Sun Directory Server Enterprise Edition 7.0 Release Notes

Part No: 820–4805
November 2009

ORACLE

100609@24378

Contents

Preface

These release notes contain important information available at the time of release. New features and enhancements, known limitations and problems, technical notes, and other information are addressed here. Read this document before you begin using Directory Server Enterprise Edition.

How This Book Is Organized

This book includes the following chapters.

Chapter 2, "Compatibility Issues," addresses compatibility with previous component product versions, and with potential upcoming changes to Directory Server Enterprise Edition software.

Chapter 3, "Installation Notes," covers topics related to installation, including hardware and software requirements.

Chapter 4, "Directory Server Bugs Fixed and Known Problems," covers fixes and issues for Directory Server.

Chapter 5, "Directory Proxy Server Bugs Fixed and Known Problems," covers fixes and issues for Directory Proxy Server.

Chapter 6, "Identity Synchronization for Windows Bugs Fixed and Known Problems," covers fixes and issues for Identity Synchronization for Windows.

Chapter 7, "Directory Server Resource Kit Bugs Fixed and Known Problems," introduces Directory Server Resource Kit. This chapter also covers fixes and issues for Directory Server Resource Kit.

Sun Directory Server Enterprise Edition Documentation Set

This documentation set explains how to use Sun 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/1819.1`.

The following table lists all the available documents.

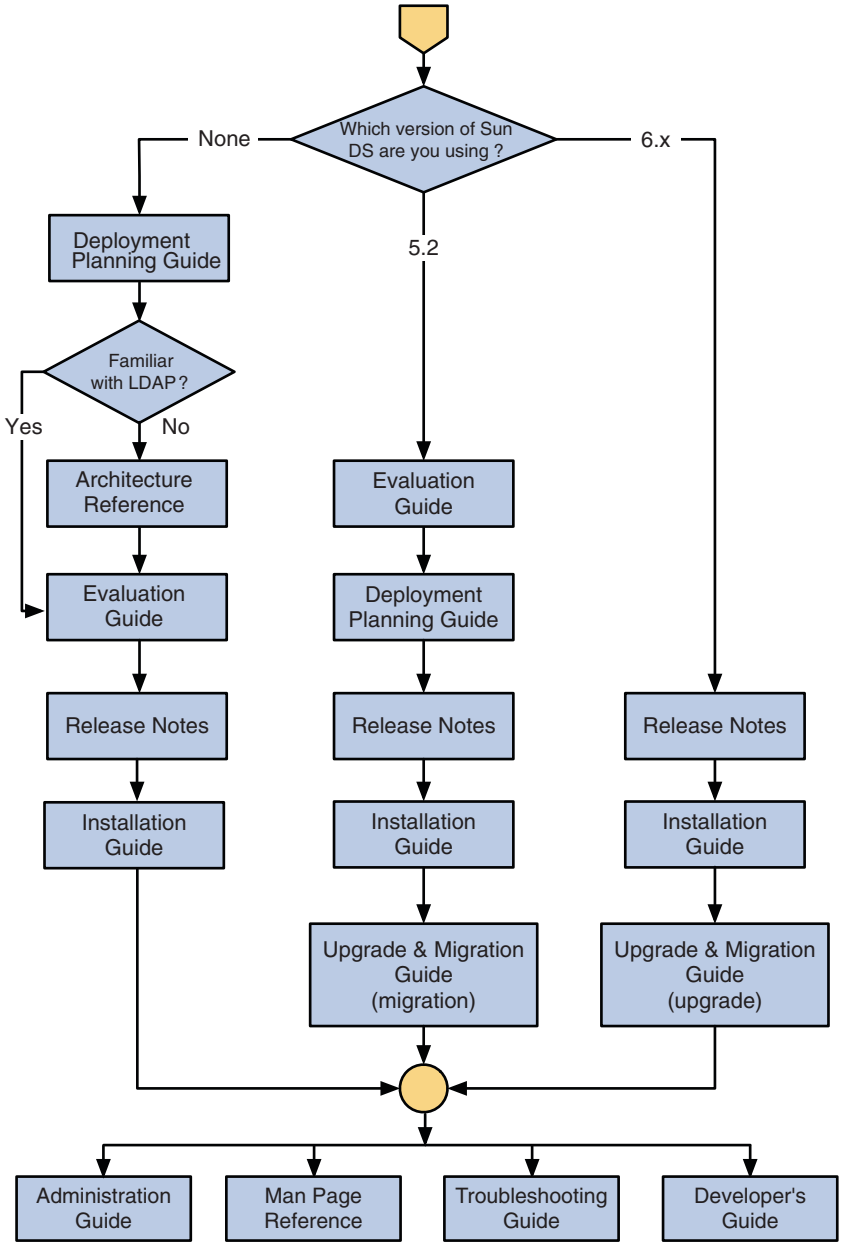
TABLE P–1 Directory Server Enterprise Edition Documentation

Document Title	Contents
Sun Directory Server Enterprise Edition 7.0 Release Notes	Contains the latest information about Directory Server Enterprise Edition, including known problems.
Sun Directory Server Enterprise Edition 7.0 Documentation Center	Contains links to key areas of the documentation set that help you to quickly locate the key information.
Sun Directory Server Enterprise Edition 7.0 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.
Sun Directory Server Enterprise Edition 7.0 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.
Sun Directory Server Enterprise Edition 7.0 Installation Guide	Explains how to install the Directory Server Enterprise Edition software. Shows how to configure the installed software and verify the configured software.
Sun Directory Server Enterprise Edition 7.0 Upgrade and Migration Guide	Provides upgrade instructions to upgrade the version 6 installation and migration instructions to migrate version 5.2 installations.
Sun Directory Server Enterprise Edition 7.0 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.
Sun Directory Server Enterprise Edition 7.0 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.
Sun Directory Server Enterprise Edition 7.0 Reference	Introduces technical and conceptual foundations of Directory Server Enterprise Edition. Describes its components, architecture, processes, and features.
Sun Directory Server Enterprise Edition 7.0 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.

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

Document Title	Contents
Sun Directory Server Enterprise Edition 7.0 Troubleshooting Guide	Provides information for defining the scope of the problem, gathering data, and troubleshooting the problem areas by using various tools.
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.
Sun Java System Identity Synchronization for Windows 6.0 Installation and Configuration Guide	Describes how to install and configure Identity Synchronization for Windows.
Additional Installation Instructions for Sun Java System Identity Synchronization for Windows 6.0	Provides additional installation instructions in context of Directory Server Enterprise Edition 7.0.

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



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://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 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.

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 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 *Sun Directory Server Enterprise Edition 7.0 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)	`/opt/SUNWdsee/dsee6/bin`	*install-path*`/dsrk/bin`
`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 the C shell, Bourne shell, and Korn shell.

TABLE P–5 Shell Prompts

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

Shell Prompts in Command Examples

The following table shows default system prompts and superuser prompts.

TABLE P–6 Shell Prompts

Shell	Prompt
C shell on UNIX and Linux systems	`machine_name%`
C shell superuser on UNIX and Linux systems	`machine_name#`
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–7 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

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/`)

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 Feedback.

◆ ◆ ◆ CHAPTER 1

New Features in Directory Server Enterprise Edition 7.0

These release notes provide current information on the date they are published. However, if the English version of the release notes has a more recent publication date, it might be updated with more current information that is not provided in other versions. Consult the English version of the release notes for the most current information.

This section contains the following information:

What's New in Directory Server Enterprise Edition 7.0

New Features in Directory Server

New DB Entry Format

To reduce the database entry size, the existing database entry format is changed. The internal representation of an entry changed from an ASCII LDIF format to a tagged binary format. The data stored in the database does not have the characteristic starting of `dn:` anymore, the first byte of an entry being a value bigger than `0xE0` (hence all values `0xE0` to `0xFF` are to be considered reserved for internal use).

For compatibility reasons entries can be a mix of LDIF and binary representations, but any modification will write the entry in binary format.

Suffix entries data can be compressed when written to disk to minimize their disk footprint. Compression is enabled according to the settings of the `compression-mode` and `compression-entries` properties,

For additional information, refer to the Chapter 8, "Writing Entry Store and Entry Fetch Plug-Ins," in *Sun Directory Server Enterprise Edition 7.0 Developer's Guide*.

Copyless Restore

To save disk space, you can restore a server by moving files in place of copying them. You can perform the copyless restore by setting a flag with the `restore` command.

For more information, see "Binary Restore" in *Sun Directory Server Enterprise Edition 7.0 Administration Guide*

IPv6 Support on Windows

Instances installed on Windows systems now support Internet Protocol version 6.

Likewise, server instances on other operating systems also support IPv6.

New Command for Account Management

The `dsutil` command now performs the functions formerly provided by the `ns-activate`, `ns-inactivate`, and `ns-accountstatus` commands.

New Backup Feature

Backup operations perform a database verify on archived data when the `--flags verify-db` option is specified.

Index Filter Analyzer

The index filter analyzer identifies index lists where the number of entries exceeds the maximum number of indexable entries (the `ALLID` threshold) and monitors user searches using such index lists. The index filter analyzer is enabled using the `dsconf enable-index-filter-analyzer` command.

New Features in Directory Proxy Server

Entry Aggregation

Entry aggregation results in the following:

- Optimizes queries to secondary data view
- Searches for secondary data view first when required
- Handles large result sets (VLV control) better
- Requests Grouping to secondary source

JDBC Data View

JDBC data view now supports Date and Blob.

Optimized Monitoring and Logging

Directory Proxy Server now uses a new logging engine implementation that performs more efficiently on multi-core systems.

Connection Handlers

- New criteria based on LDAP groups
- Management of the maximum throughput

Coordinator Data View

New type of data view to address more use cases, for example, company mergers.

For more information, see "Creating and Configuring Coordinator Data Views" in *Sun Directory Server Enterprise Edition 7.0 Administration Guide*.

Distribution Algorithm

An enhanced regex distribution algorithm is added, as described in "Configuring Pattern Matching Distribution Algorithm" in *Sun Directory Server Enterprise Edition 7.0 Administration Guide*.

Join Data View Searches

To optimize the performance of searches of a join data view, Directory Proxy Server makes use of Virtual List View (vlv) indexes. It helps you to avoid the scenario where search hits the size limits due to the lots of entries from one data source and very few from the others. To use VLV indexes, see "Browsing Index" in *Sun Directory Server Enterprise Edition 7.0 Reference*.

Behavioral Changes in Directory Server Enterprise Edition 7.0

This section includes all the behavioral changes that are made in this release.

Change in Product Layout

The Directory Server Enterprise Edition product layout is changed as mentioned below:

- All commands are available in *install-path*`/dsee7/bin`.
- The plug-ins are available in *install-path*`/dsee7/lib`.

For a complete list of file locations, see "Software Layout for Directory Server Enterprise Edition" in *Sun Directory Server Enterprise Edition 7.0 Reference*.

Replica Update Vector in LDIF

Starting with Directory Server Enterprise Edition 7.0, the export process (`dsadm export`) always puts the Replica Update Vector (RUV) as last entry in the exported LDIF file.

Load Libraries for Sun Microsystems Plug-In From the Installation Directory

Directory Server Enterprise Edition loads the libraries for Sun Microsystems plug-ins from the path where the software is installed. The libraries are no more loaded from the path mentioned in the LDIF.

Optimized Import

Global Import Process

A new threading model improves import performance on multi-core machines.

Parallel Merging

If an import is multi-pass, merging of the indexes happens in parallel if there is enough memory for holding the index and its temporary files. The parallel merging of indexes results in improved performance.

Compliance with RFC 4522

When a search operation returns attributes whose syntax requires binary transfer, it appends the `;binary` qualifier to the attribute name. To disable compliance with RFC 4522, set the `compat-flag` property to `no-rfc4522`.

New Administrative Commands and Functionality

This sections describes changes in the behavior of administrative commands.

- The `dsadm` and `dpadm` commands provide the new `list-running-instances` and `stop-running-instances` options for listing and stopping locally running servers.
- The `dsadm` and `dpadm` commands provide new options for managing certificates, `--validity` and `--keysize`, described in `dsadm`(1M) and `dpadm`(1M).
- The `dsadm` command also provides additional options for managing certificates, `--sigalg`, `--phone`, `--email`, and `--dns` described in `dsadm`(1M) .

- The `dpadm set-flags` command supports two new flags, `jvm-path` and `server-umask`, described in `dpadm(1M)`.
- Several commands were available in previous versions of Directory Server Enterprise Edition but whose functions are now provided by other commands, as described in "Command Line Changes" in *Sun Directory Server Enterprise Edition 7.0 Upgrade and Migration Guide*
- Some commands were removed from Directory Server Enterprise Edition, as described in "Command Line Changes" in *Sun Directory Server Enterprise Edition 7.0 Upgrade and Migration Guide*.

Binary Backup

A binary backup modifies the backup files by running a database recovery, thus flushing backup transaction logs to the backup databases. To leave the backup as it is, use the `--flags no-recovery` option.

Faster Re-indexing

Re-indexing is performed more efficiently, reusing some recent import techniques and speed improvements.

Index State

The `dsconf info` command reports which attributes need to be re-indexed (for example, after a configuration change).

Enabled SSL Ciphers in Root DSE

The root DSE contains the list of supported ciphers as reported by the security library. In release 7.0, the root DSE also contains the ciphers that are available for SSL negotiation under the `enabledSSLCiphers` attribute, and it is by default a subset of all the supported ciphers.

◆ ◆ ◆ CHAPTER 2

Compatibility Issues

This chapter covers features that have been deprecated or removed from Directory Server Enterprise Edition component products. This chapter also covers features that are susceptible to removal, and functionality that is susceptible to deprecation for Directory Server Enterprise Edition component products.

This chapter includes the following sections:

Classifications of interface stability are provided per manual page entry in *Sun Directory Server Enterprise Edition 7.0 Man Page Reference*.

Platform Support

In Directory Server Enterprise Edition 7.0, support for the following platforms is removed:

- Windows 2000
- Red Hat Advanced Server 3.0
- J2SE platform 1.4
- SUSE 9
- Solaris 10 x86 32–bit
- Native package installation for Windows
- Native package installation for Red Hat
- Native package installation for HP-UX

Native package installation is supported only for the Solaris operating system.

