Sun Java System Directory Server Enterprise Edition 6.3.1 Release Notes

Part No: 820–5817
May 2010

100713@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 1, "Compatibility Issues," addresses compatibility with previous component product versions, and with potential upcoming changes to Directory Server Enterprise Edition software.

Chapter 2, "Installation Notes," covers topics related to installation, including hardware and software requirements.

Chapter 3, "Directory Server Bugs Fixed and Known Problems," covers fixes and issues for Directory Server.

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

Chapter 5, "Identity Synchronization for Windows Bugs Fixed and Known Problems," covers fixes and issues for Identity Synchronization for Windows.

Chapter 6, "Directory Editor Bugs Fixed and Known Problems," covers fixes and issues for Directory Editor.

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.

Directory Server Enterprise Edition Documentation Set

This Directory Server Enterprise Edition documentation set explains how to use Sun Java System Directory Server Enterprise Edition to evaluate, design, deploy, and administer directory services. In addition, it shows how to develop client applications for Directory Server Enterprise Edition. The Directory Server Enterprise Edition documentation set is available at *Sun Java System Directory Server Enterprise Edition 6.3 Documentation Center*.

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

TABLE P–1 Directory Server Enterprise Edition Documentation

Document Title	Contents
Sun Java System Directory Server Enterprise Edition 6.3.1 Release Notes	Contains the latest information about Directory Server Enterprise Edition, including known problems.
Sun Java System Directory Server Enterprise Edition 6.3 Release Notes	Contains information about installing Identity Synchronization for Windows, Directory Editor, and Directory Server Resource Kit.
Sun Java System Directory Server Enterprise Edition 7.0 Documentation Center	Contains links to key areas of the documentation set.
Sun Java System Directory Server Enterprise Edition 6.3 Evaluation Guide	Introduces the key features of this release. Demonstrates how these features work and what they offer in the context of a fictional deployment that you can implement on a single system.
Sun Java System Directory Server Enterprise Edition 6.3 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 Java System Directory Server Enterprise Edition 6.3 Installation Guide	**Note –** To install Directory Server Enterprise Edition 6.3.1, use the instructions in Chapter 2, “Installation Notes,” of these release notes. Do not attempt to use the installation instructions in *Sun Java System Directory Server Enterprise Edition 6.3 Installation Guide* to install version 6.3.1. Explains how to install the Directory Server Enterprise Edition 6.3 software. Shows how to select which components to install, configure those components after installation, and verify that the configured components function properly. For instructions on installing Directory Editor, go to `http://docs.sun.com/coll/DirEdit_05q1` collection. Make sure you read the information in *Sun Java System Directory Server Enterprise Edition 6.3.1 Release Notes* concerning Directory Editor before you install Directory Editor.
Sun Java System Directory Server Enterprise Edition 6.3 Migration Guide	Provides migration instructions from the earlier versions of Directory Server, Directory Proxy Server, and Identity Synchronization for Windows.

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

Document Title	Contents
Sun Java System Directory Server Enterprise Edition 6.3 Administration Guide	Provides command-line instructions for administering Directory Server Enterprise Edition. For hints and instructions on using the Directory Service Control Center, DSCC, to administer Directory Server Enterprise Edition, see the online help provided in DSCC. For instructions on administering Directory Editor, go to `http://docs.sun.com/coll/DirEdit_05q1`. For instructions on installing and configuring Identity Synchronization for Windows, see Part II, "Installing Identity Synchronization for Windows," in *Sun Java System Directory Server Enterprise Edition 6.3 Installation Guide*.
Sun Java System Directory Server Enterprise Edition 6.3 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 Java System Directory Server Enterprise Edition 6.3 Reference	Introduces the technical and conceptual foundations of Directory Server Enterprise Edition. Describes its components, architecture, processes, and features. Also provides a reference to the developer APIs.
Sun Java System Directory Server Enterprise Edition 6.3 Man Page Reference	Describes the command-line tools, schema objects, and other public interfaces that are available through Directory Server Enterprise Edition. Individual sections of this document can be installed as online manual pages.
Sun Java System Directory Server Enterprise Edition 6.3 Troubleshooting Guide	Provides information for defining the scope of the problem, gathering data, and troubleshooting the problem areas 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. The Identity Synchronization for Windows product is still at version 6.0.

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. It was originally developed by Sun Microsystems, Inc. to benchmark and analyze the performance of LDAP directory servers. SLAMD is available as an open source application under the Sun Public License, an OSI-approved open source license. To obtain information about SLAMD, go to `http://www.slamd.com/`. SLAMD is also available as a java.net project. See `https://slamd.dev.java.net/`.

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

Directory Server Enterprise Edition can be licensed as a standalone product, as a component of Sun Java Enterprise System, as part of a suite of Sun products, such as the Sun Java Identity Management Suite, or as an add-on package to other software products from Sun. Java Enterprise System is a software infrastructure that supports enterprise applications distributed across a network or Internet environment. If Directory Server Enterprise Edition was licensed as a component of Java Enterprise System, you should be familiar with the system documentation at `http://docs.sun.com/coll/1286.3`.

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 the documentation, and gives the locations of commands on different operating systems and deployment types.

Default Paths

The table in this section describes the default paths that are used in this document. For complete descriptions of the files installed, see the following product documentation.

- Chapter 14, “Directory Server File Reference,” in *Sun Java System Directory Server Enterprise Edition 6.3 Reference*
- Chapter 25, “Directory Proxy Server File Reference,” in *Sun Java System Directory Server Enterprise Edition 6.3 Reference*

TABLE P–2 Default Paths

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

Command Locations

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

TABLE P–3 Command Locations

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

TABLE P–3 Command Locations *(Continued)*

Command	Java ES, Native Package Distribution	Zip Distribution
certutil	Solaris - /usr/sfw/bin/certutil Red Hat - /opt/sun/private/bin/certutil	*install-path*/dsee6/bin/certutil
dpadm(1M)	*install-path*/dps6/bin/dpadm	*install-path*/dps6/bin/dpadm
dpconf(1M)	*install-path*/dps6/bin/dpconf	*install-path*/dps6/bin/dpconf
dsadm(1M)	*install-path*/ds6/bin/dsadm	*install-path*/ds6/bin/dsadm
dsccmon(1M)	*install-path*/dscc6/bin/dsccmon	*install-path*/dscc6/bin/dsccmon
dsccreg(1M)	*install-path*/dscc6/bin/dsccreg	*install-path*/dscc6/bin/dsccreg
dsccsetup(1M)	*install-path*/dscc6/bin/dsccsetup	*install-path*/dscc6/bin/dsccsetup
dsconf(1M)	*install-path*/ds6/bin/dsconf	*install-path*/ds6/bin/dsconf
dsee_deploy(1M)	Not provided	*install-path*/dsee6/bin/dsee_deploy
dsmig(1M)	*install-path*/ds6/bin/dsmig	*install-path*/ds6/bin/dsmig
entrycmp(1)	*install-path*/ds6/bin/entrycmp	*install-path*/ds6/bin/entrycmp
fildif(1)	*install-path*/ds6/bin/fildif	*install-path*/ds6/bin/fildif
idsktune(1M)	Not provided	At the root of the unzipped zip distribution
insync(1)	*install-path*/ds6/bin/insync	*install-path*/ds6/bin/insync
ns-accountstatus(1M)	*install-path*/ds6/bin/ns-accountstatus	*install-path*/ds6/bin/ns-accountstatus
ns-activate(1M)	*install-path*/ds6/bin/ns-activate	*install-path*/ds6/bin/ns-activate
ns-inactivate(1M)	*install-path*/ds6/bin/ns-inactivate	*install-path*/ds6/bin/ns-inactivate
repldisc(1)	*install-path*/ds6/bin/repldisc	*install-path*/ds6/bin/repldisc
schema_push(1M)	*install-path*/ds6/bin/schema_push	*install-path*/ds6/bin/schema_push
smcwebserver	Solaris, Linux - /usr/sbin/smcwebserver Windows - *install-path*\share\webconsole\bin\smcwebserver	This command pertains only to DSCC when it is installed using native packages distribution.

TABLE P–3 Command Locations *(Continued)*

Command	Java ES, Native Package Distribution	Zip Distribution
`wcadmin`	Solaris, Linux - `/usr/sbin/wcadmin`	This command pertains only to DSCC when it is installed using native packages distribution.
	Windows - *install-path*`\share\webconsole\bin\wcadmin`	

Typographic Conventions

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

TABLE P–4 Typographic Conventions

Typeface	Meaning	Example
`AaBbCc123`	The names of commands, files, and directories, and onscreen computer output	Edit your `.login` file. Use `ls -a` to list all files. `machine_name% you have mail.`

`AaBbCc123`	What you type, contrasted with onscreen computer output	`machine_name%` **`su`**
		`Password:`

AaBbCc123	A placeholder to be replaced with a real name or value	The command to remove a file is `rm` *filename*.
AaBbCc123	Book titles, new terms, and terms to be emphasized (note that some emphasized items appear bold online)	Read Chapter 6 in the *User's Guide*. A *cache* is a copy that is stored locally. Do *not* save the file.

Shell Prompts in Command Examples

The following table shows default system prompts and superuser prompts.

TABLE P–5 Shell Prompts

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

TABLE P–5 Shell Prompts *(Continued)*

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

Symbol Conventions

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

TABLE P–6 Symbol Conventions

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

Revision History

The following table describes the changes in versions of this document.

TABLE P–7 Revision History

Date	Description of Changes
February 2009	Initial release
December 2009	Primarily the Directory Proxy Server 6.3.1 update 1 patch that corrects issues in the Directory Proxy Server component of Directory Server Enterprise Edition 6.3.1, known issues and possible workarounds in Directory Server, and known issues and possible workarounds in Identity Synchronization for Windows.

TABLE P–7 Revision History *(Continued)*

Date	Description of Changes
May 2010	Updated information about installing security patches 142807–02 and 143463–01

CHAPTER 1

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 Java System Directory Server Enterprise Edition 6.3 Man Page Reference*.

Platform Support

In future releases of Directory Server Enterprise Edition, support for Windows 2000, Red Hat Advanced Server 3.0, and J2SE platform 1.4 may be removed. Support for the native install package releases for platforms other than the Solaris operating system might be removed. Support for 32–bit versions of the software might be discontinued for some platforms. To be prepared, plan the transition to 64–bit versions of the software and to newer versions of the supported operating systems. See "Operating System Requirements" on page 27 for details of the newer versions of supported operating systems.

Directory Server Enterprise Edition 6.3.1 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*.

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 Java System products on selected system virtualization and OS combinations to help validate that the Sun Java System 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 Java System 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 6.3 software. Sun Microsystems does not certify every combination of OS and hardware, but relies on the underlying VMware technology implementation. Full deployment of the Directory Server Enterprise Edition 6.3 software on the VMware technology is not recommended.

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

For details on supported hardware platforms for this release of Directory Server Enterprise Edition, see “Hardware Requirements” on page 26.

For details on supported operating systems and OS versions for this release of Directory Server Enterprise Edition, see “Operating System Requirements” on page 27.

Directory Server Changes

The legacy command-line tools for managing Directory Server instances are deprecated.

The following tools might be removed from a future release.

- `bak2db`
- `db2bak`
- `db2ldif`
- `ldif2db`
- `restart-slapd`
- `start-slapd`
- `stop-slapd`

New command line tools, `dsadm` and `dsconf`, and other commands replace the functionality provided by the tools listed. See “Command Line Changes” in *Sun Java System Directory Server Enterprise Edition 6.3 Migration Guide* for details.

For a detailed discussion of administration related Directory Server changes, see Chapter 5, "Architectural Changes in Directory Server," in *Sun Java System Directory Server Enterprise Edition 6.3 Migration Guide*.

Before migrating a replicated server topology, review Chapter 4, "Migrating a Replicated Topology," in *Sun Java System Directory Server Enterprise Edition 6.3 Migration Guide*. Support for legacy replication with Directory Server 4 has been removed from this release. Sun Microsystems ended support for Directory Server 4 in January 2004.

Note – Migration from versions of Directory Server 5 is not supported. Directory Server 5 installations can be migrated to 6.0, 6.1, .6.2, or 6.3 and then upgraded to 6.3.1 as described in "Installation Instructions" on page 34.

When you create a Directory Server instance, password policy is configured initially backwards-compatible. After upgrading, you 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.

Also, when you create a Directory Server instance, support for the modify DN operation is disabled. After upgrade all 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.

Directory Server chaining is deprecated and might be removed in a future release. Chaining is not configurable through Directory Service Control Center, nor is chaining configurable through the new command line tools. Most deployments enabled by chaining are now enabled using features of Directory Proxy Server. For example, data distribution, global account lockout across an entire replication topology, and merging directory information trees can be done with Directory Proxy Server. For legacy applications that continue to rely on chaining, you can configure the chained suffix plug-in with the `ldapmodify` command to set attributes for chaining. The attributes are listed in `dse.ldif`(4).

Chapter 2, "Changes to the Plug-In API Since Directory Server 5.2," in *Sun Java System Directory Server Enterprise Edition 6.3 Developer's Guide* and Chapter 3, "Changes to the Plug-In API From Directory Server 4 to Directory Server 5.2," in *Sun Java System Directory Server Enterprise Edition 6.3 Developer's Guide* detail plug-in API changes. Interfaces identified there as deprecated might be removed in a future release.

Directory Proxy Server Changes

To access Directory Proxy Server 6.0, 6.1, 6.2, and 6.3 instances using the Directory Proxy Server 6.3.1 commands, no migration is required. All Directory Proxy Server 5.x instances need to be migrated before using with the Directory Proxy Server 6.3.1 commands. See Chapter 6, "Migrating Directory Proxy Server," in *Sun Java System Directory Server Enterprise Edition 6.3 Migration Guide* for details.

Identity Synchronization for Windows Changes

Directory Server Enterprise Edition 6.3.1 does not provide any changes to Identity Synchronization for Windows. Refer to the *Sun Java System Directory Server Enterprise Edition 6.3 Release Notes* for any needed information.

The Identity Synchronization for Windows product is still at version 6.0.

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

Future releases of Identity Synchronization for Windows might discontinue support for all versions and service packs of Microsoft Windows NT. Microsoft ended support for Windows NT in June 2004.

Before upgrading Identity Synchronization for Windows, read Chapter 7, "Migrating Identity Synchronization for Windows," in *Sun Java System Directory Server Enterprise Edition 6.3 Migration Guide*.

Directory Server Resource Kit Changes

Directory Server Enterprise Edition 6.3.1 does not provide any changes to Directory Server Resource Kit. See Chapter 7, "Directory Server Resource Kit Bugs Fixed and Known Problems," for further information.

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 Java System Directory Server Enterprise Edition 6.3 Man Page Reference* for the manual pages for the LDAP client tools.

Directory Editor Changes

Directory Server Enterprise Edition 6.3.1 does not provide any changes to Directory Editor. See the *Sun Java System Directory Server Enterprise Edition 6.3 Release Notes* for further information.

Directory Editor might be deprecated in a future release.

Chapter 6, "Directory Editor Bugs Fixed and Known Problems," explains more about this release of Directory Editor.

Software Support

The following Directory Server Enterprise Edition components might be deprecated in a future release:

- Agent for Sun Cluster support
- Directory Editor

The Sun Java Web Console (Lockhart) will no longer be supported for deploying the DSCC console in Directory Server Enterprise Edition 7.

◆ ◆ ◆ CHAPTER 2

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.

Caution – The Sun Java System Directory Server Enterprise Edition 6.3.1 Security Patchzip 142807-02 must be applied **on top of a Directory Server Enterprise Edition 6.3.1 ZIP** installation. For directions see "Installing Directory Server Enterprise Edition 6.3.1 Security Patchzip 142807-02" on page 48.

Caution – The Sun Java System Directory Server 6.3.1 Security Patch 143463-01 must be applied **on top of Directory Server Enterprise Edition 6.3.1** installation. For directions see "Installing Directory Server Enterprise Edition 6.3.1 Security Patch 143463-01" on page 49.

Note – Sun Directory Proxy Server 6.3.1 update 1 patch 141958–01 is designed to be applied on top of Directory Server Enterprise Edition 6.3.1 to fix issues in the Directory Proxy Server component. For more information, refer to "Directory Proxy Server 6.3.1 Update 1" on page 92.

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 Java System 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.oracle.com/support/premier/index.html`

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.

Previous Solaris licences 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`.

What's New in Directory Server Enterprise Edition 6.3.1

Directory Server Enterprise Edition 6.3.1 is a patch release that corrects issues known in the Directory Server Enterprise Edition releases 6.0 through 6.3. This release does not add new features to the Directory Server Enterprise Edition releases 6.0 through 6.3.

Getting the Software

Directory Server Enterprise Edition 6.3.1 is a maintenance release that is applied to an existing installation of Directory Server Enterprise Edition 6.0, 6.1, 6.2, or 6.3. You can download Sun Java System Directory Server Enterprise Edition 6.0, 6.1, 6.2, or 6.3 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 6.3.1 is available in the following distributions.

- Native package distribution
- Zip distribution

Directory Server Enterprise Edition 6.3.1 is available in the following forms.

