify, and delete selected attributes or users accounts in one directory environment and propagate the changes automatically to the other directory environment.

Identity Synchronization for Windows enables you to control the flow of object deletions and object activations and inactivations between Directory Server and Windows.

You can use Identity Synchronization for Windows to synchronize data with multiple Active Directory and Windows NT domains and with multiple Active Directory forests. The centralized system auditing makes it possible for you to monitor installation and configuration status, day-to-day system operations, and any error conditions related to your deployment from a single, centralized location.

Group Synchronization With Active Directory

Identity Synchronization for Windows supports synchronization of user groups between Directory Server and Active Directory. You can map a group on Directory Server to either Domain Global Distribution, or to Domain Global Security on Active Directory.

For more information aboutgroup synchronization, see "Configure Identity Synchronization for Windows to Detect and Synchronize Groups Related Changes between Directory Server and Active Directory" in *Sun Java System Directory Server Enterprise Edition 6.0 Installation Guide*.

Failover Support for Multimaster Replicas

Identity Synchronization for Windows supports synchronizing users in a single replicated suffix.

Integrated Administration Server Support for Windows Synchronization

The installer might not find an existing Administration Server for the selected directory source on the local host. However, Identity Synchronization for Windows ships with Administration Server. When the installer does not find a local Administration Server, the installer adds the Administration Server at the specified Server Root location.

Where to Go From Here

To read more about the features presented in this chapter, refer to the following documentation.

Feature	Documentation
Deploying Identity Synchronization for Windows	*Sun Java System Identity Synchronization for Windows 6.0 Deployment Planning Guide*
Using the Identity Synchronization for Windows command-line utilities	Appendix A, "Using the Identity Synchronization for Windows Command Line Utilities," in *Sun Java System Directory Server Enterprise Edition 6.0 Installation Guide*

Feature	Documentation
Sample XML configuration documents	Appendix B, "Identity Synchronization for Windows LinkUsers XML Document Sample," in *Sun Java System Directory Server Enterprise Edition 6.0 Installation Guide*
Configuring multiple Windows domains and using Synchronization User Lists (SULs)	Appendix D, "Defining and Configuring Synchronization User Lists for Identity Synchronization for Windows," in *Sun Java System Directory Server Enterprise Edition 6.0 Installation Guide*
Synchronizing users in a single replicated suffix	Appendix E, "Identity Synchronization for Windows Installation Notes for Replicated Environments," in *Sun Java System Directory Server Enterprise Edition 6.0 Installation Guide*
Group synchronization	"Configure Identity Synchronization for Windows to Detect and Synchronize Groups Related Changes between Directory Server and Active Directory" in *Sun Java System Directory Server Enterprise Edition 6.0 Installation Guide*

A

Standards and RFCs Supported by Directory Server Enterprise Edition

Directory Server Enterprise Edition software supports the RFCs and standards listed here.

Note – RFCs 2251 through 2256 as well as several others have been made obsolete by a new set of RFCs, RFCs 4510 through 4520. The new RFCs are listed in this appendix.

DSMLv2 (http://www.oasis-open.org/committees/dsml/docs/DSMLv2.xsd)
Directory Services Markup Language v2

FIPS 180-1 (http://www.itl.nist.gov/fipspubs/fip180-1.htm)
Secure Hash Standard (SHA-1)

RFC 1777 (http://www.ietf.org/rfc/rfc1777.txt)
Lightweight Directory Access Protocol (v2)

RFC 1778 (http://www.ietf.org/rfc/rfc1778.txt)
The String Representation of Standard Attribute Syntaxes

RFC 1779 (http://www.ietf.org/rfc/rfc1779.txt)
A String Representation of Distinguished Names

RFC 2079 (http://www.ietf.org/rfc/rfc2079.txt)
Attribute Type and Object Class to Hold URIs

See the rfc2079(5dssd) man page.

RFC 2246 (http://www.ietf.org/rfc/rfc2246.txt)
The TLS Protocol Version 1.0

RFC 2247 (http://www.ietf.org/rfc/rfc2247.txt)
Using Domains in LDAP/X.500 Distinguished Names

See the rfc2247(5dssd) man page.

RFC 2307 (http://www.ietf.org/rfc/rfc2307.txt)
An Approach for Using LDAP as a Network Information Service

See the `rfc2307`(5dssd) man page.

RFC 2377 (http://www.ietf.org/rfc/rfc2377.txt)
Naming Plan for Internet Directory-Enabled Applications

Only the `uidObject` class is defined in the Directory Server schema. The name forms are not defined in the schema. Name form definitions would interfere with legitimate uses of attributes other than `dc` in the RDNs of the associated objects.