If you have Directory Server Enterprise Edition installed on a platform that is no more supported in version 7.0, upgrade your operating system to the version mentioned in the table below:

Previous Operating System Version	Minimum Operating System Version Required to Install 7.0
Red Hat Enterprise Linux 3 x86	Red Hat Enterprise Linux 4 x86
Red Hat Enterprise Linux 3 x64	Red Hat Enterprise Linux 4 x64
SUSE Linux Enterprise Server 9 32–bit	SUSE Linux Enterprise Server 10 32-bit
SUSE Linux Enterprise Server 9 x64	SUSE Linux Enterprise Server 10 x64
Microsoft Windows 2000 Server	Microsoft Windows 2003 Server
Hewlett Packard HP-UX 11.11	Hewlett Packard HP-UX 11.23

See "Operating System Requirements" on page 33 for details of the supported operating systems.

System Virtualization Support

System virtualization is a technology that enables multiple operating system (OS) instances to execute independently on shared hardware. Functionally, software deployed to an OS hosted in a virtualized environment is generally unaware that the underlying platform has been virtualized. Sun performs testing of its Sun products on selected system virtualization and OS combinations to help validate that the Sun products continue to function on properly sized and configured virtualized environments as they do on non-virtualized systems. For information about Sun support for Sun products in virtualized environments, see System Virtualization Support in Sun Java System Products.

For this release, Sun Microsystems supports any OS running on the VMware technology provided that the OS is already supported natively for the Directory Server Enterprise Edition 7.0 software. Sun Microsystems does not certify every combination of OS and hardware, but relies on the underlying VMware technology implementation. Production deployment of the Directory Server Enterprise Edition 7.0 software on the VMware technology is not recommended.

For details on supported hardware platforms for this release of Directory Server Enterprise Edition, see "Hardware Requirements" on page 31.

For details on supported operating systems and OS versions for this release of Directory Server Enterprise Edition, see "Operating System Requirements" on page 33.

Directory Server Enterprise Edition 7.0 supports Logical Domains, (LDoms), on the SPARC platform for Solaris 10 Update 3 and later versions. For more information about LDoms, see the *Logical Domains (LDoms) 1.0.1 Administration Guide*.

Note – Installation of Identity Synchronization for Windows in a virtualized environment is not supported.

Software Support

Removed Software Components

The following Directory Server Enterprise Edition components are removed in this release:

- Directory Editor
- Agent for Sun Cluster support
- Sun Java Web Console (Lockhart)

Changes in the Directory Service Control Center

This section describes changes in the behavior of the Directory Service Control Center (DSCC)

- The DSCC is now supported on Sun Web Server 7, GlassFish 2.1, and BEA WebLogic platforms.
- The DSCC is now available in internationalized versions.
- The DSCC is no longer supported on Sun Java Web Console. (Only manual WAR-file deployment of the DSCC is supported on Sun Java Web Console).

Compatibility Notes

This section lists the features that have been removed or deprecated in this release and also mentions the features or commands that might be removed in the next release:

- In the password policy, the `DS5-compatible-mode` interoperability mode is deprecated. In this version, you must use the `DS6–mode` interoperability mode.
- Some version 5.2 commands are removed in Directory Server 7.0, as described in "Command Line Changes" in *Sun Directory Server Enterprise Edition 7.0 Upgrade and Migration Guide*
- The following legacy scripts have been replaced with the commands:

Legacy Script	New Command
`start-slapd`	`dsadm start`

`ldif2db`	`dsadm import`
`db2ldif`	`dsadm export`
`bak2db`	`dsadm restore`
`db2bak`	`dsadm archive`
`restart-slapd`	`dsadm restart`
`stop-slapd`	`dsadm stop`

For more information, see "Command Line Changes" in *Sun Directory Server Enterprise Edition 7.0 Upgrade and Migration Guide*.

- Before migrating a replicated server topology, review Chapter 5, "Migrating a Replicated Topology," in *Sun Directory Server Enterprise Edition 7.0 Upgrade and Migration Guide*.
- When you create a Directory Server instance, password policy is configured initially backwards-compatible. After upgrading, you should change the compatibility mode to enable richer password policy configuration. Directory Server manages the conversion. In a future release, the backwards-compatible password policy configuration might be removed.
- When you create a Directory Server instance, support for the modify DN operation is disabled. After upgrading all the server instances in your replication topology, the modify DN operation can be replicated properly. At that point, you can enable support for the modify DN operation on each server instances. Use the `dsconf set-server-prop moddn-enabled:on` command for this purpose.

  The modify DN operation is disabled during server instance creation to provide compatibility with version 5.2 instances.
- The `db-path` suffix property (`dsconf set-suffix-prop` *suffix-name* `db-path:`*/new/directory* and `dsconf create-suffix --db-path`) is deprecated and might be removed in a future release. Use the `db-path` server property to store all the suffixes in a different directory than the instance directory.
- Sun is currently working on resolving issues with the stability of the `dsadm repack` subcommand under stress. As a safety measure, Sun has temporarily disabled the `dsadm repack` subcommand for the 7.0 release.

  Therefore, if you try to run `dsadm repck`, it will display the following message:

  ```
  :[19/Oct/2009:11:51:50 +0200] - WARNING<99999> - conn=-1 op=-1 msgId=-1
  -  The repack function is temporarily disabled for the 7.0 release.
  ```

  Contact your support representative for more details.
- Chapter 2, "Changes to the Plug-In API Since Directory Server 5.2," in *Sun Directory Server Enterprise Edition 7.0 Developer's Guide* details plug-in API changes. Interfaces identified there as deprecated might be removed in a future release.

- Directory Server Enterprise Edition 7.0 does not provide any changes to Identity Synchronization for Windows.

  The current version for Identity Synchronization for Windows product is 6.0.

  Before upgrading Identity Synchronization for Windows, read Chapter 8, "Migrating Identity Synchronization for Windows," in *Sun Directory Server Enterprise Edition 7.0 Upgrade and Migration Guide*.
- Directory Server Enterprise Edition 7.0 does not provide any changes to Directory Server Resource Kit.
- The LDAP utility manual pages on Sun Solaris systems do not document the version of the LDAP utilities `ldapsearch`, `ldapmodify`, `ldapdelete`, and `ldapadd` delivered with Directory Server Enterprise Edition. The commands might no longer be delivered separately on Solaris systems, but instead integrated with the commands provided by the operating system in a future version. See *Sun Directory Server Enterprise Edition 7.0 Man Page Reference* for the manual pages for the LDAP client tools.

◆ ◆ ◆ CHAPTER 3

Installation Notes

This chapter tells you where to download Directory Server Enterprise Edition software, and lists primary installation requirements.

This chapter includes the following sections:

Refer to the Sun Directory Services blog (`http://blogs.sun.com/directoryservices/`) for the most current information about the Directory product line.

Support Services and Licenses

Before you start with the product installation, make sure you read the support and licensing information thoroughly.

Support Services

Sun Software Service Standard, Premium and Premium Plus plan offerings are available for Sun Directory Server Enterprise Edition and can be purchased either through a Sun sales representative, an authorized Sun reseller, or online at `http://www.sun.com/sales/index.jsp`. These service plans include telephone and online technical support, on-demand software updates, online system administration resources, support notification services and one-stop interoperability assistance (Premium and Premium Plus plans only). In addition, the Premium Plus plan features a customer advocate and a customer-focused support team.

For complete feature set information, visit: http://www.sun.com/service/serviceplans/software/overview.xml

You may access the service lists describing all Sun service program offerings at: http://www.sun.com/servicelist

Licenses for Directory Server Enterprise Edition Managed Entries

Licenses are provided based on the number of entries you plan to manage using Directory Server Enterprise Edition. After a license is provided, you can replicate the entries as many times as required to get maximum flexibility out of your directory implementation. The only condition is that you do not change any of the replicated entries and store all of the replicated entries on the same operating system. If the replicated entries are stored on any other operating system, you must purchase a license for those entries.

Solaris licences up to version Solaris 10 update 5, provided 200,000 free entries for Directory Server. In this case, the licences covered only the core directory server component, not the other Directory Server Enterprise Edition components. You can still purchase an upgrade from core directory server component to full Directory Server Enterprise Edition. To get support for those 200,000 Directory Server entries, a Software Service Plan for Directory Server must be purchased. The Solaris Service Plan does not cover those entries.

You can review the latest license for a given version of a product before downloading it from http://www.sun.com/software/products/directory_srvr_ee/get.jsp.

Getting the Software

You can download Sun Directory Server Enterprise Edition 7.0 software from the following location.

http://www.sun.com/software/products/directory_srvr_ee/get.jsp

The download page serves as a starting point to direct you to the proper downloads depending on the distribution type you need to download. Directory Server Enterprise Edition 7.0 is available in the following distributions.

- Native package distribution (for Solaris only)
- Zip distribution (for all platforms)

Note – Before you install Sun Java System Identity Synchronization for Windows version 6.0, you *must* read the Technical Note. This Technical Note provides additional installation instructions to install Identity Synchronization for Windows for Directory Server Enterprise Edition 7.0.

Sun Java System Identity Synchronization for Windows version 6.0 is not bundled with the Sun Directory Server Enterprise Edition 7.0 distribution. You can download the Identity Synchronization for Windows software from `http://www.sun.com/software/products/directory_srvr_ee/get.jsp`.

Hardware Requirements

This section covers hardware requirements for Directory Server Enterprise Edition software.

Directory Server Enterprise Edition Hardware Requirements

Directory Server Enterprise Edition software requires the following hardware.

Component	Platform Requirement
RAM	1-2 GB for evaluation purposes Minimum 4 GB for production servers
Local disk space	400 MB disk space for binaries. By default, binaries installed from native packages are placed in `/opt` on UNIX systems. For evaluation purposes, an additional 2 GB local disk space for server software might be sufficient. If you are using Directory Server, consider that entries stored in Directory Server use local disk space. Directory Server does not support logs and databases installed on NFS-mounted file systems. Sufficient space should be provided for the database on a local file system in, for example, `/var/opt` or `/local`. For a typical production deployment with a maximum of 250,000 entries and no binary attributes such as photos, 4 GB might be sufficient. Directory Server may use more than 1.2 GB of disk space for its log files. This should be taken into account that 4 GB storage space is only for the databases, not the logs. Directory Server supports SAN disk storage. Before using SAN disk, you need to understand the layout and the design of the disk because the write performance of the system is affected if many applications simultaneously access data from the same disk. Directory Proxy Server does not support installation on NFS-mounted file systems. Sufficient space should be provided for the instance, and for all files used by the instance on a local file system in, for example, `/var/opt` or `/local`. Directory Proxy Server can use more than 1.2 GB of disk space for its log files.

Identity Synchronization for Windows Hardware Requirements

Identity Synchronization for Windows software requires the following hardware.

Component	Platform Requirement
RAM	512 MB for evaluation purposes wherever components are installed. More memory is preferred.
Local disk space	400 MB disk space for minimal installation alongside Directory Server.

Operating System Requirements

This section covers operating systems, patches and service packs required to support Directory Server Enterprise Edition component products.

Directory Server Enterprise Edition Operating System Requirements

The Directory Server Enterprise Edition software is validated with full installations of the operating systems listed here, not with reduced "base", "End User", or "core" installations. Certain operating systems require additional service packs or patches as shown in the following table.

Supported OS Versions for Directory Server Enterprise Edition	Distribution Type Supported	Additional Required Software and Comments
Solaris 10 U5 Operating System for SPARC 64-bit and x64	Native packages and zip distribution	The recommended patch clusters available at these sites: ■ For SPARC, the recommended patch cluster available at `http://sunsolve.sun.com/pdownload.do?target=10_Recommended.zip` ■ For x64, the recommended patch cluster available at `http://sunsolve.sun.com/pdownload.do?target=10_x86_Recommended.zip`
Solaris 9 Operating System for SPARC 64-bit and x86	Native packages and zip distribution	The recommended patch clusters available at these sites: ■ For SPARC, the recommended patch cluster available at `http://sunsolve.sun.com/pdownload.do?target=9_Recommended.zip` ■ For x86, the recommended patch cluster available at `http://sunsolve.sun.com/pdownload.do?target=9_x86_Recommended.zip`

Supported OS Versions for Directory Server Enterprise Edition	Distribution Type Supported	Additional Required Software and Comments
Solaris 10 U5 Trusted extension Operating System for SPARC 64-bit and x64	Native packages and zip distribution	The recommended patch clusters available at these sites: ■ For SPARC, the recommended patch cluster available at `http://sunsolve.sun.com/pdownload.do?target=10_Recommended.zip` ■ For x64, the recommended patch cluster available at `http://sunsolve.sun.com/pdownload.do?target=10_x86_Recommended.zip`
OpenSolaris 2009.06 Operating System for SPARC 64–bit and x64	Zip distribution	No additional patches required.
Red Hat Enterprise Linux 5 U3 Operating System for x64	Zip distribution	No additional patches required.
Red Hat Enterprise Linux 4 Enterprise Server and Advanced Server U8 Operating System for x64 and x86	Zip distribution	No additional patches required.
SuSE Linux Enterprise Server 10 U2 Operating System for x32	Zip distribution	No additional patches required.
SuSE Linux Enterprise Server 10 U2 Operating System for x64	Zip distribution	No additional patches required.
HP-UX 11iv2 PA-RISC 64–bit	Zip distribution	No additional patches required.
Microsoft Windows Server 2003 Standard Edition for x86 and x64	Zip distribution	Service Pack 2
Microsoft Windows Server 2003 Enterprise Edition for x86 and x64	Zip distribution	Service Pack 2
Microsoft Windows Server 2008 Standard Edition for x86 and x64	Zip distribution	Service Pack 1
Microsoft Windows Server 2008 Enterprise Edition for x86 and x64	Zip distribution	Service Pack 1

- For all supported versions of Microsoft Windows, Directory Server and Directory Proxy Server run only in 32-bit mode, and the filesystem type must be NTFS.
- Directory Server Enterprise Edition 7.0 32-bit is not supported on 64-bit platforms except Microsoft Windows.
- If a new service pack or update for a supported platform is released, Directory Server Enterprise Edition 7.0 supports that.

Note that installations on SUSE Linux Enterprise Server require you to reset several Java environment variables. See *Sun Directory Server Enterprise Edition 7.0 Installation Guide* for more details.

Directory Server Enterprise Edition delivers Java 1.6 and supports both Java 1.5 and 1.6.

Identity Synchronization for Windows Operating System Requirements

Identity Synchronization for Windows components run on the operating system versions listed here. Certain operating systems require additional service packs or patches as shown in the following tables.