- Native patch – patches to upgrade Directory Server Enterprise Edition 6.0, 6.1, 6.2, and 6.3 native packages installed using the Java ES installer.
- Zip based distribution – patches to Directory Server Enterprise Edition 6.0, 6.1, 6.2, and 6.3 zip installations.

Directory Server Enterprise Edition 6.3.1 patches are available through SunSolve (`http://sunsolve.sun.com`).For information on patch numbers, see “Installation Instructions” on page 34.

For the detailed information on what you need to install based on your current installation, refer to “Installation Instructions” on page 34.

Hardware Requirements

This section covers hardware requirements for Directory Server Enterprise Edition component products.

- "Directory Server Hardware Requirements" on page 26
- "Directory Proxy Server Hardware Requirements" on page 26

Directory Server Hardware Requirements

Directory Server software requires the following hardware.

Component	Platform Requirement
RAM	1-2 GB for evaluation purposes Minimum 2 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 Hardware Requirements

Directory Proxy Server software requires the following hardware.

Component	Platform Requirement
RAM	1-2 GB for evaluation purposes Minimum 2GB for production servers

Component	Platform Requirement
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 per server instance is sufficient to hold server logs when the default configuration is used. 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`.

Operating System Requirements

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

Directory Server, Directory Proxy Server, and Directory Server Resource Kit Operating System Requirements

Directory Server, Directory Proxy Server, and Directory Server Resource Kit share the same operating system requirements. The Directory Server Enterprise Edition software has been 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, Directory Proxy Server, and Directory Server Resource Kit	Additional Required Software and Comments
Solaris 10 Operating System for SPARC, 32-bit x86, Intel x64, and AMD x64 architectures	Patches: ■ (SPARC) 118833, 119689, 119963, 122032, and 119254 or substitute patches, in addition to 127127 ■ (x86/x64) 118855, 119964, 121208, 122033, and 119255 or substitute patches, in addition to 127128

Supported OS Versions for Directory Server, Directory Proxy Server, and Directory Server Resource Kit	Additional Required Software and Comments
Solaris 9 Operating System for SPARC and x86 architectures	Patches: ■ (SPARC) 111711, 111712, 111722, 112874, 112963, 113225, 114344, 114370, 114371, 114372, and 114373 or substitute patches, in addition to 112960–56 or later. ■ (x86) 111713, 111728, 113986, 114345, 114427, 114428, 114429, 114430, 114432, 116545, and 117172 or substitute patches, in addition to 114242–41 or later.
Red Hat Enterprise Linux Advanced Server AS and ES 3.0 Update 4 for x86 and AMD x64	No additional software is required. On 64–bit Red Hat systems, Directory Server runs in 32–bit mode but Directory Proxy Server runs in 64–bit mode.

Red Hat Enterprise Linux Advanced Server AS and ES 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/`.
	On 64–bit Red Hat systems, Directory Server runs in 32–bit mode but Directory Proxy Server runs in 64–bit mode.

SuSE Linux Enterprise Server 10 for x86 and AMD x64	Service Pack 1 Supported only for the zip distribution of Directory Server Enterprise Edition. On 64–bit SuSE systems, Directory Server runs in 32–bit mode but Directory Proxy Server runs in 64–bit mode.
SuSE Linux Enterprise Server 9 for x86 and AMD x64	Service Pack 4 Supported only for the zip distribution of Directory Server Enterprise Edition. On 64–bit SuSE systems, Directory Server runs in 32–bit mode but Directory Proxy Server runs in 64–bit mode.
Microsoft Windows 2000 Server	Service Pack 4

Supported OS Versions for Directory Server, Directory Proxy Server, and Directory Server Resource Kit	Additional Required Software and Comments
Microsoft Windows 2000 Advanced Server	Service Pack 4
Microsoft Windows 2003 Server Standard Edition	Service Pack 2
Microsoft Windows 2003 Server Enterprise Edition	Service Pack 2
Note – Microsoft Windows 2008 is not supported in Directory Server Enterprise Edition 6.3.1	
Hewlett Packard HP-UX 11iV2	(11.23) PA-RISC 64–bit Supported only for the zip distribution of Directory Server Enterprise Edition.

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.

To avoid downloading most individual patches, obtain Solaris patch clusters . To obtain Solaris patch clusters, follow these steps:

1. Go to the SunSolve patch page at `http://sunsolve.sun.com/pub-cgi/show.pl?target=patchpage`.
2. Click the Recommended Patch Clusters link.
3. Download the patch cluster for your Solaris OS and Java ES versions.

Note that installations on SuSE Linux Enterprise Server require you to reset several Java environment variables. See *Sun Java System Directory Server Enterprise Edition 6.3 Installation Guide* for more details.

Software Dependency Requirements

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, Directory Server requires ActivePerl software to use account activation and manual schema replication commands. Directory Server Enterprise Edition does not provide ActivePerl. The dependency concerns the following commands.

- `ns-accountstatus`(1M)
- `ns-activate`(1M)

- `ns-inactivate`(1M)
- `schema_push`(1M)

On Microsoft Windows systems, you must disable the pop-up blocker to make Directory Service Control Center work properly.

The Directory Service Control Center supports the following application servers:

- Sun Java System Application Server 8.2.
- Tomcat 5.5.

For more information, see "Installing Directory Service Control Center From Zip Distribution" in *Sun Java System Directory Server Enterprise Edition 6.3 Installation Guide*.

Directory Proxy Server will work with any LDAPv3 compliant directory servers, but it is tested only with Sun Java System Directory Server.

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

JDBC Data Source	JDBC Driver
DB2 v9	IBM DB2 JDBC Universal Driver Architecture 2.10.27
JavaDB 10.2.2.0	Apache Derby Network Client JDBC Driver 10.2.2.0
Microsoft SQL Server 2005	sqljdbc.jar 1.2.2323.101
MySQL 5.0	MySQL-AB JDBC Driver mysql-connector-java-5.0.4
Oracle 9i Database Oracle 10g Database	Oracle JDBC driver 10.2.0.2.0

On Microsoft Windows systems, the `dsee_deploy` command cannot properly register software with the Common Agent Container, `cacao`, when you run the command from an MKS shell. This can occur when your MKS `PATH` does not include the *system-drive:*`\system32` folder. Alternatively, run the command on the Microsoft Windows native command line.

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.

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.

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.

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)	Netscape Communicator 7.1, Mozilla 1.7.12, and Firefox 1.0.7, 1.5, and 2.0
Red Hat Linux 4, Red Hat Linux 3 and SuSE Linux	Mozilla 1.7.12 and Firefox 1.0.7, 1.5, and 2.0
Windows XP	Netscape Communicator 8.0.4, Microsoft Internet Explorer 6.0SP2 and 7.0, Mozilla 1.7.12, and Firefox 1.0.7, 1.5, and 2.0
Windows 2000/2003	Netscape Communicator 8.0.4, Microsoft Internet Explorer 6.0 SP1 and 7.0, Mozilla 1.7.12, and Firefox 1.0.7, 1.5, and 2.0

Installation Privileges and Credentials

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

- "Directory Server, Directory Proxy Server, Directory Service Control Center, and Directory Server Resource Kit Privileges" on page 32

Directory Server, Directory Proxy Server, Directory Service Control Center, and Directory Server Resource Kit Privileges

You must have the following privileges when installing Directory Server, Directory Proxy Server, or Directory Service Control Center from the Java Enterprise System native package based distribution.

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

You can install Directory Server, Directory Proxy Server, and Directory Server Resource Kit from the zip distribution without special privileges. See the *Sun Java System Directory Server Enterprise Edition 6.3 Installation Guide* for details.

Before You Upgrade

You must consider the following points before applying the Directory Server Enterprise Edition 6.3.1 patch.

- Native package based distribution. All Directory Server and Directory Proxy Server instances, including the DSCC registry, must be stopped before the Directory Server Enterprise Edition 6.3.1 patch is applied.

  If you apply the patch without stopping the server instances, the instances might crash the next time you restart them.

Note – On Windows, the following dsadm command fails to stop the DSCC registry.

```
dsadm.exe stop C:\Program Files\Sun\JavaES5\DSEE\var\dscc6\dcc\ads
```

As a workaround, kill the bin_slapd.exe process using Task Manager and login as Administrator. You can now start and stop the DSCC registry successfully. The owner of the DSCC registry remains the same, that is, SYSTEM.

For native package based distribution: after applying patches to upgrade Directory Server Enterprise Edition, you must restart Sun Web Console using the following command:

```
# smcwebserver restart
```

To use the localized console, apply the Directory Server Enterprise Edition 6.3 localized patch (if it is not already applied) before the Directory Server Enterprise Edition 6.3 core patch. If you apply the 6.3.1 core patch before applying the 6.3 localization patch, then run the following commands in the specified order.

```
# dsccsetup console-unreg
# dsccsetup console-reg
```

For more information, see bug 6583131 in "Known Directory Server Issues in 6.3.1" on page 59.

- Zip based distribution. All Directory Server and Directory Proxy Server instances must be stopped before the Directory Server Enterprise Edition 6.3.1 zip distribution is applied on top of one of the applicable zip installations:
  - Directory Server Enterprise Edition 6.0
  - Directory Server Enterprise Edition 6.1
  - Directory Server Enterprise Edition 6.2
  - Directory Server Enterprise Edition 6.3

  This check is done by the dsee_deploy command itself, but is not performed on the Microsoft Windows 2000 platform. For more information, see 6660462 in "Known Directory Server Issues in 6.3.1" on page 59.

  If you apply the patch without stopping the server instances, the instances might crash the next time you restart them.

  Note that the patchzip is not applied to the Directory Service Control Center until you undeploy and then redeploy the WAR file. This requirement is related to bug 6583131 in "Known Directory Server Issues in 6.3.1" on page 59.

Installation Instructions

Note – Directory Server Enterprise Edition 6.3.1 is a maintenance release that delivers bug fixes mainly for Directory Service Control Center, Directory Proxy Server, and Directory Server. Only the upgrade mode is offered within 6.3.1 using Native Packages or ZIP distribution.

If you plan to install Directory Server Enterprise Edition 6.0, 6.1, 6.2, or 6.3 please refer to the Sun Java System Directory Server Enterprise Edition Installation Guide for 6.0, 6.1, 6.2, or 6.3. See "Directory Server Enterprise Edition Documentation Set" on page 8.

These installation instructions provide step-by-step instructions for installing Directory Service Control Center, Directory Proxy Server, Directory Server, Directory Server Resource Kit, and Identity Synchronization for Windows components of Directory Server Enterprise Edition.

Caution – The Sun Java System Directory Server Enterprise Edition 6.3.1 Security Patchzip 142807-02 must be applied **on top of a Directory Server Enterprise Edition 6.3.1 ZIP** installation. For directions see "Installing Directory Server Enterprise Edition 6.3.1 Security Patchzip 142807-02" on page 48.

Note – This guide does not cover installation with other Java Enterprise System (Java ES) products. If you plan to install Directory Server and Directory Service Control Center software with other Java ES software, read the installation instructions for Java ES software at `http://docs.sun.com/coll/1286.3`. For Microsoft Windows, read the installation instructions for Java ES software at Java Enterprise System 5 for Microsoft Windows.

This section covers the following parts.

- "Upgrading Directory Server Enterprise Edition to 6.3.1 Using Native Packages" on page 39
- "Upgrading Directory Server Enterprise Edition to 6.3.1 Using ZIP distribution" on page 46

The following table identifies information for you to use to upgrade Directory Server Enterprise Edition to version 6.3.1 based on your current installation and the type of distribution you are using.

TABLE 2–1 Upgrade Paths to Directory Server Enterprise Edition 6.3.1

Previous Directory Server Enterprise Edition Version	Software Distribution	Related Information
None	Native Packages (Solaris and Linux)	Use the following steps to install Directory Server Enterprise Edition 6.0, component of Sun Java Enterprise System 5 and apply patches to upgrade to version 6.3.1 update 1. 1. Install Directory Server Enterprise Edition 6.0 part of Sun Java ES 5, as described in "Software Installation" in *Sun Java System Directory Server Enterprise Edition 6.0 Installation Guide*. 2. Upgrade to version 6.3.1 as described in "Upgrading Directory Server Enterprise Edition to 6.3.1 Using Native Packages" on page 39. 3. Install Directory Proxy Server 6.3.1 update 1 Patch 141958-01 as described in "Installation Notes for Directory Proxy Server 6.3.1 Update 1" on page 102. 4. Install Directory Server Enterprise Edition 6.3.1 Security Patch 143463-01 as described in "Installing Directory Server Enterprise Edition 6.3.1 Security Patch 143463-01" on page 49.
5.x	Native Packages (Solaris and Linux)	Use the following steps to install Directory Server Enterprise Edition 6.0, component of Sun Java Enterprise System 5, upgrade to 6.3, migrate 5.x instances to 6.3, and apply patches to upgrade to latest version. 1. Install Directory Server Enterprise Edition 6.0 part of Sun Java ES 5, as described in "Software Installation" in *Sun Java System Directory Server Enterprise Edition 6.0 Installation Guide*. 2. Upgrade Directory Server Enterprise Edition to version 6.3, as described in "Software Installation" in *Sun Java System Directory Server Enterprise Edition 6.3 Installation Guide*. 3. Migrate all the Directory Server 5.x instances to 6.3, as described in the *Sun Java System Directory Server Enterprise Edition 6.3 Migration Guide*. 4. Upgrade to version 6.3.1, as described in "Upgrading Directory Server Enterprise Edition to 6.3.1 Using Native Packages" on page 39. 5. Install Directory Proxy Server 6.3.1 update 1 Patch 141958-01 as described in "Installation Notes for Directory Proxy Server 6.3.1 Update 1" on page 102. 6. Install Directory Server Enterprise Edition 6.3.1 Security Patch 143463-01 as described in "Installing Directory Server Enterprise Edition 6.3.1 Security Patch 143463-01" on page 49.

TABLE 2–1 Upgrade Paths to Directory Server Enterprise Edition 6.3.1 *(Continued)*

Previous Directory Server Enterprise Edition Version	Software Distribution	Related Information
None	Native Packages (Windows)	Use the following steps to install the Directory Server Enterprise Edition 6.0 component of Sun Java Enterprise System 5 and apply patches to upgrade to version 6.3.1 update 1. 1. Install Directory Server Enterprise Edition 6.0 part of Sun Java ES 5, as described in the *Sun Java Enterprise System 5 Installation Guide for Microsoft Windows*. 2. Upgrade to version 6.3.1 as described in "Upgrading Directory Server Enterprise Edition to 6.3.1 Using Native Packages" on page 39. 3. Install Directory Proxy Server 6.3.1 update 1 Patch 141958-01 as described in "Installation Notes for Directory Proxy Server 6.3.1 Update 1" on page 102. 4. Install Directory Server Enterprise Edition 6.3.1 Security Patch 143463-01 as described in "Installing Directory Server Enterprise Edition 6.3.1 Security Patch 143463-01" on page 49.
5.x	Native Packages (Windows)	Use the following steps to install Directory Server Enterprise Edition 6.0 component of Sun Java Enterprise System 5, upgrade to version 6.3, migrate 5.x instances to 6.3, and apply patches to upgrade to latest version. 1. Install Directory Server Enterprise Edition 6.0 part of Sun Java ES 5, as described in the *Sun Java Enterprise System 5 Installation Guide for Microsoft Windows*. 2. Upgrade Directory Server Enterprise Edition to version 6.3, as described in "Software Installation" in *Sun Java System Directory Server Enterprise Edition 6.3 Installation Guide*. 3. Migrate all the Directory Server 5.x instances to 6.3, as described in the *Sun Java System Directory Server Enterprise Edition 6.3 Migration Guide*. 4. Upgrade to version 6.3.1, as described in "Upgrading Directory Server Enterprise Edition to 6.3.1 Using Native Packages" on page 39. 5. Install Directory Proxy Server 6.3.1 update 1 Patch 141958-01 as described in "Installation Notes for Directory Proxy Server 6.3.1 Update 1" on page 102. 6. Install Directory Server Enterprise Edition 6.3.1 Security Patch 143463-01 as described in "Installing Directory Server Enterprise Edition 6.3.1 Security Patch 143463-01" on page 49.

TABLE 2–1 Upgrade Paths to Directory Server Enterprise Edition 6.3.1 *(Continued)*

Previous Directory Server Enterprise Edition Version	Software Distribution	Related Information
None	Zip	Use the following steps to install Directory Server Enterprise Edition 6.3, upgrade directly to 6.3.1, and apply 6.3.1 update 1. 1. Install Directory Server Enterprise Edition 6.3, as described in "To Install Directory Server Enterprise Edition 6.3 From Zip Distribution" in *Sun Java System Directory Server Enterprise Edition 6.3 Installation Guide*. 2. Upgrade the installation to 6.3.1, as described in "Upgrading Directory Server Enterprise Edition to 6.3.1 Using ZIP distribution" on page 46. 3. Install the Directory Service Control Center, as described in "Installing Directory Service Control Center From Zip Distribution" in *Sun Java System Directory Server Enterprise Edition 6.3 Installation Guide*. 4. Install Directory Server Enterprise Edition 6.3.1 Security Patchzip 142807-02 as described in "Installing Directory Server Enterprise Edition 6.3.1 Security Patchzip 142807-02" on page 48. 5. Install Directory Proxy Server 6.3.1 update 1 Patch 141958-01 as described in "Installation Notes for Directory Proxy Server 6.3.1 Update 1" on page 102. 6. Install Directory Server Enterprise Edition 6.3.1 Security Patch 143463-01 as described in "Installing Directory Server Enterprise Edition 6.3.1 Security Patch 143463-01" on page 49.