RFC 2605 (http://www.ietf.org/rfc/rfc2605.txt)
Directory Server Monitoring MIB

Directory Server supports part of this RFC.

RFC 2713 (http://www.ietf.org/rfc/rfc2713.txt)
LDAP Schema for Java Objects

See the `rfc2713`(5dssd) man page .

RFC 2739 (http://www.ietf.org/rfc/rfc2739.txt)
Calendar Attributes for vCard and LDAP

Directory Server supports part of this RFC.

RFC 2788 (http://www.ietf.org/rfc/rfc2788.txt)
Network Services Monitoring MIB

RFC 2798 (http://www.ietf.org/rfc/rfc2798.txt)
Definition of the `inetOrgPerson` *LDAP Object Class*

See the `rfc2798`(5dssd) man page .

RFC 2831 (http://www.ietf.org/rfc/rfc2831.txt)
Using Digest Authentication as a SASL Mechanism

Currently, only the `auth` protection quality can be used.

RFC 2849 (http://www.ietf.org/rfc/rfc2849.txt)
LDAP Data Interchange Format (LDIF)

RFC 2891 (http://www.ietf.org/rfc/rfc2891.txt)
LDAP Server-Side Sort Control

RFC 2926 (http://www.ietf.org/rfc/rfc2926.txt)
Conversion of LDAP Schemas to and from SLP Templates

No SLP-specific attribute syntaxes referenced in this document have been implemented. References to those syntaxes have been replaced with references to the IA5 String syntax.

RFC 3045 (http://www.ietf.org/rfc/rfc3045.txt)
Storing Vendor Information in the LDAP Root DSE

See the rfc3045(5dssd) man page.

RFC 3062 (http://www.ietf.org/rfc/rfc3062.txt)
LDAP Password Modify Extended Operation

RFC 3296 (http://www.ietf.org/rfc/rfc3296.txt)
LDAP Named Subordinate References

See the rfc3296(5dssd) man page.

RFC 3671 (http://www.ietf.org/rfc/rfc3671.txt)
Collective Attributes in LDAP

Directory Server supports part of this RFC.

RFC 3698 (http://www.ietf.org/rfc/rfc3698.txt)
LDAP Additional Matching Rules

Directory Server supports part of this RFC.

RFC 3829 (http://www.ietf.org/rfc/rfc3829.txt)
LDAP Authorization Identity Controls

RFC 3866 (http://www.ietf.org/rfc/rfc3866.txt)
Language Tags and Ranges in LDAP

Directory Server supports part of this RFC.

RFC 4370 (http://www.ietf.org/rfc/rfc4370.txt)
LDAP Proxied Authorization Control (v2)

RFC 4422 (http://www.ietf.org/rfc/rfc4422.txt)
Simple Authentication and Security Layer (SASL)

RFC 4505 (http://www.ietf.org/rfc/rfc4505.txt)
Anonymous Simple Authentication and Security Layer (SASL) Mechanism

RFC 4511 (http://www.ietf.org/rfc/rfc4511.txt)
Lightweight Directory Access Protocol (v3)

RFC 4512 (http://www.ietf.org/rfc/rfc4512.txt)
Lightweight Directory Access Protocol (LDAP): Directory Information Models

RFC 4513 (http://www.ietf.org/rfc/rfc4513.txt)
Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms

RFC 4514 (http://www.ietf.org/rfc/rfc4514.txt)
Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names

RFC 4515 (http://www.ietf.org/rfc/rfc4515.txt)
Lightweight Directory Access Protocol (LDAP): String Representation of Search Filters

RFC 4516 (http://www.ietf.org/rfc/rfc4516.txt)
Lightweight Directory Access Protocol (LDAP): Uniform Resource Locator

RFC 4517 (http://www.ietf.org/rfc/rfc4517.txt)
Lightweight Directory Access Protocol (LDAP): Syntaxes and Matching Rules

RFC 4519 (http://www.ietf.org/rfc/rfc4519.txt)
Lightweight Directory Access Protocol (LDAP): Schema for User Applications

RFC 4522 (http://www.ietf.org/rfc/rfc4522.txt)
Lightweight Directory Access Protocol (LDAP): The Binary Encoding Option

RFC 4523 (http://www.ietf.org/rfc/rfc4523.txt)
Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates

Directory Server Enterprise Edition software supports part of this RFC.

RFC 4524 (http://www.ietf.org/rfc/rfc4524.txt)
COSINE LDAP/ X.500 Schema

RFC 4532 (http://www.ietf.org/rfc/rfc4522.txt)
Lightweight Directory Access Protocol (LDAP) "Who am I?" Operation