Supported OS Versions for Identity Synchronization for Windows	Additional Required Software and Comments
Solaris 10 Operating System for SPARC, x86, and AMD x64 architectures	Patches: ■ For SPARC, the recommended patch cluster available at `http://sunsolve.sun.com/pdownload.do?target=10_Recommended.zip` ■ For x64, the recommended patch cluster available at `http://sunsolve.sun.com/pdownload.do?target=10_x86_Recommended.zip`
Solaris 9 Operating System for SPARC and x86 architectures	Patches: ■ For SPARC, the recommended patch cluster available at `http://sunsolve.sun.com/pdownload.do?target=9_Recommended.zip` ■ For x86, the recommended patch cluster available at `http://sunsolve.sun.com/pdownload.do?target=9_x86_Recommended.zip`

Supported OS Versions for Identity Synchronization for Windows	Additional Required Software and Comments

Red Hat Enterprise Linux Advanced Server 4.0 Update 2 for x86 and AMD x64	The following compatibility libraries are recommended:
	`compat-gcc-32-3.2.3-47.3.i386.rpm`
	`compat-gcc-32-c++-3.2.3-47.3.i386.rpm`
	The following compatibility library is required:
	`compat-libstdc++-33-3.2.3-47.3.rpm`
	Even when running Red Hat on a 64-bit system, 32-bit system libraries are installed.
	These compatibility libraries are available from Red Hat media or `https://www.redhat.com/rhn/rhndetails/update/`.

Microsoft Windows 2003 Server Standard Edition	Service Pack 1
Microsoft Windows 2003 Server Enterprise Edition	Service Pack 1

Note – Identity Synchronization for Windows is not supported on SUSE or HP-UX systems.

Software Dependency Requirements

Directory Server Enterprise Edition Software Dependency Requirements

The key software dependency requirements are as following:

- Directory Server relies on the Network Security Services, NSS, layer for cryptographic algorithms. NSS has been validated to work with the Sun cryptographic framework provided on Solaris 10 systems, which supports cryptographic acceleration devices.
- On Microsoft Windows systems, you must disable the pop-up blocker to make Directory Service Control Center work properly.
- Directory Proxy Server will work with any LDAPv3 compliant directory servers, but it is tested only with Sun Directory Server.
- On Solaris 10, `rc.scripts` are deprecated so commands like `dsadm autostart` are not supported. Instead use Solaris 10 Service Management Facility (SMF) to handle these types of requests. For example, `dsadm enable-service`. For more information on SMF, see the Solaris operating system documentation.

Supported Application Servers for Directory Service Control Center

The Directory Service Control Center supports the following application servers:

- Sun Java System Application Server 9.1
- GlassFish 2.1
- Tomcat 5.5 and 6.0
- Sun Java System Web Server 7.0
- BEA WebLogic Server 10.0

For more information, see Appendix A, "Deploying DSCC WAR File With Supported Application Servers," in *Sun Directory Server Enterprise Edition 7.0 Installation Guide*.

Supported JDBC Data Sources

For virtualization, Directory Proxy Server has been validated with the following JDBC data sources, using the drivers mentioned below. Though Directory Proxy Server works with all the JDBC 3 compliant drivers.

JDBC Data Source	JDBC Driver
DB2 v9	IBM DB2 JDBC Universal Driver Architecture 2.10.27
Microsoft SQL Server 2005	sqljdbc.jar 1.2.2323.101
MySQL 5.x	MySQL-AB JDBC Driver mysql-connector-java-5.0.4
Oracle 10g Database	Oracle JDBC driver 10.2.0.2.0 (See "Directory Proxy Server 7.0 Limitations" on page 68 for more information.)
JavaDB 10.5.3.0	Apache Derby Network Client JDBC Driver 10.5.3.0

Supported Browsers for Directory Service Control Center

The following table displays the browsers for each operating system that supports Directory Service Control Center.

Operating System	Supported Browser
Solaris 10 and Solaris 9 (SPARC and x86)	Firefox 2 and 3
Red Hat Linux and SUSE Linux	Firefox 2 and 3
Windows 2003/2008	Microsoft Internet Explorer 6 and 7, and Firefox 2 and 3

Identity Synchronization for Windows and Directory Server Plug-in Requirements in a Firewall Environment

Each Directory Server plug-in must be able to reach the Directory Server connector's server port, which was chosen when the connector was installed. Plug-ins that run in Directory Server Master replicas must be able to connect to Active Directory's LDAP, port 389, or LDAPS, port 636. The plug-ins that run in other Directory Server replicas must be able to reach the master Directory Server LDAP and LDAPS ports.

Identity Synchronization for Windows Software Dependency Requirements

Before you can install Identity Synchronization for Windows, you must install the prerequisite Sun Java System software components, including JRE and Message Queue.

- No JRE is provided with Identity Synchronization for Windows.

  Identity Synchronization for Windows installer requires J2SE or JRE 1.5.0_09.

- The Identity Synchronization for Windows bundle for this release includes Message Queue 3.6 with a license restricted in the context of Directory Server Enterprise Edition.

  When installing Identity Synchronization for Windows, you must specify the path to the version of Message Queue to use. The Identity Synchronization for Windows installation program then installs a required broker into Message Queue, so that Identity Synchronization for Windows can use Message Queue for synchronization.

  On Windows systems, Identity Synchronization for Windows supports only Message Queue 3.6. You therefore install Message Queue 3.6 provided with the Identity Synchronization for Windows bundle.

  Message Queue 3.7 is, however, installed as a Java Enterprise System shared component. On Windows systems by default you can therefore end up with both Message Queue 3.6 and Message Queue 3.7 installed. If you install Java Enterprise System components alongside Identity Synchronization for Windows on a Windows system, be sure Message Queue 3.7 is not selected.

Identity Synchronization for Windows Requirements in a Firewall Environment

You can run Identity Synchronization for Windows in a firewall environment. The following sections list the server ports that you must expose through the firewall.

Message Queue Requirements

By default, Message Queue uses dynamic ports for all services except for its port mapper. To access the Message Queue broker through a firewall, the broker should use fixed ports for all services.

After installing the core, you must set the `imq.<service_name>.<protocol_type>.port` broker configuration properties. Specifically, you must set the `imq.ssljms.tls.port` option. Refer to the Message Queue documentation for more information.

Installer Requirements

The Identity Synchronization for Windows installer must be able to communicate with the Directory Server acting as the configuration directory.

- If you are installing an Active Directory connector, the installer must be able to contact Active Directory's LDAP port, 389.
- If you are installing a Directory Server connector or a Directory Server plug-in (subcomponent), the installer must be able to contact the Directory Server LDAP port, default 389.

Core Component Requirements

The Message Queue, system manager, and command line interface must be able to reach the Directory Server where the Identity Synchronization for Windows configuration is stored.

Console Requirements

The Identity Synchronization for Windows console must be able to reach the following:

- Active Directory over LDAP, port 389, or LDAPS, port 636
- Active Directory Global Catalog over LDAP, port 3268, or LDAPS, port 3269
- Each Directory Server over LDAP or LDAPS
- Administration Server
- Message Queue

Connector Requirements

All connectors must be able to communicate with Message Queue.

In addition, the following connector requirements must be met.

- The Active Directory connector must be able to access the Active Directory Domain Controller over LDAP, port 389, or LDAPS, port 636.
- The Directory Server connector must be able to access Directory Server instances over LDAP, default port 389, or LDAPS, default port 636.

Installation Privileges and Credentials

This section covers privileges or credentials required for installation of Directory Server Enterprise Edition component products.

Directory Server Enterprise Edition Privileges

When installing Directory Server Enterprise Edition from native packages based distribution on Solaris systems, you must install as `root`.

You can install Directory Server Enterprise Edition from the zip distribution without special privileges. See the *Sun Directory Server Enterprise Edition 7.0 Installation Guide* for details.

Identity Synchronization for Windows Installation Privileges and Credentials

To install Identity Synchronization for Windows, you must provide credentials for the following.

- Configuration Directory Server.
- Directory Server being synchronized.
- Active Directory.

  See Chapter 3, "Installing Core," in *Sun Java System Identity Synchronization for Windows 6.0 Installation and Configuration Guide* for details.

In addition, you must have the following privileges to install Identity Synchronization for Windows.

- On Solaris and Red Hat systems, you must install as `root`.
- On Windows systems, you must install as `Administrator`.

Note – When you enter passwords by using the text-based installer, the program automatically masks the passwords so passwords are not echoed in the clear. The text-based installer is supported on Solaris and Red Hat systems only.

Installation Notes for Identity Synchronization for Windows

Before installing fresh bits of Identity Synchronization for Windows, be sure to read Chapter 2, "Preparing for Installation," in *Sun Java System Identity Synchronization for Windows 6.0 Installation and Configuration Guide*.

Using Windows 2003 Server and Identity Synchronization for Windows

On Windows 2003 Server, the default password policy enforces strict passwords, which is not the default password policy on Windows 2000.

◆ ◆ ◆ CHAPTER 4

Directory Server Bugs Fixed and Known Problems

This chapter contains important, product-specific information available at the time of release of Directory Server.

This chapter includes the following sections:

Bugs Fixed in Directory Server 7.0

This section lists the bugs fixed since the last release of Directory Server.

TABLE 4–1 Bugs Fixed in Directory Server 7.0

Bug ID	Description
4987124	UIDs for entries are not required to be unique.
5087249	Network connections remain established regardless of the settings of the `tcp_keepalive_interval` and `tcp_ip_abort_interval` attributes.
6192090	The `insync` command cannot parse a host specification provided to it if the host specification contains an at sign (`@`).
6250000	Non-unique values of `nsuniqueid` can be added to a replication topology and cause replication to fail.
6283810	Using the `ldapmodify` command to delete an attribute can cause replication to fail.
6292310	Modifying an entry's RDN at the same time as modifying an attribute value of the entry's parent puts the directory server in deadlock.
6295323	A memory leak occurs in searches that return virtual attributes.
6340125	If a change log is created and read simultaneously, the directory server can fail.

TABLE 4–1 Bugs Fixed in Directory Server 7.0 *(Continued)*

Bug ID	Description
6341382	Read errors can occur when SASL security is enabled.
6356373	The indirect Class of Service feature does not support multiple templates as documented.
6382134	The `ldapcompare` command can fail if a Class of Service is configured.
6386671	`ou=groups` can contain duplicate data.
6479754	Replication can fail after SSL is configured as documented.
6490419	The `ldapsearch` command can return inconsistent results.
6497556	On Windows installations, the `dsadm info` command can display the incorrect owner of `ns-slapd`.
6498501	On HP-UX installations, the `dsadm stop` and `restart` commands can behave inconsistently when the monitoring plug-in is enabled.
6499077	The warning message for an unregistered suffix contains extra characters.
6500908	Certificates with names that contain localized characters cannot be listed or deleted correctly.
6504891	The `dsadm autostart` command can return incorrect error messages.
6506019	On HP-UX installations, the directory server can fail when the GNU debugger (GDB) releases the `ns-slapd` process.
6536777	On UNIX installations, the JVM of the Sun Java System Application Server must be started with `-Djava.awt.headless=true` to enable replication topology rendering.
6542953	Multiple ZIP installations do not manage all CACAO ports correctly.
6548467	The DSCC cannot be accessed through its URL when a previous connection is still open.
6550543	DSCC can return errors when run with Java 1.6.
6551672	The Sun Java System Application Server returns an `Unable to create SASL client conn for auth mechanism` message and cannot communicate with CACAO.
6557499	Registering and deploying JESMF creates defunct processes.
6561787	DSCC parses `dsinstancemain.confirmreadonly` incorrectly.
6562921	Data passed to Windows service management must maintain the correct character case.
6572853	The Class of Service statistics monitor reports results incorrectly.
6579286	On Windows installations, the `dsrepair` command fails because of a missing directory in the `PATH` environment variable.
6579820	On Windows installations, the `plcheck` command fails.
6582585	DSCC cannot access the log files when the instance path contains multi-byte characters.

TABLE 4–1 Bugs Fixed in Directory Server 7.0 *(Continued)*

Bug ID	Description
6586725	A memory leak occurs in multi-master replication over SSL.
6593775	DSCC does not display all suffixes.
6594285	DSCC fails to support RBAC.
6617936	When the `repldisc` command encounters an error connecting to a replica over SSL, its credentials are not properly handled.
6620846	The `repldisc` command in interactive mode should not request the host name and port number.
6620851	The `repldisc` command in interactive mode should not request replicas that cannot be connected.
6634048	External use of the reversible password plug-in can cause replication to fail.
6640806	Re-indexing requires too much time to complete.
6641259	The DSCC displays a message that describes the Replication Settings tab incorrectly.
6642364	Some password policy updates appear in replicated audit logs but not in the local audit log.
6644137	The DSCC displays a message that describes the Promote/Demote Suffix function incorrectly.
6644368	The `repldisc` command fails to compare host names correctly.
6645742	Replication stops between servers of different versions after a failed login of a known user with an incorrect password.
6646794	The DSCC ACI wizard produces invalid ACIs when multiple `targetattr` values are selected.
6650039	A replication master can fail when replication stops normally.
6651645	Passwords cannot be changed through proxied authorization when `pwdReset` is set to `true`.
6659728	Performance can be degraded when the access log is enabled.
6662669	The `dsconf set-log-prop` command does not change permissions on log files in a timely manner.
6663553	Extra spaces in an ACI string can cause incorrect ACI evaluations.
6670977	The DSCC fails to display a long ACI.
6675384	Complex Class-of Service deployments can cause the directory server to fail.
6680142	Several text files require correction.
6680718	Rotation can become deadlocked.
6683182	A user password can become expired even if `passwordMaxAge` is set to a high value.
6683870	The DSCC can corrupt entries with binary attributes during modification.