TABLE 2–1 Upgrade Paths to Directory Server Enterprise Edition 6.3.1 *(Continued)*

Previous Directory Server Enterprise Edition Version	Software Distribution	Related Information
5.x	Zip	Use the following steps to install Directory Server Enterprise Edition 6.3, migrate 5.x instances to 6.3, upgrade to 6.3.1, and apply 6.3.1 update 1. 1. Install Directory Server Enterprise Edition 6.3, as described in "To Install Directory Server Enterprise Edition 6.3 From Zip Distribution" in *Sun Java System Directory Server Enterprise Edition 6.3 Installation Guide*. 2. Migrate all the Directory Server 5.x instances to 6.3, as described in the *Sun Java System Directory Server Enterprise Edition 6.3 Migration Guide*. 3. Upgrade the installation to 6.3.1, as described in "Upgrading Directory Server Enterprise Edition to 6.3.1 Using ZIP distribution" on page 46. 4. Install the Directory Service Control Center, as described in "Installing Directory Service Control Center From Zip Distribution" in *Sun Java System Directory Server Enterprise Edition 6.3 Installation Guide*. 5. Install Directory Server Enterprise Edition 6.3.1 Security Patchzip 142807-02 as described in "Installing Directory Server Enterprise Edition 6.3.1 Security Patchzip 142807-02" on page 48. 6. Install Directory Proxy Server 6.3.1 update 1 Patch 141958-01 as described in "Installation Notes for Directory Proxy Server 6.3.1 Update 1" on page 102. 7. Install Directory Server Enterprise Edition 6.3.1 Security Patch 143463-01 as described in "Installing Directory Server Enterprise Edition 6.3.1 Security Patch 143463-01" on page 49.
6.0, 6.1, 6.2, or 6.3	Native	Use the following steps to upgrade the installation to 6.3 1 and apply 6.3.1 update 1 1. Upgrade the installation to 6.3.1, as described in "Upgrading Directory Server Enterprise Edition to 6.3.1 Using Native Packages" on page 39. 2. Install Directory Proxy Server 6.3.1 update 1 Patch 141958-01 as described in "Installation Notes for Directory Proxy Server 6.3.1 Update 1" on page 102. 3. Install Directory Server Enterprise Edition 6.3.1 Security Patch 143463-01 as described in "Installing Directory Server Enterprise Edition 6.3.1 Security Patch 143463-01" on page 49.

TABLE 2–1 Upgrade Paths to Directory Server Enterprise Edition 6.3.1 *(Continued)*

Previous Directory Server Enterprise Edition Version	Software Distribution	Related Information
6.0, 6.1, 6.2, or 6.3	Zip	Use the following steps to upgrade the installation to 6.3.1, apply 6.3.1 update 1 and install the Directory Service Control Center (if it is not already installed). 1. Upgrade the installation to 6.3.1, as described in "Upgrading Directory Server Enterprise Edition to 6.3.1 Using ZIP distribution" on page 46. 2. Install Directory Server Enterprise Edition 6.3.1 Security Patchzip 142807-02 as described in "Installing Directory Server Enterprise Edition 6.3.1 Security Patchzip 142807-02" on page 48. 3. Install Directory Proxy Server 6.3.1 update 1 Patch 141958-01 as described in "Installation Notes for Directory Proxy Server 6.3.1 Update 1" on page 102. 4. Install the Directory Service Control Center, as described in "Installing Directory Service Control Center From Zip Distribution" in *Sun Java System Directory Server Enterprise Edition 6.3 Installation Guide*. 5. Install Directory Server Enterprise Edition 6.3.1 Security Patch 143463-01 as described in "Installing Directory Server Enterprise Edition 6.3.1 Security Patch 143463-01" on page 49.

Note – In general, it is a good practice to back up the directory databases regularly and particularly before upgrading the directory server. See the *Sun Java System Directory Server Enterprise Edition 6.3 Administration Guide* for information about backing up the database.

Upgrading Directory Server Enterprise Edition to 6.3.1 Using Native Packages

▼ To Upgrade Shared Components Using Patches

Before You Begin Before upgrading Directory Server Enterprise Edition to 6.3.1 using native packages, you must upgrade the shared components. On Solaris and Red Hat systems you must be `root`, on Windows systems, you must be `Administrator` to perform this procedure.

Using patches, you can upgrade shared components on Solaris, Linux, and Windows. On Linux, to install patches you must use `installpatch`. The `installpatch` script is delivered with the patch.

Select the platform as per your requirements and install all the patches specified for that platform. If newer patch revisions become available, use the newer ones instead of those shown in the table.

Description	Solaris 10 SPARC and Solaris 9 SPARC	Solaris 10 x86, AMD x64 and Solaris 9 x86	Linux
International Components for Unicode (ICU)	119810-05 (Solaris 10) 114677-15 (Solaris 9)	119811-05 (Solaris 10) 114678-15 (Solaris 9)	126368-04
Sun Java Web Console (SJWC)	125952-05 (Solaris 10) 125950-05 (Solaris 9)	125953-05 (Solaris 10) 125951-05 (Solaris 9)	125954-05
Network Security Services/Netscape Portable Runtime/Java Security Services (NSS/NSPR/JSS)	Refer to the table below for complete patch information.	Refer to the table below for complete patch information.	121656-17
Java Dynamic Management Kit Runtime	119044-03	119044-03	119046-03
Common Agent Container Runtime	123893-04	123896-04	123899-03
Sun Java Monitoring Framework (MFWK)	125444-11	125446-11 (Solaris 10 64-bit and Solaris 10 32-bit) 125445-11 (Solaris 10 32-bit and Solaris 9 32-bit)	125447-11
Sun LDAP C SDK 6.0	136798–01	136799–01 (Solaris 9 x86) 136800–01 (Solaris 10 x86 and AMD64)	139535–01

Choose the right NSS/NSPR/JSS patch for your system by getting the package version of SUNWpr and SUNtls on your system.

```
# pkginfo -l SUNWpr | grep VERSION
# pkginfo -l SUNWtls | grep VERSION
```

Then choose the right patch series from the table below.

Solaris	Package Version	Network Security Services/Netscape Portable Runtime/Java Security Services (NSS/NSPR/JSS) patch
Solaris 9 SPARC	SUNWpr: VERSION=4.1.2,REV=2002.09.03.00.17 SUNWtls: VERSION=3.3.2,REV=2002.09.18.12.49	119211-17
Solaris 9 x86	SUNWpr: VERSION=4.1.3,REV=2003.01.09.13.59 SUNWtls: VERSION=3.3.3,REV=2003.01.09.17.07	119212-17
Solaris 10 SPARC	SUNWpr: VERSION=4.5.1,REV=2004.11.05.02.30 SUNWtls: VERSION=3.9.5,REV=2005.01.14.17.27	119213-17
Solaris 10 x86	SUNWpr: VERSION=4.5.1,REV=2004.11.05.03.44 SUNWtls: VERSION=3.9.5,REV=2005.01.14.19.03	119214-17
Solaris 9 SPARC and Solaris 10 SPARC	SUNWpr: VERSION=4.6.4,REV=2006.11.16.20.40 SUNWtls: VERSION=3.11.4,REV=2006.11.16.20.40	125358-06
Solaris 9 x86 and Solaris 10 x86	SUNWpr: VERSION=4.6.4,REV=2006.11.16.21.41 SUNWtls: VERSION=3.11.4,REV=2006.11.16.21.41	125359-06

The following table lists the Shared Components patches for Windows platform.

Description	Windows
Windows Installer Patch	126910-02
Sun Java Web Console (SJWC)	125955-05
Network Security Services/Netscape Portable Runtime/Java Security Services (NSS/NSPR/JSS)	125923-06
Common Agent Container Runtime	126183-07
Sun Java Monitoring Framework (MFWK)	125449-09

Before upgrading Directory Server Enterprise Edition 6.0, 6.1, 6.2, or 6.3 to 6.3.1, you need to upgrade the shared components.

1. **Shut down any processes using the shared components.**

2. **If applicable, shut down the shared components.**

3. **Obtain the latest upgrade patches as shown in the tables above.**

   For more information on how to obtain the patches, see "Getting the Software" on page 25.

4. **Apply the appropriate patches for the shared components.**

   Read the README.patchID file for detailed patch installation procedures.

5. **Verify that the patch upgrades were successful.**

   Read the README.patchID file for verification procedure.

6. **If applicable, restart the shared components.**

7. **To Upgrade the Common Agent Container shared component on Windows, run the following commands in the same order as listed below:**

```
# cacaoadm prepare-uninstall
# 126183-04.exe
# cacao-install-path\share\cacao_2\configure.bat
# cacao-install-path\share\cacao_2\bin\cacaoadm rebuild-dependencies
```

8 **If your installation uses Identity Synchronization for Windows and you have applied the latest NSS patch 3.12 on your system, set symbolic links to the new libraries delivered in NSS patch 3.12, as shown in the following example. The default value of the `SERVER_ROOT` path name is** `/var/mps/serverroot`.

```
$ cd /var/mps/serverroot/lib
$ ln -s /usr/lib/mps/secv1/libnssdbm3.so libnssdbm3.so
$ ln -s /usr/lib/mps/secv1/libnssutil3.so libnssutil3.so
$ ln -s /usr/lib/mps/secv1/libsqlite3.so libsqlite3.so

$ cd /var/mps/serverroot/lib/sparcv9
$ ln -s /usr/lib/mps/secv1/sparcv9/libnssdbm3.so libnssdbm3.so
$ ln -s /usr/lib/mps/secv1/sparcv9/libnssutil3.so libnssutil3.so
$ ln -s /usr/lib/mps/secv1/sparcv9/libsqlite3.so libsqlite3.so
```

▼ To Upgrade Directory Server Enterprise Edition Using Native Packages

Before You Begin Make sure all the shared components are up-to-date. For more information, see “To Upgrade Shared Components Using Patches” on page 39.

If you already have Directory Server Enterprise Edition 6.0, 6.1, 6.2, or 6.3 installed, upgrade to version 6.3.1 using the following procedure.

On Solaris and Red Hat systems, you must be root to perform these steps and Administrator on Windows systems.

All the Directory Server instances, Directory Proxy Server instances, and configuration information remain unaffected after you complete the Directory Server Enterprise Edition upgrade.

The following table displays the patch numbers that are required to upgrade Directory Server Enterprise Edition on different platforms. If newer patch revisions become available, use the newer ones instead of those shown in the table.

Description	Directory Server Enterprise Edition Core	Directory Server Enterprise Edition Localization
Patch ID: Solaris SPARC	125276-08	125937-06
Patch ID: Solaris 9 x86	125277-08	125938-06
Patch ID: Solaris 10 x86 or AMD x64	125278-08	125938-06
Patch ID: Linux	125309-08	125939-06

Description	Directory Server Enterprise Edition Core	Directory Server Enterprise Edition Localization
Patch ID: Windows	125311-08	
The Directory Server Enterprise Edition 6.1 patch was not delivered for Windows so this patch is not applicable to upgrade 6.1 installation.	The localized patch is delivered within the base patch.	

Note – To make the localized Directory Server Enterprise Edition work successfully, install the localized patches before installing the core patches.

Each localization patch contains all the supported languages for the selected platform.

---

1. **Stop the DSCC registry.**

   - On Solaris

     ```
     # dsadm stop /var/opt/SUNWdsee/dscc6/dcc/ads
     ```

   - On Linux

     ```
     # dsadm stop /var/opt/sun/dscc6/dcc/ads
     ```

   - On Windows, the following `dsadm` command fails to stop the DSCC registry.

     ```
     dsadm.exe stop C:\Program Files\Sun\JavaES5\DSEE\var\dscc6\dcc\ads
     ```

     As a workaround, kill the bin_slapd.exe process using Task Manager, and log in as Administrator. You can now start and stop the DSCC registry successfully. The owner of the DSCC registry remains the same, that is, SYSTEM.

2. **Stop any running instances of Directory Server and Directory Proxy Server.**

3. **Upgrade the shared components. See “To Upgrade Shared Components Using Patches” on page 39.**

4. **Download the Directory Server Enterprise Edition 6.3.1 patch.**

   See “Getting the Software” on page 25 for more details.

5. **Change to the directory where you have saved the patch listed in the preceding table.**

6. **Run the following command to install the patch.**

   - Solaris OS

Before upgrading Directory Server Enterprise Edition, you must install 119254-38 on Solaris 10 SPARC and 119255-38 on Solaris 10 x86. See "Getting the Software" on page 25 for information on downloading patches.

Alternatively, use -G with the patchadd command on Solaris 10 SPARC and Solaris 10 x86 while applying the Directory Server Enterprise Edition upgrade patch. For example:

```
 # patchadd -G patch-id
```

For other versions of Solaris, use the following command:

```
# patchadd patch-id
```

- Linux

  a. Open the directory where the `installpatch` file is located.

  b. Run `installpatch`.

  ```
  # ./installpatch
  ```

- Windows

  a. Open the folder where the `patch-id.exe` executable file is located.

  b. Double-click `patch-id.exe`.

  c. After the successful installation of the patch, run the following commands:

  ```
  # dsccsetup console-unreg
  # dsccsetup console-reg
  ```

7 **Start the Directory Server instances and Directory Proxy Server instances, if any.**

8 **Start Web Console and Common Agent Container.**

9 **Restart the DSCC registry.**

- On Solaris

```
# dsadm start /var/opt/SUNWdsee/dscc6/dcc/ads
```

- On Linux

```
# dsadm start /var/opt/sun/dscc6/dcc/ads
```

- On Windows

```
dsadm.exe start C:\Program Files\Sun\JavaES5\DSEE\var\dscc6\dcc\ads
```

Upgrading Directory Server Enterprise Edition to 6.3.1 Using ZIP distribution

▼ To Upgrade Directory Server Enterprise Edition to 6.3.1 Using ZIP Distribution

Before You Begin

Caution – Back up the Directory Server Enterprise Edition installation directory, if any, before upgrading to Directory Server Enterprise Edition 6.3.1, as later you will not be able to restore any previous Directory Server Enterprise Edition installation.

You can install the zip distribution as a non-root user.

The `dsee_deploy` command automatically updates the installation if it finds any previous installation. However, in the case of SuSE Linux 9 and HP-UX, before you upgrade the Directory Server Enterprise Edition installation, you must first upgrade the operating system to SuSE Linux 9 SP4 and HP-UX 11.23 respectively. Then use following procedure to upgrade your Directory Server Enterprise Edition installation to 6.3.1.

1 **Stop CACAO and any running instances of Directory Server and Directory Proxy Server associated with the installation that you intend to patch. Also stop the application server that hosts the WAR file and the DSCC registry.**

2 **If the system you are upgrading is hosted on SuSE Linux 9 or HP-UX, upgrade your operating system.**

- Upgrade SuSE Linux 9 SP3 to SuSE Linux 9 SP4.

  On SuSE 64-bit, `.pam-32bit-9-yyyymmddhhmm.rpm` is a prerequisite for CACAO to start, and you must install it if it is not already present on your system.

- Because Directory Server Enterprise Edition 6.0 and 6.1 support only HP-UX 11.11, you must upgrade your operating system to HP-UX 11.23 before upgrading Directory Server Enterprise Edition to 6.3.1.

Refer to the operating system documentation for information about how to upgrade the operating system, how to preserve the partition where Directory Server Enterprise Edition is installed, and where to get the latest patch bundles.

3 **Upgrade Directory Server Enterprise Edition to 6.3.1**

a. **Use the `dsee_deploy` command from Directory Server Enterprise Edition 6.3.1 zip distribution, with the same installation path, and CACAO port used your previous**

installation of Directory Server Enterprise Edition 6.0, 6.1, 6.2, or 6.3. The `dsee_deploy` command will restart CACAO and DSCC registry.

i. **Obtain the zip distribution for this installation.**

   Refer to the following table for information about the appropriate zip patch for your system. If newer patch revisions become available, use the newer ones instead of those shown in the table.

   All the multilingual files are included in the above mentioned patches.

Operating System	Patch number
Solaris SPARC	126748-05
Solaris 9 x86	126749-05
Solaris 10 x86 and AMD x64	126750-05
Red Hat Linux	126751-05
SuSE Linux	126751-05
HP-UX	126752-05
Windows	126753-05

ii. **Install the prerequisite patches or service packs for your platform, as described in "Operating System Requirements" on page 27.**

iii. **Change to the zip distribution directory that contains the `dsee_deploy` command.**

iv. **Upgrade your Directory Server Enterprise Edition installation currently installed at *install_path* with the `dsee_deploy`(1M) command.**

```
$ ./dsee_deploy install -i install-path options
```

   On Windows installations, browse to the zip distribution folder that contains the dsee_deploy command and run the following command:

```
dsee_deploy install -i install-path options
```

   For example, the following command upgrades your existing Directory Server Enterprise Edition previously installed at `/local` directory, assuming that you have write access to the directory.

```
$ ./dsee_deploy install -i /local
```

   You can also use the `--no-inter` option to install in non-interactive mode, accepting the license without confirmation. Non-interactive mode is particularly useful for silent installation.

