Oracle® Directory Server Enterprise Edition Evaluation Guide

11 *g* Release 1 (11.1.1.5.0)

Part No: 821–1223
May 2011

ORACLE

110713@25097

Contents

Preface

This *Evaluation Guide* describes the key features available in Directory Server Enterprise Edition software.

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, "Overview of Directory Server Enterprise Edition," provides an introduction to the Directory Server Enterprise Edition components and describes the Directory Server Enterprise Edition administration model.

Chapter 2, "Service Manageability," shows the powerful features available for managing your directory service, including the Web-based Directory Service Control Center and the advanced command-line interface.

Chapter 3, "High Data Availability and Integrity," provides a quick tour of the Directory Server Enterprise Edition features that provide high data availability and integrity.

Chapter 4, "Tuned for Performance," provides an introduction to the Directory Server features of DSEE that help you tune your deployment for best performance.

Chapter 5, "Enhanced Security," describes the features of DSEE that secure identity to the highest degree possible

Chapter 6, "Managed Scalability," describes the features of DSEE that give it the ability to support hundreds of millions and even billions of entry deployments.

Chapter 7, "Virtual Directory," demonstrates DSEE virtual directory capabilities, which aggregate a single namespace from multiple heterogeneous data repositories.

Chapter 8, "Synchronizing Directory Server With Windows Users and Groups," 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, "Standards and RFCs Supported by Directory Server Enterprise Edition," summarizes the standards and RFCs supported by this version of the Directory Server Enterprise Edition software.

Oracle Directory Server Enterprise Edition Documentation Set

This documentation set explains how to use Oracle 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://download.oracle.com/docs/cd/E20295_01/index.htm`.

The following table lists the documents that make up the Directory Server Enterprise Edition documentation set.

TABLE P–1 Directory Server Enterprise Edition Documentation

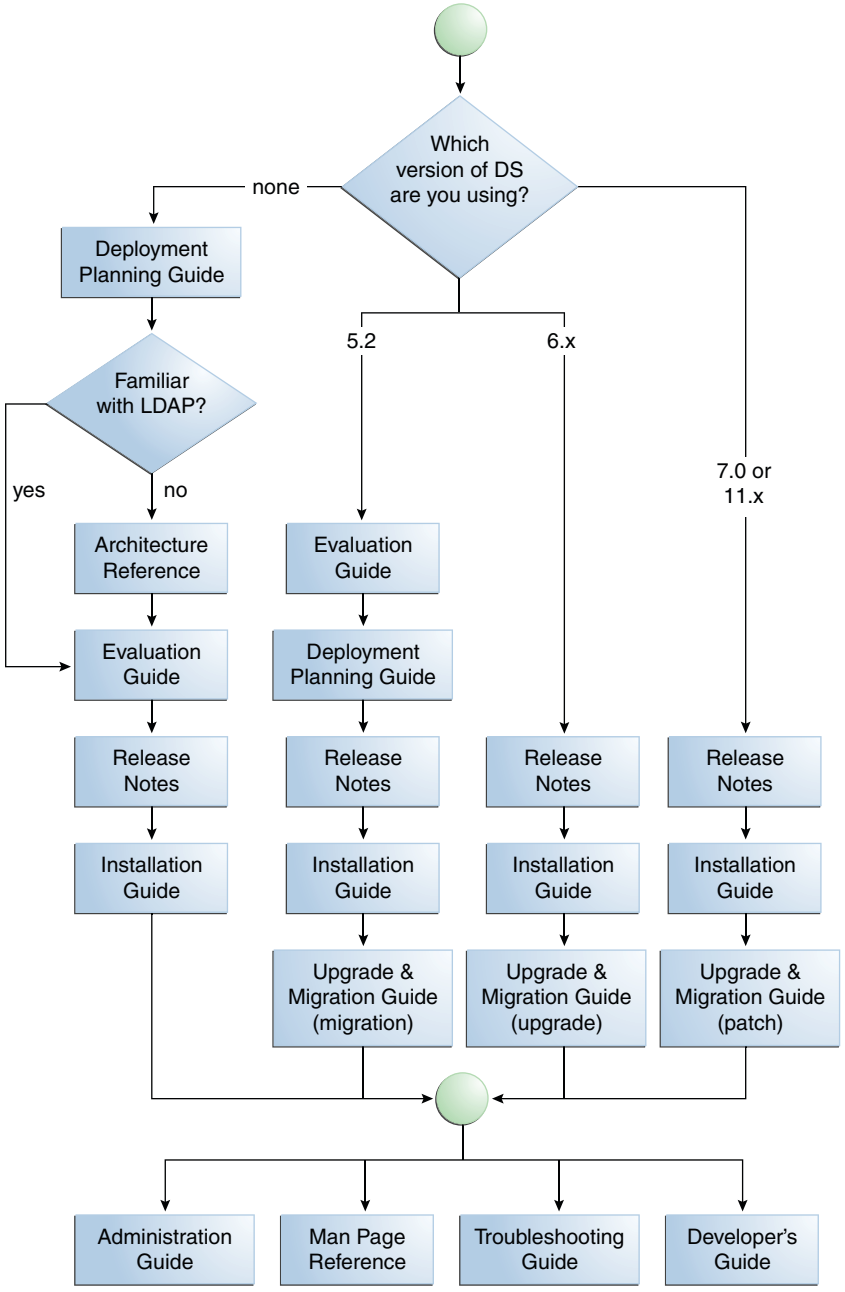
Document Title	Contents
Oracle Directory Server Enterprise Edition Release Notes	Contains the latest information about Directory Server Enterprise Edition, including known problems.
Oracle Directory Server Enterprise Edition Evaluation Guide	Introduces the key features of this release. Demonstrates how these features work and what they offer in the context of a deployment that you can implement on a single system.
Oracle Directory Server Enterprise Edition 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.
Oracle Directory Server Enterprise Edition Installation Guide	Explains how to install the Directory Server Enterprise Edition software. Shows how to configure the installed software and verify the configured software.
Oracle Directory Server Enterprise Edition Upgrade and Migration Guide	Provides instructions for upgrading versions 11.1.1.3, 7.x, and 6 installations, and instructions for migrating version 5.2 installations.