TABLE 4–1 Bugs Fixed in Directory Server 7.0 *(Continued)*

Bug ID	Description
6684993	Under certain circumstances, the password policy attribute `pwdMinLength` is not enforced.
6686131	The DSCC displays some links incorrectly.
6686199	The directory server can fail if the `uniqueness-among-attribute-set` plug-in is configured.
6686632	The directory server fails if a pre-op plug-in performs an access control check on an entry before deleting it.
6687304	Changes to client authentication made with the DSCC do not become effective until the directory server is restarted.
6688454	Pass-through authentication can prevent the directory server from stopping correctly.
6688891	The audit log contains old passwords.
6689290	DSCC can display incorrect message text when starting and stopping the directory server.
6689454	Errors can occur if a database is restored and the backup has a very large change log.
6690684	A server instance bound to a specific IP address can fail to become registered.
6700232	The directory server can become deadlocked when accessing the change log.
6704259	Replication operations require too much time.
6704261	A multiple-pass LDIF import operation can produce an incorrect index.
6704754	The Logging property `rotation-time` cannot be set to `undefined` even though it is listed as an allowed value
6705319	DSCC does not disable a referral completely.
6706009	The DSCC does not handle subtype attributes correctly when editing entries.
6707089	The directory server can fail when evaluating an ACI.
6707164	A binary restore of the database recreates the replication change log.
6708194	The DSCC cannot set the time-base log rotation and deletion policy to Do Not Automatically Rotate/Delete.
6708615	The directory server fails when stopping the server when indexing is active.
6711123	Backup and export files can become invalid if infrequently updated masters receive updates.
6712614	The `starttls` command runs slowly.
6715303	The directory server fails when fetching values of a virtual attribute.
6715911	The directory server can fail when creating a new suffix in the Top entry if the name of the suffix contains a back slash (\).
6716661	The `repl-schedule` property should be multivalued.

TABLE 4–1 Bugs Fixed in Directory Server 7.0 *(Continued)*

Bug ID	Description
6717507	Enabling replication can incorrectly update VLV indexes
6718308	The DSCC does not log all messages when restoring the database.
6723208	The DSCC corrupts `mailSieveRuleSource` when it updates a user.
6726890	The change log is not always trimmed correctly.
6731941	The number of simultaneous pass-through authentications cannot be limited.
6735966	On Windows installations, the directory server can fail under load when encryption is disabled.
6736172	The directory server can add the `cACertificate` and `crossCertificatePair` properties twice.
6737227	The directory server can fail under load during DN normalization.
6739300	The retro change log can grow very large when managing large static groups.
6740791	A memory leak can occur in the directory server when binding users whose password policy is assigned in a Class of Service.
6742347	In Windows installations, the directory server does not stop during shutdown when registered as a service.
6746125	The ldapsearch command can return incorrect results for a search of `certificateRevocationList` with non-existent subtypes.
6746574	When set to on, `nsslapd-return-exact-case` does not work correctly for `certificateRevocationList`.
6748713	The directory server can close a connection before `idletimeout` has elapsed.
6750238	In Windows installations, the first attempt of the directory server to restart after the system is rebooted can fail with System Event ID 7022.
6750240	`des-plugin.so` is not signed.
6751358	Prioritized replication does not work as designed.
6751952	Replication stops and restarts when a send update now operation occurs.
6752586	Identity Synchronization for Windows plug-in does not start.
6752738	An exported LDIF can include an entry's Replica Update Vector.
6753742	Upgrading a multi-master replication topology can fail.
6755852	The directory server cannot be installed on some Japanese Windows systems.
6756240	The directory server can fail because of polling issues.
6759200	directory server can fail because of binding with SASL.

TABLE 4–1 Bugs Fixed in Directory Server 7.0 *(Continued)*

Bug ID	Description
6759886	DEL operations are replicated in a multi-master topology, `modifiersname` is logged incorrectly in the audit log of the consumer.
6763091	The password policy assigned to a user entry through a role is not effective until the directory server is restarted.
6764616	Replication can fail if the suffix name contains a space.
6768405	The `dsconf` command does not correctly handle a hyphen (`-`).
6771728	Replication can fail if a MOD CSN (Change Sequence Number) is smaller than the previous ADD CSN.
6772760	The directory server can fail if it is stopped immediately after it is started.
6772870	A consumer can become unsynchronized when `ds-polling-thread-count` is greater than 1.
6772918	The `dsconf info` command does not always detect the directory server's version number.
6773132	The `dsconf export` command does not log an error when it fails because the target file system is full.
6777643	The `insync` operation can fail.
6779940	The `dsconf matching-rule` property for indexes should be multi-valued.
6779962	The `dsadm export` command cannot index collation plug-in matching rules.
6783425	The `searchrate` command can fail when processing a complex filter.
6789448	An error can occur when the `pwd-accept-hashed-pwd-enabled` property is set.
6790060	ACI evaluation during unindexed searches can require too much time.
6791372	The directory server can fail when the `authrate` command is running.
6793557	The directory server can fail when the DSML plug-in receives a corrupted DSML message.
6796266	The directory server can fail when it is stopped if the `memberof` plug-in is not completely preloaded.
6797187	The `dsadm add-selfsign-cert` command adds self-inconsistent certificates to the database.
6798026	On Windows installations, the directory server can crash during search operations.
6806271	In multi-master replication topologies, the directory server can fail to detect duplicate values for attributes with more than eight values.
6809149	Recovery from a database failure can cause the heap to be corrupted.
6821682	The `dsconf` command does not handle the `dsml-min-parser-count` and `dsml-max-parser-count` properties correctly.

TABLE 4–1 Bugs Fixed in Directory Server 7.0 *(Continued)*

Bug ID	Description
6827661	On some Windows installations, the `dsadm stop` command does not stop the directory server.
6834291	The sequence of plug-in operation should be reordered.
6835539	The DSCC can encounter an error when creating or modifying a specialized password policy.
6835550	In multi-master replication topologies, replication can fail after importing a replica.
6837200	The change log trimming thread can cause the directory server to fail at startup.
6837808	ACI evaluation during a modify operation can corrupt the heap.
6846693	The directory server can crash after importing new entries.
6846934	ACIs with the `ip` keyword are not always evaluated correctly.
6849485	The server could crash during a DSML search if the bind password needed to be changed.
6849928	Importing can fail to create a replica correctly.
6850042	The ZIP distribution of the directory server should use non-default port numbers.
6850537	Search requests should return binary attributes in accordance with RFC 4522.
6851491	The directory server can crash during Class of Service operations.
6852119	A memory leak can occur when importing an LDIF with replication meta-data.
6853884	The `dsmig migrate-config` command logs a configuration warning for the Strong Password Check plug-in.

Known Problems and Limitations in Directory Server

This section lists known problems and limitations at the time of release.

Directory Server 7.0 Limitations

Do not change file permissions by hand.

Changes to file permissions for installed Directory Server Enterprise Edition product files can in some cases prevent the software from operating properly. Only change file permissions when following instructions in the product documentation, or following instructions from Sun support.

To workaround this limitation, install products and create server instances as a user having appropriate user and group permissions.

Do not replicate the `cn=changelog` suffix.

Although nothing prevents you from setting up replication for the `cn=changelog` suffix, doing so can interfere with replication. Do not replicate the `cn=changelog` suffix. The `cn=changelog` suffix is created by the retro changelog plug-in.

The wrong SASL library is loaded when `LD_LIBRARY_PATH` contains `/usr/lib`.

When `LD_LIBRARY_PATH` contains `/usr/lib`, the wrong SASL library is used, causing the `dsadm` command to fail after installation.

Use the LDAP replace operation to change `cn=config` attributes.

An LDAP modify operation on `cn=config` can only use the replace sub-operation. Any attempt to add or delete an attribute will be rejected with `DSA is unwilling to perform`, error `53`. While Directory Server 5 accepted adding or deleting an attribute or attribute value, the update was applied to the `dse.ldif` file without any value validation, and the DSA internal state was not updated until the DSA was stopped and started.

Note – The `cn=config` configuration interface is deprecated. Where possible use the `dsconf` command instead.

To work around this limitation, the LDAP modify replace sub-operation can be substituted for the add or delete sub-operation. No loss in functionality occurs. Furthermore, the state of the DSA configuration is more predictable following the change.

On Windows systems, Directory Server does not allow Start TLS by default.

This issue affects server instances on Windows systems only. This issue is due to performance on Windows systems when Start TLS is used.

To work around this issue, consider using the `-P` option with the `dsconf` command to connect using the SSL port directly. Alternatively, if your network connection is already secured, consider using the `-e` option with the `dsconf` command. The option lets you connect to the standard port without requesting a secure connection.

Replication update vectors may reference retired servers.

After you remove a replicated Directory Server instance from a replication topology, replication update vectors can continue to maintain references to the instance. As a result, you might encounter referrals to instances that no longer exist.

The Common Agent Container is not started at boot time.

To work around this issue when installing from native packages, use the `cacaoadm enable` command as `root`.

To work around this issue on Windows, choose Log On from the properties of Common Agent Container service, enter the password of the user running the service, and press Apply. If you have not already done this setting, you will receive a message stating that the account `user name` has been granted the Log On As A Service right.

`max-thread-per-connection-count` is not useful on Windows systems.

The Directory Server configuration properties `max-thread-per-connection-count` and `ds-polling-thread-count` do not apply for Windows systems.

Console does not allow administrator login on Windows XP

Console does not allow administrator to logon to the server running Windows XP.

As a workaround to this problem, the guest account must be disabled and the registry key `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\ForceGuest` must be set to `0`.

Changing Index Configurations on the Fly

If you change an index configuration for an attribute, all searches that include that attribute as a filter are treated as not indexed. To ensure that searches including that attribute are properly processed, use the `dsadm reindex` or `dsconf reindex` commands to regenerate existing indexes every time you change an index configuration for an attribute. See Chapter 12, "Directory Server Indexing," in *Sun Directory Server Enterprise Edition 7.0 Administration Guide* for details.

Number of connections and operations are not enforced on PTA servers

The maximum number of connections (`maxconns`) and the maximum number of operations (`maxops`) are not enforced on PTA servers.

When installed with the ZIP distribution, Directory Server uses port 21162 as the default of the Common Agent Framework (CACAO).

The default port of the Common Agent Framework (CACAO) is 11162. When installed with the native distribution, Directory Server uses this default port. However, when installed with the ZIP distribution, Directory Server uses port 21162 by default. Be sure to specify the right port number when creating or registering a server instance with DSCC.

Known Directory Server Issues in 7.0

This section lists the known issues that are found at the time of Directory Server 7.0 release.

2113177 Directory Server has been seen to crash when the server is stopped while performing online export, backup, restore, or index creation.

2129151 The Directory Server hangs when running the `stop-slapd` command.

2133169 When entries are imported from LDIF, Directory Server does not generate `createTimeStamp` and `modifyTimeStamp` attributes.

LDIF import is optimized for speed. The import process does not generate these attributes. To work around this limitation, add rather than import the entries. Alternatively, preprocess the LDIF to add the attributes before import.

4979319 Some Directory Server error messages refer to the *Database Errors Guide*, which does not exist. If you cannot understand the meaning of a critical error message that is not documented, contact Sun support.

6401484 The `dsconf accord-repl-agmt` command cannot align authentication properties of the replication agreement when SSL client authentication is used on the destination suffix.

To work around this issue, store the supplier certificate in the configuration on the consumer, following these steps. The examples command shown are based on two instances on the same host.

1. Export the certificate to a file.

   The following example shows how to perform the export for servers in `/local/supplier` and `/local/consumer`.

   ```
   $ dsadm show-cert -F der -o /tmp/supplier-cert.txt \
     /local/supplier defaultCert
   $ dsadm show-cert -F der -o /tmp/consumer-cert.txt \
     /local/consumer defaultCert
   ```

2. Exchange the client and supplier certificates.

   The following example shows how to perform the exchange for servers in `/local/supplier` and `/local/consumer`.

   ```
   $ dsadm add-cert --ca /local/consumer supplierCert \
     /tmp/supplier-cert.txt
   $ dsadm add-cert --ca /local/supplier consumerCert \
     /tmp/consumer-cert.txt
   ```

3. Add the SSL client entry on the consumer, including the `supplierCert` certificate on a `usercertificate;binary` attribute, with the proper `subjectDN`.

4. Add the replication manager DN on the consumer.

   ```
   $ dsconf set-suffix-prop suffix-dn repl-manager-bind-dn:entryDN
   ```

5. Update the rules in `/local/consumer/alias/certmap.conf`.

6. Restart both servers with the `dsadm start` command.

6410741 Directory Service Control Center sorts values as strings. As a result, when you sort numbers in Directory Service Control Center, the numbers are sorted as if they were strings.

An ascending sort of 0, 20, and 100 results in the list 0, 100, 20. A descending sort of 0, 20, and 100 results in the list 20, 100, 0.

6412131 The certificate names containing multi-byte characters are shown as dots in the output of the `dsadm show-cert` *instance-path valid-multibyte-cert-name* command.

6416407 Directory Server does not correctly parse ACI target DNs containing escaped quotes or a single escaped comma. The following example modifications cause syntax errors.

```
dn:o=mary\"red\"doe,o=example.com
changetype:modify
add:aci
aci:(target="ldap:///o=mary\"red\"doe,o=example.com")
 (targetattr="*")(version 3.0; acl "testQuotes";
 allow (all) userdn ="ldap:///self";)
```

```
dn:o=Example Company\, Inc.,dc=example,dc=com
changetype:modify
add:aci
aci:(target="ldap:///o=Example Company\, Inc.,dc=example,dc=com")
 (targetattr="*")(version 3.0; acl "testComma";
 allow (all) userdn ="ldap:///self";)
```

Examples with more than one comma that has been escaped have been observed to parse correctly, however.

6428448 The `dpconf` command has been seen to display the `Enter "cn=Directory Manager" password:` prompt twice when used in interactive mode.

6446318 On Windows, SASL authentication fails due to the following two reasons:

- SASL encryption is used.

  To workaround the issue caused by the SASL encryption, stop the server, edit `dse.ldif`, and reset SASL to the following.

  ```
  dn: cn=SASL, cn=security, cn=config
    dssaslminssf: 0
    dssaslmaxssf: 0
  ```

- The installation is done using native packages.

  To workaround the issue caused by the native packages installation , set `SASL_PATH` to *install-dir*`\share\lib`.

6449828 Directory Service Control Center does not properly display `userCertificate` binary values.

6461602 The `dsrepair fix-entry` does not work if the source is a tombstone and if the target is an entry (DEL not replicated).

Workaround: Use the `dsrepair delete-entry` command to explicitly delete the entry. Then use the `dsrepair add-entry` command to add the tombstone.

6468074 It is not clear from the name of the `passwordRootdnMayBypassModsCheck` configuration attribute that the server now allows any administrator to bypass password syntax checking when modifying another user's password, when the attribute is set.

6469154 On Windows, the output of `dsadm` and `dpadm` commands, and help messages are not localized in Simplified and Traditional Chinese languages.

6469296 Although the Directory Service Control Center allows you to copy the configuration of an existing server, it does not allow you to copy the plug-in configuration.

6469688 On Windows systems, the `dsconf` command has been seen to fail to import LDIF with double-byte characters in the LDIF file name.

To work around this issue, change the LDIF file name so that it does not contain double-byte characters.