During the installation process, a WAR file is saved on your system. The WAR file contains the DSCC web application which when deployed with the application server enables you to access and manage the server instances through web console. The functionality is similar to DSCC in native packages. For more information about the WAR file, see "Installing Directory Service Control Center From Zip Distribution" in *Sun Java System Directory Server Enterprise Edition 6.3 Installation Guide*.

During the installation process, the multilingual packages are also installed.

v. **Deploy the latest dscc.war file in the application server**

For step-by- step information, refer to "Installing Directory Service Control Center From Zip Distribution" in *Sun Java System Directory Server Enterprise Edition 6.3 Installation Guide*.

vi. **Restart Directory Server and Directory Proxy Server instances and the application server for WAR file.**

4 **Start daemons only when both operating system and Directory Server Enterprise Edition are upgraded.**

Installing Directory Server Enterprise Edition 6.3.1 Security Patchzip 142807-02

Caution – The Sun Java System Directory Server Enterprise Edition 6.3.1 Security Patchzip 142807-02 must be applied **on top of a Directory Server Enterprise Edition 6.3.1 ZIP** installation. This patch delivers NSS 3.12.5 as well as SASL 2.19.20090601.

Note – This patch cannot be applied to versions of Directory Server Enterprise Edition earlier than 6.3.1. For directions to upgrade to version 6.3.1, see Table 2–1.

To install Directory Server Enterprise Edition 6.3.1 Security Patchzip 142807-02, download it from http://sunsolve.sun.com (`http://sunsolve.sun.com`) and follow the installation instructions provided in the README file.

Installing Directory Server Enterprise Edition 6.3.1 Security Patch 143463-01

Caution – The Sun Java System Directory Server 6.3.1 Security Patch 143463-01 must be applied on top of a Directory Server Enterprise Edition 6.3.1 installation.

Note – This patch cannot be applied to versions of Directory Server Enterprise Edition earlier than 6.3.1. For directions to upgrade to version 6.3.1, see Table 2–1.

To install Directory Server Enterprise Edition 6.3.1 Security Patch 143463-01, download it from http://sunsolve.sun.com (`http://sunsolve.sun.com`) and follow the installation instructions provided in the README file.

Confirm that the installation of patch 143463-01 is successful by running this command and verifying that the response is the same as shown here:

```
./dsadm -V
[dsadm]
dsadm              : 6.3.1               B2008.1121.0156 ZIP

[slapd 64-bit]
Sun Microsystems, Inc.
Sun-Java(tm)-System-Directory/6.3.1_sec B2010.0201.1612 64-bit
ns-slapd           : 6.3.1               B2008.1121.0156 ZIP
Slapd Library      : 6.3.1_sec           B2010.0201.1612
Front-End Library  : 6.3.1               B2008.1121.0156
```

Uninstallation Instructions

If you plan to uninstall Directory Server Enterprise Edition 6.0, 6.1, 6.2, or 6.3 please refer to the chapter 3. "Uninstalling Directory Server Enterprise Edition" of Sun Java System Directory Server Enterprise Edition Installation Guide for 6.0, 6.1, 6.2, or 6.3. See the“Directory Server Enterprise Edition Documentation Set” on page 8.

This section describes the following topics:

- “Downgrading from Directory Server Enterprise Edition 6.3.1 Using Native Packages” on page 50
- “Downgrading from Directory Server Enterprise Edition 6.3.1 Using ZIP Distribution” on page 52

Downgrading from Directory Server Enterprise Edition 6.3.1 Using Native Packages

After you upgrade to Directory Server Enterprise Edition 6.3.1 you might want to restore your previous Directory Server Enterprise Edition installation. This section provides complete information about how to downgrade the Directory Server Enterprise Edition installation.

▼ To Downgrade Directory Server Enterprise Edition Using Native Package

Downgrading Directory Server Enterprise Edition restores the previous working copy of your Directory Server Enterprise Edition installation and retains all your configuration information that you had before upgrading to Directory Server Enterprise Edition 6.3.1.

1. **Stop all running server instances.**

2. **Run the following command to remove the patch.**

   Remove the localization patch before you remove the base patch to clean up the system. Refer to Patch Table for Native Package in "Upgrading Directory Server Enterprise Edition to 6.3.1 Using Native Packages" on page 39 for the patch ID for each platform.

   - Solaris

     ```
     # patchrm patch-id
     ```

   - Linux

     Go to the directory where the Directory Server Enterprise Edition 6.3, 6.2, 6.1, or 6.0 .rpm files are stored and run the following command repetitively for all the rpm files as specified in the table below. The set of rpm files that you choose depends on the previous installation of Directory Server Enterprise Edition you had.

     Make sure that after downgrading you have all the 6.0, 6.1, 6.2, or 6.3 rpm files. Downgrading the subset of the rpm files results in corrupted installation.

Localized 6.3 rpm files	`sun-ldap-console-gui-l10n-6.3-1.i386.rpm`
	`sun-ldap-console-gui-help-l10n-6.3-1.i386.rpm`
	`sun-ldap-proxy-client-l10n-6.3-1.i386.rpm`
	`sun-ldap-proxy-l10n-6.3-1.i386.rpm`
	`sun-ldap-directory-client-l10n-6.3-1.i386.rpm`
	`sun-ldap-directory-l10n-6.3-1.i386.rpm`
	`sun-ldap-shared-l10n-6.3-1.i386.rpm`

Base 6.3 rpm files	`sun-ldap-console-gui-6.3-7.i386.rpm`
	`sun-ldap-console-gui-help-6.3-7.i386.rpm`
	`sun-ldap-console-agent-6.3-7.i386.rpm`
	`sun-ldap-console-cli-6.3-7.i386.rpm`
	`sun-ldap-console-common-6.3-7.i386.rpm`
	`sun-ldap-proxy-man-6.3-7.i386.rpm`
	`sun-ldap-proxy-client-6.3-7.i386.rpm`
	`sun-ldap-proxy-config-6.3-7.i386.rpm`
	`sun-ldap-proxy-6.3-7.i386.rpm`
	`sun-ldap-directory-man-6.3-7.i386.rpm`
	`sun-ldap-directory-client-6.3-7.i386.rpm`
	`sun-ldap-directory-config-6.3-7.i386.rpm`
	`sun-ldap-directory-dev-6.3-7.i386.rpm`
	`sun-ldap-directory-6.3-7.i386.rpm`
	`sun-ldap-shared-6.3-7.i386.rpm`

Localized 6.2 rpm files	`sun-ldap-console-gui-l10n-6.2-6.i386.rpm`
	`sun-ldap-console-gui-help-l10n-6.2-6.i386.rpm`
	`sun-ldap-proxy-client-l10n-6.2-6.i386.rpm`
	`sun-ldap-proxy-l10n-6.2-6.i386.rpm`
	`sun-ldap-directory-client-l10n-6.2-6.i386.rpm`
	`sun-ldap-directory-l10n-6.2-6.i386.rpm`
	`sun-ldap-shared-l10n-6.2-6.i386.rpm`

Base 6.2 rpm files	`sun-ldap-console-gui-6.2-5.i386.rpm`
	`sun-ldap-console-gui-help-6.2-5.i386.rpm`
	`sun-ldap-console-agent-6.2-5.i386.rpm`
	`sun-ldap-console-cli-6.2-5.i386.rpm`
	`sun-ldap-proxy-man-6.2-5.i386.rpm`
	`sun-ldap-proxy-client-6.2-5.i386.rpm`
	`sun-ldap-proxy-config-6.2-5.i386.rpm`
	`sun-ldap-proxy-6.2-5.i386.rpm`
	`sun-ldap-directory-man-6.2-5.i386.rpm`
	`sun-ldap-directory-client-6.2-4.i386.rpm`
	`sun-ldap-directory-config-6.2-5.i386.rpm`
	`sun-ldap-directory-6.2-5.i386.rpm`
	`sun-ldap-shared-6.2-5.i386.rpm`

Localized 6.1 rpm files	`sun-ldap-console-gui-l10n-6.1-3.i386.rpm`
	`sun-ldap-console-gui-help-l10n-6.1-3.i386.rpm`
	`sun-ldap-proxy-client-l10n-6.1-3.i386.rpm`
	`sun-ldap-proxy-l10n-6.1-3.i386.rpm`
	`sun-ldap-directory-client-l10n-6.1-3.i386.rpm`
	`sun-ldap-directory-l10n-6.1-3.i386.rpm`
	`sun-ldap-shared-l10n-6.1-3.i386.rpm`

Base 6.1 rpm files	`sun-ldap-console-gui-6.1-2.i386.rpm`
	`sun-ldap-console-gui-help-6.1-2.i386.rpm`
	`sun-ldap-console-agent-6.1-2.i386.rpm`
	`sun-ldap-console-cli-6.1-2.i386.rpm`
	`sun-ldap-proxy-man-6.1-2.i386.rpm`
	`sun-ldap-proxy-client-6.1-2.i386.rpm`
	`sun-ldap-proxy-config-6.1-2.i386.rpm`
	`sun-ldap-proxy-6.1-2.i386.rpm`
	`sun-ldap-directory-man-6.1-2.i386.rpm`
	`sun-ldap-directory-client-6.1-2.i386.rpm`
	`sun-ldap-directory-config-6.1-2.i386.rpm`
	`sun-ldap-directory-6.1-2.i386.rpm`
	`sun-ldap-shared-6.1-2.i386.rpm`

- Windows

  a. Run the `dsccsetup` dismantle command to dismantle the DSCC.

  b. Double-click the `Uninstall_`*patch-id*`.bat` file to remove the patch. The `Uninstall_`*patch-id*`.bat` file is stored in the folder where the patch is saved.

  c. Downgrade Common Agent Container. See the uninstallation steps in the 126183-04 patch README.

     a. Run the `cacaoadm` `prepare-uninstall` command.

     b. Double-click `Uninstall_126183-04.bat` to remove the patch

Downgrading from Directory Server Enterprise Edition 6.3.1 Using ZIP Distribution

Directory Server Enterprise Edition 6.3.1 installation does not downgrade to the previous version. If you need to revert to the previous Directory Server Enterprise Edition version, restore the backup copy that you saved before upgrading to Directory Server Enterprise Edition 6.3.1.

To remove Directory Server Enterprise Edition completely, refer to 6.3 Installation Guide chapter “To Remove Software Installed From the Zip Distribution” in the *Directory Server Enterprise Edition 6.3 Installation Guide*.

CHAPTER 3

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 6.3.1" on page 53
- "Known Problems and Limitations in Directory Server" on page 56

Bugs Fixed in Directory Server 6.3.1

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

6344894 When synchronizing multi-domain Active Directory with Identity Synchronization for Windows, synchronization fails on Directory Server because of Active Directory's referrals.

6439482 An ACI problem may enable users to guess correct values.

6490419 A filter using a wildcard for an integer attribute may lead to inconsistent ldapsearch results.

6557125 When Active Directory servers are unavailable, Directory Server hangs in Identity Synchronization for Windows plug-ins.

6557128 When logging through a stale connector, Directory Server crashes in Identity Synchronization for Windows plug-ins.

6557499 After deploying Directory Server Enterprise Edition, defunct processes are created. This issue affects only the ZIP distribution on HP-UX.

6579286 The `dsrepair` tool does not work correctly on Microsoft Windows systems.

6579820 The `replcheck` tool does not work correctly on Microsoft Windows systems.

6586725 Replication over SSL may create memory leaks.

6593775 In the Suffix Usage tab of the DSCC console on versions of Directory Server Enterprise Edition 6, refresh does not display all suffixes.

6626454 When a long ACI is added, versions of Directory Server Enterprise Edition 6 might crash.

6632250 With large compound search filters, search performance is poor.

6634048 Use of the reversible password plug-in (des-plugin) might break replication.

6640464 Versions of Directory Server Enterprise Edition 6 do not support multiple certificate-authority certificates using the same dn in the certificate database.

6643813 Use of a large number of masters prevents proper monitoring of replication.

6645742 Enabling a password policy in a replication topology that includes both Directory Server Enterprise Edition 5.2 and Directory Server Enterprise Edition 6 causes replication to fail.

6650039 A race condition can cause a crash at the end of a replication session.

6650749 Some maintenance operations can cause a database recovery when the server restarts.

6651645 Use of `pwdReset` in a password policy prevents changing a password through proxy authorization.

6663553 A space after the quotation marks in an ACI string can cause erroneous ACI evaluations.

6670977 The DSCC console might fail to display a long ACI.

6675384 A complex CoS can reduce performance.

6680718 Insufficient access rights during logfile rotation cause versions of Directory Server Enterprise Edition 6 to hang.

6683182 Password policies now support a password timeout limit of 315360000 seconds (slightly less than 10 years), reduced from 2147483647 seconds (approximately 68 years).

6683353 If the NSS pin code is longer than eight characters, versions of Directory Server Enterprise Edition 6 do not start.

6683818 A candidate list of more than 2.5 million entries causes a server crash.

6683870 Using DSCC to edit an attribute with a binary syntax corrupts the attribute's value.

6685118 A race condition in opening and closing a connection can crash versions of Directory Server Enterprise Edition 6 in `connection_getIp_string`.

6686199 If attribute uniqueness plug-in is configured but not enabled, versions of Directory Server Enterprise Edition 6 can crash.

6686632 A race condition in ACI evaluation can cause the directory server to crash.

6687533 If a maintenance operation occurs while changelog trimming is running, a database panic or crash can occur.

6688454 Pass-through authentication prevents ns-slapd from shutting down.

6688891 When the password policy is running in compatibility mode, the password values are displayed in the clear in `auditlog` regardless of the value of `passwordStorageScheme`.

6689454 Restoring a backup containing a large `changelog` (larger than 30,000 database pages) logs the following messages:

```
DEBUG - conn=-1 op=-1 msgId=-1 -  libdb: Lock table is out of available locks
ERROR<8232> - Replication  - conn=-1 op=-1 msgId=-1 - Internal error
Truncate of changelog file failed, error 12 (Not enough space)
```

6698812 Under Sun Cluster 3.2 control on Solaris 10 AMD64, Directory Server fails to start.

6700232 A race condition between changelog trimming and operation on the trimmed entry can cause the directory server to hang.

6704259 If the replication group size is larger than one, etimes of replicated operations are incorrectly computed.

6704261 An index can be imported incorrectly in multi-pass import.

6705319 Referral cannot be disabled with DSCC once it has been enabled.

6706009 DSCC does not handle attributes with subtypes correctly.

6707089 A race condition with an ACI containing DNS rules causes in DS crash.

6707164 The Replication changelog gets emptied after a backup restore with message as below

```
INFORMATION - NSMMReplicationPlugin - conn=-1 op=-1 msgId=-1 - replica_reload_ruv:
 Warning: new data for replica does not match the data in the changelog. Recreating the
changelog file. This could affect replication with replica’s consumers in which case the
consumers should be reinitialized.
```

6708615 Directory Server crashes when stopping the server while indexing is occurring.

6710024 If Directory Server crashes while under Sun Cluster 3.2 control, cluster failover is initiated, but it requires more than 4 minutes.

6711123 Rarely updated masters might result in backups becoming quickly obsolete.

6717507 In a replication configuration, deleting entries creates incorrect VLV indexes.

6718308 Database restore messages are inconsistent between DSCC and error log files.

6726890	In a race condition, the Directory Server Enterprise Edition 6.3 changelog is not trimmed.
6732563	In a race condition, deleting a suffix can result in a database panic error.
6740791	When a password policy is assigned using CoS, the directory server might not release memory.
6750240	In versions of Directory Server Enterprise Edition 6, the `des-plugin.so` is not signed.
6754084	The zipped distribution delivers JRE 1.5.0_12 instead 1.5.0_9 as in previous releases.
6756826	A race condition between updating and flushing database pages can cause a directory server crash, database panic errors, or lose of updates.
6759200	A SASL bind on a connection can lead to a directory server crash
6772870	Consumers can become out of sync when `ds-polling-thread-count` is greater than 1 (which is likely on a CMT machine).

Known Problems and Limitations in Directory Server

The following sections list known problems and limitations at the time of release.

- "Directory Server Limitations" on page 56
- "Known Directory Server Issues in 6.3.1" on page 59

Directory Server 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.

Database cache may be outdated after failover on Sun Cluster.

The Directory Server supports Sun Cluster 3.2. When Directory Server runs on Sun Cluster, and `nsslapd-db-home-directory` is set to use a directory that is not shared, multiple instances share database cache files. After a failover, the Directory Server instance on the new node uses its potentially outdated database cache files.

To work around this limitation, either use a directory for `nsslapd-db-home-directory` that is shared, or systematically remove the files under `nsslapd-db-home-directory` at Directory Server startup.

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 property `max-thread-per-connection-count` does not apply for Windows systems.

A Microsoft Windows bug shows service startup type as disabled.