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

Document Title	Contents
Oracle Directory Server Enterprise Edition Administration Guide	Provides command-line instructions for administering Directory Server Enterprise Edition. For hints and instructions about using the Directory Service Control Center, DSCC, to administer Directory Server Enterprise Edition, see the online help provided in DSCC.
Oracle Directory Server Enterprise Edition Reference	Introduces technical and conceptual foundations of Directory Server Enterprise Edition. Describes its components, architecture, processes, and features.
Oracle Fusion Middleware Man Page Reference for Oracle Directory Server Enterprise Edition	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.
Oracle Directory Server Enterprise Edition Developer's Guide	Shows how to develop directory client applications with the tools and APIs that are provided as part of Directory Server Enterprise Edition.
Oracle Directory Server Enterprise Edition Troubleshooting Guide	Provides information for defining the scope of the problem, gathering data, and troubleshooting the problem areas by using various tools.
Oracle Identity Synchronization for Windows 6.0 Deployment Planning Guide	Provides general guidelines and best practices for planning and deploying Identity Synchronization for Windows.
Oracle Identity Synchronization for Windows 6.0 Installation and Configuration Guide	Describes how to install and configure Identity Synchronization for Windows.
Additional Installation Instructions for Oracle Identity Synchronization for Windows 6.0	Provides installation instructions for Identity Synchronization for Windows 6.0 SP1.

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

FIGURE P–1 ODSEE Documentation Map



Related Reading

The SLAMD Distributed Load Generation Engine is a Java application that is designed to stress test and analyze the performance of network-based applications. This application 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) supports accessing the Directory Server using LDAP and DSML v2 from Java applications. For information about JNDI, see `http://www.oracle.com/technetwork/java/jndi/index.html`. The *JNDI Tutorial* contains detailed descriptions and examples of how to use JNDI. This tutorial is at `http://download.oracle.com/javase/jndi/tutorial/`.

Identity Synchronization for Windows uses Message Queue with a restricted license. Message Queue documentation is available at `http://docs.sun.com/coll/1307.6`.

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 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 documentation, and provides 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 complete descriptions of the files installed, see Chapter 1, “Directory Server Enterprise Edition File Reference,” in *Oracle Directory Server Enterprise Edition Reference*.

TABLE P–2 Default Paths

Placeholder	Description	Default Value
install-path	Represents the base installation directory for Directory Server Enterprise Edition software.	When you install from a zip distribution using unzip, the *install-path* is the *current-directory*/dsee7. When you install from a native package distribution, the default *install-path* is /opt/SUNWdsee7.
instance-path	Represents the full path to an instance of Directory Server or Directory Proxy Server. Documentation uses /local/dsInst/ 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. On Solaris systems, the /var directory is recommended:
serverroot	Represents the parent directory of the Identity Synchronization for Windows installation location	Depends on your installation. Note that the concept of a *serverroot* no longer exists for Directory Server and Directory Proxy 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 log files 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 log files	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	Native Package Distribution	Zip Distribution
`cacaoadm`	`/usr/sbin/cacaoadm`	Solaris, Linux, HP—UX — *install-path*`/bin/cacaoadm`
		Windows - *install-path*`\bin\cacaoadm.bat`
`certutil`	`/usr/sfw/bin/certutil`	*install-path*`/bin/certutil`
`dpadm`(1M)	*install-path*`/bin/dpadm`	*install-path*`/bin/dpadm`
`dpconf`(1M)	*install-path*`/bin/dpconf`	*install-path*`/bin/dpconf`
`dsadm`(1M)	*install-path*`/bin/dsadm`	*install-path*`/bin/dsadm`
`dsccmon`(1M)	*install-path*`/bin/dsccmon`	*install-path*`/bin/dsccmon`
`dsccreg`(1M)	*install-path*`/bin/dsccreg`	*install-path*`/bin/dsccreg`
`dsccsetup`(1M)	*install-path*`/bin/dsccsetup`	*install-path*`/bin/dsccsetup`
`dsconf`(1M)	*install-path*`/bin/dsconf`	*install-path*`/bin/dsconf`
`dsmig`(1M)	*install-path*`/bin/dsmig`	*install-path*`/bin/dsmig`
`dsutil`(1M)	*install-path*`/bin/dsutil`	*install-path*`/bin/dsutil`
`entrycmp`(1)	*install-path*`/bin/entrycmp`	*install-path*`/bin/entrycmp`
`fildif`(1)	*install-path*`/bin/fildif`	*install-path*`/bin/fildif`
`idsktune`(1M)	Not provided	At the root of the unzipped zip distribution
`insync`(1)	*install-path*`/bin/insync`	*install-path*`/bin/insync`
`ldapsearch`(1)	*install-path*`/dsrk/bin/ldapsearch`	*install-path*`/dsrk/bin/ldapsearch`
`repldisc`(1)	*install-path*`/bin/repldisc`	*install-path*`/bin/repldisc`

Typographic Conventions

The following table describes the typographic conventions 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	Placeholder: replace 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	Read Chapter 6 in the *User's Guide*. A *cache* is a copy that is stored locally. Do *not* save the file. **Note:** Some emphasized items appear bold online.

Shell Prompts in Command Examples

The following table shows the default UNIX system prompt and superuser prompt for shells that are included in the Oracle Solaris OS. Note that the default system prompt that is displayed in command examples varies, depending on the Oracle Solaris release.

TABLE P–5 Shell Prompts

Shell	Prompt
Bash shell, Korn shell, and Bourne shell	`$`
Bash shell, Korn shell, and Bourne shell for superuser	`#`
C shell	`machine_name%`
C shell for superuser	`machine_name#`

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.
→	Indicates menu item selection in a graphical user interface.	File → New → Templates	From the File menu, choose New. From the New submenu, choose Templates.

Documentation, Support, and Training

See the following web sites for additional resources:

- Documentation (`http://www.oracle.com/technetwork/indexes/documentation/index.html`)
- Support (`http://www.oracle.com/us/support/systems/index.html`)
- Training (`http://education.oracle.com`) – Click the Sun link in the left navigation bar.

Oracle Software Resources

Oracle Technology Network (`http://www.oracle.com/technetwork/index.html`) offers a range of resources related to Oracle software:

- Discuss technical problems and solutions on the ODSEE Discussion Forum (`http://forums.oracle.com/forums/forum.jspa?forumID=877`) and the Directory Services blog (`http://blogs.oracle.com/directoryservices/`).
- Get hands-on step-by-step tutorials with Oracle By Example (`http://www.oracle.com/technetwork/tutorials/index.html`).

- Download ODSEE 11g Example Files (`http://www.oracle.com/technetwork/middleware/id-mgmt/learnmore/odsee11113-examples-350399.zip`).

◆ ◆ ◆ CHAPTER 1

Overview of Directory Server Enterprise Edition

This chapter provides an introduction to theOracle Directory Server Enterprise Edition components, describes the DSEE administration model, and refers to the latest features. This chapter covers the following topics:

About Directory Server Enterprise Edition

Directory Server Enterprise Edition provides secure, highly available, scalable directory services for storing and managing identity data. Directory Server Enterprise Edition is the foundation of an enterprise identity infrastructure. It enables mission-critical enterprise applications and large-scale extranet applications to access consistent and reliable identity data.