6483290 Neither Directory Service Control Center nor the `dsconf` command allows you to configure how Directory Server handles invalid plug-in signatures. Default behavior is to verify the plug-in signatures, but not to require that they are valid. Directory Server logs a warning for invalid signatures.

To change the server behavior, adjust the `ds-require-valid-plugin-signature` and `ds-verify-valid-plugin-signature` attributes on `cn=config`. Both attributes take either `on` or `off`.

6485560 Directory Service Control Center does not allow you to browse a suffix that is configured to return a referral to another suffix.

6488197 After installation and after server instance creation on Windows systems, the file permissions to the installation and server instance folder allow access to all users.

To work around this issue, change the permissions on the installations and server instance folders.

6488284 For the HP-UX platform, Directory Server Enterprise Edition man pages for the following sections cannot be accessed from the command line:

- `man5dpconf`.
- `man5dsat`.
- `man5dsconf`.
- `man5dsoc`.
- `man5dssd`.

To workaround this issue, access the man pages at *Sun Directory Server Enterprise Edition 7.0 Man Page Reference*. From that location, you can download a PDF of all Directory Server Enterprise Edition man pages.

6490557 An attempt to enter an invalid CoS Template results in a crash in versions of Directory Server 6.

6490653 When enabling referral mode for Directory Server by using Directory Service Control Center through Internet Explorer 6, the text in the confirm referral mode window is truncated.

To work around this issue, use a different browser such as Mozilla web browser.

6491849 After upgrading replica, and moving servers to new systems, you must recreate replication agreements to use new host names. Directory Service Control Center lets you delete the existing replication agreements, but does not allow you to create new agreements.

6492894 On Red Hat systems, the `dsadm autostart` command does not always ensure that the server instances start at boot time.

6494997 The `dsconf` command does not prompt for the appropriate `dsSearchBaseDN` setting when configuring DSML.

6495004 On Windows systems, Directory Server has been seen to fail to start when the base name of the instance is `ds`.

6497894 The `dsconf help-properties` command is set to work properly only after instance creation. In addition, the correct list of values for the `dsml-client-auth-mode` command should be `client-cert-first | http-basic-only | client-cert-only`.

6500936 In the Native patch delivery, the miniature calendar that is used to pick dates for filtering access logs is not properly localized in Traditional Chinese.

6501320 When creating an index on custom schema, a suffix level change of the *all-ids-threshold* is not permeated completely by the DSCC.

6503509 Some output displayed by the `dsccmon`, `dsccreg`, `dsccsetup`, and `dsccrepair` commands is not localized.

6503546 Changing the locale of the system and starting DSCC, does not display the pop-up window message in the locale that you selected.

6504180 On Solaris 10, the password verification fails for instances with multi-byte characters in their DN on English and Japanese locales.

6504549 The discovery of an instance of the Directory Server by the Java Enterprise System Monitoring Framework is not successful if the `ns-slapd` process was started remotely using `rsh`.

6507312 On HP-UX systems, applications using NSPR libraries crash and dump core after investigation with `gdb`. The problem occurs when you attach `gdb` to a running Directory Server instance, then use the `gdb quit` command.

6520646 Clicking Browse DSCC online help does not display the online help when you are using Internet Explorer.

6527999 The Directory Server plug-in API includes `slapi_value_init()()`, `slapi_value_init_string()()`, and `slapi_value_init_berval()()` functions.

These functions all require a "done" function to release internal elements. However, the public API is missing a `slapi_value_done()()` function.

6541040 When modifying the password policy using the Directory Service Control Center, attributes that have not changed may be unknowingly reset.

Using the Directory Service Control Center to manage the default password policy does not causes any error. However, using the Directory Service Control Center to manage specialized password policies can cause unchanged attributes to be reset.

6542857 When you use the Service Management Facility (SMF) on Solaris 10 to enable a server instance, the instance might not start when you reboot the system and return the following error:

```
svcadm: Instance "svc:/instance_path" is in maintenance state.
```

To work around this problem, use a local user to create Directory Server and Directory Proxy Server servers.

6547992 On HP-UX, the `dsadm` and `dpadm` commands might not find `libicudata.sl.3` shared library.

As a workaround to this problem, set the `SHLIB_PATH` variable.

```
env SHLIB_PATH=${INSTALL_DIR}/dsee6/private/lib dsadm
```

6551685 The `dsadm autostart` can make native LDAP authentication to fail when you reboot the system.

As a workaround, reverse the order of reboot scripts. The default order is `/etc/rc2.d/S71ldap.client` and `/etc/rc2.d/S72dsee_directory`.

6557480 On Solaris 9 and Windows, when you access the online help from the console configured using Web archive file (WAR), it displays an error.

6559825 If you modify the port number using DSCC on a server that has replicated suffixes, problems arise when setting replication agreement between servers.

6587801 Directory Service Control Center and the `dsadm` command from versions 6.1 or later do not display built-in CA certificates of Directory Server instances that were created with the `dsadm` command from version 6.0.

To workaround this issue:

Add the 64-bit module with 64-bit version of `modutil`:

```
$ /usr/sfw/bin/64/modutil -add "Root Certs 64bit" \
-libfile  /usr/lib/mps/64/libnssckbi.so -nocertdb \
-dbdir /instance-path/alias -dbprefix slapd- -secmod secmod.db
```

6630897 The output of the `dsadm show-*-log l` command does not include the correct lines. It can include the last lines of a previously rotated log.

6630924 The output of the `dsadm show-*-log` command is not correct if some lines in the log contain more than 1024 characters.

6634397 For servers registered in DSCC as listening on all interfaces (0.0.0.0), attempting to use `dsconf` to modify the listen-address of the servers results in DSCC errors.

To have SSL port only and secure-listen-address setup with Directory Server Enterprise Edition 6.3, use this workaround:

1. Unregister the server from DSCC:

   ```
   dsccreg remove-server /local/myserver
   ```

2. Disable the LDAP port:

   ```
   dsconf set-server-prop ldap-port:disabled
   ```

3. Set up a secure-listen-address:

   ```
   $ dsconf set-server-prop secure-listen-address:IPaddress
   ```

   ```
   $ dsadm restart /local/myserver
   ```

4. Register the server using DSCC. In the Register Server wizard, specify the server's IP address. This operation cannot be undone.

6637242 After deploying the WAR file, the View Topology button does not always work. A Java exception sometimes occurs, which is based on `org.apache.jsp.jsp.ReplicationTopology_jsp._jspService`

6640755 In Windows, in the Korean locale, the `dsadm start` command does not display the `nsslapd` error log when `ns-slapd` fails to start.

6648240 Changing or deleting an attribute in the Additional Indexes table of the Indexes tab in the Directory Service Control Center can lead to stale information being displayed until the browser is refreshed.

6689432 The error message displayed after a failed try to set `use-cert-subject-as-bind-dn` to `false` contains wrong property names.

6696857 If a Directory Proxy Server instance has only secure-listen-socket/port enabled through DSCC and if server certificate is not default (for example, if it is a certificate-Authority-signed certificate), then DSCC cannot be used to manage the instance.

To work around this problem, unregister the DPS instance and then register it again. Another solution is to update the userCertificate information for the DPS instance in the DSCC registry using the server certificate.

6720595 On UNIX systems, an attempt to change the path of any log file with `dsconf set-log-prop` or DSCC fails if the new path of the log file does not already exist.

6725346 Database names can contain only ASCII (7-bit) alphanumeric characters, hyphens (-), and underscores (_). Directory Server does not accept multibyte characters (such as in Chinese or Japanese character sets) in strings for database names, file names, and path names. To work around this issue when creating a Directory Server suffix having multibyte characters, specify a database name that has no multibyte characters. When creating a suffix on the command line, for example, explicitly set the `--db-name` option of the `dsconf create-suffix` command.

```
$ dsconf create-suffix --db-name asciiDBName multibyteSuffixDN
```

Do not use the default database name for the suffix. Do not use multibyte characters for the database name.

6750837 Specification of network drives on Microsoft Windows is case-sensitive. Because of this, using both `C:/` and `c:/`, for example, in DSEE administrative commands can cause replication to fail after the masters are restarted. As a workaround, use the 'DSEE_HOME/ds6/bin/dsconf accord-repl-agmt' to correct the replication agreement.

6751354 Specification of network drives on Microsoft Windows is case-sensitive. Because of this, using both `C:/` and `c:/`, for example, in DSEE administrative commands can produce various error messages, such as the following:

```
WARNING<4227> - Plugins - conn=-1 op=-1 msgId=-1 -
Detected plugin paths from another install, using current install
```

To avoid these warnings, be sure to use `C:/` consistently.

6752625 Online help in DSCC might link to unknown web pages. In particular, some wizard menus might suggest the following:

```
For more information about data source configuration,
see the "Sun Directory Server Enterprise Edition Reference."
```

Selecting the link to the DSEE Reference document produces an error message.

To work around this problem, select the link with the third mouse-button and choose the Open Link in New Window command from the pop-up menu. The selected document appears in the new browser window.

6753020 In a Multi-Master Replication configuration including 5.2 consumers, maximum of 4 version 7.0 servers are supported.

6776034 The DSCC Agent cannot be registered in CACAO on Solaris 9. If the `SUNWxcu4` package is missing from the system, then the command *DSEE_HOME*`/dscc6/bin/dsccsetup cacao-reg` fails with the error, `Failed to configure Cacao.`

To fix this issue, install the missing `SUNWxcu4` package on your system.

6783994 The `-f` option does not work with the `ldapcompare` command.

6845087 On Windows, CLI displays garbage characters.

6853393 DSCC does not support host synonyms. When replicating the DSCC suffix, the host name in the replication agreement must match the host name in the DSCC registry.

6876315 If the user running the `dsmig` command does not own the target directory server instance, the command fails because it does not have adequate permission to generate and access migrated files.

The `dsmig` command can run successfully if it is run by the user who owns the target directory server and has at least read access to the source directory server. If these conditions cannot be met, perform the migration by exporting the database and importing it to the new directory server.

6885178 The man page for `hosts_access` incorrectly states that IPv6 is not supported on Windows systems.

6891486 Some debug messages and Error #20502, `Serious failure during database checkpointing, err=2 (No such file or directory)`, can sometimes be logged right before the import processing starts. Such messages can be ignored, as they refer to the old suffix data being deleted.

6894136 If you set the idle timeout to a very small value, for example, `2s` on a server instance, DSCC might display connection errors and prevent some operations that take long time to complete (like rotating logs). Make sure you set the idle timeout to at least `10s` or `20s`, and adjust the idle timeout according to your network latency.

6898825 On Windows 2008, Common Agent Framework sometimes refuses to be started from Windows Service Manager.

As a workaround, start the CACAO service manually using the `cacaoadm start` command.

6955408 On Windows systems, running the `dsccsetup dismantle` command does not completely remove the CACAO Windows service.

Workaround. After you have run the `dsccsetup dismantle` command, run `cacaoadm prepare-uninstall` before you uninstall Directory Server Enterprise Edition. This removes the CACAO Windows service.

◆ ◆ ◆ CHAPTER 5

Directory Proxy Server Bugs Fixed and Known Problems

This chapter contains important, product-specific information available at the time of release of Directory Proxy Server.

This chapter includes the following sections:

Bugs Fixed in Directory Proxy Server 7.0

This section lists the bugs fixed since the last release of Directory Proxy Server.

Bug ID	Description
6351249	The `dpcfg` command does not validate the values of properties that it handles.
6417166	The directory server does not observe the resource limit policy's `minimum-search-filter-substring-length` property.
6446600	The directory server does not always handle ACI notification changes coming from an LDAP source.
6468142	Attribute names are stored differently in virtual view and in LDIF.
6468198	The directory server should apply a default value to any virtual attribute that does not have a value set.
6468593	All monitoring elements should have a value set for the `statusDescription` property.
6468694	Search operations do not return complete information when an entry does not exist.
6469976	The `dpadm split-ldif` command should provide more statistics, such as the number of entries skipped.

Bug ID	Description
6475156	For some properties, the `dpcfg` command changes the property's value and sets `is-restart-required` to false, although the directory server must be restarted for the change to take effect.
6489771	Connection handlers bind anonymous binds incorrectly.
6491133	Multibyte certificate attributes are not handled correctly.
6491845	The DSCC does not display default values for Controls Allowed Through Proxy.
6492447	The `dpconf` command should not be able to set the `scriptable-alerts-command` attribute.
6495493	The `dpadm` command logs a `SUNWdsee7-config` is not installed message if `SUNWdsee7-config` is relocated.
6520362	The `dpconf` `get-jdbc-data-source-prop` and `set-jdbc-data-source-prop` commands should support connection number properties.
6527010	Directory Proxy Server cannot write JDBC attributes implying many-to-many (N:N) relationship between tables in the JDBC database.
6527837	The proxy server should open fewer initial connections to LDAP servers.
6536823	The proxy server closes client connections too frequently.
6537654	The proxy server opens new connections to JDBC back ends too frequently.
6539650	On Linux installations, the proxy server cannot create a multibyte DN.
6547755	The DSCC does not create multibyte certificate names correctly.
6550554	In the `zh_cn/ja` locale, the DSCC cannot create a multibyte proxy server instance.
6554232	The proxy server cannot get the full list of attributes using the asterisk character (*) on a joined data view.
6561139	The proxy server cannot roll back a JDBC transaction after an SQL exception.
6562213	The proxy server can log the wrong operation number when using virtual groups.
6562601	The DSCC does not display a certificate's properties.
6567644	The proxy server submits incorrect requests to the database.
6573259	When the `ldapsearch` command fails on a joined view, its returns internally mapped DNs in its error output
6573264	The `ldapsearch` command should return error 32 when the base-DN does not exist in a JDBC source.
6590816	Setting the `connectionIdleTimeOutInSec` property in the LDAP listener causes the DSCC to fail.
6592394	In Windows installations, the `dpadm create` command accepts an invalid DN.