A Microsoft Windows 2000 Standard Edition bug (`http://support.microsoft.com/kb/287516/en-us`) causes the Directory Server service to appear as disabled after the service has been deleted from Microsoft Management Console.

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 13, "Directory Server Indexing," in *Sun Java System Directory Server Enterprise Edition 6.3 Administration Guide* for details.

The console does not allow you to create a Directory Server or Directory Proxy Server instance if the Directory Manager's password contains a space character. (6830908)

If the Directory Manager's password contains a space character, the Directory Manager account cannot create a directory server or directory proxy server instance by using the console.

Due to the same issue, the command `dsccsetup ads-create –w` *password-file* fails if the password file contains a space character.

DSEE6.0 PatchZIP delivery does not support SMF. (6886089)

In instances installed from the zip distribution of DSEE 6.0 and later releases, the `dsadm` and `dpadm` commands do not support the Service Management Facility (SMF). If the instance is registered to SMF manually, it is controlled by SMF so that if the instance is stopped via the `dsadm` or `dpadm` commands or through DSCC, SMF restarts the instance.

The SMF feature is fully supported only in the native distribution of DSEE 6.0 and later releases.

Known Directory Server Issues in 6.3.1

This section lists the known issues that are found at the time of Directory Server 6.3.1 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.

2151022 If certificates contain localized names, the certificate cannot be deleted properly. They also cannot be listed properly.

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.

6358392 When removing software, the `dsee_deploy uninstall` command does not stop or delete existing server instances.

To work around this limitation, follow the instructions in the *Sun Java System Directory Server Enterprise Edition 6.3 Installation Guide*.

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.

6478568 The `dsadm enable-service` command does not work correctly with Sun Cluster.

6480753 The `dsee_deploy` command has been seen to hang while registering the Monitoring Framework component into the Common Agent Container.

6482378 The supported `SSLCiphers` attribute on the root DSE lists NULL encryption ciphers not actually supported by the server.

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 Java System Directory Server Enterprise Edition 6.3 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`.

6497053 When installing from the zip distribution, the `dsee_deploy` command does not provide an option to configure SNMP and stream adaptor ports.

To workaround this issue,

1. Enabled Monitoring Plug-in using the web console or `dpconf`.
2. Using `cacaoadm set-param`, change `snmp-adaptor-port`, `snmp-adaptor-trap-port` and `commandstream-adaptor-port`.

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`.

6506019 On HP-UX, detaching the `gdb` from a running process of `ns-slapd`, kills the process and generates core dump.

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.

6539650 Directory Server instance with multi-byte characters in its path may fail to be created in DSCC, to start or perform other regular tasks.

Some of these issues can be resolved by using the charset that was used to create the instance. Set the charset using the following commands:

```
# cacaoadm list-params | grep java-flags
  java-flags=-Xms4M -Xmx64M

# cacaoadm stop
# cacaoadm set-param java-flags="-Xms4M -Xmx64M -Dfile.encoding=utf-8"
# cacaoadm start
```

Use only the ASCII characters in the instance path to avoid these issues.

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
```

6550543 You might encounter an error when DSCC is used with the combination of Tomcat 5.5 and JDK 1.6.

As a workaround, use JDK 1.5 instead.

6551672 Sun Java System Application Server bundled with Solaris 10 cannot create SASL client connection for authenticated mechanism and does not communicate with common agent container.

As a workaround, change the JVM used by application server by editing the *appserver-install-path*`/appserver/config/asenv.conf` file and replace the `AS_JAVA` entry with `AS_JAVA="/usr/java"`. Restart your Application Server domain.

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.

6571672 If unzip is unavailable on the system, `dsee_deploy` does not install any product.

6583131 To use a localized Directory Service Control Center, apply the Directory Server Enterprise Edition 6.3.1 localized patch before the Directory Server Enterprise Edition 6.3.1 core patch, or run the following commands in the specified order.

```
# dsccsetup console-unreg
# dsccsetup console-reg
```

There is no need to run the `dsccsetup console-unreg` and `console reg` commands if you apply the Directory Server Enterprise Edition 6.3.1 localized patch before the Directory Server Enterprise Edition 6.3.1 patch.

For zip based installation, the Directory Server Enterprise Edition 6.3.1 localized patch is not automatically applied to the Directory Service Control Center. As a workaround, undeploy and then redeploy the WAR file.

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
```

6594285 The Directory Service Control Center has no RBAC capability.

6595805 For encoding other than UTF-8, and when the install path contains non-ASCII characters, then the `dsee_deploy` tool fails to set up the Java Enterprise System Monitoring Framework inside the common agent container.

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`

6638990 / 6641357 The `ldapmodify` bulk import command can damage existing data. Specifying the option `-B` *suffix* causes all the existing data in the suffix to be removed.

The `ldapmodify` man page is therefore incorrect when it states that bulk import using the `ldapmodify` command does not erase entries that already exist.

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

6644161 In the Korean locale, clicking the Remove Attribute button in Encrypted Attributes Section of the Directory Service Control Center shows the following incomplete error message:

```
You have chosen to remove
```

The message should be as follows:

```
You have chosen to remove {0} from the list of encrypted attributes.
In order for the database files to reflect the configuration and
to work properly you must Initialize the Suffix.
Do you want to continue?
```

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.

6650105 On the Windows 2000 zip distribution, with the Tomcat 5.5 Application Server and using Internet Explorer 6, in the "Step 3: Assign Access Rights" of the "New DS Access Control Instruction" wizard in Directory Service Control Center, clicking on the "Delete" button of the "Assign Rights to Specified Users: " listbox, can produce an exception similar to the following:

```
The following error has occurred:
Handler method "handleAssignACIToDeleteButtonRequest" not implemented,
or has wrong method signature
Show Details
Hide Details
com.iplanet.jato.command.CommandException: Handler method
"handleAssignACIToDeleteButtonRequest" not implemented, or has wrong method signature
     com.iplanet.jato.view.command.DefaultRequestHandlingCommand.execute
(DefaultRequestHandlingCommand.java:167)
     com.iplanet.jato.view.RequestHandlingViewBase.handleRequest
(RequestHandlingViewBase.java:308)
     com.iplanet.jato.view.ViewBeanBase.dispatchInvocation(ViewBeanBase.java:802)
```

6653574 Replication from Directory Server 6.X master to a 5.1 master is not working properly.

6658483 In traditional Chinese, in the Directory Service Control Center the translation of the string "Initialize Suffix with Data..." in the Replication Settings tab of a suffix is confusing.

6660462 Before upgrading from Directory Server Enterprise Edition 6.2 to Directory Server Enterprise Edition 6.3, the `ntservice` for each instance of Directory Server or the Directory Proxy Server must be manually stopped, but the `dsee_deploy` command fails to identify running instances of Directory Server or the Directory Proxy Server on the Microsoft Windows 2000 platform.

On the zip distribution of Microsoft Windows 2000, when upgrading, the `dsee_deploy` command can fail. The error message is as follows:

```
error: cannot delete old
C:/local/upg6263/./dsee6/lib/bin/dsee_ntservice.exe
```

This indicates that an instance of the Directory Server or the Directory Proxy Server is still running. To stop the instance or instances, in Microsoft Windows 2000, select on Start > Settings > Control Panel, and choose Administrative Tools, then Services. For each service of the Directory Server or the Directory Proxy Server displayed in the right column, right click the instance and select Stop.

6663685 In the Directory Service Control Center, the Copy Suffix Configuration operation can produce erroneous pop-up windows.

6687375 DSCC cannot necessarily retrieve agent certificates that it creates. DSCC attempts to store the certificate in the 'agent-profile' in the DSCC registry, but if the DSCC registry's `ldap-port` is bound to the loopback interface, the certificate cannot be stored. However, the DSCC can read the DSCC registry because by design, so it must use `localhost` to communicate with DSCC registry.

To work around this limitation, use the `ldapmodify` command to create `agent-profile` in the DSCC registry.

6689290 An attempt to stop/start/restart server through a localized DSCC can lead to display garbled localized messages.

As a workaround edit the `cacao.properties` file and remove `-Dfile.encoding=utf-8` flag then restart cacao under the preferred locale.

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.

6703850 Versions of Directory Server 5 and Directory Server Enterprise Edition 6 may encounter a performance issue when using Veritas file system (VxFS) version 4.1 and 5.0 on Solaris 9 and Solaris 10 (SPARC or x86). The performance issue is located within the fdsync system call and affects, for example, Directory Server checkpointing. This issue is addressed with Solaris VMODSORT feature. Refer to http://sunsolve.sun.com/search/document.do?assetkey=1-66-201248-1 for further information.

Directory Server Enterprise Edition 6 can encounter a performance issue (CR 6703850) when using the Veritas file system with the VMODSORT feature. This issue occurs when a page is added at the of the file (for example, `id2entry.db3`) This error causes the `ftruncate` system call use as many resources as when using the Veritas file system without the VMODSORT feature.

6705472 Password policies measure password length by the number of bytes, so a password containing multi-byte characters can meet password-length policy even if the password contains fewer characters than the policy's specified minimum. For example, a 7-character password with one 2-byte character satisfies a password policy with password minimum length set to 8.

6707789 Example 1 of the man page for the modrate command contains usage errors. The following example is correct:

```
modrate -D uid=hmiller,ou=people,dc=example,dc=com -w hillock  -b "uid=test%d,ou=test,dc=example,dc=com" \
 -C 3 -r 100  -M ’description:7:astring’
```

6712064 The `nsslapd-groupevalsizelimitis` property is not documented. The following description applies to this property.

NAME `nsslapd-groupevalsizelimit`-maximum number of static group members for ACI evaluation.

DESCRIPTION Defines the maximum number of members that a static group (including members of its sub-groups) can have for ACI evaluation.

Entry DN	`cn=config`
Valid Range	`0` to the maximum 64-bit integer value A value of `-1` means infinite.
Default Value	`5000`
Syntax	Integer
Example	`nsslapd-groupevalsizelimit: 5000`

ATTRIBUTES See the attributes(5) man page for descriptions of the following attributes:

ATTRIBUTE TYPE	ATTRIBUTE VALUE
Availability	SUNWldap-directory
Stability Level	Obsolete: Scheduled for removal after this release

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.

6722534 The value of `minheap` is incorrectly described in the *Sun Java System Directory Server Enterprise Edition 6.3 Man Page Reference*. The value of `minheap` is twice the amount of heap memory used by the server at startup.

6723208 An attempt to edit an attribute value containing a carriage return results in corruption of the value.

6723590 Due to a potential database corruption present but undetected in version 6.2, before upgrading from Directory Server Enterprise Edition 6.2 to 6.3.1, rebuild the database by exporting it to an LDIF file and then reimport the LDIF file. In a replicated environment, rebuild or reinitialize all servers. Exporting, importing, and initializing servers in a replicated environment are described in the *Sun Java System Directory Server Enterprise Edition 6.3 Administration Guide*.

Note – This applies only to an upgrade from Directory Server Enterprise Edition 6.2. It does not apply to upgrades from version 6.0, 6.1, or 6.3.

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.

6742347 Directory Server Enterprise Edition 6 does not stop gracefully during Windows shutdown when registered as a service. At system restart, the following message is logged in the error log file:

```
WARNING<20488> - Backend Database - conn=-1 op=-1 msgId=-1 -  Detected Disorderly
Shutdown last time Directory Server was running, recovering database.
```

To work around this problem, stop the Directory Service manually before shutdown or reboot.

To stop the instances in Microsoft Windows, select Start > Settings > Control Panel, and select Administrative Tools and then Services. For each service of the Directory Server displayed in the right column, right click the instance and select Stop. Alternatively, run this command:

```
$ dsadm.exe stop instance-path
```

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.

6752475 Back-end database errors can be reported on Windows 2000. This problem exists only on Microsoft Windows. When it occurs, the following error messages are logged in the error logs:

```
ERROR<20742> - Backend Database - conn=-1 op=-1 msgId=-1 -  BAD MAP 1, err=5
ERROR<20741> - Backend Database - conn=-1 op=-1 msgId=-1 -  BAD EV 1, err=5
```

This error is usually harmless, but rarely it can cause a crash (6798026) when an instance spawned by a user (administrator or any other user) conflicts with an instance spawned by another user (a windows service, administrator or any other user).

To work around this problem in production, all instances must be registered as services.

To work around this problem during testing, if no instance is started as windows service, then new instances must be started by the same user. If an instance is started as a windows service, the only workaround is to start the new instances using a Remote Desktop Connection (rdesktop).

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 Java System
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, replication from versions of Directory Server 6 to Directory Server 5.2 masters (with a maximum of four servers) works correctly.

6753742 In a Multi-Master Replication configuration, the migration of masters from JES 4 to Directory Server 6.3 might fail. For example, the following error message can appear after performing step 6 of "Migrating the Masters" in *Sun Java System Directory Server Enterprise Edition 6.3 Migration Guide*:

```
INFORMATION - NSMMReplicationPlugin - conn=-1 op=-1 msgId=-1 -  _replica_configure_ruv: failed to create
replica ruv tombstone entry (suffix); LDAP error - 53
```

To work around this problem, use these steps:

1. Stop all JES 4 masters.

2. Edit the `dse.ldif` configuration file manually and change `nsslapd-readonly: on` to `nsslapd-readonly: off`.
3. Run the `dsmig migrate-config` migration command.

6755852 Attempts to install DSEE6.3 patchzip (and later) on Japanese Windows always fail when deploying JESMF in Cacao, with results similar to the following:

```
Deploying JESMF in Cacao...
## Failed to run install-path/dsee6/cacao_2/bin/cacaoadm.bat deploy
install-path/dsee6/mfwk/xml/com.sun.mfwk.xml
####
#### Cannot execute command deploy: The connection has been closed by the server .
####
## Exit code is 1
Failed to register DS in JESMF.
Error: Cannot register mfwk into cacao framework:
```

Use the following steps to complete the installation after the failure:

1. Add the following to `mfwk.properties` in order to start Cacao.

   ```
   com.sun.mfwk.agent.objects=false
   ```

2. Run the following command to restart Cacao.

   ```
   cacaoadm start
   ```

   Confirm that Cacao continues to run.

3. Run the following two commands:

   ```
   $ dsccsetup mfwk-unreg
   $ dsccsetup mfwk-reg -t
   ```

4. Run the following command to confirm that `mfwk` is properly registered in Cacao framework

   ```
   $ install-path/dsee6/cacao_2/bin/cacaoadm list-modules
   ```

   If `mfwk` is properly registered, the command returns these results:

   ```
   List of modules registered:
   com.sun.cacao.agent_logging 1.0
   com.sun.cacao.command_stream_adaptor 1.0
   com.sun.cacao.efd 2.1
   com.sun.cacao.instrum 1.0
   com.sun.cacao.invoker 1.0
   com.sun.cacao.mib2simple 1.0
   com.sun.cacao.rmi 1.0
   com.sun.cacao.snmpv3_adaptor 1.0
   com.sun.cmm.ds 1.0
   ```

```
com.sun.directory.nquick 1.0
com.sun.mfwk 2.0
```

5. Copy the following two files to *install-path*`/dsee6/bin`:

   installer-path`\DSEE_ZIP_Distribution\dsee_deploy.exe`
   installer-path`\DSEE_ZIP_Distribution\dsee_data\listrunnings.exe`

6756152/2168088 LDAP commands do not work on Windows (IPv6 enable)

6772760 An attempt to stop the server immediately after it starts might cause a crash in versions of DSEE 6.

6772879 The Directory Server Enterprise Edition 5.x password policy manages attributes with a `password*` naming pattern, and the Directory Server Enterprise Edition 6.x password policy manages attributes with a `pwd*` naming pattern. When running in Directory Server Enterprise Edition compatibility mode (such that attributes of both policies are managed), if a password policy's functionality is disabled, then some values of related attributes can differ between the 5.x attributes and the 6.x attributes. For example, if `passwordUnlock` is set to `off`, then the value of `pwdLockoutDuration` can be `0` at the same time that the value of `passwordLockoutDuration` is <>`0`.

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.`

6777338 In case of a Multi-Master Replication migration from Directory Server 5.2 to Directory Server 6.3, the "Manual Reset of Replication Credentials" in *Sun Java System Directory Server Enterprise Edition 6.3 Migration Guide* is not complete. The procedure directs you to run this command:

```
dsconf set-server-prop -h host -p port def-repl-manager-pwd-file:filename
```

It is also necessary to run this undocumented command:

```
dsconf set-repl-agmt-prop -p port_master1 replicated_suffix master2:port_master2 auth-pwd-file:filename
```

The `dsmig migrate-config` command returns commands that must be launched to reset replication credentials properly.

6786078 A non-existent Sun Microsystems plug-in can be considered to have a valid signature. The following warning message is displayed:

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

This warning message appears only for plug-ins with a vendor of Sun Microsystems.

6790060 An unindexed search involving ACI evaluation that returns few entries can cause very low search performance. This issue applies only to this release DSEE6.3.1.

6791372 A memory shortage resource can cause versions of Directory Server 6 to crash. The following error message is written in the server `errorlog` file:

```
ERROR<5122> - binder-based resource limits - conn=-1 op=-1 msgId=-1 -
      System error: resource shortage  PR_NewRWLock() failed for reslimit
```

6827661 A directory server instance cannot be stopped by using `dsadm stop`command via Remote Desktop if the directory server instance was started via the console or the `dsadm start`command locally.

