Sun Java System Directory Server Enterprise Edition Bundle Patch 6.3.1.1.2 Release Notes

Part No: E26994
July 2013

ORACLE

130708@25097

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 Bundle Patch 6.3.1.1.2 Release Notes	(This document) Explains how to install the latest patch (Bundle Patch) on top of an existing Directory Server Enterprise Edition 6.3.1 or 6.3.1.1.1 installation.
Sun Java System Directory Server Enterprise Edition 6.3.1 Release Notes	Contains important information available at the time of the Directory Server Enterprise Edition 6.3.1 release. New features and enhancements, known limitations and problems, technical notes, and other information about version 6.3.1 are addressed here.
Sun Java System Directory Server Enterprise Edition 6.3 Release Notes	Contains important information available at the time of the Directory Server Enterprise Edition 6.3 release. New features and enhancements, known limitations and problems, technical notes, and other information about version 6.3 are addressed here.
Sun Java System Directory Server Enterprise Edition 6.3 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 Directory Server Enterprise Edition 6.3. 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.

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

Document Title	Contents
Sun Java System Directory Server Enterprise Edition 6.3 Installation Guide	**Note –** To install Directory Server Enterprise Edition Bundle Patch 6.3.1.1.2, use the instructions in Chapter 2, "Installation Notes." Do not attempt to use the installation instructions in *Sun Java System Directory Server Enterprise Edition 6.3 Installation Guide* to install version 6.3.1.1.2. 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, read the installation instructions in the *Sun Java System Directory Editor 1 2005Q1 Installation and Configuration Guide*. (`http://download.oracle.com/docs/cd/E19483-01/819-2191/index.html`) Make sure you read the information in *Sun Java System Directory Server Enterprise Edition 6.3 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.
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 the Directory Editor, see the *Sun Java System Directory Editor 1 2005Q1 Installation and Configuration Guide* (`http://download.oracle.com/docs/cd/E19483-01/819-2191/index.html`).
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.

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

Document Title	Contents
Oracle 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 now at version 6.0 Service Pack 1. For best results, install Identity Synchronization for Windows 6.0 Service Pack 1. For detailed information, see *Installation Instructions for Identity Synchronization for Windows 6.0 Service Pack 1* (`http://docs.oracle.com/cd/E20295_01/html/821-1581/index.html`).

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.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://www.oracle.com/technetwork/java/jndi/`. The *JNDI Tutorial* contains detailed descriptions and examples of how to use JNDI. This tutorial is at `http://download.oracle.com/javase/jndi/tutorial/`.

Directory Server Enterprise Edition was 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 was a software infrastructure that supported enterprise applications distributed across a network or Internet environment. Directory Server Enterprise Edition was licensed as a component of Java Enterprise System, and 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.oracle.com/cd/E19340-01/820-6740/index.html`.

Identity Synchronization for Windows works with Microsoft Windows password policies.

- Information about password policies for Windows 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 the *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, the default *install-path* is the current directory. You can set the *install-path* using the `-i` option of the `dsee_deploy` command. See the *Sun Java System Directory Server Enterprise Edition 6.3 Man Page Reference* 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`.

TABLE P–2 Default Paths *(Continued)*

Placeholder	Description	Default Value
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 in the *Sun Java System Directory Server Enterprise Edition 6.3 Man Page Reference*.

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`
`certutil`	Solaris - `/usr/sfw/bin/certutil`	*install-path*`/dsee6/bin/certutil`
	Red Hat - `/opt/sun/private/bin/certutil`	
`dpadm`	*install-path*`/dps6/bin/dpadm`	*install-path*`/dps6/bin/dpadm`
`dpconf`	*install-path*`/dps6/bin/dpconf`	*install-path*`/dps6/bin/dpconf`
`dsadm`	*install-path*`/ds6/bin/dsadm`	*install-path*`/ds6/bin/dsadm`
`dsccmon`	*install-path*`/dscc6/bin/dsccmon`	*install-path*`/dscc6/bin/dsccmon`
`dsccreg`	*install-path*`/dscc6/bin/dsccreg`	*install-path*`/dscc6/bin/dsccreg`