Bug ID	Description
6594076	Mod operations fail when a DN is mapped for an LDAP data view.
6596223	An incorrect filter-join-rule causes an SQL error to be returned in the LDAP result.
6596876	The value of the `connectionIdleTimeOutInSec` attribute should be measured in seconds and not milliseconds.
6597598	Null pointer exceptions can occur during modification operations.
6597608	LDAP transactions can succeed only partially.
6599118	Modifying a non-string column with a string value returns SQL error messages.
6599722	The proxy server can store incorrect values.
6616197	Write operations to a secondary table fail when an attribute in `filter-join-rule` is non-numeric.
6616898	The `objectclass` attribute cannot be stored in a secondary data view.
6618968	Optimization for a join view should not occur when one entry is returned from a secondary view.
6622852	Virtual transformation of `def-value` on a DN does not work as expected.
6630730	A null pointer exception occurs in `FailoverLoadBalancingAlgorithm.getSearchConnection`.
6637173	An entry's DN is no returned when no access rights exist on requested secondary attributes.
6637608	`ArrayIndexOutOfBoundsException` and `NegativeArraySizeException` errors can occur under heavy load.
6638374	An entry cannot be added through a join view if its UID attribute contains capital letters.
6639044	An incorrect return code occurs when attempting to mod-delete an attribute without its value mapped to a single-row table.
6639635	A modify-replace operation fails on an unset attribute mapped to a single-row table.
6640879	The proxy server should return error 32 when using the source of an `attr-name-mapping` in the base of a search.
6640884	The proxy server should not forward a search implying the source of `attr-name-mapping` to the directory server back end.
6641888	Search operations return entries that contain attributes not present in `viewable-attr`.
6641925	An add operation through a join view always creates the entry on a secondary JDBC data source.
6642559	Write virtual transformations do not always work correctly.
6642578	Writing virtual transformations do not work as expected when an entry is modified.
6642686	`remove-attr-value` read virtual transformations do not work correctly if attribute is multi-valued

Bug ID	Description
6643121	The `ldapmodify` command fails when the foreign key is a `VARCHAR`.
6643181	Problems can occur with JDBC data sources if string attributes are too long.
6643701	The `maxOperationPerInterval` and `operationRateCheckInterval` properties do not work as expected.
6646107	An ADD operation can fail when using a value longer than the column size.
6648665	The `max-client-connections` property does not work if no operation is performed on the connection.
6649071	Translated GUI text should be consistent.
6651837	User DNs are not correctly normalized, causing ACIs to fail.
6652476	Add operations can fail when schema checking is enabled if `objectclass:top` or a naming attribute is missing.
6653253	A race condition in `FailoverLoadBalancingAlgorithm` can cause the proxy server to fail.
6653453	Persistent Searches over SSL via the proxy server to the directory server fail to return expected data.
6654625	Existing connections are disconnected when garbage collection is triggered to run
6656324	The proxy server always converts DN values into lower case in ADD operations.
6659381	The proxy server JVM fails under high search load using JDK 1.6.
6661001	Reject operations are forwarded to the backend server.
6661375	Sockets can remain in the `CLOSE_WAIT` state.
6661474	The proxy server can miscalculate the connection numbers in connection pools.
6661981	The `attr-name-mappings` property cannot be set if `source-attr` is a substring of `client-attr`.
6663112	In Linux 64–bit installations, the proxy server cannot be started in 32–bit mode.
6665983	Modifying an attribute that is not part of object-class does not work properly.
6670752	The proxy server can throw this exception: `java.io.IOException: Timeout when waiting to read from input stream`
6671579	Virtualization fails to resolve a virtually mapped base within a search filter.
6676073	Incorrect attribute handling can cause modify operations in join data view to be routed incorrectly.
6676076	Null pointer exceptions can occur in modify operations in join data view.
6678386	Bind connections are not released and no more binds can be made when the maximum number of binds is reached.

Bug ID	Description
6680717	`StringIndexOutOfBoundsException` can occur when omitting the join-rule in a join view.
6681502	Memory monitoring is disabled by default.
6681932	A `remove-attr-value` write virtual transformation does not work correctly.
6682004	The rule for a write `remove-attr-value` virtual transformation should be set on `view-attribute-value`.
6686099	A server exception occurs when an ACI is stored in LDAP and the LDAP source is not available.
6688180	An entry is duplicated under `cn-monitor` and incorrect values are stored for `numDroppedOperations` and `receivedOperations`.
6688187	The time-resolution attribute does not become effective until the server is restarted.
6689377	The default referral policy is set to `discard`.
6689466	The `dpconf` command does not access the `cert-search-bind-dn` and `cert-search-bind-pwd` properties.
6689577	A client cannot connect to the proxy server in the clear when `ssl-policy` is set to `client` in the data source.
6691341	Monitoring with `average-traffic-sampling-interval` does not work correctly.
6692090	The `operationPerIntervalPeak` property is specified in operations per interval while `operationPerIntervalLastAverage` property is specified in operations per second.
6692627	An error can occur when decoding a search filter when using an LDAP browser.
6692693	The proxy server does not use `max-op-count-per-interval` correctly.
6697494	Shared attributes cannot be deleted through a join view when an entry is absent.
6702095	When `jdbc-attr` is added to a table of existing object-class, its meta-data is not retrieved dynamically.
6702169	Attribute value mapping of a DN does not work correctly if the entry is not one level below the data view's base DN.
6706567	Join optimization does not work correctly with DN join rules when the primary and secondary view base are different.
6707006	Filter join rules are not handled correctly in join data view.
6707110	Search operations fail when a search filter contains attributes that are not part of `jdbc-object-class`.
6711054	The proxy server does not support the SQL Server SQL type `smalldatetime`.
6711320	One-level scope searches on some nonexistent `cn=monitor` child entries return incorrect search results.

Bug ID	Description
6713382	DN normalization fails to translate the sequences `\dd` or `%dd` found in attributes values.
6714425	The `ldapsearch` command does not handle a quoted asterisk correctly.
6714448	The `ldapsearch` command can incorrectly handle non-numeric characters in integer searches.
6714856	Exceptions can occur in join data view.
6717836	Replacing an attribute found in a multi-row primary table can set other attributes in that table to null.
6717943	The default size limit for properties is set incorrectly.
6720614	An error message is displayed when the proxy server starts.
6721702	A JDBC search can fail when the primary table is not a single-row table.
6724559	The proxy server should filter out requests that contain unallowed controls.
6727763	Deleting an attribute found in a multi-row primary table deletes the matching entry.
6728378	A null pointer exception can occur in a join data view during an add operation when no DN/object class rule is specified.
6728746	The proxy server can not add an entry containing more than two object classes to a JDBC source.
6730825	An attribute hiding rule does not return the filter attribute in the rule.
6731666	The proxy server ignores the `process-bind` attribute value on data views.
6734365	Attribute mapping is not cleared by use of another data view.
6734438	The proxy server fails at startup if a mail alert is configured and the mail transfer agent is not available.
6734559	Virtual DN mapping fails when depending on a virtual attribute.
6734722	Backend connections remain in the `CLOSE_WAIT` state.
6735304	An attribute with a null value cannot be hidden.
6736621	The bind DN is rejected when a transformation fails.
6737084	DNs can be mapped incorrectly.
6739414	The proxy server changes the case of characters in attribute names.
6739456	The configuration and log files should be accessible by groups.
6739974	The proxy server returns attribute name mappings in lower case only.
6741401	An `ldapmodify add` operation fails if the foreign key is stored in a multi-row primary table.
6741403	The `ldapsearch` command can fail because of in incorrect join in a SELECT statement.

Bug ID	Description
6741410	The `TYPE_OR_VALUE_ALREADY_EXISTS` message should be returned when an existing value is added to an attribute.
6742935	The `NO_SUCH_ATTRIBUTE` message should be returned when a delete operation is performed on a multi-valued attribute.
6743357	A search operation with attribute filtering and multiple conditionals in the search filter returns error 1.
6748387	The proxy server should log a message when an operation changes state.
6750354	The proxy server should support requests for certificates with a `keylength` of 2048 bits.
6751692	The `dpadm start` command fails when using the `MaxTenuringThreshold` Java argument.
6752963	Exception messages can be logged incorrectly.
6754091	A join view operation with a `filter-join-rule` returns `StringIndexOutOfBoundsException`.
6757759	The proxy server can fail because of an incorrect JVM memory state.
6758244	A search operation on a JDBC source with a base scope and a DN filter on glue entries should not return all attributes.
6758812	The `enabled-admin-alert` property should accept a value of `none` and not accept a value of `all`.
6759391	The instance path in `cn=monitor` should be normalized.
6760526	The `dppadm start` command should create a `DPS.pid` file.
6760951	The configuration schema contains an inconsistency with the directory configuration schema.
6761017	A worker thread deadlock can occur.
6761032	The `searchMode` property is defined incorrectly.
6761875	High CPU use can occur, requiring that the proxy server be restarted.
6764073	The proxy server can fail when configured to use proxied authentication.
6766175	The `ldapsearch` command does not return an attribute with an empty value from a JDBC source.
6767244	The proxy server fails to bind to the secondary view when using a join view.
6767776	The proxy server cannot use DN mapping on the root DSE.
6768924	The proxy server does not recognize a split macro in a virtual transformation as a macro.
6778090	A compare operation does not work correctly on a virtual attribute in a join view.
6778091	A compare operation does not work correctly on a secondary attribute in a join view.
6782659	The `SO_KEEPALIVE` option is not set when a socket is created.
6784464	The `dpconf` command should support the `useTcpKeepAlive` attribute.

Bug ID	Description
6794720	One-level searches on a data view from a JDBC source returns an unexpected error.
6795597	Search performance on a join data view is poor when the primary view candidate list is large.
6801024	A warning message at startup should provide more information about the cause of the warning.
6802371	The `acceptBacklog` property is ignored for channel-based listeners.
6807446	A join view can return case-sensitive attribute values twice.
6808701	Inactivity heartbeats are not sent often enough for backend connections.
6808704	Inactivity heartbeats are not sent for bound backend connections.
6808706	Backend server checks might not occur often enough because of last server activity.
6813566	The proxy server must be restarted for changes to `monitoring-interval` and `monitoring-bind-timeout` to take effect.
6818788	The proxy server should provide the backend heartbeat more reliably.
6819304	A null pointer exception occurs when searching on `cn=monitor` when defining a failover pool with no source.
6819752	Persistent Search clients might not receive entry change notifications.
6821752	Resources used by a persistent search are not cleaned up after the client disconnects.
6828842	The proxy server can return error 1 when no backend servers are available, and it should return error 52.
6832043	Client affinity should not be enabled when `useAffinity=false` and `affinityPolicy` are explicitly set
6832498	The proxy server should not use MD5 as the signature algorithm in signed certificates.
6835898	The `dpconf` command does not correctly handle attributes with a value of a single letter for `Attribute/Entry Hiding`.
6845410	Renaming an attribute can break some BIND DNs.
6847524	DNs with special characters are not written correctly in the configuration file.

Known Problems and Limitations in Directory Proxy Server

This section lists known problems and limitations at the time of release.

Directory Proxy Server 7.0 Limitations

This section lists product limitations.

Do not change file permissions by hand.

Changes to file permissions for installed Directory Server Enterprise Edition product files can in some cases prevent the software from operating properly. Only change file permissions when following instructions in the product documentation, or following instructions from Sun support.

To workaround this limitation, install products and create server instances as a user having appropriate user and group permissions.

Self-signed server certificates cannot be renewed.

When creating a self-signed server certificate, make sure you specify a validity long enough that you do not have to renew the certificate.

Directory Proxy Server does not ensure atomicity with the join data view write operations.

To ensure atomicity, do not use the join data view for write operations. If you perform write operations on join data view, use an external mechanism to prevent or detect inconsistencies. You can monitor inconsistencies by monitoring Directory Proxy Server error log.

Wrong default value in man pages

The `log-buffer-size(5dpconf)` man page displays the wrong default size of the access log buffer. The default buffer size for access log is `1M`.

The man pages for pattern matching distribution algorithm incorrectly show the respective properties as single-valued. The properties are multi-valued.

When Oracle is the JDBC source, the `ldapsearch` command does not return an attribute with an empty value.

Oracle handles an empty string as NULL. The empty string and NULL are both valid values for an LDAP entry, but it is not possible to distinguish the two in Oracle. This issue was corrected for other JDBC sources in issue 6766175, as noted in "Bugs Fixed in Directory Proxy Server 7.0" on page 61.

Known Directory Proxy Server Issues in 7.0

This section lists the known issues that are found at the time of Directory Proxy Server 7.0 release.

5042517	The modify DN operation is not supported for LDIF, JDBC, join and access control data views.
6355714	Currently, `getEffectiveRight` control is supported only for LDAP data views and does not yet take into account ACIs local to the proxy.
6386073	After generation of a CA-Signed Certificate request, when you refresh, the certificate is displayed as a self-signed certificate.

6388022 If the SSL port used by Directory Proxy Server is incorrect, after a secure search request on that port Directory Proxy Server may close all connections.

6390118 Directory Proxy Server fails to count the number of referral hops properly when configured to use authentication based on the client application credentials rather than proxy authorization.

6390220 It is possible to specify the `base-dn` property when creating a data view, but it is not possible to set the `base-dn` property to "", the root dse, after creating the data view.

6410741 Directory Service Control Center sorts values as strings. As a result, when you sort numbers in Directory Service Control Center, the numbers are sorted as if they were strings.

An ascending sort of 0, 20, and 100 results in the list 0, 100, 20. A descending sort of 0, 20, and 100 results in the list 20, 100, 0.

6439604 After configuring alerts, you must restart Directory Proxy Server for the change to take effect.

6447554 Directory Proxy Server fails to rename an entry moving to another data view when numeric or lexicographic data distribution is configured.

6461510 In Directory Proxy Server, referral hop limit does not work.

6469154 On Windows, the output of `dsadm` and `dpadm` commands, and help messages are not localized in Simplified and Traditional Chinese languages.

6488197 After installation and after server instance creation on Windows systems, the file permissions to the installation and server instance folder allow access to all users.

To work around this issue, change the permissions on the installations and server instance folders.

6488297 On Windows, DSCC initialization can only be performed by Administrator user

6493349 Directory Service Control Center removes commas when changing the DN for an existing excluded subtree, or alternate search base.

6494540 After enabling or disabling non secure LDAP access for the first time, you must restart Directory Proxy Server for the change to take effect.

6497547 Time limit and size limit settings work only with LDAP data sources.

6497992 After using the command `dpadm set-flags cert-pwd-store=off`, Directory Proxy Server cannot be restarted using Directory Service Control Center.

6501867 The `dpadm start` command has been seen to fail when used with a server instance name combining both ASCII and multi-byte characters.

6505112 When setting the `data-view-routing-custom-list` property on an existing connection handler, an error occurs with data view names containing characters that must be escaped, such as commas.

To work around this issue, do not give data views names that contain characters that must be escaped. For example, do not use data view names containing DNs.

6511264 When using the DN renaming feature of Directory Proxy Server, notice that repeating DN components are renamed to only one replacement component.