Directory Server Enterprise Edition provides a central repository for storing and managing identity profiles, access privileges, application and network resource information. Directory Server Enterprise Edition integrates smoothly into multi-platform environments. It also provides secure, on-demand synchronization of passwords, users, and groups with Microsoft Active Directory.

Prior to Directory Server Enterprise Edition, these functions were part of four separate product offerings including Directory Server, Directory Proxy Server, Directory Server Resource Kit and Identity Synchronization for Windows. These and other products are now components of one comprehensive, integrated solution.

Quality of Service Requirements for a Robust Directory Service

The more users and applications in an enterprise, the more critical is the need for a robust directory service. Directory Server Enterprise Edition addresses the challenges faced by a rapidly changing and expanding enterprise by providing the following quality of service requirements:

- **Availability.** A measure of how often the system's resources and services are accessible to end users, often expressed as the *uptime* of the system.
- **Scalability.** The ability to add capacity, and users, to a deployed system over time. Scalability typically involves adding resources to the system but should not require changes to the deployment architecture.
- **Security.** A complex combination of factors that describe the integrity of a system and its users. Security includes authentication and authorization of users, security of data, and secure access to the deployed system.
- **Interoperability.** The ease with which the system operates in conjunction with other systems.
- **Serviceability.** The ease with which a deployed system can be maintained. Maintenance tasks include monitoring the system, repairing problems that arise, and upgrading hardware and software components.

This chapter briefly describes how the components of Directory Server Enterprise Edition fill the quality of service requirements. The requirements are discussed in detail in the remainder of this guide.

Directory Server Enterprise Edition Components and Their Capabilities

- Directory Server Enterprise Edition (DSEE) serves as the backbone to an enterprise identity infrastructure. DSEE includes the following components:
- “Directory Server” on page 19
- “Directory Proxy Server” on page 21
- “Directory Service Control Center ” on page 21
- “Identity Synchronization for Windows” on page 22
- “Directory Server Resource Kit” on page 22

Each of these components addresses one or more of the quality of service requirements described previously. This section describes the components and illustrates how they fit together to provide a robust directory service.

Directory Server

Directory Server provides a scalable, high-performance data store for identity information. Directory Server supports the Lightweight Directory Access Protocol (LDAP) v3 and the Directory Service Markup Language (DSML) v2 natively for standards-based access. With LDAP and DSML over HTTP or SOAP (Simple Object Access Protocol), clients anywhere on a network are able to securely search and update directory data objects. Clients are also able to receive changes made by other applications and to authenticate users or applications even through firewalls.

Directory Server and Security

Directory Server provides several security features to achieve compliance with information security policies. These features ensure that only users with proper authorization have access to information.

- **Macro-level, dynamic access control instructions (ACIs).** Provide a means for defining access down to the level of an LDAP attribute. Access control policies can be defined once, and then reused across the directory tree. Macro ACIs can be used to optimize the number of ACIs in the directory, thereby reducing the complexity of the security framework.
- **Role-based access.** Enables you to provide access that is based on information in a user's entry. Roles are defined and administered like groups, but roles provide more efficient grouping mechanisms for applications. Roles can be used in ACIs to control access to data. They can also be used by Class of Service (CoS), a capability of Directory Server to create virtual attributes that can apply to many entries at the same time. These virtual attributes reduce storage requirements on entries. They also allow a single change to update an unlimited number of related entries.
- **Get Effective Rights control.** Provides a means for determining what access a user has to a set of information. Administrators who maintain access policies for the directory service can tighten security by auditing the permissions of directory users and applications. This capability can also be used to build applications with adaptive interfaces that are based on the user's rights.
- **Encryption mechanisms.** Protect data on the disk and during transfer through communications channels. Directory Server also supports fractional replication and data hiding based on access. These mechanisms can be used to comply with European Union and other international privacy regulations.
- **Multiple password policies.** Can be defined on a per-user basis or targeted to certain groups. These policies help to ensure that users change passwords on a regular basis and that unauthorized access to an account is blocked.

Directory Server and Availability

Directory Server natively supports a variety of access protocols and offers a highly flexible, scalable replication environment that helps to ensure availability in distributed environments.

Directory Server replication prevents a single point of failure for applications that are using these protocols to access identity data. Directory Server supports a theoretically unlimited number of masters and read-only consumers in a replicated environment across both local and wide area networks. Special features of the replication protocol allow for optimizations when replicating data over high-latency networks. For more information, see "Using Replication and Redundancy for High Availability" in *Oracle Directory Server Enterprise Edition Deployment Planning Guide*.

Directory Server and Scalability

Directory Server provides for both vertical and horizontal growth without major deployment redesign. This level of scalability becomes increasingly critical as deployment grows.

Depending on the hardware, Directory Server can provide sustained search performance of 20,000 entries per second on a single machine and horizontal scalability to several thousand searches per second. For information about how to deploy Directory Server for read scalability, see Chapter 10, "Designing a Scaled Deployment," in *Oracle Directory Server Enterprise Edition Deployment Planning Guide*.

The requirement to store and update information constantly increases with the expansion of use across the organization. Update performance of Directory Server is close to relational database-write performance. For information about how to deploy Directory Server for write scalability, see Chapter 10, "Designing a Scaled Deployment," in *Oracle Directory Server Enterprise Edition Deployment Planning Guide*.

Directory Server provides linear CPU scalability to up to 28 CPUs for "read from cache" operations. It allows access to maximum memory capacity and delivers high performance that accommodates large directories on a single system for maximum hardware benefit.

Directory Server and Serviceability

Directory Server provides a comprehensive set of management tools for administering individual servers as well as the entire directory service.

A centralized, web-based administration console can be used to configure and manage multiple Directory Servers. The interface includes all the tools required for effective, day-to-day server administration and service from configuration to monitoring. In addition, the `dsadm` and `dsconf` command-line utilities can be used dynamically while the servers are running. These management features mean that most management operations can be performed while the directory is online, thus maximizing availability.

Management flexibility simplifies the deployment of the directory service into many different environments. The command-line utilities make remote management as easy as if the service were in a local data center.

Directory Proxy Server

Directory Proxy Server is an LDAP application-layer protocol gateway. It is designed to deliver enhanced directory access control, schema compatibility, and high availability.

Directory Proxy Server and Availability

With features such as configurable load balancing, failover, and failback, Directory Proxy Server ensures that systems have access to required data.

Directory Proxy Server works with Directory Server to ensure reliability and to protect against denial-of-service attacks. Directory Proxy Server automatically routes requests appropriately and provides secure firewall-like services for Directory Server.

To prevent a single point of failure for mission-critical applications, Directory Proxy Server detects outages and routes traffic around affected areas, effectively load balancing requests across systems. When the affected areas are restored to operation, Directory Proxy Server detects the restored servers automatically.