TABLE P–3 Command Locations *(Continued)*

Command	Java ES, Native Package Distribution	Zip Distribution
`dsccsetup`	*install-path*`/dscc6/bin/dsccsetup`	*install-path*`/dscc6/bin/dsccsetup`
`dsconf`	*install-path*`/ds6/bin/dsconf`	*install-path*`/ds6/bin/dsconf`
`dsee_deploy`	Not provided	*install-path*`/dsee6/bin/dsee_deploy`
`dsmig`	*install-path*`/ds6/bin/dsmig`	*install-path*`/ds6/bin/dsmig`
`entrycmp`	*install-path*`/ds6/bin/entrycmp`	*install-path*`/ds6/bin/entrycmp`
`fildif`	*install-path*`/ds6/bin/fildif`	*install-path*`/ds6/bin/fildif`
`idsktune`	Not provided	At the root of the unzipped zip distribution
`insync`	*install-path*`/ds6/bin/insync`	*install-path*`/ds6/bin/insync`
`ns-accountstatus`	*install-path*`/ds6/bin/ns-accountstatus`	*install-path*`/ds6/bin/ns-accountstatus`
`ns-activate`	*install-path*`/ds6/bin/ns-activate`	*install-path*`/ds6/bin/ns-activate`
`ns-inactivate`	*install-path*`/ds6/bin/ns-inactivate`	*install-path*`/ds6/bin/ns-inactivate`
`repldisc`	*install-path*`/ds6/bin/repldisc`	*install-path*`/ds6/bin/repldisc`
`schema_push`	*install-path*`/ds6/bin/schema_push`	*install-path*`/ds6/bin/schema_push`
`smcwebserver`	Solaris, Linux - `/usr/sbin/smcwebserver`	This command pertains only to DSCC when it is installed using native packages distribution.
	Windows - *install-path*`\share\webconsole\bin\smcwebserver`	
`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	`$`
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.

TABLE P–6 Symbol Conventions *(Continued)*

Symbol	Description	Example	Meaning
`{ | }`	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.

◆ ◆ ◆ 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 Directory Server Enterprise Edition, support for Windows 2000, Red Hat Advanced Server 3.0, and J2SE platform 1.4 has been removed. Support for the native install package releases for platforms other than the Solaris operating system has been 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 25 for details of the newer versions of supported operating systems.

JDK versions 1.5 and 1.6 are supported in this release.

Identity Synchronization for Windows 6.0 Service Pack 1 can synchronize with Windows Active Directory 2008.

Directory Server Enterprise Edition Bundle Patch 6.3.1.1.2 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. Some testing has been performed on selected system virtualization and OS combinations to help validate that the products continue to function on properly sized and configured virtualized environments as they do on non-virtualized systems.

For this release, support is provided for any OS running on the Oracle VM technology provided that the OS is already supported natively for the Directory Server Enterprise Edition 6.3 software. Certification is not provided for every combination of OS and hardware, and support relies on the underlying Oracle VM technology implementation. Production deployment of the Directory Server Enterprise Edition 6.3 software on the Oracle VM technology has not been extensively tested. Directory Server Enterprise Edition also supports Solaris Zones and Logical Domains (LDoms), which are part of Oracle VM technology.

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 24.

For details on supported operating systems and OS versions for this release of Directory Server Enterprise Edition, see "Operating System Requirements" on page 25.

Directory Server Changes

Starting with Directory Server Enterprise Edition Bundle Patch 6.3.1.1.1, the use of Cacao and the use of Java Enterprise Monitoring Framework (JESMF) are deprecated and will be replaced in a future release. Also, commands `dsccsetup initialize` and `dsccsetup dismantle` should be considered deprecated and will be removed in a future release.

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 the *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 the *Sun Java System Directory Server Enterprise Edition 6.3 Migration Guide*.

Before migrating a replicated server topology, see "Chapter 4, Migrating a Replicated Topology" in the *Sun Java System Directory Server Enterprise Edition 6.3 Migration Guide.*

Note – Migration from Directory Server 5.x to 6.3.1.1.2 is not supported. For best results, migrate Directory Server 5.x installations directly to Oracle Directory Server Enterprise Edition 11*g* R1. For detailed information, see *Oracle Directory Server Enterprise Edition Upgrade and Migration Guide 11 g Release 1 (11.1.1.5.0)* (`http://docs.oracle.com/cd/E20295_01/html/821-1219/index.html`).