Consider for example that you want to rename DNs that end in `o=myCompany.com` to end in `dc=com`. For entries whose DN repeats the original component, such as `uid=userid,ou=people,o=myCompany.com,o=myCompany.com`, the resulting renamed DN is `uid=userid,ou=people,dc=com`, and not `uid=userid,ou=people,o=myCompany.com,dc=com`.

6520368 The JDBC connection configuration to access Oracle 9 through Directory Proxy Server is not exactly as described in the documentation.

Consider the following configuration, with an Oracle 9 server listening on host `myhost`, port 1537 with the instance having system identifier (SID) `MYINST`. The instance has a database `MYNAME.MYTABLE`.

Typically, to configure access through to `MYTABLE`, set the following properties.

- On the JDBC data source, set `db-name:MYINST`.
- On the JDBC data source, set `db-url:jdbc:oracle:thin:myhost:1537:`.
- On the JDBC table, set `sql-table:MYNAME.MYTABLE`

If these settings do not work, configure access through to `MYTABLE` with the following settings.

- On the JDBC data source, set `db-name:(CONNECT_DATA=(SERVICE_NAME=MYINST)))`
- On the JDBC data source, set `db-url:jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=myhost)(PORT=1537)))`
- On the JDBC table, set `sql-table:MYNAME.MYTABLE`

6542857 When you use the Service Management Facility (SMF) on Solaris 10 to enable a server instance, the instance might not start when you reboot the system and return the following error:

```
svcadm: Instance "svc:/instance_path" is in maintenance state.
```

To work around this problem, use a local user to create Directory Server and Directory Proxy Server servers.

6547759 On HP-UX, if you access DSCC with multiple browser sessions set to different locales, DSCC might display some strings in a locale that is different from the locale set in the browser.

6551076 Console does not retrieve the backend status of the Directory Proxy Server instance if a machine has multiple host names.

6573439 In DSCC, in the More View Options of an instance, the date shown under the Access Logs, Error Logs, and Audit Logs tabs is not localized.

6583798 In DSCC 6.0, `useTCPNoDelay` is set to `false` by default when creating a data source with DSCC, while the default value of `use-tcp-no-delay` is set to `true` when creating instance through the administrative command `dpconf create-ldap-data-source`.

6588319 In DSCC configured using Tomcat server, the title of the Help and Version pop-up windows displays the multi-byte strings garbled.

6590460 The string `owner` in the output of the `dpadm show-cert` *dps-instance-path* command is not translated in Simplified Chinese and Traditional Chinese.

6639674 If the Directory Proxy Server configuration property `allow-bind-operations` is set to `false`, it is not possible to connect on an SSL port using the `dpconf` command line argument with the `--secure-port` option. Connection by Start TLS (default) or by clear connection (the `--unsecured` option) are still possible.

6640597 Directory Proxy Server does not change the DN of an ADD operation when the operation follows a referral in which the `basedn` is different from that of the original machine. Attempting an ADD against a Directory Proxy Server instance that has a Directory Server instance that is set to follow referrals, as opposed to just forwarding referrals, results in the ADD being rejected on the referred server because of an incorrect `basedn`.

Using the `ldapmodify` command to executing the ADD directly against the Directory Server instances allows the ADD to work.

6649984 No warning is issued when you set a password of insufficient length for the certificate database. If the password is too short, it is accepted by the Directory Service Control Center. Issuing the `dpadm` command with `cert` subcommands can then result in the commands hanging.

6723858 The proxy server bypasses the `requires-bind-password` property on the backend directory server.

6757756 The `dpadm list-running-instances` command does not list all the instances that are started from the current installation but lists the only instances that belong to the current user.

6791946 On OpenSolaris, when alerts are raised, Directory Proxy Server does not log them in syslog.

6874624 An obsolete definition remains in the `28pilot.ldif` file.

To work around this issue, add the following alias specification to the `28pilot.ldif` file:

```
objectClasses: ( 0.9.2342.19200300.100.4.4 NAME ('newPilotPerson' 'pilotPerson') DESC <...>)
```

6874631 The `uidObject` objectclass is missing from the schema.

To work around this issue, add the following objectclass to the `00core.ldif` file:

```
objectClasses: ( 1.3.6.1.1.3.1 NAME 'uidObject' SUP top AUXILIARY MUST uid X-ORIGIN 'RFC 4519')
```

6889439 Directory Proxy Server reports a schema violation on attributes `timeResolutionMode` and `timeResolutionInMillisec`.

This message is harmless. To work around it, use the following steps:

1. Make sure that you have access to the jar program. This program is shipped with any JDK installation.
2. Stop the Directory Proxy Server instance.
3. Change the current directory to the Directory Server installation directory.
4. Run the following command to extract the schema file from the Directory Proxy Server archive

```
$ jar xvf dsee7/lib/jar/dps.jar com/sun/directory/proxy/config/config_schema.ldif
```

5. Use a text editor to edit the schema file, `com/sun/directory/proxy/config/config_schema.ldif` and make these changes.
   a. Delete the attribute `attributeTypes` containing the string `NAME ( 'useNanoTimeforEtimes' )`.
   b. Add a new attribute `attributeTypes` with the following content:

      ```
      attributeTypes: ( "" NAME ( 'timeResolutionInMilliSec' ) DESC '' \
      SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE X-ORIGIN 'DPS' )
      ```

      Make sure to delimit parentheses with spaces.
   c. Search for the attribute `objectClasses` containing the string `NAME 'topConfigEntry'`.
   d. In this attribute line, search for the string `useNanoTimeforEtimes` and rename it as `timeResolutionMode`
   e. Save the file and close it.

6. Run the following command to apply the changes done to the schema file to the Directory Proxy Server archive:

```
$ jar uvf dsee7/lib/jar/dps.jar com/sun/directory/proxy/config/config_schema.ldif
```

6899299 On Windows Server 2008, if the server instance is setup to start at boot by using the `dpadm enable-service` command, the `dpadm info` command displays the status of the instance as Stopped. In that case, the instance cannot be stopped or restarted using the `dpadm` command or DSCC.

Use Windows Service manager to enable the server instance to start when the Windows server machine starts up.

◆ ◆ ◆ CHAPTER 6

Identity Synchronization for Windows Bugs Fixed and Known Problems

This chapter contains product-specific information available at the time of release of Identity Synchronization for Windows.

This chapter includes "Known Problems and Limitations in Identity Synchronization for Windows" on page 75:

Known Problems and Limitations in Identity Synchronization for Windows

This section lists known problems and limitations at the time of release.

Identity Synchronization for Windows Limitations

This section lists product limitations. Limitations are not always associated with a change request number.

Identity Synchronization for Windows requires `sun-sasl-2.19-4.i386.rpm` to install successfully.

On Linux, before installing Identity Synchronization for Windows, make sure that the `sun-sasl-2.19-4.i386.rpm` package is installed on your system. Otherwise the Identity Synchronization for Windows installation would fail. You can get the SASL package from the shared components of the JES 5 distribution or later.

Do not change file permissions by hand.

Changes to file permissions for installed Directory Server Enterprise Edition product files can in some cases prevent the software from operating properly.

To workaround this limitation, install products as a user having appropriate user and group permissions.

No failover for the Identity Synchronization for Windows core service.

If you loose the system where Identity Synchronization for Windows core services are installed, you need to install it again. There is no failover for the Identity Synchronization for Windows core service.

Take a backup of `ou=services` (configuration branch of Identity Synchronization for Windows DIT) in LDIF format and use this information while reinstalling Identity Synchronization for Windows.

Change in authentication behavior on Microsoft Windows 2003 SP1.

When you install Windows 2003 SP1, by default users are allowed one hour to access their accounts using their old passwords.

As a result, when users change their passwords on Active Directory, the on-demand sync attribute `dspswvalidate` is set to true, and the old password can be used to authenticate against Directory Server. The password synchronized on Directory Server is then the prior, old password, rather than the current Active Directory password.

See the Microsoft Windows support documentation (`http://support.microsoft.com/?kbid=906305`) for details on how to turn off this functionality.

Remove `serverroot.conf` before you remove Administration Server

To uninstall Administration Server, remove `/etc/mps/admin/v5.2/shared/config/serverroot.conf` before you remove the Administration Server package.

Mention the admin jars path in `CLASSPATH`

`CLASSPATH` should contain the location of the admin jars, otherwise a `noClassDefFound` error is displayed during resynchronization.

Configure PSO password policy settings to match Directory Server Enterprise Edition

Active Directory 2003 and earlier versions use global policy objects (GPO), which are global and domain-wide. Consequently, the password policy and account lockout settings are global in nature. However, as of Active Directory 2008 (or 2008 R2), domain-level, fine-grained password setting objects (PSO) can be applied to individual users or groups. Identity Synchronization for Windows requires the password policy and account lockout settings to be uniform between Active Directory and Directory Server Enterprise Edition Make sure that the account lockout settings defined for the PSO match with the Directory Server Enterprise Edition account lockout policy for a particular user or group. Specifically, make sure that the following PSO attributes match the settings in Directory Server Enterprise Edition:

`msDS-LockoutThreshold`	Specifies how many failed password attempts are allowed before locking out user account
`msDS-LockoutDuration`	Specifies how long the account is locked out after too many failed password attempts

If Active Directory is set to return referrals, on-demand synchronization can require a long period of time and return an `UNWILLING TO PERFORM` error message. As a workaround, use the `ldapmodify` command to apply the following change to the directory server where the Identity Synchronization for Windows plug-in is running.

```
dn: cn=config,cn=pwsync,cn=config
changetype: modify
add: followreferrals
followreferrals: FALSE
```

No support for read-only domain controllers

Identity Synchronization for Windows requires a writable domain controller for synchronizing user creation and modification. It does not support a read-only controller.

Group synchronization fails if attribute mapping, creation expression, and RDN attribute are not specified as recommended.

You must set attribute mapping, creation expression, and RDN attribute as mentioned below:

- The attribute mapping between Sun Directory Server and Active Directory must be defined as mentioned below:

  ```
  DS    < -----  >  AD
  cn                cn
  uid               samaccountname
  ```

- The creation expression must be defined as mentioned below:

  ```
  for DS: uid=%uid%,<sync_base>
  for AD: cn=%cn%,<sync_base>
  ```

- For Sun Directory Server users, the `RDN` attribute that belongs to synchronized groups must be `uid`.

Behavior to update an attribute concurrently is undefined.

In group synchronization, the concurrent modifications of an attribute of an entry is not defined.

Performing Data Recovery When System or Application Fails

After hardware or application failure, you might have to restore the data from backup in some of the synchronized directory sources.

After completing the data recovery, however, you must perform an additional procedure to ensure that the synchronization can proceed normally.

The connectors generally maintain information about the last change that was propagated to the message queue.

This information, which is called the connector state, is used to determine the subsequent change that the connector has to read from its directory source. If the database of a synchronized directory source is restored from a backup, then the connector state might no longer be valid.

Windows-based connectors for Active Directory and for Windows NT also maintain an internal database. The database is a copy of the synchronized data source. The database is used to determine what has changed in the connected data source. The internal database is no longer be valid once the connected Windows source is restored from a backup.

In general, the `idsync resync` command can be used to repopulate the recovered data source.

Note – Resynchronization cannot be used to synchronize passwords with one exception. The `-i ALL_USERS` option can be used to invalidate passwords in Directory Server. This works if the resynchronization data source is Windows. The SUL list must also include only Active Directory systems.

Use of the `idsync resync` command, however, might not be an acceptable option in every situation.

Caution – Before executing any of the steps detailed that follow, make sure that synchronization is stopped.

Bidirectional Synchronization

Use the `idsync resync` command with the appropriate modifier settings, according to the synchronization settings. Use the recovered directory source as the target of the `resync` operation.

Unidirectional Synchronization

If recovered data source is a synchronization destination, then the same procedure can be followed as for bidirectional synchronization.

If recovered data source is a synchronization source, then `idsync resync` can still be used to repopulate the recovered directory source. You need not change the synchronization flow settings in the Identity Synchronization for Windows configuration. The `idsync resync` command allows you to set synchronization flow independent of the configured flows with the `-o Windows|Sun` option.

Consider the following scenario as an example.

Bidirectional synchronization is setup between Directory Server and Active Directory.

- The database of a Microsoft Active Directory server has to be recovered from a backup.

- In Identity Synchronization for Windows, this Active Directory Source is configured for the SUL `AD`.
- Bidirectional synchronization for modifies, creates and deletes is setup between this Active Directory Source and a Sun Directory Server Source.

▼ To Perform Unidirectional Synchronization

1. **Stop synchronization.**

   ```
   idsync stopsync -w - -q -
   ```

2. **Resynchronize Active Directory Source. Also, resynchronize modifies, creations, and deletes.**

   ```
   idsync resync -c -x -o Sun -l AD -w - -q -
   ```

3. **Restart synchronization.**

   ```
   idsync startsync -w - -q -
   ```

Directory Source Specific Recovery Procedures

The following procedures correspond to specific directory sources.

Microsoft Active Directory

If Active Directory can be restored from a backup, then follow the procedures in the sections covering either bidirectional, or unidirectional synchronization.

You might, however, have to use a different domain controller after a critical failure. In this case, follow these steps to update the configuration of the Active Directory Connector.

▼ To Change the Domain Controller

1. **Start the Identity Synchronization for Windows management console.**
2. **Select the Configuration tab. Expand the Directory Sources node.**
3. **Select the appropriate Active Directory Source.**
4. **Click Edit controller, and then select the new domain controller.**

   Make the selected domain controller the NT PDC FSMO role owner of the domain
5. **Save the configuration.**
6. **Stop the `Identity Synchronization` service on the host where the Active Directory Connector is running.**

7 **Delete all the files except the directories, under** *ServerRoot*`/isw-`*hostname*`/persist/ADP`*xxx*. **Here,** *xxx* **is the number portion of the Active Directory Connector identifier.**

For example, `100` if the Active Directory Connector identifier is `CNN100`.

8 **Start the** `Identity Synchronization` **service on the host where the Active Directory Connector is running.**

9 **Follow the steps according to your synchronization flow in the unidirectional or the bidirectional synchronization sections.**

Fail Over and Directory Server

Either the Retro Changelog database, or the database with synchronized users, or both can be affected by a critical failure.