To work around this issue, run the following command to enable the service:

```
dsadm enable-service --type WIN_SERVICE instance-path
```

6831959 Because of a problem described in Vulnerability Note VU#836068, MD5 vulnerable to collision attacks (`http://www.kb.cert.org/vuls/id/836068`), Directory Server Enterprise Edition should avoid using the MD5 algorithm in signed certificates.

Use the following steps to determine the signature algorithm of a certificate.

1. Run the following command to display the list of certificates defined in a specific Directory Server instance.

   ```
   $ dsadm list-certs instance-path
   ```

2. Run the following command on each defined certificate to determine whether the certificate is signed with the MD5 algorithm:

   ```
   $ dsadm show-cert instance-path cert-alias
   ```

   The following example shows typical output from the `dsadm show-cert` command for a MD5–signed certificate:

   ```
   Certificate:
      Data:
      [...]
      Signature Algorithm: PKCS #1 MD5 With RSA Encryption
      [...]
   ```

Run the following command to remove any MD5–signed certificates from the database:

```
$ dsadm remove-cert instance-path cert-alias
```

Use the following steps to update the certificate database password. (The `dsadm` command generates a default certificate database password when creating a directory server instance.)

1. Stop the Directory Server instance.
2. Run the following command:

   ```
   $ dsadm set-flags instance-path cert-pwd-prompt=on
   ```

   A message appears, prompting you for a password.
3. Enter a password that is at least eight characters long.
4. Restart the Directory Server instance and provide the `Internal (Software) Token` when prompted for it.

Replace any MD5–signed certificates with SHA-1–signed certificates. Use one of the following procedures, depending on whether your installation uses a self-signed certificate or a certificate acquired from a Certificate Authority.

Use the following steps to generate and store a self-signed certificate:

1. As a Directory Server administrator, run the following command to issue a self-signed certificate using the SHA-1 signing algorithm. (For more information about the `certutil` command, see http://www.mozilla.org/projects/security/pki/nss/tools/certutil.html

   ```
   $ certutil -S -x -n certName -s subject -d certs-db-path \
   -P "slapd-" -t "CTu,u,u" -Z SHA1
   ```

`-S`	Specifies generation of an individual certificate and adding it to the database.
`-x`	Specifies generation of a self-signed certificate
`-n` *certName*	Specifies the certificate's alias name, for example, `defaultCert`
`-s` "*subject*"	Specifies the certificate owner for new certificates or certificate requests, for example, `CN=...,OU=...`
`-d` *instance-path*`/alias`	Specifies the database directory to contain the certificate and key database files.
`-P "slapd-"`	Specifies the certificate database prefix
`-t "CTu,u,u"`	Specifies the trust arguments

`-Z SHA1`	Specifies SHA-1 as the certificate signature algorithm

The following example shows a typical use:

```
$ install-path/dsee6/bin/certutil -S -x -n "A-New-Cert" \
  -s "CN=myhostname,CN=8890,CN=Directory Server,O=CompanyName" \
  -d instance-path/alias \
  -P "slapd-" -t "CTu,u,u" -Z SHA1
```

The command displays this prompt:

```
[Password or Pin for "NSS Certificate DB"]
```

2. Enter the new certificate database password that you created.

Use the following steps to generate and store a certificate acquired from a Certificate Authority (CA):

1. Run the following command to issue a CA-Signed Server Certificate request:

```
$ certutil -R -s subject -d certs-db-path -P "slapd -a  -Z SHA1 -o output-file
```

`-R`	Specifies to generate a CA-signed Server Certificate request
`-s` "*subject*"	Specifies the certificate owner for new certificates or certificate requests, for example, `CN=...,OU=...`
`-d` *instance-path*`/alias`	Specifies the database directory to contain the certificate and key database files.
`-P` "`slapd-`"	Specifies the certificate database prefix
`-a`	Specifies that the certificate request be created in ASCII format instead of the default binary format
`-o` *output-file*	Specifies the output file for storing the certificate request

The following example shows a typical use:

```
$ install-path/dsee6/bin/certutil -R \
-s "CN=myhostname,CN=7601,CN=Directory Server,O=CompanyName" \
-d instance-path/alias \
-P "slapd-"  -a -o /tmp/cert-req.txt
```

The command displays this prompt:

```
[Password or Pin for "NSS Certificate DB"
```

2. Enter the new certificate database password that you created.
3. Make sure that your Certificate Authority is no longer using the MD5 signature algorithm, and then send the certificate request to the Certificate Authority (either internal to your company or external, depending on your rules) to receive a CA-signed server certificate as described in "To Request a CA-Signed Server Certificate" in *Sun Java System Directory Server Enterprise Edition 6.3 Administration Guide*.
4. When the Certificate Authority sends you the new certificate, run the following command to add the certificate to the certificates database:

   ```
   $ dsadm add-cert ds-instance-path cert-alias signed-cert-alias
   ```

   This step is described in "To Add the CA-Signed Server Certificate and the Trusted CA Certificate" in *Sun Java System Directory Server Enterprise Edition 6.3 Administration Guide*.
5. If the trusted Certificate Authority certificate is not already stored in the certificate database, run the following command to add it:

   ```
   $ dsadm add-cert --ca instance-path trusted-cert-alias
   ```

   This step is described in "To Add the CA-Signed Server Certificate and the Trusted CA Certificate" in *Sun Java System Directory Server Enterprise Edition 6.3 Administration Guide*.
6. Run the following command to verify that the new certificate is being used.

   ```
   $ dsadm show-cert instance-path cert-alias

   Certificate:
      Data:
      [...]
      Signature Algorithm: PKCS #1 SHA-1 With RSA Encryption
      [...]
   ```

6834291

When the `pwd-must-change-enabled` property set to `on` and user account operations are invoked with the proxied authorization control, the only operation that can be performed on behalf of a user with a reset password is modification of the user's account password.

For versions prior to Directory Server Enterprise Edition 6.3.1, this operation was rejected as `account unusable` (as described in CR 6651645). Directory Server Enterprise Edition 6.3.1 added support for changing a reset password using proxied authorization, however, applying the 6.3.1 patch to an existing deployment caused the following issue.

When an account password has been administratively reset, an operation on the account using proxied authorization is not strictly enforced to modifying the userpassword attribute. -

The cause of this issue is a change in the Directory Server plug-in ordering, which is not corrected for any existing instances during the 6.3.1 patch application. Any Directory Server instance created after upgrading to Directory Server Enterprise Edition 6.3.1 has the correct plug-in ordering.

For a Directory Server instance created before upgrading to Directory Server Enterprise Edition 6.3.1, an administrator must correct the instance's plug-in ordering list using the ldapmodify command.

The following example assumes the plug-in ordering has not be modified from the original ordering. If the deployment uses a custom ordering, modify the example to include the customization, but make sure that ACL preoperation precedes any PwP preoperation.

Restart the instance for the change to take effect.

```
$ install-path/dsrk6/bin/ldapmodify
dn: cn=plugins, cn=config
changetype:modify
replace: plugin-order-preoperation-finish-entry-encode-result
plugin-order-preoperation-finish-entry-encode-result: ACL preoperation,PwP preoperation
-
replace: plugin-order-preoperation-search
plugin-order-preoperation-search: ACL preoperation,*
-
replace: plugin-order-preoperation-compare
plugin-order-preoperation-compare: ACL preoperation,*
-
replace: plugin-order-preoperation-add
plugin-order-preoperation-add: ACL preoperation,PwP preoperation,*
-
replace: plugin-order-internalpreoperation-add
plugin-order-internalpreoperation-add: PwP internalpreoperation,*
-
replace: plugin-order-preoperation-modify
plugin-order-preoperation-modify: ACL preoperation,PwP preoperation,*
-
replace: plugin-order-internalpreoperation-modify
plugin-order-internalpreoperation-modify: PwP internalpreoperation,*
-
replace: plugin-order-preoperation-modrdn
plugin-order-preoperation-modrdn: ACL preoperation,*
-
```

```
replace: plugin-order-preoperation-delete
plugin-order-preoperation-delete: ACL preoperation,*
-
replace: plugin-order-bepreoperation-add
plugin-order-bepreoperation-add: PwP bepreoperation,*
-
replace: plugin-order-bepreoperation-modify
plugin-order-bepreoperation-modify: PwP bepreoperation,*
```

6867762

When logs are rotated according to `rotation-time` or `rotation-interval`, the exact time at which the rotation occurs depends on several variables, including the following:

- the values of the `rotation-time`, `rotation-interval`, `rotation-now`, and `rotation-size` properties
- scheduling of the housekeeping thread
- the effective size of the log file when the rotation condition is satisfied

The *timestamp* in the rotated log file (for example, `access.`*timestamp*) can therefore not be guaranteed.

6872923

The First Login Password Policy scenario described in "To Set Up a First Login Password Policy" in *Sun Java System Directory Server Enterprise Edition 6.3 Administration Guide* is not complete. Before running the example, make sure that the Global Password Policy default entry (`"cn=Password Policy,cn=config"`) is configured with the `Password Must Change` property set to `TRUE`.

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.

6902940

Configuration of Cacao can fail on Windows when the environment variable `PERL5LIB` is set to a pre-existing PERL version.

To work around this issue, edit both of the script files. For a ZIP installation of Directory Server Enterprise Edition, edit both of these files:

- *installPath*`/dsee6/cacao_2/configure.bat`
- *installpath*`/dsee6/cacao_2/bin/cacaoadm.bat`

For Sun Java Enterprise System 5 installations of Directory Server Enterprise Edition, edit both of these files:

- `C:\Program Files\Sun\JavaES5\share\cacao_2\configure.bat`
- `C:\Program Files\Sun\JavaES5\share\cacao_2\bin\cacaoadm.bat`

Edit each file and add this line at the beginning of each file:

```
set PERL5LIB=
```

6920893 On Windows installations, the `ldapsearch`, `ldapmodify`, `ldapcompare`, and `ldapdelete` commands fail when multibyte characters are specified as the value for SASL bind options `authid` and `authzid`. Instead of receiving the raw characters, the command receives characters converted incorrectly by the code page used by the installation.

To prevent this conversion and provide to the command the raw characters, use one of the following code pages:

- Code page 1252 for Windows western Europe
- Code page 932 (Shift_JIS) for Windows Japanese

A programmatic solution is to create a new program to fork/exec the command (for example, ldapsearch) and provide the SASL bind arguments through the exec (and so without code-page translation).

6928378 The Administration Guide incorrectly states that you can use the Directory Service Control Center to set a referral to make a suffix be read-only. This capability is not implemented in the Directory Service Control Center unless replication is enabled for this suffix.

CHAPTER 4

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 6.3.1

This section lists the bugs fixed in Directory Proxy Server release 6.3.1.

6492941 An unavailable JDBC source results in a search failure through a JOIN view (LDAP + JDBC), even if no data is required from this JDBC source.

6513526 Running `ldapsearch` on `cn=monitor` returns the leaf entry before the parent entry, a condition that can cause some tools to fail.

6597598 Modifications through a join view of LDAP and JDBC might trigger a NULL pointer exception.

6597607 When no secondary attributes are requested, performance should not be impacted by requests against secondary data sources

6597608 An attempt to apply two modifications as part of a single LDAP transaction can succeed partially if one attribute is not present.

6616898 When using a join view of LDAP and JDBC, the `objectclass` attribute cannot be stored on the secondary view.

6618968 When searching through a join view, the search should be conducted first on the secondary view, in the case that no attributes from the primary view are present in the search filter (and even if several entries are returned from the secondary view).

6630730 A high search load can lead to a NULL pointer exception.

6637173 When searching on a join view of LDAP and JDBC, an entry might not be returned if the bind user has no access right on the requested secondary attributes.

6637608 When running a high search load, exceptions `ArrayIndexOutOfBounds` or `NegativeArraySizeException` can be triggered

6638374 Adding an entry through a join view fails if the `uid` attribute contains capital letters.

6641925 When adding an entry through a join view of LDAP and JDBC, the entry is added in the JDBC view even if no secondary JDBC attributes are included in the add request.

6643181 When adding or replacing an attribute through a join view of LDAP and JDBC, the value is truncated if it is too long for the SQL database.

6646107 When adding an entry through a join view of LDAP and JDBC, the column size is not checked before updating or adding a string (`varchar`) value that results in a database error

6653253 Search stress tests lead to unexpected errors due to a race condition in `FailoverLoadBalancingAlgorithm`.

6653453 Persistent searches over SSL fail to return data.

6654625 Memory management policy in DPS leads to existing connections being disconnected at the same time that GC is triggered (when memory is low).

6656324 When an entry is added, DN values are not always converted to lowercase.

6658613 When a shared attribute (that may exist on two data sources) is deleted through a join view of LDAP and JDBC, an error is returned if the attribute does not exist on one of the two views.

6659381 A JVM crash can occur in 64–bit mode using JDK 1.6 under high search load.

6660383 When JDBC source treats its column values as case sensitive (typically DB2), an attempt to delete a JDBC attribute value can fail.

6661375 Sockets can be stuck in the CLOSE_WAIT state, causing the server to become unresponsive.

6661474 Frequently opened and then closed connections to the server can cause the server to become unresponsive at some time later until a restart is performed.

6663112 On AMD64 Linux machines, the server is unable to start in 32-bit mode.

6670752 Under heavy load, the server can experience timeouts, causing operations to the directory server to be retried.

6671579 When using a virtually mapped base within a search filter, no result are returned under certain circumstances.

6676073 When a Join view is used, modifications intended for the secondary data view can be incorrectly routed to the primary data view.

6680717 Failing to set up a Join rule while configuring a Join view containing a JDBC view can cause a StringIndexOutOfBoundsException exception.

6692627 Some specific search filters can cause the server to return decoding errors.

6697494 When using a Join view containing a JDBC view, an attempt to delete an attribute of an entry that only exists in the directory service fails.

6729861 The `dpadm -V` fails to detect the JVM version.

6734722 The server can let connections to the directory server remain in the `CLOSE_WAIT` state, causing directory server to become unresponsive.

6753712 A search filter containing an attribute of a non-string type (such as float or date) can fail to retrieve results from the JDBC view.

6761017 Internal worker threads can become deadlocked, causing server to become unresponsive.

6761875 High CPU spikes can occur on the server, causing all services on the machine to become unresponsive.

6764873 Improvements to the management of the bound connections to minimize close wait.

6766175 `ldapsearch` can return an empty attribute's value of an entry from MySQL, Derby, or DB2 JDBC back end. With an ORACLE JDBC back end, an empty attribute's value is not returned.

Known Problems and Limitations in Directory Proxy Server

This section lists known problems and limitations at the time ofDirectory Server Enterprise Edition 6.3.1 release.

Note – Sun Directory Proxy Server 6.3.1 update 1 patch 141958–01 is designed to be applied on top of Directory Server Enterprise Edition 6.3.1 to fix issues in the Directory Proxy Server component. For more information, refer to "Directory Proxy Server 6.3.1 Update 1" on page 92.

Directory Proxy Server 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.

Known Directory Proxy Server Issues in 6.3.1

This section lists the known issues that are found at the time of Directory Proxy Server 6.3.1 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.

6356465 Directory Proxy Server can reject ACIs that specify subtypes to the target attribute, such as `(targetattr = "locality;lang-fr-ca")..`

6360059 Directory Proxy Server cannot resume the JDBC data source connection that is restored after the data source connection failure. Directory Proxy Server can resume the connection only after restarting the Directory Proxy Server instance.

6383532 Directory Proxy Server must be restarted when the authentication mode configuration is changed.

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.

6458935 When working with join data views, Directory Proxy Server does not take data distribution algorithms in the views that make up the join.

To work around this issue, configure data distribution at the level of the join data view when using joins and data distribution together.

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.

6469780 Creation of JDBC data source entries is not dynamically detected. If you create a JDBC server before creating a JDBC data view, the data view is ignored until the next restart of the server. After configuring a JDBC data source, therefore, you must restart Directory Proxy Server for the change to be detected.

6486578 For JDBC object classes, where one class, A, uses a table as secondary and another class, B, uses that same table as its only primary, then requests on B do not work. The Directory Proxy Server fails to ignore the `filter-join-rule` property when it is used in a primary table.

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.

6490763 Access Manager, when accessing Directory Server through Directory Proxy Server, has been seen to encounter caching problems related to persistent searches after Directory Server is restarted.

To work around this issue, restart either Access Manager or Directory Proxy Server after restarting Directory Server.

For further fine tuning, you can increase the number of and delay between Access Manager attempts to reestablish persistent search connections. You can increase these parameters by changing the following properties in the `AMConfig.properties` file.

- Increase `com.iplanet.am.event.connection.num.retries`, which represents the number of attempts. The default is 3 attempts.
- Increase `com.iplanet.am.event.connection.delay.between.retries`, which represents the number of milliseconds delay between attempts. The default is 3000 milliseconds.

6490853 If you run a search using JDBC data view configured with DB2 database and there are large number of entries to be returned in the search result, an error might occur after returning `1,344` entries.