For more information, see "Using Directory Proxy Server as Part of a Redundant Solution" in *Oracle Directory Server Enterprise Edition Deployment Planning Guide*.

Directory Proxy Server and Security

Directory Proxy Server accommodates large numbers of users who are accessing the directory and minimizes the security risks associated with providing this level of access. Security features enable administrators to determine where a request is coming from, whether the request is allowed, and what type of authentication is required. In the event of a search request, Directory Proxy Server can also ensure that the request meets minimum requirements.

Directory Proxy Server uses groups to define how to identify an LDAP client and what restrictions to enforce on clients that match a particular group. Groups can be defined using a variety of criteria.

To protect private directory information from unauthorized access, Directory Proxy Server can configure a fine-grained access control policy on LDAP directories. Such a policy can include controlling who can perform different types of operations on different parts of directories. Directory Proxy Server can be configured to prevent certain kinds of operations typically performed by web trawlers and robots in search of information.

Directory Service Control Center

Directory Service Control Center (DSCC) is a graphical user interface used to administer Directory Server and Directory Proxy Server instances. DSCC is configured by deploying the war file with any of the supported application servers. 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.

Identity Synchronization for Windows

Identity Synchronization for Windows provides basic synchronization of identity data between Directory Server Enterprise Edition and Microsoft Active Directory.

Identity Synchronization for Windows fulfills the requirement of interoperability. Synchronization of key identity data such as passwords eliminates the need for users to modify passwords several times to accommodate different application authentication mechanisms.

Use of a non intrusive implementation for synchronizing key identity data eliminates the time-consuming and maintenance-intensive need to install a client component on Active Directory servers.

Identity Synchronization for Windows enables users to change passwords and other identity data in either the Windows environment or the web-based application environment. In this way, Identity Synchronization for Windows maintains synchronization between Active Directory and Directory Server. Disabled accounts can also be synchronized between Active Directory and Directory Server. This synchronization ensures conformance of access policies to applications and data between the Windows desktops and web-based applications.

Directory Server Resource Kit

The Directory Server Resource Kit provides tools and application programming interfaces (APIs) for deploying, accessing, tuning, and maintaining Directory Server Enterprise Edition. These utilities help to implement and maintain more robust LDAP-based solutions.

Performance testing and capacity planning tools help administrators to measure performance and to perform capacity planning on installations of Directory Server Enterprise Edition. Debugging and maintenance tools help with troubleshooting as well as daily maintenance of Directory Server Enterprise Edition. Deployment utilities and tools facilitate the rollout of new installations of Directory Server Enterprise Edition and migration to new releases. LDAP productivity tools include sample LDAP applications that were developed using Directory Server Enterprise Edition.

In addition, Sun has developed SLAMD, a powerful load-generation testing application that includes all the tests needed to thoroughly performance-test Directory Server Enterprise Edition applications. SLAMD is available free of charge at `http://www.slamd.com`.

DSEE Administration Model

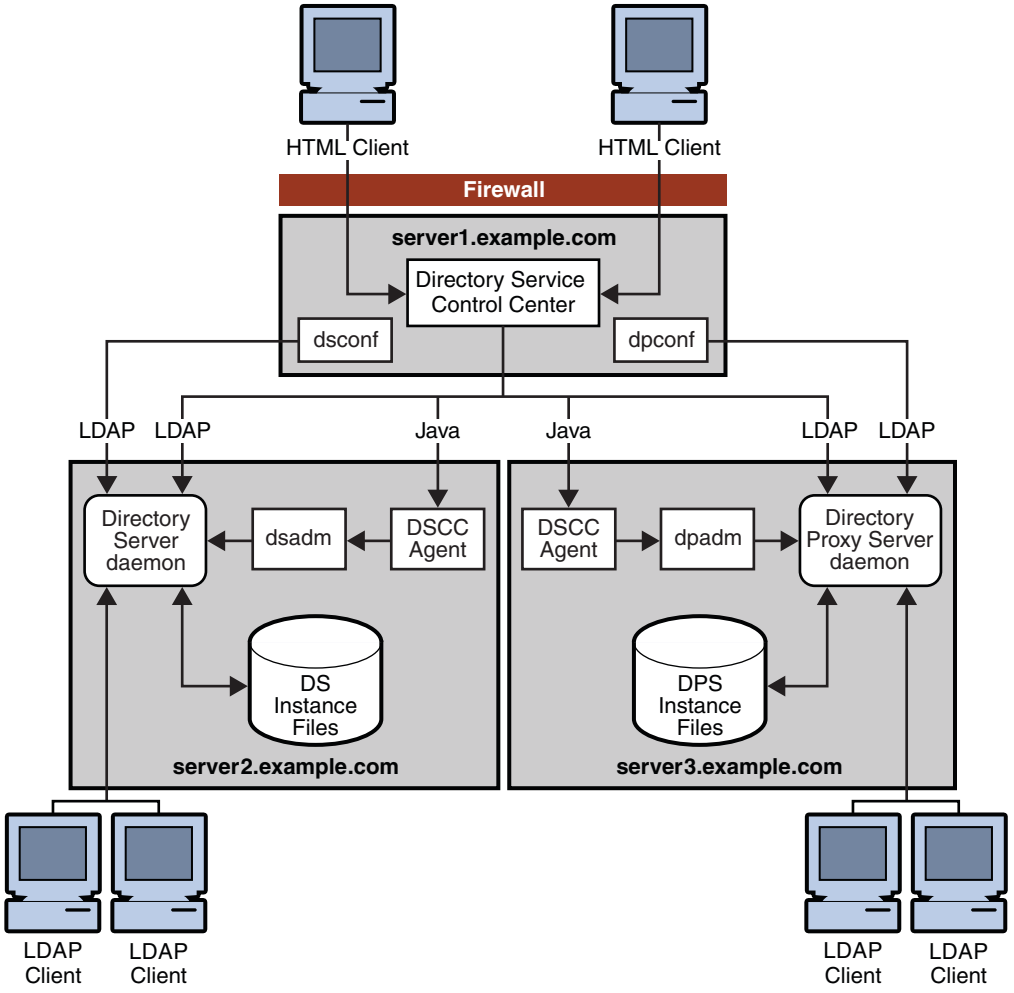
Before you can evaluate the features of DSEE, you need to understand the basics of DSEE architecture.

DSEE provides two 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 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.
- **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.

For a more in-depth description of DSEE administration model, see "Directory Server Enterprise Edition Administration Model" in *Oracle Directory Server Enterprise Edition Deployment Planning Guide*.