▼ To Manage Directory Server Fail Over

1 **Retro Changelog Database.**

Changes that the Directory Server connector could not process might have occurred in the Retro Changelog database. Restoration of the Retro Changelog database only makes sense if the backup contains some unprocessed changes. Compare the most recent entry in the *ServerRoot*`/isw-`*hostname*`/persist/ADP`*xxx*`/accessor.state` file with the last `changenumber` in the backup. If the value in `accessor.state` is greater than or equal to the `changenumber` in the backup, do not restore the database. Instead, recreate the database.

After the Retro Changelog database is recreated, make sure that you run `idsync prepds`. Alternatively, click Prepare Directory Server from the Sun Directory Source window in the Identity Synchronization for Windows management console.

The Directory Server connector detects that the Retro Changelog database is recreated and log a warning message. You can safely ignore this message.

2 **Synchronized Database.**

If no backup is available for the synchronized database, then the Directory Server connector has to be reinstalled.

If the synchronized database can be restored from a backup, then follow the procedures in either the bidirectional or the unidirectional synchronization sections.

Known Identity Synchronization for Windows 6.0 Issues

This section lists known issues. Known issues are associated with a change request number.

4997513 On Windows 2003 systems, the flag that indicates the user must change his password at the next login is set by default. On Windows 2000 systems, the flag is not set by default.

When you create users on Windows 2000 and 2003 systems with the `user must change pw at next login` flag set, users are created on Directory Server with no password. The next time the users log into Active Directory, the users must change their passwords. The change invalidates their passwords on Directory Server. The change also forces on-demand synchronization the next time those users authenticate to Directory Server.

Until users change their password on Active Directory, users are not able to authenticate to Directory Server.

5077227 Problems can occur when attempting to view the Identity Synchronization for Windows console with PC Anywhere 10 with Remote Administration 2.1. PC Anywhere version 9.2 has been seen not to cause errors. If problems persist, remove the remote administration software. Alternatively, VNC can be used. VNC is not known to cause any issues when displaying the Identity Synchronization for Windows console.

5097751 If you install Identity Synchronization for Windows on a Windows system that is formatted with FAT 32 system, then no ACLs are available. Furthermore, no access restrictions are enforced for the setup. To ensure security, use only Windows NTFS system to install Identity Synchronization for Windows.

6251334 User deletion synchronization cannot be stopped even after changing the Active Directory source. Deletion synchronization therefore continues when the Synchronized Users List has been mapped to a different organizational unit, `OU`, in the same Active Directory Source. The user appears to have been deleted on the Directory Server instance. The user appears as deleted even if the user is deleted from the Active Directory source which does not have a SUL mapping.

6254516 When Directory Server plug-in is configured on the consumers with command-line, the plug-in does not create a new subcomponent ID for the consumers. The plug-in configuration does not create new IDs for consumers.

6288169 The password synchronization plug-in for Identity Synchronization for Windows tries to bind to the Active Directory for accounts that have not been synchronized even before checking the `accountlock` and `passwordRetryCount`.

To resolve this issue, enforce a password policy on the LDAP server. Also, configure Access Manager to use the following filter on user search:

```
(| ( !(passwordRetryCount=*) ) (passwordRetryCount <=2) )
```

This workaround, however, throws a user not found error when too many login attempts are made over LDAP. The workaround does not block the Active Directory account.

6331956 Identity Synchronization for Windows console fails to start if `o=NetscapeRoot` is replicated.

6332183 Identity Synchronization for Windows might log exceptions stating that a user already exists, if the Add action flows from Directory Server to the Active Directory before the Delete can. A race condition might occur where the add operation is performed before the delete operation during synchronization, thus cause Active Directory to log an exception.

For example, if a user, `dn: user1, ou=isw_data`, is added to an existing group, `dn: DSGroup1,ou=isw_data`, when the user is deleted from the group, the `uniquemember` of the group is modified. If the same user is added to a group that has the same DN, (for `userdn: user1, ou=isw_data`), an Add operation is performed. At this point, Identity Synchronization for Windows might log exceptions stating that the user already exists.

6332197 Identity Synchronization for Windows throws errors when groups, with user information of users not yet created, are synchronized on Directory Server.

6335193 You might try to run the resynchronization command to synchronize users from Directory Server to Active Directory. The creation of the group entity fails if unsynchronized users are added to an unsynchronized group.

To resolve this issue, you should run the `resync` command twice for the synchronization to happen correctly.

6336471 Identity Synchronization for Windows plug-in cannot search through chained suffixes. As a result, the modify and bind operations cannot be performed on the Directory Server instance.

6337018 Identity Synchronization for Windows should support exporting the Identity Synchronization for Windows Configuration to an XML file.

6339444 You can specify the scope of synchronization with the Synchronization Users List using the Browse button on the Base DN pane. When you specify the scope, the subsuffixes are not retrieved.

To work around this issue, add ACIs to permit anonymous access for reads and searches.

6379804 During the upgrade of core components of Identity Synchronization for Windows to version 1.1 SP1 on Windows systems, the `updateCore.bat` file contains a hard-coded incorrect reference to Administration Server. As a result, the upgrade process does not complete successfully.

To resolve this problem, replace two instances of references to Administration Server in the upgrade script.

Replace the following instructions on lines 51 and 95 of the upgrade script. Change lines as follows.

```
net stop "Sun Java(TM) System Administration Server 5.2"
```

Instead, the lines should read as follows:

```
net stop admin52-serv
```

After making the specified changes, rerun the upgrade script.

6386664 Identity Synchronization for Windows synchronizes user and group information between Active Directory and Directory Server when group synchronization feature is enabled. The synchronization should ideally happen only after issuing the `resync` command from the command line.

6388815 Active Directory connectors and Directory Server connectors crash when an attempt is made to synchronize nested groups as such synchronization is not currently supported.

6388872 For Windows Creation Expressions in a Directory Server to Active Directory, the flow `cn=%cn%` works both for users and groups. For every other combination, Identity Synchronization for Windows shows errors during synchronization.

6444341 The Identity Synchronization for Windows uninstallation program is not localized. `WPSyncResources_`*X*`.properties` files fail to be installed in the `/opt/sun/isw/locale/resources` directory.

To work around this issue, copy the missing `WPSyncResources_`*X*`.properties` files from the `installer/locale/resources` directory by hand.

6444878 Install and set up Java Development Kit version 1.5.0_06 before running Administration Server.

6444896 When performing a text-based installation of Identity Synchronization for Windows, leaving the administrator password empty and typing return causes the installation program to exit.

6452425 If you install Identity Synchronization for Windows on a Solaris system where the `SUNWtls` package version 3.11.0 is installed, the Administration Server might not launch. To resolve this, uninstall the `SUNWtls` package before you install Identity Synchronization for Windows.

6452538 On Windows platforms, Message Queue 3.5 used by Identity Synchronization for Windows requires a `PATH` value less than 1 kilobyte in length. Longer values are truncated.

6472296 After installation in the Japanese locale on Windows systems, Identity Synchronization for Windows user interfaces are not fully localized.

To work around this issue, include `unzip.exe` in the `PATH` environment variable before starting the installation.

6477567 In Directory Server Enterprise Edition 7.0, the Directory Server plug-in for Identity Synchronization for Windows is installed with Directory Server installation. The Identity Synchronization for Windows installer does not install the Directory Server plug-in. Instead Identity Synchronization for Windows only configures the plug-in.

In this release of Identity Synchronization for Windows, the text-based installer does not prompt you to configure the Directory Server plug-in for Identity Synchronization for Windows during the installation process. As a workaround, run the `Idsync dspluginconfig` command in the terminal window after the Identity Synchronization for Windows installation is completed.

6485333 The installer and uninstaller on Windows systems are not internationalized.

6486505 On Windows, Identity Synchronization for Windows supports only English and Japanese locales.

6492125 The Identity Synchronization for Windows online help contents displays square boxes instead of multi-byte characters for CCK locales.

6501874 Account lockout synchronization fails from Directory Server to Active Directory when Directory Server password compatibility mode, `pwd-compat-mode`, is set to `DS6-migration-mode`, or `DS6-mode`.

6501886 When the Active Directory domain administrator password changes, the Identity Synchronization for Windows Console has been seen to show a warning. The warning shown is `Invalid credentials for Host-`*`hostname.domainnname`*, even when the password used is valid.

6529349 On Solaris SPARC, Identity Synchronization for Windows might not uninstall due to the absence of the `/usr/share/lib/mps//jss4.jar` file. It happens only during the installation of the product, when the installer detects the already installed instance of the `SUNWjss` package and does not update it.

As a workaround, while installing the product, add `/usr/share/lib/mps/secv1/jss4.jar` in the Java class path.

```
$JAVA_EXEC -Djava.library.path=./lib \
-classpath "${SUNWjss}/usr/share/lib/mps/secv1/jss4.jar:\
${SUNWjss}/usr/share/lib/mps/jss4.jar:\
${SUNWxrcsj}/sfw/share/lib/xerces-200.jar:./lib/installsdk.jar:\
./lib/ldap.jar:./lib/webstart.jar:\
${SUNWiquc}/usr/share/lib/jms.jar:.:./lib/install.jar:\
```

```
./resources:./locale/resources:./lib/common.jar:\
./lib/registry.jar:./lib/ldapjdk.jar:./installer/registry/resources" \
-Djava.util.logging.config.file=./resources/Log.properties \
-Djava.util.logging.config.file=../resources/Log.properties \
-Dcom.sun.directory.wps.logging.redirectStderr=false \
-Dcom.sun.directory.wps.logging.redirectStdout=false \
uninstall_ISW_Installer $1
```

6544353 Identity Synchronization for Windows does not support the Force new password at first login request made by an administration while resetting the password on Windows operating system.

6572575 For the group synchronization to work successfully during `resync`, both the user and group should reside at the same level in the synchronization scope. Otherwise, it displays an error.

6594767 On machines running Microsoft Windows, with a domain controller installed, authentication fails while creating new server or registering an existing server with Webconsole. As a workaround, specify the userID with the domain name for the domain controller.

6691600 Linking users from Directory Server to Active Directory or from Active Directory to Directory Server fails if any of the Directory Server entries contains an auxiliary objectclass.

To resolve this issue, add all the auxiliary objectclasses in the Auxiliary objectclass in the Identity Synchronization for Windows console.

6709099 The `idsync dspluginconfig` subcommand fails to configure the plugin on the new Directory Server source. If `idsync dspluginconfig` is used in the uninstall mode, it removes the `SUBC` value of the active Identity Synchronization for Windows configuration server.

6721443 If debug log is enabled, the connector quits unexpectedly and displays the `NullPointerException & ArrayIndexOutOfBoundsException` exception.

To resolve this issue, disable the debug logging.

6725352 While getting the Synthetic boolean value from the Controller OutTask, the connector quits unexpectedly

6728359 Group synchronization from Directory Server to Active Directory partially fails if the number of members are more than `1000`. The group synchronization operation synchronizes only the first `1000` members and discards rest of them.

6728372 Group synchronization from Directory Server to Active Directory fails, if the user entries that belong to a group are not present at sync base level.

For example, if your sync base is `ou=employees,dc=example,dc=com` then the user `dn` must be `uid=user-1,ou=employees,dc=example,dc=com`. Group synchronization fails if the user `dn` is of the form `uid=user-1,ou=sales,ou=employees,dc=example,dc=com`. In this example, the `ou=sales` container between user and sync base causes the group synchronization to fail.

6740714 The object cache rejects the changes that are requested on a group that contains `1500` or more members.

6740715 The resync operation fails for group entries, if it encounters wrong `RDN` member value.

6744089 The member conversion from Directory Server to Active Directory fails if the member changes are not logged first in the retro changelog.

6749286 While synchronizing large static group, the Directory Server connector wrongly puts debug log entries in the audit log.

6749294 The connection between Active Directory and Active Directory connector times out during the synchronization of large static group, which causes the synchronization operation to fail.

6749923 The resync operation from Directory Server to Active Directory always creates the Domain Global Security group even if the group type is configured as Domain Global Distribution.

6758690 The synchronization of attributes with empty value fails. It happens because Active Directory does not accept the empty values while the LDAP server accepts the empty values.

6762863 In a non-English locale, the group flow from Directory Server to Active Directory is always shown as Domain Global Security irrespective of the group flow configuration.

6773492 Identity Synchronization for Windows connector restarts repeatedly if it cannot parse the retro-changelog entry successfully.

6793036 Group synchronization from Active Directory to Directory Server fails if DIT root is set as a synchronization root.

6796659 The `idsync resync` stops responding when group synchronization is enabled and synchronization base is high in DIT.

6854004 When dealing with RCL entries, the Directory Server connector might stop responding.

6862596 After applying the `125359-08` patch, the Identity Synchronization for Windows administration console does not work as expected.

6862663 If the `119214-19` patch is installed prior to the Identity Synchronization for Windows core, the `dsadm` command stops working.

◆ ◆ ◆ CHAPTER 7

Directory Server Resource Kit Bugs Fixed and Known Problems

This chapter contains important, product-specific information available at the time of release of Directory Server Resource Kit.

This chapter includes the following sections:

Bugs Fixed in Directory Server Resource Kit

This section lists the bug fixed since the last release of Directory Server Resource Kit.

6565893 The `idsktune` command does not support SuSE Enterprise Linux 10.

Known Problems and Limitations in Directory Server Resource Kit

This section lists known problems and limitations at the time of release.

5081543 `searchrate` crashes on Windows systems when using multiple threads.

5081546 `modrate` crashes on Windows systems when using multiple threads.

5081549 `authrate` crashes on Windows systems when using multiple threads.

5082507 The `dsmlsearch` command `-D` option takes an HTTP user ID rather than a bind DN.

To work around this issue, provide the user ID that is mapped to a DN in Directory Server.

6379087 NameFinder has been seen to fail to deploy in Sun Java System Application Server on Windows systems.

6393554 NameFinder has been seen to throw a page not found error after deployment.

To work around this issue, rename `nsDSRK/nf` to `nsDSRK/NF`.

6393586 Cannot add more than two users to My Selections list in NameFinder.

6393596 NameFinder search should fetch entries for values other than Last Name, First Name, Email, and Given Name.

6393599 NameFinder search should allow searches for groups.

6576045 Killing `modrate` and `searchrate` launcher does not kill actual `modrate` and `searchrate` processes respectively.

6754994 The `idsktune` command reports system limits incorrectly with `getrlimit()`. The following warning messages appear:

```
WARNING: processes are limited by RLIMIT_DATA to 2047 MB in size.
WARNING: processes are limited by RLIMIT_VMEM to 2047 MB in size.
WARNING: processes are limited by RLIMIT_AS to 2047 MB in size.
```