To overcome this limitation, increase the number of large packages by setting the value of the `CLI/ODBC` configuration keyword `CLIPkg` to a value up to `30`. Even then the search result is limited to maximum of 11,712 Entries.

For more information, see DB2 documentation.

6491133 When creating a self-signed certificate using Directory Service Control Center, do not use multi-byte characters for the certificate names.

6491845 The default LDAP controls allowed through Directory Proxy Server are not displayed by Directory Service Control Center.

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.

6510583 Unlike previous versions, as stated in the manual page allowed-ldap-controls(5dpconf), Directory Proxy Server does not allow the server side sort control by default.

You can enable Directory Proxy Server support for the server side sort control by adding server-side-sorting to the list of allowed LDAP controls specified by the allowed-ldap-controls property.

```
$ dpconf set-server-prop \
 allowed-ldap-controls:auth-request \
 allowed-ldap-controls:chaining-loop-detection \
 allowed-ldap-controls:manage-dsa \
 allowed-ldap-controls:persistent-search \
 allowed-ldap-controls:proxy-auth-v1 \
 allowed-ldap-controls:proxy-auth-v2 \
 allowed-ldap-controls:real-attributes-only \
 allowed-ldap-controls:server-side-sorting
```

Notice that you must repeat the existing settings. Otherwise, only the server side sort control is allowed.

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`

6527010 Directory Proxy Server cannot write JDBC attributes implying many-to-many (N:N) relationship between tables in the JDBC database.

6539650 Directory Proxy Server instances with multi-byte DN and created using DSCC, fail to start on Linux.

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.

6547755 Directory Proxy Server instance with multi-byte characters in its path may fail to be created in DSCC, to start or perform other regular tasks.

Some of these issues can be resolved by using the charset that was used to create the instance. Set the charset using the following commands:

```
# cacaoadm list-params | grep java-flags
  java-flags=-Xms4M -Xmx64M

# cacaoadm stop
# cacaoadm set-param java-flags="-Xms4M -Xmx64M -Dfile.encoding=utf-8"
# cacaoadm start
```

Use only the ASCII characters in the instance path to avoid these issues.

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.

6565106 If duplicate entries are present in RDBMS table matching a DN pattern found in JDBC object class, then duplicate subtree (non-leaf) nodes would be returned by

Directory Proxy Server when search is performed against the JDBC data view. For example, if there is a DN pattern `ou` in a JDBC object class and there are duplicate entries (say, `sales`) present in the RDBMS column mapped to JDBC attribute `ou`, then there would be duplicate nodes like `ou=sales` present in the search result.

To resolve this issue, do the following:

1. Create an RDBMS view by taking the values from the table that contains the column mapped to `ou` JDBC attribute in such a way that there are no duplicated entries.
2. Replace the RDBMS table name with the RDBMS view name in the JDBC object class with the DN pattern `ou`. The limitation of this approach is that since RDBMS views are read-only, no values for the JDBC attribute `ou` could be added through Directory Proxy Server.

6567644 DPS constructs illegal DB requests.

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.

6592543 The pop-up windows prompting the confirmation for stopping or unregistering servers display the doubled apostrophes in the French locale.

6597598 When performing modifications using the `modrate` tool against a joint view, with both LDAP and JDBC, nullpointer exceptions occur when using more than 1 thread. The errors are similar to the following:

```
java.lang.NullPointerException  com.sun.directory.proxy.server.JoinDataView.
processModifyRequest(JoinDataView.java:916)
com.sun.directory.proxy.server.JoinDataViewOpContext.processModifyRequest
(JoinDataViewOpContext.java:243) com.sun.directory.proxy.server.ModifyOperation.
processOperation(ModifyOperation.java:502 com.sun.directory.proxy.server
.WorkerThread.runThread(WorkerThread.java:150)
com.sun.directory.proxy.util.DistributionThread.run
(DistributionThread.java:225)
```

6609603 When a new data source is added to a data source pool, server restart is required.

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.

6642559 Writing virtual transformations does not work for the `remove-attr-value` transformation model.

6642578 Writing virtual transformations does not work as expected when an entry is modified.

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.

6711054 Attempting to add an attribute value of `smalldatetime` SQL TYPE triggers the following exception:

```
ldap_modify: Operations error
ldap_modify: additional info: java.lang.Exception:
java.lang.Exception: com.microsoft.sqlserver.jdbc.SQLServerException: Conversion failed
 when converting datetime from character string.
```

Directory Proxy Server 6.3.1 Update 1

The following sections discuss Directory Proxy Server 6.3.1 update 1:

- “About Directory Proxy Server 6.3.1 Update 1” on page 93
- “Bugs Fixed in Directory Proxy Server 6.3.1 Update 1” on page 99
- “Installation Notes for Directory Proxy Server 6.3.1 Update 1” on page 102
- “Known Problems and Limitations in Directory Proxy Server 6.3.1 Update 1” on page 105

About Directory Proxy Server 6.3.1 Update 1

This patch corrects issues only in the Directory Proxy Server component of the Directory Server Enterprise Edition product. It is designed to be applied on top of Directory Server Enterprise Edition 6.3.1. The Directory Server component of Directory Server Enterprise Edition 6.3.1 remains unchanged.

Note – This update cannot be applied to versions of Directory Server Enterprise Edition earlier than 6.3.1. For directions to upgrade to version 6.3.1, see Table 2–1, “Upgrade Paths to Directory Server Enterprise Edition 6.3.1.”

This section discusses the following subjects:

- “What's New in This Release” on page 93
- “Enhancements in Directory Proxy Server 6.3.1 Update 1” on page 93
- “Supported Platforms” on page 98

What's New in This Release

This update is a minor release that primarily fixes the bugs described in “Bugs Fixed in Directory Proxy Server 6.3.1 Update 1” on page 99.

Directory Proxy Server 6.3.1 update 1 also introduces new behavior in persistent search operations. If a client application is very slow in reading the persistent search responses from the directory proxy server, the proxy server response queue becomes overloaded. In this case, the server can close the connection with the following client notification:

```
LDAP_NOTICE_OF_DISCONNECTION [ 1.3.6.1.4.1.1466.20036 ]
```

An informative message similar to the following is also logged:

```
[11/Aug/2009:18:13:51 +0200] - DISCONNECT - INFO  - conn=19 \
reason="admin limit exceeded" \
msg="client didn’t read any data during 160 milliseconds."
```

Enhancements in Directory Proxy Server 6.3.1 Update 1

Directory Proxy Server 6.3.1 update 1 provides the following enhancements:

Capability to set and get `JAVA HOME` using `dpadm set-flags/get-flags` (6765629)

A pathname can be set for `JAVA_HOME` and take precedence over the value of `JAVA_HOME` defined in the environment, as shown in the following example:

```
$ dpadm set-flags instance-path jvm-path=/usr/jdk/latest/
```

Capability to set and get the umask value of DPS configuration and log files (6739456)

The dpadm command changes the umask value, and at the next restart of the DPS instance, the configuration file's permissions are modified according with the new umask value. The log file's permission is also set similarly at the next file rotation. The following example shows a typical use:

```
$ dpadm set-flags instance-path umask=22
```

Unable to add a new virtual transformation with same "MODEL, ACTION, ATTR_NAME" (6722238)

An administrator is now allowed to define different virtual transformations on the same MODEL, ACTION, ATTR_NAME.

Directory Proxy Server 6.3.1 update 1 also adds new properties and updates existing properties, as described in the following list. New properties are noted as “New.” Properties that are changed from their specification in DSEE 6.3.1 are noted as “Updated.”

close-client-connection (New)

Dynamic (no restart required)

Level: connection-handler

Type: boolean

Default: false

Description: Indicates whether the connection handler should close the client connection when no data source is available.

data-view-use-internal-client-identity (New)

Dynamic (no restart required)

Level: connection-handler

Type: boolean

Default: false

Description: Indicates the need to not always use incoming client identity at binding to a remote LDAP server.

Documentation: This property is a flag indicating the need to not always use incoming client identity at binding to a remote LDAP server.

db-vendor (New)

Dynamic (no restart required)

Level: jdbc-data-source

Type: enumeration

`mysql`	RDBMS back-end is MySQL.
`derby`	RDBMS back-end is Apache Derby/Java DB.
`db2`	RDBMS back-end is DB2.
`oracle`	RDBMS back-end is Oracle.
`ms-sql-server`	RDBMS back-end is Microsoft SQL Server.
`generic`	RDBMS back-end is not defined. If possible, Directory Proxy Server determines the vendor name from the `db-url` defined in `jdbc-data-source`.

Default: `generic`

Description: Vendor name of the JDBC data source

Documentation: This property specifies the vendor name of the JDBC data source. This should be set if a third party IDBC driver other than the one provided by the database vendor is used to connect to the RDBMS back-end. This data is used to construct vendor-specific SQL statements when possible that might improve performance.

numeric-lower-bound (Updated)

Dynamic (no restart required)

Level: `jdbc-data-view`, `join-data-view`, `ldap-data-view`, and `ldif-data-view`

New type: long

Old type (for DPS 6.0 to 6.3.1): integer

The other attributes remain the same as before.

numeric-upper-bound (Updated)

Dynamic (no restart required)

Level: `jdbc-data-view`, `join-data-view`, `ldap-data-view`, and `ldif-data-view`

New type: long

Old type (for DPS 6.0 to 6.3.1): integer

The other attributes remain the same as before.

down-monitoring-interval (New)

Static (restart required)

Level: `ldap-data-source`

Type: duration in seconds (lower bound: `1`)

Default: inherited (value of `monitoring-interval`)

Description: Interval at which availability monitor polls failed connections to detect their recovery

Documentation: This property specifies the polling interval. When a connection is found to be down, the availability monitor polls the connection at this interval to detect its recovery. If not specified, the value of the `monitoring-interval` property is used.

monitoring-retry-count (New)
Static (restart required)

Level: `ldap-data-source`

Type: integer (lower limit: `1`)

Default: `3`

Description: Number of retries to perform before flagging the connection as down

Documentation: This property specifies the number of times that the availability monitor polls the connection when it is first detected as down. This allows the connection to be flagged as up faster. If the connection still fails after the specified number of retries, the value of the `down-monitor-interval` property is then used as the polling interval.

use-tcp-keep-alive (New)
Dynamic (no restart required)

Level: `ldap-data-source`

Type: boolean

Default: `true`

Description: Specifies whether `SO_KEEPALIVE` is enabled for connections between the server and the data source

Documentation: This property is a flag indicating whether or not `SO_KEEPALIVE` should be enabled for connections between the server and the data source.

use-tcp-keep-alive (New)
Dynamic (no restart required)

Level: `ldap-listener` and `ldaps-listener`

Type: boolean

Default: `true`

Description: Specifies whether `SO_KEEPALIVE` is enabled for connections between clients and listener

Documentation: This property is a flag indicating whether or not `SO_KEEPALIVE` should be enabled for connections between clients and listener.

allow-unauthenticated-operations (Updated)
Dynamic (no restart required)

Level: server

Type: boolean

Default: `true`

New description: Indicates whether the server accepts unauthenticated operations

Old description (for DPS 6.0 to DPS 6.3.1): Indicates whether the server accepts operations from anonymous clients

New documentation: This property is a flag indicating whether or not Directory Proxy Server accepts unauthenticated operations. The mode used to tread the bind operation is specified by `allow-unauthenticated-operations-mode`

Old documentation (for DPS 6.0 to DPS 6.3.1): This property is a flag indicating whether or not Directory Proxy Server allows anonymous clients to perform operations.

allow-unauthenticated-operations-mode (New)
Dynamic (no restart required)

Level: server

Type: enumeration

`anonymous-only`	When no password is specified, only anonymous binds are allowed
`dn-identified-only`	When no password is specified, only binds with a DN specified are allowed
`anonymous-and-dn-identified`	When no password is specified, anonymous binds and binds with a DN specified are allowed

Default: `anonymous-and-dn-identified`

Description: Mode to treat bind operations without password

Documentation: This property indicates how to Directory Proxy Server treats operations without bind password when `allow-unauthenticated-operations` is set to true.

time-resolution (Updated)
Static (restart required)

Level: server

Type: duration in milliseconds

New default: 250

Old default (for DPS 6.0 to 6.3.1): 500

New documentation: This property specifies the time interval between consecutive system calls that retrieve time from the OS. For details about operations that take less than 250 milliseconds, reduce the `time-resolution` period or change the value of the `time-resolution-mode` property. If set to 0 milliseconds, the proxy behaves as if the value of the `time-resolution-mode` property was set to system-milli. This property is ignored when the value of the `time-resolution-mode` property is set to `system-milli` or `system-micro`.

Old documentation (for DPS 6.0 to 6.3.1): This property specifies the time interval between consecutive system calls that retrieve time from the OS. For details about operations that take less than 500 milliseconds, reduce the `time-resolution` period. If set to 0 milliseconds, the proxy systematically performs a system call to retrieve the current time. Otherwise the time is cached and retrieved only every `time-resolution` period. This time is displayed in the logs.

The description remains the same as before.

time-resolution-mode (New)

Static (restart required)

Level: server

Type: enumeration

`custom-resolution`	Use a thread performing a system call every `time-resolution` milliseconds
`system-milli`	Use a system call retrieving time in milliseconds
`system-micro`	Use a system call retrieving time in microseconds

Default: `custom-resolution`

Description: Mode used to retrieve system time

Documentation: This property specifies the mode used to retrieve time from the OS.

Supported Platforms

Directory Proxy Server 6.3.1 update 1 is available for all supported Directory Server Enterprise Edition 6.3.1 platforms. For more information, see “Hardware Requirements” on page 26 and “Operating System Requirements” on page 27.

Bugs Fixed in Directory Proxy Server 6.3.1 Update 1

This section lists the bugs fixed in Directory Proxy Server 6.3.1 update 1.

6567644 Directory Proxy Server constructs illegal database requests.

6590816 Setting `connectionIdleTimeOutInSec` for LDAP listener can disable DSCC.

6641888 A search operation can return entries that contain attributes that are not present in `viewable-attr`.

6648665 The `max-client-connections` property is not enforced if no operation is performed on the connection.

6681502 Memory monitoring is disabled by default.

6686150 The numeric distribution algorithm should use `long` instead of `int` to set numeric bounds.

6717943 The Directory Proxy Server default size limit for resource properties uses the incorrect integer for unlimited.

6721192 DN transformations fail.

6721749 The setting of `add-attr-value` can cause DN transformations to produce incorrect output.

6722222 The bindDN should be mapped when binding to a LDAP server. (using DN mapping rule of the DV of the bindDN).

6722238 It is not possible to add a new virtual transformation with same "MODEL, ACTION, ATTR_NAME".

6723858 The `requires-bind-password` property set on a back-end directory server is not enforced.

6734559 Virtual DN mapping fails when depending on a virtual attribute.

6736621 Bind DN is rejected when transformation fails, even when it falls into the view.

6737084 Wrong DN mapping for the from server direction.

6739414 Upper/lowercase characters in attribute names are being transformed by 6.3 Directory Proxy Server.

6739456 A customer requested for Directory Proxy Server to set group permissions for config and log files (umask 117, chmod 660).

6751692 The `dpadm start` command dumps a core when using the `MaxTenuringThreshold` java argument.

6758793 DN mapping can drop renamed entries.

6760526 The `dpadm` does not generate a `DPS.pid` file.

6760951 Directory Proxy Server configuration schema are inconsistent with the `SystemMonitorThread.java` feature.

6761032 The server and console are inconsistent for searchMode parameter.

6764073 Directory Proxy Server fails when configured to use proxied authentication.

6765629 Allow for `JAVA HOME` to be set using `dpadm set-flags`.

6767776 DN mapping cannot be used on rootDSE.

6774589 Directory Proxy Server requires virtual DN transformation with multi-valued naming attributes.

6778262 Microseconds time granularity should be provided for etimes.

6778308 The `splitldif` command ignores virtual transformations.

6780423 Under heavy load, sockets can remain in the close wait state.

6782659 The `SO_KEEPALIVE` option is not set in Directory Proxy Server 6.3 (that is, setKeepAlive() != True) when a socket is created.