What's New at a Glance

For the list of new features and behavioral changes, see Chapter 1, "New Features in Oracle Directory Server Enterprise Edition 11g Release 1 (11.1.1.5.0)," in *Oracle Directory Server Enterprise Edition Release Notes*.

◆ ◆ ◆ CHAPTER 2

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

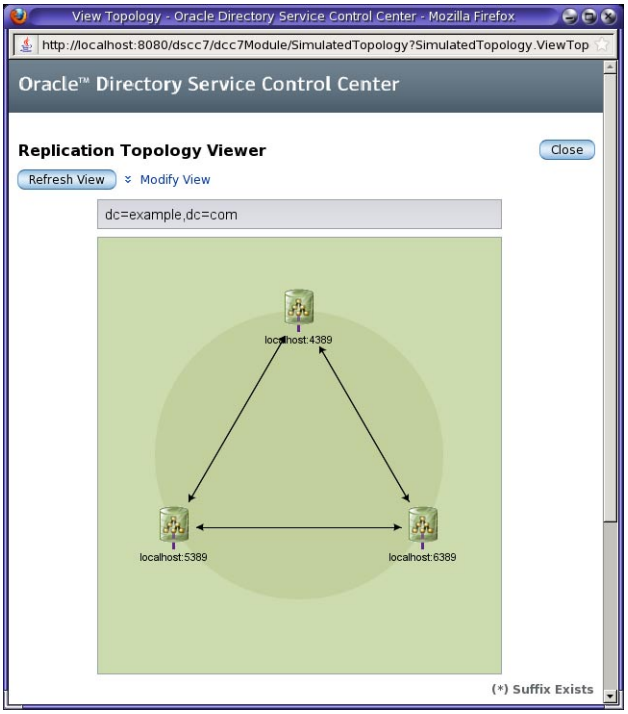
The primary interface for DSEE is the Directory Service Control Center (DSCC). The DSCC enables you to perform almost all administrative tasks.

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.

For information about starting and using the DSCC, see "Directory Service Control Center Interface" in *Oracle Directory Server Enterprise Edition 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 Server logs, 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.

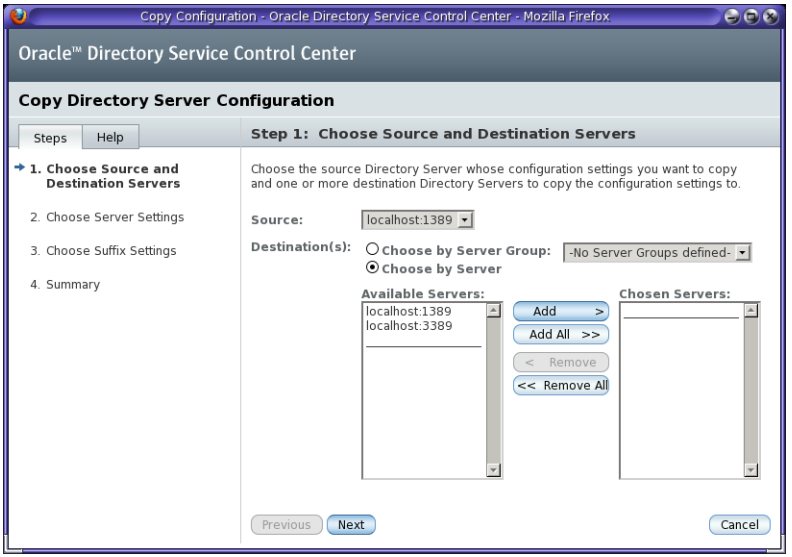
Configuration and Suffix Cloning

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.

Overview of the Commands

The DSEE includes the following 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/SUNWdsee7/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 and Migration

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.

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. You can also install the Directory Service Control Center as a non-root user using the WAR file.

Operating system-specific packaging formats, such as `SVR4` for Solaris, requires installation as a privileged user.

User-Specified Installation Path

Both the zip distribution and native packages 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 packaging 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 are consumed 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.

Automated Migration Tool (`dsmig`)

The `dsmig` tool migrates a single Directory Server instance. The `dsmig` tool allows you to migrate your schema, security information, and configuration information, including replication data, from Directory Server 5.2 and 5.2.x to 11*g* Release 1 (11.1.1.5.0).

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 running.

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).

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 *Oracle Directory Server Enterprise Edition Administration Guide*
Installing DSEE	Part I, "Installing and Uninstalling Directory Server Enterprise Edition," in *Oracle Directory Server Enterprise Edition Installation Guide*
Upgrading or Migrating Directory Server	*Oracle Directory Server Enterprise Edition Upgrade and Migration Guide*
Indexing	Chapter 12, "ODSEE Indexing," in *Oracle Directory Server Enterprise Edition Administration Guide*
Directory schema	Chapter 11, "ODSEE Schema," in *Oracle Directory Server Enterprise Edition Administration Guide*
Replication configuration	Chapter 10, "ODSEE Replication," in *Oracle Directory Server Enterprise Edition Administration Guide*
Static and dynamic groups	"Managing Groups" in *Oracle Directory Server Enterprise Edition Administration Guide*
Tuning the all IDs threshold property	`all-ids-threshold`(5dsconf) man page

◆ ◆ ◆ CHAPTER 3

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
- Replicated account lockout attributes
- Monitoring replication convergence

Unlimited Masters for Replication

In a multi-master 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 has no limits on the number of masters, allowing your multi-master 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 *Oracle Directory Server Enterprise Edition Administration Guide* for instructions on configuring prioritized replication using command-line tools.

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 *Oracle Directory Server Enterprise Edition Deployment Planning Guide* for an overview of the topic.

Monitoring Replication Convergence

Directory Server quickly calculates the number of pending replication changes. 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 *Oracle Directory Server Enterprise Edition 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.

You can use the `dsconf import`, `dsconf export`, `dsconf backup`, and `dsconf restore`commands in an asynchronous mode by setting the `-a` flag.

Compacting Database Files

Directory Server now allows you to compact the database files to reduce disk use and reduce backup time. You can compact an existing suffix using the `dsadm repack` command. The instance must be stopped before running this command.

For more information about compacting your database files using the `dsadm` command, see the `dsadm`(1M) man page.

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. Set the frozen mode using the `dsconf set-server-prop` command as follows:

```
dsconf set-server-prop read-write-mode:frozen
```

Once this property is set, you can safely take the file system snapshot.

See "Backing Up a File System" in *Oracle Directory Server Enterprise Edition 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 and the data directory paths that correspond to the `dsconf` command properties `db-env-path`, `db-log-path`, and `db-path` 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 values 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 data directory path settings with the server online, but before you restart the server to put the change into effect, you must perform the following procedure.