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

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

Directory Server Enterprise Edition Bundle Patch 6.3.1.1.2 can manage any 6.x instances of Directory Proxy Server; no migration is required. You must migrate all Directory Proxy Server 5.x instances before using with the Directory Proxy Server 6.3.1.1.2 commands. See "Chapter 6, Migrating Directory Proxy Server" in the *Sun Java System Directory Server Enterprise Edition 6.3 Migration Guide* for details.

Identity Synchronization for Windows Changes

Directory Server Enterprise Edition Bundle Patch 6.3.1.1.2 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. However, for best results, install Identity Synchronization for Windows 6.0 Service Pack 1. For detailed information, see *Installation Instructions for Identity Synchronization for Windows 6.0 Service Pack 1* (`http://docs.oracle.com/cd/E20295_01/html/821-1581/index.html`).

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 "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 Bundle Patch 6.3.1.1.2 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.

Software Support

The following components are deprecated in Directory Server Enterprise Edition 7.0 and later versions:

- Agent for Sun Cluster support
- Directory Editor

  Directory Server Enterprise Edition Bundle Patch 6.3.1.1.2 does not provide any changes to Directory Editor. Chapter 6, "Directory Editor Bugs Fixed and Known Problems," explains more about this release of Directory Editor. See the *Sun Java System Directory Server Enterprise Edition 6.3 Release Notes* for further information.

The Sun Java Web Console (Lockhart) is no longer supported for deploying the DSCC console in Directory Server Enterprise Edition 7 and Oracle Directory Server Enterprise Edition 11*g* R1.

◆ ◆ ◆ 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 Oracle Directory Services blog (`http://blogs.oracle.com/directoryservices/`) for the most current information about the Directory Server product line.

Support Services and Licenses

Before you start with the product installation, make sure you read your Oracle terms and conditions.

What's New in Directory Server Enterprise Edition Bundle Patch 6.3.1.1.2

Directory Server Enterprise Edition **Bundle Patch 6.3.1.1.2** is a patch release that corrects known issues in the Directory Server Enterprise Edition versions 6.0 through 6.3, including some enhancements in the Directory Server and Directory Proxy Server. The following highlights important changes in this release:

- The repack of the database now can be applied to individual database files.

  The `dsadm repack` command repacks or compacts an existing suffix. Usage:

  ```
  dsadm repack [-b backend][ -T FILE_TYPE ...] INSTANCE_PATH SUFFIX_DN
  [SUFFIX_DN...]
  ```

  The `-b` option enables you to specify the name of the backend instead of the suffix name. At least one suffix DN or one backend name must be specified.

  The `-T` option specifies which type of file needs to be repacked. Possible values are `entries|indexes|changelog`.

  The server instance must be stopped before running this command.

- The Directory Proxy Server part of Directory Enterprise Edition Bundle Patch 6.3.1.1.2 also adds the following new properties:

  monitoring-search-scope Dynamic (no restart required)

  Dynamic (no restart required)

  Level: ldap-data-source

  Type: string

  Default : base

  Description : This property specifies the scope (base, subtree, one) used in a search operation. The availability monitor uses the search operation to test a connection to the data source.

  connect-to-parent Dynamic (no restart required)

  Level: abstract-data-view

  Type: boolean

  Default: true

  Description: Specifies whether the data view handles searches whose search base is handled by another data view.

filter-primary-join-rule	Dynamic (no restart required) Level: abstract-data-view Type: string (LDAP filter string) Example: `objectClass=person` Default: none Description: Controls retrieval of secondary entries; secondary entries are retrieved only if the primary entry matches that filter.

- Native package distributions are not supported for Linux and Windows platforms.

Getting the Software

Directory Server Enterprise Edition Bundle Patch 6.3.1.1.2 is a maintenance release that is applied to an existing installation of Directory Server Enterprise Edition Versions 6.3.1 or 6.3.1.1.1. You cannot apply Directory Server Enterprise Edition Bundle Patch 6.3.1.1.2 to an installation of Directory Server that is not version 6.3.1 or 6.3.1.1.1.

You can download Sun Java System Directory Server Enterprise Edition Bundle Patch 6.3.1.1.2 software from My Oracle Support (`https://support.oracle.com/`). My Oracle Support serves as a starting point to direct you to the proper downloads depending upon the distribution type you need to download.