6798674 The fix for CR 6513526 can introduce regressions because of null values in `ConfigAttribute` objects.

6802371 The `acceptBacklog` property is ignored for channel-based listeners.

6808701 Inactivity heartbeats are not send often enough because of last activity on a backend connection.

6808704 Inactivity heartbeats are not sent for bound backend connections.

6808706 Backend server checks might not occur often enough because of last server activity.

6809099 The `ldapsearch` run on monitor entries can give inconsistent output.

6809712 An availability check should make sure that the backend server is down before cutting all connections.

6817976 A connection can become blocked in case of abandon request.

6818788 Better accuracy is required in the backend heart-beat.

6818926 A file descriptor leak occurs in server socket.

6819304 A null pointer exception can occur when searching on `cn=monitor` if a failover pool is defined with no source.

6819315 Directory Proxy Server continues opening connections to the directory server after an attempt to bind... fails.

6819752	Persistent search clients may not receive entry change notifications.
6821356	Two connections can share the same identifier.
6821752	Persistent searches are not cleaned up after client disconnect.
6823036	The proactive monitoring interval should be set to 1 second when a datasource is detected as down.
6823593	Directory Proxy Server associates different client operations with the same backend connection.
6827104	Backend connections are not closed but reused if idle is more than `inactivity-timeout`, causing a connection leak.
6827129	Connection pool housekeeping and health-check processing should be DEBUG.
6828462	Two simultaneous long binds assign the same backend connection to two clients connections.
6828841	Setting an incorrect `jvm-path` hangs the restart without any warning.
6828842	Directory Proxy Server returns the wrong error code when no back-end servers are available
6828896	An option should be provided to close client connection in case of "cannot retrieve backend connection".
6832043	Client affinity should not be enabled when useAffinity=false and affinityPolicy is explicitely set.
6835931	Directory Proxy Server cannot be started if one of the data source host is unreachable.
6836922	The `dpconf` command should support new attributes introduced in Directory Proxy Server 6.3.1_update 1.
6837295	The `dpconf` command should support bind DN mapping.
6837392	More simple versioning should be provided for management of Directory Proxy Server properties.
6837970	The `dpconf` should support `monitorRetryCount`.
6839452	Client affinity ignores the data source's read-only flag.
6844727	Implementation of fixes for CR 6714425 and 6714448 should be completed.
6851216	A lowercase join expression can cause SQL requests to fail.
6854864	Directory Proxy Server 6.3.1 performance is inadequate when more than 100 clients are performing persistent searches.

6855978	Persistent search thread looping and the Directory Proxy Server can no longer handle persistent searches
6859116	The performance of the persistent search is inadequate.
6860746	Creating 20 persistent searches and then stopping them causes persistent search functionality to fail.
6868131	Directory Proxy Server returns `StringIndexOutOfBoundsException` in certain cases of attribute mapping and virtual transformation.
6868804	The transformation and mapping rules do not perform as expected.
6870051	Threads can be released prematurely, producing an ASN.1 exception.
6870452	The Directory Proxy Server returns an incorrect error when the back end goes down.
6870496	An unexpected null pointer exception can be raised.
6874644	Under some circumstances, the password storage scheme can be ignored by the JDBC data view.
6879124	The Directory Proxy Server can return identical results when different users bind on a client connection.
6881972	Under some circumstances, the Directory Proxy Server can fail to start when using JDBC.
6886109	An unexpected ASN1 exception can occur and not be handled.

Installation Notes for Directory Proxy Server 6.3.1 Update 1

This discusses the following topics:

- "Getting the Software" on page 102
- "Installation Instructions" on page 103

Getting the Software

Directory Proxy Server 6.3.1 update 1 is a patch that is applied to an existing installation of Directory Server Enterprise Edition 6.3.1. If you are running Directory Server Enterprise Edition version earlier than 6.3.1, you must first upgrade to version 6.3.1 as described in Chapter 2, "Installation Notes," before applying the patch for Directory Proxy Server 6.3.1 update 1.

You can download the Directory Proxy Server 6.3.1 update 1 patch from `http://www.sun.com/software/products/directory_srvr_ee/get.jsp`.

Directory Proxy Server 6.3.1 update 1 is a unique patch for all the DSEE platforms:

- Solaris SPARC
- Solaris 9 x86
- Solaris 10 x86 and AMD x64
- Red Hat Linux
- SuSe Linux
- HP-UX
- Windows

For each platform, the following distributions are available:

- Native package distribution (except for HP-UX)
- Zip distribution

Directory Proxy Server 6.3.1 update 1 patch 141958-01 is available through SunSolve (`http://sunsolve.sun.com`) and applies to both of the following kinds of installation:

- Directory Server Enterprise Edition 6.3.1 native packages installed using the Java ES installer
- Directory Server Enterprise Edition 6.3.1 zip installations

Installation Instructions

This section describes how to install the Directory Proxy Server 6.3.1 update 1.

▼ To Install the Patch on Both Zip and Native Package Installations of Directory Proxy Server 6.3.1

Before You Begin

Note – Back up the Directory Server Enterprise Edition installation directory before applying the Directory Proxy Server 6.3.1 update 1 patch, because you cannot restore an earlier Directory Proxy Server configuration later. This advice applies to both Zip and Native Packages installations.

1. **Download Patch 141958-01 from Sunsolve to a *downloaded-patch-path* directory.**

2. **Stop the Directory Proxy Server instances associated with the installation that you intend to patch.**

3. **On Windows systems, open a Command Prompt window. On UNIX systems, open a terminal window.**

4 **Change the current directory to the directory with installation software for the platform and distribution (zip or native) that you want to update:**

The following example shows a typical command for this purpose:

```
$ cd downloaded-patch-path/SunOS_x64/zip/delivery
```

The following table shows the locations of installation software under the *downloaded-patch-path* directory.

Operating System	Directory Containing the Zip Delivery	Directory Containing the Native Package Delivery
Solaris SPARC	`SunOS/zip/delivery`	`SunOS/native/delivery`
Solaris 9 x86	`SunOS_x86/zip/delivery`	`SunOS_x86/native/delivery`
Solaris 10 x86 and AMD x64	`SunOS_x64/zip/delivery`	`SunOS_x64/native/delivery`
Red Hat Linux	`Linux/zip/delivery`	`Linux/native/delivery`
SuSE Linux	`Linux/zip/delivery`	`Linux/native/delivery`
HP-UX	`Hpux/zip/delivery`	`N/A`
Windows	`Windows/zip/delivery`	`Windows/native/delivery`

5 **On UNIX systems, launch the installation script.**

Run the following command:

```
$ Install dsee631-install-path
```

where *dsee631-install-path* is the path to the directory where Directory Server Enterprise Edition 6.3.1 is installed.

The following messages appear:

```
--------------------------------------------------------------------
IMPORTANT :
Make sure all the DPS instances associated with the Directory Proxy Server
installation being patched are shutdown prior to apply the Directory Proxy
Server 6.3.1 Update 1 Patch
--------------------------------------------------------------------
Do you want to proceed with the installation (y/Y to proceed, n/N to abort) [n] ?
```

Enter **`y`** for yes. The installation program applies the patch on the Directory Server Enterprise Edition 6.3.1 installation that you specified.

6 **On Windows installations, run the following command in the Command Prompt window:**

```
Install.exe
```

A wizard opens and requests that you browse and select the correct installation path for installing the Directory Proxy Server 6.3.1 update 1 patch. To patch a 6.3.1 ZIP installation, select the directory where you installed Directory Server Enterprise Edition 6.3.1. To patch a Native Package installation, select `C:\Program Files\Sun\JavaES5\DSEE`.

The wizard applies the patch on Directory Server Enterprise Edition 6.3.1.

7 **Confirm that the installation is successful by running these two commands and verifying that the response is the same as shown here:**

```
$ dpadm -V
[dpadm]
dpadm               : 6.3.1.1             B2009.1106.0156 ZIP

[DPS]
Sun Microsystems, Inc.
Sun-Java(tm)-System-Directory-Proxy-Server/6.3.1.1 B2009.1106.0259
$ dpconf -V
[dpconf]
clip.jar        : 6.3.1    B2008.1121.0155
dpcfg.jar       : 6.3.1.1  B2009.1106.0155
dpcfgcli.jar    : 6.3.1.1  B2009.1106.0155
common.jar      : 6.3.1    B2008.1121.0155
common_cfg.jar  : 6.3.1    B2008.1121.0155
```

8 **This step is required if the Directory Server Enterprise Edition 6.3.1 that you are patching includes hot fix for CR 6722222.**

If the hot fix for CR 6722222 (Map bindDN when binding to a LDAP server (using DN mapping rule of the DV of the bindDN)) has been applied, run the following command in all the instances for every connection handler:

```
$ dpconf set-connection-handler-prop -p port -h host connection handler \
  data-view-use-internal-client-identity:true
```

This property is a flag that indicates that it is not always required to use incoming client identity at binding to a remote LDAP server. After CR 6722222 is applied, the default behavior can now be configured with a connection handler property, as shown in the example.

9 **Restart all proxy server instances.**

Known Problems and Limitations in Directory Proxy Server 6.3.1 Update 1

This section lists the known problems and limitations that are found at the time of the Directory Proxy Server 6.3.1 update 1 release.

Note – Known issues and limitations in Directory Proxy Server 6.3.1 persist even after the patch for Directory Proxy Server 6.3.1 update 1 is applied. Refer to "Known Problems and Limitations in Directory Proxy Server" on page 85 for information about these issues.

Known Limitations in Directory Proxy Server 6.3.1 Update 1

This section lists the known limitation that is found at the time of the Directory Proxy Server 6.3.1 update 1 release.

As described in "JDBC Object Classes" in *Sun Java System Directory Server Enterprise Edition 6.3 Reference*, defining JDBC tables uses primary and secondary tables. Directory Proxy Server does not allow a secondary table to be the primary table of a third table. That is, Directory Proxy Server does not support more than one level of join-rule.

Known Problems in Directory Proxy Server 6.3.1 Update 1

This section lists the known problems that are found at the time of the Directory Proxy Server 6.3.1 update 1 release.

6728746 In release 6.3, if an entry has more than two object classes, adding an entry through a join view (LDAP and JDBC) fails because of the fix for CR 6636463. To add such an entry, these object classes must be defined as a super-class in the `jdbc-object-class` configuration entry by the following `ldapmodify`, because `dpconf set-jdbc-object-class-prop` can add only one super-class.

This example adds the following entry:

```
dn: uid=test,ou=people,o=join
sn: User
cn: Test User
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
uid: test
userpassword: password
givenname: Test
mail: test@example.com
telephonenumber: 8888-8888
roomnumber: 8000
```

The JDBC view is defined as shown in the following example, which was functional before release 6.3.

```
dn: cn=person,cn=example-view,cn=data views,cn=config
secondaryTable: country1
secondaryTable: phone1
primaryTable: employee1
objectClass: top
objectClass: configEntry
objectClass: jdbcObjectClassMapping
dnPattern: uid
cn: person
superclass: top
```

Because `objectClass:organizationalPerson` and `objectClass:inetOrgPerson` both exist in the entry being added, it is necessary to specify both object classes as super classes, as demonstrated by following `ldapmodify` command.

```
$ ldapmodify -p dpsPort -D "cn=Proxy manager" -w password
dn: cn=person,cn=example-view,cn=data views,cn=config
changetype: modify
add: superClass
superClass: inetOrgPerson
-
add: superClass
superClass: organizationalPerson
```

After this `ldapmodify` example runs, `jdbc-object-class` is defined as shown in the following example.

```
dn: cn=person,cn=example-view,cn=data views,cn=config
secondaryTable: country1
secondaryTable: phone1
primaryTable: employee1
objectClass: top
objectClass: configEntry
objectClass: jdbcObjectClassMapping
dnPattern: uid
cn: person
superclass: top
superclass: inetOrgPerson      Added
superclass: organizationalPerson      Added
```

6826694 Although the default setting for the `log-level-data-sources-detailed` property is documented as being none, the actual default value is `all`. However, setting `log-level-data-sources-detailed`to any value other than none impacts server performance and makes the `access` file grow quickly. For that reason, the value of the `log-level-data-sources-detailed` setting is automatically set to `none` when a DPS server instances is created. It is recommended that you not set this setting to some other value.

6832498 Because of a problem described in Vulnerability Note VU#836068, MD5 vulnerable to collision attacks (`http://www.kb.cert.org/vuls/id/836068`), Directory Proxy Server should avoid using the MD5 algorithm in signed certificates.

Use the following steps to determine the signature algorithm of a certificate.

1. Run the following command to display the list of certificates defined in a specific Directory Proxy Server instance:

   ```
   $ dpadm list-certs instance-path
   ```

2. Run the following commands on each defined certificate to determine whether the certificate is signed with the MD5 algorithm:

   ```
   $ dpadm show-cert -F ascii -o cert-output-file \
   dps-instance-path  cert-alias

   $ dsadm add-cert ds-instance-path cert-alias \
   cert-output-file

   $ dsadm show-cert ds-instance-path  cert-alias
   ```

   The following example shows typical output from the `dsadm show-cert` command for a certificate signed with the MD5 signature algorithm:

   ```
   Certificate:
      Data:
      ...
      Signature Algorithm: PKCS #1 MD5 With RSA Encryption
      ...
   ```

3. Run the following command to remove any MD5–signed certificates from the database:

   ```
   $ dsadm remove-cert instance-path  cert-alias
   ```

Use the following steps to update the certificate database password. (The `dpadm` command generates a default certificate database password when creating a directory proxy server instance.)

1. Stop the Directory Proxy Server instance.
2. Run the following command:

   ```
   $ dpadm set-flags instance-path cert-pwd-prompt=on
   ```

A message appears, prompting you for a password.

3. Enter a password that is at least eight characters long.
4. Restart the Directory Proxy Server instance and provide the `Internal (Software) Token` when prompted for it.

Replace any certificates using the MD5 function with certificates that use the SHA-1 signature algorithm. Use one of the following procedures, depending on whether your installation uses a self-signed certificate or a certificate acquired from a Certificate Authority.

Use the following steps to generate and store a self-signed certificate:

1. Run the following command:

   ```
   $ dpadm add-selfsign-cert  --sigalg SHA1withRSA \
   dps-instance-path  cert-alias
   ```

   Note – The default signature algorithm is `MD5withRSA`.

   The following prompt appears:

   ```
   [Password or Pin for "NSS Certificate DB"]
   ```

2. Enter the new certificate database password.

Use the following steps to generate and store a certificate acquired from a Certificate Authority (CA):

1. Run the following command to issue a CA-Signed Server Certificate request:

   ```
   $ dpadm request-cert  --sigalg SHA1withRSA instance-path  cert-alias
   ```

2. Make sure that your Certificate Authority is no longer using the MD5 signature algorithm, and then send the certificate request to the Certificate Authority (either internal to your company or external, depending on your rules) to receive a CA-signed server certificate as described in "To Request a CA-Signed Server Certificate" in *Sun Java System Directory Server Enterprise Edition 6.3 Administration Guide*.
3. When the Certificate Authority sends you the new certificate, run the following command to add the certificate to the certificates database:

   ```
   $ dpadm add-cert instance-path  cert-alias
   ```

   This step is described in "Creating, Requesting and Installing Certificates for Directory Proxy Server" in *Sun Java System Directory Server Enterprise Edition 6.3 Administration Guide*.

4. If the trusted Certificate Authority certificate is not already stored in the certificate database, run the following command to add it:

   ```
   $ dpadm add-cert --ca instance-path trusted-cert-alias
   ```

   This step is described in "Creating, Requesting and Installing Certificates for Directory Proxy Server" in *Sun Java System Directory Server Enterprise Edition 6.3 Administration Guide*.

5. Run the following commands to verify that the new certificate is being used.

   ```
   $ dpadm show-cert -F ascii -o cert-output-file \
     dps-instance-path cert-alias

   $ dsadm add-cert ds-instance-path cert-alias \
     cert-output-file

   $ dsadm show-cert ds-instance-path cert-alias
   ```

6854861 With a Microsoft SQL Server back end, when using `smalldate` fields, only the long version of dates are supported, or else a conversion error occurs, as shown in the following example.

```
ldap_modify: Operations error
ldap_modify: additional info: java.lang.Exception: \
com.microsoft.sqlserver.jdbc.SQLServerException: \
Conversion failed when converting datetime from character string.
```

Note – The long version of a date uses the form *YYYY*-*MM*-*DD HH*:*MM*.

CHAPTER 5

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.

If your installation uses Identity Synchronization for Windows and you have applied the latest NSS patch 3.12 on your system, set symbolic links to the new libraries delivered in NSS patch 3.12, as described in step 8 of "To Upgrade Shared Components Using Patches" on page 39.

Identity Synchronization for Windows Bugs Fixed and Known Problems

Directory Server Enterprise Edition 6.3.1 includes no changes to Identity Synchronization for Windows. See the *Sun Java System Directory Server Enterprise Edition 6.3 Release Notes* for more information.

This section lists known problems and limitations exposed in Identity Synchronization for Windows product after the release of Directory Server Enterprise Edition 6.3.1.

6572575 Groups and members of group must reside at the same level in the DIT to be synchronized properly. Also, groups cannot have more than 1001 members.

6721443 If debug logs for ISW connectors are activated, connectors fail to reach synchronization step.

6879679 If the Solaris operating system is rebooted by the `shutdown -i6 -g0 -y` command, the stop method for Identity Synchronization for Windows is not called, and the `pid` in the `pid.txt` file is not cleared. As a result, sometimes Identity Synchronization for Windows can fail to start automatically after rebooting the operating system.

To work around this limitation, create a hard link from `/etc/rc2.d/K41isw` to `/etc/rc0.d/K41isw`.

```
$ ln /etc/rc2.d/K41isw /etc/rc0.d/K41isw
```

◆ ◆ ◆ CHAPTER 6

Directory Editor Bugs Fixed and Known Problems

This chapter contains product-specific information available at the time of release of Directory Editor.

Directory Editor Bugs Fixed and Known Problems

Directory Server Enterprise Edition 6.3.1 includes no changes to Directory Editor. See the *Sun Java System Directory Server Enterprise Edition 6.3 Release Notes* for more information.

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 section: "Known Problems and Limitations in Directory Server Resource Kit" on page 115

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 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.

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

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.
```