▼ To Change the Data Directory Path With the Server Online

Before You Begin The reference manual pages indicate that after you change the server `db-env-path`, `db-log-path`, or the suffix `db-path`, you must perform an export to LDIF, and then import from LDIF. Alternatively, you can move the data files. If, however, any of the steps in the following procedure do not complete successfully, or if the new configuration does not coincide exactly with the layout resulting from the steps of this procedure, you must reinitialize the server or restore from backup.

1. **Back up your server, or make sure that you can reinitialize the server from another instance.**
2. **Create the new file system directory with the same ownership and permissions as the old file system directory.**

   Make sure the new directory resides in a file system with enough free space to hold the data.
3. **Stop the server.**

   If the server is not stopped cleanly, you must reinitialize the server or restore from backup.
4. **Move, *do not copy*, the files from the old file system directory to the new file system directory.**

Parameter	`db-env-path`	`db-log-path`	`db-path`
Files to move	*instance-dir*`/db/_db.*` *instance-dir*`/db/DBVERSION`	*instance-dir*`/db/log.*`	*instance-dir*`/db/`*backend-dir*`/*`

5. **If the old directory is now empty, or contains only empty directories, delete the old directory.**
6. **Restart the server.**

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.

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 *Oracle Directory Server Enterprise Edition Deployment Planning Guide*
Backing up and restoring directory data	Chapter 8, "ODSEE Backup and Restore," in *Oracle Directory Server Enterprise Edition Administration Guide*
Using a global retro changelog	"Replication and the Retro Change Log Plug-In" in *Oracle Directory Server Enterprise Edition Reference*

Feature	Documentation
Using global account lockout	"Preventing Authentication by Using Global Account Lockout" in *Oracle Directory Server Enterprise Edition Deployment Planning Guide*
Making a file system snapshot when the database is in frozen mode	"Backing Up a File System" in *Oracle Directory Server Enterprise Edition Administration Guide*
Checking valid attribute syntax on update	"Checking Valid Attribute Syntax" in *Oracle Directory Server Enterprise Edition Administration Guide*

◆ ◆ ◆ CHAPTER 4

Tuned for Performance

This chapter describes the Directory Server features that help you tune your deployment for best performance. The Directory Server itself also includes improvements to the performance of almost all operations.

This chapter covers the following topics:

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.

You tune your cache size using the `dsconf` command. See the `dsconf`(1M) man page for more details.

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

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.

See the `server`(5dsconf) man page for details about the cache size properties that you can set.

Log Management Improvements

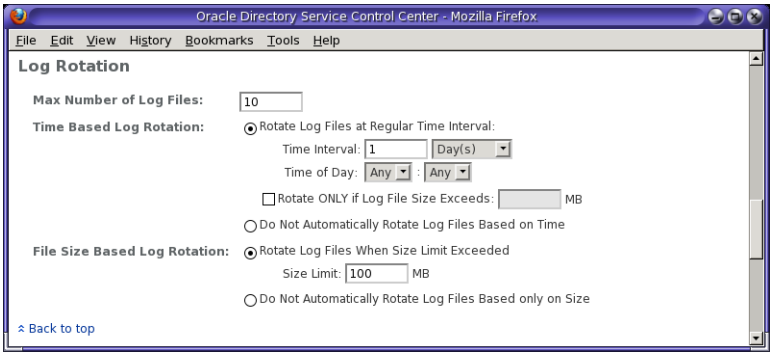
This version of Directory Server brings improvements to time-based log rotation, rotate on-demand functionality for access, error, and audit logs, and configurable permissions for log files. It also provides more flexible logging of users involved in proxy authorization.