Directory Server Enterprise Edition Bundle Patch 6.3.1.1.2 is available in the following distributions.

- Native package distribution (available for Solaris only)

  Contains native patches to upgrade installed Directory Server Enterprise Edition 6.3.1 or 6.3.1.1.1 native packages.

- Zip distribution (available for Solaris, Linux, HP-UX, and Windows)

  Contains zip-based patches to upgrade Directory Server Enterprise Edition 6.3.1 or 6.3.1.1.1 zip installations, and to upgrade 6.3.1 native installations on Solaris, Linux , HP-UX, and Windows platforms.

Directory Server Enterprise Edition Bundle Patch 6.3.1.1.2 is available through My Oracle Support (`https://support.oracle.com/`). For information on patch numbers, see "Installation Instructions" on page 32.

For the detailed information on what you need to install based on your current installation, refer to "Installation Instructions" on page 32.

Hardware Requirements

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

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 Server does not support NAS disk storage.

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
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`. Directory Server does not support NAS disk storage.

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. For more information, go to My Oracle Support (`https://support.oracle.com/`).

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, 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, 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
Red Hat Enterprise Linux Advanced Server AS and ES 3.0 Update 4 for x86 and AMD x64	Supported only for the zip distribution of Directory Server Enterprise Edition. 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	Supported only for the zip distribution of Directory Server Enterprise Edition.
	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.

Supported OS Versions for Directory Server, Directory Proxy Server, and Directory Server Resource Kit	Additional Required Software and Comments
Microsoft Windows 2000 Server	Service Pack 4 Supported only for the zip distribution of Directory Server Enterprise Edition. Microsoft ended support for Windows 2000 in July, 2010.
Microsoft Windows 2000 Advanced Server	Service Pack 4 Supported only for the zip distribution of Directory Server Enterprise Edition. Microsoft ended support for Windows 2000 in July, 2010.
Microsoft Windows 2003 Server Standard Edition	Service Pack 2 Supported only for the zip distribution of Directory Server Enterprise Edition.
Microsoft Windows 2003 Server Enterprise Edition	Service Pack 2 Supported only for the zip distribution of Directory Server Enterprise Edition.
Note – Directory Server Enterprise Edition Bundle Patch 6.3.1.1.2 cannot be executed on Windows Microsoft 2008	
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 download the patch cluster for your Solaris OS and Java ES versions, go to My Oracle Support (`https://support.oracle.com/`).

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. For detailed command information, see the *Sun Java System Directory Server Enterprise Edition 6.3 Man Page Reference*.

- `ns-accountstatus`
- `ns-activate`
- `ns-inactivate`
- `schema_push`

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 the *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 6.x, Sun Directory Server Enterprise Edition 7.0 , Oracle Directory Server Enterprise Edition 11*g* R1, and Oracle Unified Directory 11*g*.

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.

Identity Synchronization for Windows Requirements in a Firewall Environment

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

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.

Message Queue Requirements

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

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

Installer Requirements

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

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

Core Component Requirements

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

Console Requirements

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

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

Connector Requirements

All connectors must be able to communicate with Message Queue.

In addition, the following connector requirements must be met.

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

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 (SPARC and x64)	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

Operating System	Supported Browser
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. Microsoft stopped supporting Windows 2000 in July, 2010. Bundle Patch 6.3.1.1.2 supports only the platforms that were certified at the time of the Directory Server Enterprise Edition 6.3.1 release. Bundle Patch 6.3.1.1.2 is not intended to be compatible with platforms or web browsers that are certified for post-6.3.1 releases. If you plan to use more recent OS or web browser versions, then you should upgrade to Oracle Directory Server Enterprise Edition 11*g*R1.

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 31

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, 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.

Installation Instructions

Directory Server Enterprise Edition Bundle Patch 6.3.1.1.2 delivers bug fixes mainly for Directory Service Control Center, Directory Proxy Server, and Directory Server. Only the upgrade mode is offered within version 6.3.1.1.2 using Native Packages or ZIP distribution.

Upgrade is supported only from Directory Server Enterprise Edition 6.3.1 or 6.3.1.1.1 to Bundle Patch 6.3.1.1.2. If you are using a pre-6.3.1 Directory Server Enterprise Edition version , you must upgrade to Directory Server Enterprise Edition 6.3.1 before you can apply Bundle Patch 6.3.1.1.2.

This section covers the following parts.

The following table identifies information for you to use to upgrade Directory Server Enterprise Edition to version 6.3.1.1.2 based on your current installation and the type of distribution you are using.

TABLE 2–1 Upgrade Paths to Directory Server Enterprise Edition Bundle Patch 6.3.1.1.2

Current Directory Server Enterprise Edition Version	Software Distribution	Related Information
6.3.1 or 6.3.1.1.1	Zip	Apply Directory Server Enterprise Edition Bundle Patch 6.3.1.1.2 zip distribution. See "Upgrading Directory Server Enterprise Edition to 6.3.1.1.2 Using ZIP distribution" on page 39in *Directory Server Enterprise Edition Bundle Patch 6.3.1.1.2 Release Notes* (this document).

TABLE 2–1 Upgrade Paths to Directory Server Enterprise Edition Bundle Patch 6.3.1.1.2 *(Continued)*

Current Directory Server Enterprise Edition Version	Software Distribution	Related Information
6.3.1 or 6.3.1.1.1	Native Packages (Solaris)	Apply Directory Server Enterprise Edition Bundle Patch 6.3.1.1.2 native distribution. See "Upgrading Directory Server Enterprise Edition to 6.3.1.1.2 Using Native Packages" on page 35 in *Directory Server Enterprise Edition Bundle Patch 6.3.1.1.2 Release Notes* (this document).
6.3.1	Native Packages (Linux or Windows)	Apply the Directory Server Enterprise Edition Bundle Patch 6.3.1.1.2 zip distribution. See "Upgrading Directory Server Enterprise Edition 6.3.1 Native Packages to a 6.3.1.1.2 Zip installation" on page 41 in *Directory Server Enterprise Edition Bundle Patch 6.3.1.1.2 Release Notes* (this document).
6.0, 6.1, 6.2 or 6.3	Zip	Upgrade to Directory Server Enterprise Edition 6.3.1 prior to applying Directory Server Enterprise Edition Bundle Patch 6.3.1.1.2. 1. See "Upgrading Directory Server Enterprise Edition to 6.3.1 Using Zip Distribution" in *Sun Java System Directory Server Enterprise Edition 6.3.1 Release Notes* (`http://docs.oracle.com/cd/E19261-01/820-5817/gibhy/index.html`) to upgrade to version 6.3.1. 2. Also see "Installing Directory Service Control Center From Zip Distribution" in *Sun Java System Directory Server Enterprise Edition 6.3 Installation Guide*
6.0, 6.1, 6.2 or 6.3	Native Packages	Upgrade to Directory Server Enterprise Edition 6.3.1 prior to applying the Directory Server Enterprise Edition Bundle Patch 6.3.1.1.2. To upgrade to version 6.3.1, see Upgrading Directory Server Enterprise Edition to 6.3.1 Using Native Packages in Sun Java System Directory Server Enterprise Edition 6.3.1 Release Notes (`http://docs.oracle.com/cd/E19261-01/820-5817/gibfo/index.html`)
5.x	Zip or Native Packages (Solaris)	For best results, migrate to Oracle Directory Server Enterprise Edition 11*g* R1. See "Migrating Directory Server Enterprise Edition 5.2 to Version 11*g* Release 1 (11.1.1.5.0)" in *Oracle Directory Server Enterprise Edition Upgrade and Migration Guide 11 g Release 1 (11.1.1.5.0)* (`http://docs.oracle.com/cd/E20295_01/html/821-1219/toc.html`).
None	Zip	For best results, install Oracle Directory Server Enterprise Edition 11*g*R1 . See "Installing Directory Server Enterprise Edition Using Zip Distribution" in *Oracle Directory Server Enterprise Edition Installation Guide 11 g Release 1 (11.1.1.5.0)* (`http://docs.oracle.com/cd/E20295_01/html/821-1218/install-dsee-zip.html`).