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
```

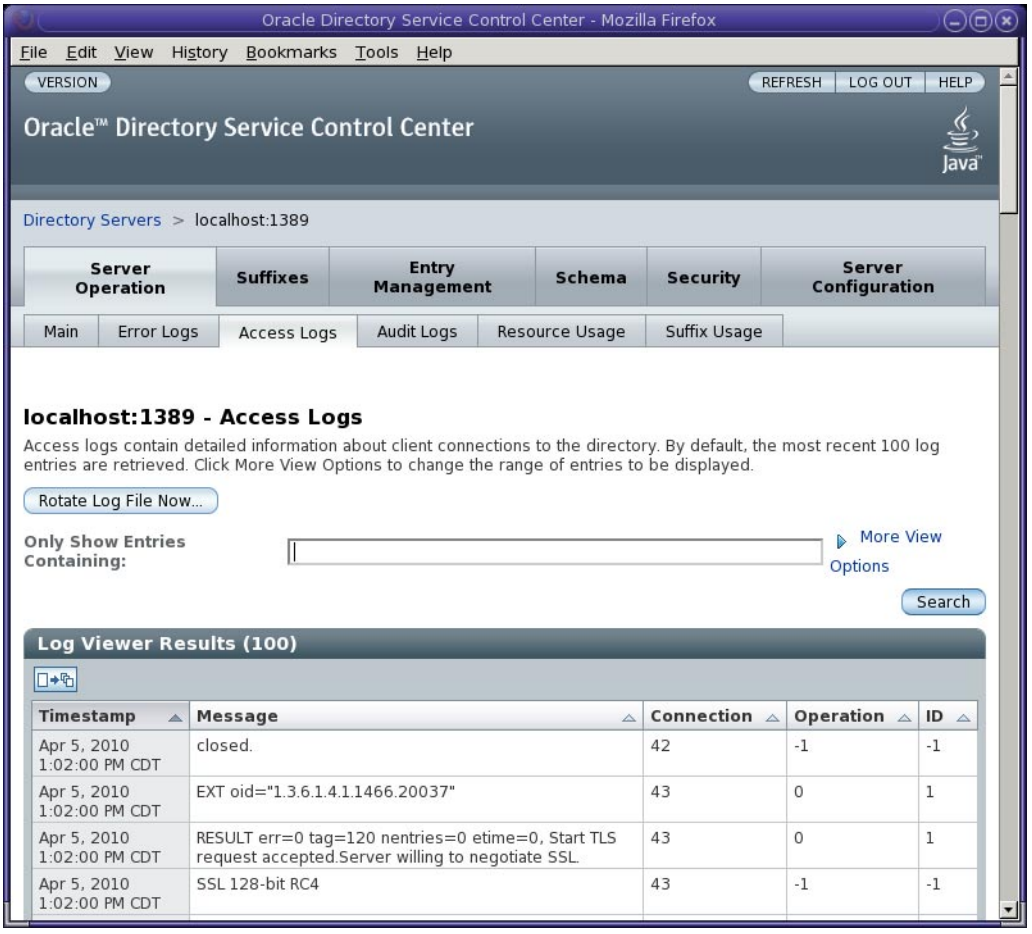
You can change the rotation interval for the access log through the command line as follows:

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

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.

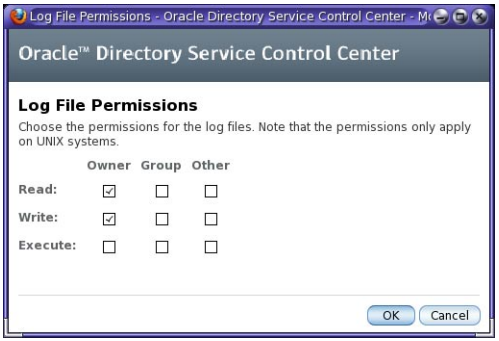
Configurable Log File Permissions Settings

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 *Oracle Directory Server Enterprise Edition Deployment Planning Guide*

Feature	Documentation
Introduction to caches and how Directory Server uses them	"Caches and How Directory Server Uses Them" in *Oracle Directory Server Enterprise Edition Reference*
Tuning cache settings for better performance	"Tuning Cache Settings" in *Oracle Directory Server Enterprise Edition Deployment Planning Guide*
Introduction to Directory Server logging	Chapter 10, "Directory Server Logging," in *Oracle Directory Server Enterprise Edition Reference*
Managing Directory Server logs	Chapter 14, "ODSEE Logging," in *Oracle Directory Server Enterprise Edition Administration Guide*

◆ ◆ ◆ CHAPTER 5

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

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 *Oracle Directory Server Enterprise Edition Administration Guide* for background on ACI bind rules.

Directory Server Enterprise Edition Password Policy

Directory Server Enterprise Edition password policy provides the following 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 password policy provides two 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 5.2 or 5.2.x password policy attributes.

See "Password Policy" in *Oracle Directory Server Enterprise Edition Upgrade and Migration Guide* for details on migrating to the new password policy.

Forced Password Change After Reset

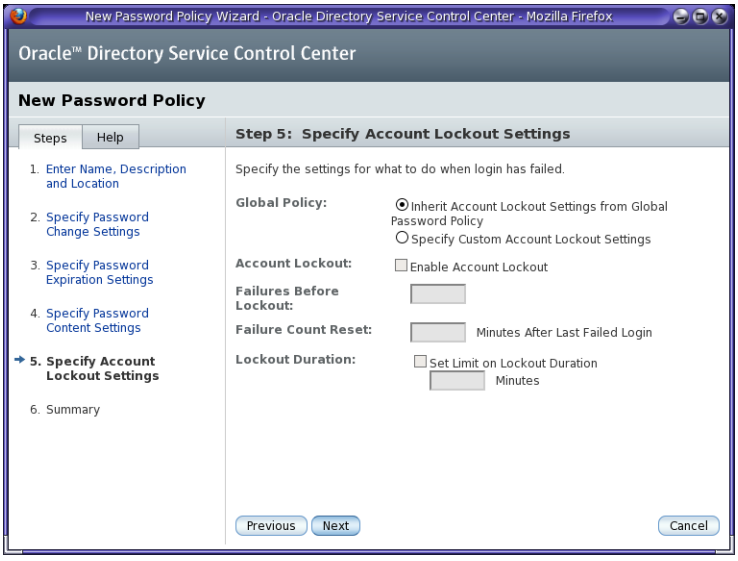
This feature of Directory Server enables administrators to force *regular* system users to change their passwords after a password reset.

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.

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 *Oracle Directory Server Enterprise Edition 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.

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, "ODSEE Password Policy," in *Oracle Directory Server Enterprise Edition Administration Guide*
Enabling global account lockout	"Preventing Authentication by Using Global Account Lockout" in *Oracle Directory Server Enterprise Edition Deployment Planning Guide*
Overview of the Directory Server Enterprise Edition password policy architecture	"Password Policy" in *Oracle Directory Server Enterprise Edition Upgrade and Migration Guide*

Feature	Documentation
Migrating to the new password policy	"Password Policy Configuration Attributes" in *Oracle Directory Server Enterprise Edition Upgrade and Migration Guide*
Configuring connection-based access control with ACIs	"ACI Bind Rules" in *Oracle Directory Server Enterprise Edition Administration Guide*

◆ ◆ ◆ CHAPTER 6

Managed Scalability

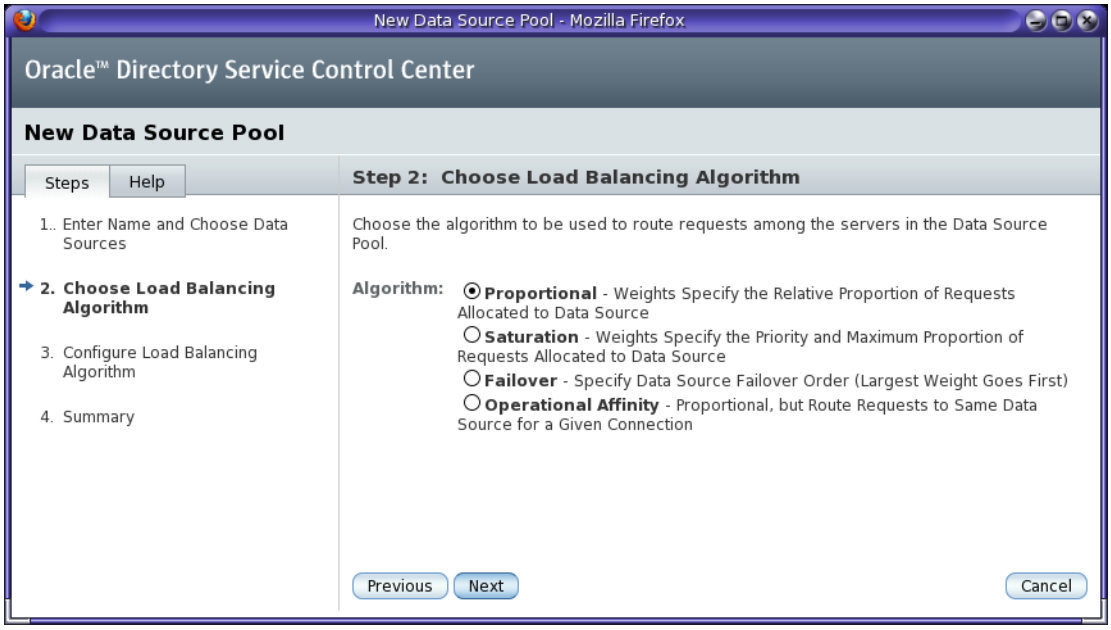
This chapter describes the features of DSEE that give it the ability to support hundreds of millions and even billions of entry deployments. DSEE allows a flat namespace, such as `ou=people`, to be split up across multiple sets of servers configured for multi-master replication. This chapter covers the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

Load Balancing and Operation-Based Routing

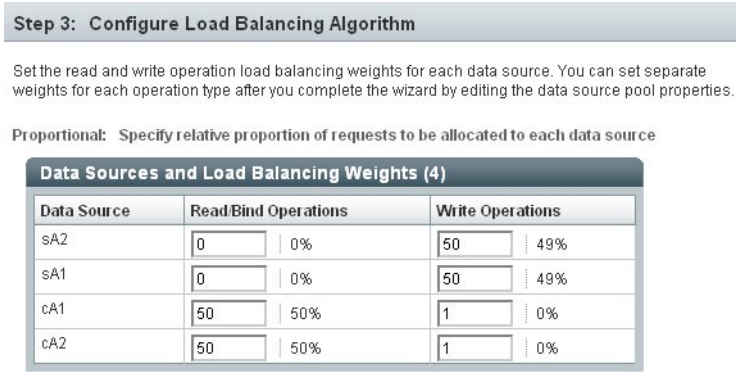
Directory Proxy Server now makes it possible both to route different LDAP operations on the same client connection to different servers and to enable successive requests on the same client connection to be sent to the same LDAP server. In addition, Directory Proxy Server offers a wider range of load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

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

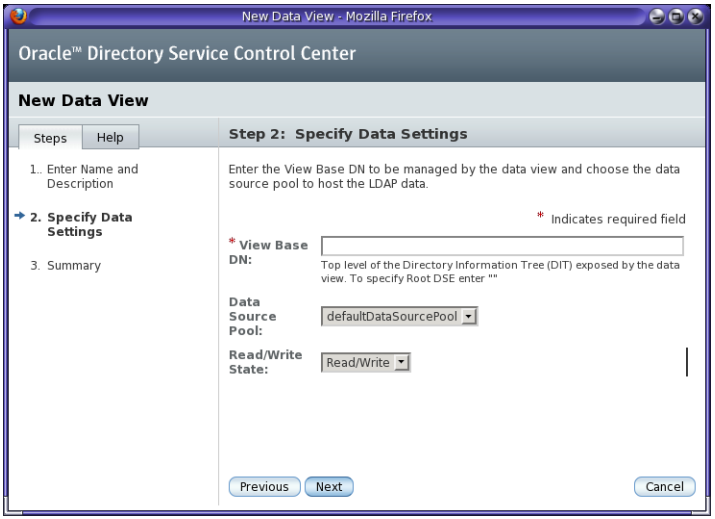
You can select your load balancing algorithms using the DSCC New Data Source Pool wizard, as illustrated in the following figure.



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.



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.



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.

See "Creating and Configuring Data Views for Example Use Cases" in *Oracle Directory Server Enterprise Edition 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 *Oracle Directory Server Enterprise Edition 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 *Oracle Directory Server Enterprise Edition Deployment Planning Guide*
Administering Directory Proxy Server	Part II, "Directory Proxy Server Administration," in *Oracle Directory Server Enterprise Edition Administration Guide*
Designing a global deployment	Chapter 11, "Designing a Global Deployment," in *Oracle Directory Server Enterprise Edition Deployment Planning Guide*
Overview of the Directory Proxy Server architecture	Part II, "Directory Proxy Server Reference," in *Oracle Directory Server Enterprise Edition Reference*
About Directory Proxy Server load balancing and client affinity	Chapter 16, "Directory Proxy Server Load Balancing and Client Affinity," in *Oracle Directory Server Enterprise Edition Reference*
Configuring load balancing	Chapter 20, "Directory Proxy Server Load Balancing and Client Affinity," in *Oracle Directory Server Enterprise Edition Administration Guide*

◆ ◆ ◆ CHAPTER 7

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 *Oracle Directory Server Enterprise Edition 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. For information about accessing data repositories that are compliant with the JDBC technology, see "JDBC Data Views" in *Oracle Directory Server Enterprise Edition 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 *Oracle Directory Server Enterprise Edition Reference*.

Access to LDAP Resources

Directory Proxy Server can access any LDAP v3 compliant LDAP directory server.

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. Directory Proxy Server supports JDBC for Java DB 10.2 , Oracle 9i and 10g, DB2 v9.1, and MySQL 5.0. 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.

Directory Proxy Server also allows you to use the same data view in multiple joins. For example, you can create a new join that combines a new data view with an existing data view. Directory Proxy Server allows you to configure this multiple data join without any restrictions.

For more information about aggregating data from different data sources, see "Join Data Views" in *Oracle Directory Server Enterprise Edition 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 *Oracle Directory Server Enterprise Edition 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 *Oracle Directory Server Enterprise Edition Deployment Planning Guide*
Creating virtual data views	Chapter 22, "Directory Proxy Server Virtualization," in *Oracle Directory Server Enterprise Edition Administration Guide*
Overview of JDBC virtual views	"JDBC Data Views" in *Oracle Directory Server Enterprise Edition Reference*
Overview of LDIF virtual views	"LDIF Data Views" in *Oracle Directory Server Enterprise Edition Reference*
Overview of join data views	"Join Data Views" in *Oracle Directory Server Enterprise Edition Reference*
Overview of transforming virtual data	"Virtual Data Transformations" in *Oracle Directory Server Enterprise Edition Reference*

◆ ◆ ◆ CHAPTER 8

Synchronizing Directory Server With Windows Users and Groups

Identity Synchronization for Windows provides 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

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 about group synchronization, see "Configure Identity Synchronization for Windows to Detect and Synchronize Groups Related Changes between Directory Server and Active Directory" in *Oracle Identity Synchronization for Windows 6.0 Installation and Configuration Guide*.

Failover Support for Multi-master 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	*Oracle 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 *Oracle Identity Synchronization for Windows 6.0 Installation and Configuration Guide*
Sample XML configuration documents	Appendix B, "Identity Synchronization for Windows LinkUsers XML Document Sample," in *Oracle Identity Synchronization for Windows 6.0 Installation and Configuration Guide*

Feature	Documentation
Configuring multiple Windows domains and using Synchronization User Lists (SULs)	Appendix D, "Defining and Configuring Synchronization User Lists for Identity Synchronization for Windows," in *Oracle Identity Synchronization for Windows 6.0 Installation and Configuration Guide*
Synchronizing users in a single replicated suffix	Appendix E, "Identity Synchronization for Windows Installation Notes for Replicated Environments," in *Oracle Identity Synchronization for Windows 6.0 Installation and Configuration Guide*
Group synchronization	"Configure Identity Synchronization for Windows to Detect and Synchronize Groups Related Changes between Directory Server and Active Directory" in *Oracle Identity Synchronization for Windows 6.0 Installation and Configuration Guide*

◆ ◆ ◆ APPENDIX 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 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/rfc4532.txt)
Lightweight Directory Access Protocol (LDAP) "Who am I?" Operation