TABLE 2–1 Upgrade Paths to Directory Server Enterprise Edition Bundle Patch 6.3.1.1.2 *(Continued)*

Current Directory Server Enterprise Edition Version	Software Distribution	Related Information
None	Native Packages (Solaris)	For best results, install Oracle Directory Server Enterprise Edition 11*g*R1. See "Installing and Uninstalling Directory Server Enterprise Edition Using Native Packages" in *Oracle Directory Server Enterprise Edition Installation Guide 11 g Release 1 (11.1.1.5.0)* (`http://docs.oracle.com/cd/E20295_01/html/821-1218/dsee-native-install.html`).

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.

Before You Upgrade

You must stop all Directory Server and Directory Proxy Server instances before applying Directory Server Enterprise Edition Bundle Patch 6.3.1.1.2.

Native Package-Based Distributions

All Directory Server and Directory Proxy Server instances, including the DSCC registry, must be stopped before Directory Server Enterprise Edition Bundle Patch 6.3.1.1.2 is applied.

To use the localized console, apply the Directory Server Enterprise Edition 6.3.1 localized patch (if it is not already applied) before the Directory Server Enterprise Edition Bundle Patch 6.3.1.1.2. If you apply the Bundle Patch 6.3.1.1.2 before applying the 6.3.1 localization patch, then run the following commands in the specified order.

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

For more information, see bug 12207124/6583131 in "Known Directory Server Issues in Bundle Patch 6.3.1.1.2" on page 51.

Zip-Based Distributions

All Directory Server and Directory Proxy Server instances must be stopped before the Directory Server Enterprise Edition Bundle Patch 6.3.1.1.2 zip distribution is applied on top the 6.3.1 zip installation.

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 12207124/6583131 in "Known Directory Server Issues in Bundle Patch 6.3.1.1.2" on page 51.

Upgrading Directory Server Enterprise Edition to 6.3.1.1.2 Using Native Packages

▼ To Upgrade Shared Components Using Patches

Before You Begin

Before upgrading Directory Server Enterprise Edition to 6.3.1.1.2 using native packages, you must upgrade the shared components. On Solaris systems you must be `root` to perform this procedure.

Using patches, you can upgrade shared components on Solaris. .

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. Note that DPS631U1 has been upgraded to 6.3.1.1.2 and validated with the level of shared components listed in this table

Description	Solaris 10 SPARC	Solaris 10 x64, AMD x64
International Components for Unicode (ICU)	119810-05 (Solaris 10)	119811-05 (Solaris 10)
Simple Authentication and Security Layer (SASL)	119345-07 (Solaris 10)	119346-07 (Solaris 10)
JDK 5.0u30	118667-32 (Solaris 10 64-bit and Solaris 9 64-bit)	118669-32 (Solaris 10)
Sun Java Web Console (SJWC)	147673-06 (Solaris 10)	147674-06 (Solaris 10)
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.
Java Dynamic Management Kit Runtime	119044-04	119044-04
Common Agent Container Runtime	123893-52	123896-52
Sun Java Monitoring Framework (MFWK)	125444-13	125446-13 (Solaris 10 64-bit and Solaris 10 32-bit) 125445-13 (Solaris 10 32-bit)
Sun LDAP C SDK 6.0	136798–05	136800–05 (Solaris 10 x64 and AMD64)

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 10 SPARC	SUNWpr: VERSION=4.5.1,REV=2004.11.05.02.30 SUNWtls: VERSION=3.9.5,REV=2005.01.14.17.27	119213-26
Solaris 10 x64	SUNWpr: VERSION=4.5.1,REV=2004.11.05.03.44 SUNWtls: VERSION=3.9.5,REV=2005.01.14.19.03	119214-26
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	125358-14
Solaris 10 x64	SUNWpr: VERSION=4.6.4,REV=2006.11.16.21.41 SUNWtls: VERSION=3.11.4,REV=2006.11.16.21.41	125359-14

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

2. **If applicable, stop the Common Agent Container and Sun Java Web Console.**

   ```
   # cacaoadm stop
   # smcswebserver stop
   ```

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 23.

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.**

```
# cacaoadm start
# smcswebserver start
```

7 **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 35.

If you already have Directory Server Enterprise Edition 6.3.1 or 6.3.1.1 installed, upgrade to version 6.3.1.1.2 using the following procedure.

You must be `root` to perform these steps.

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	125276-10	125937-06
Patch ID: Solaris 10 x64 or AMD x64	125278-10	125938-06

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.**

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

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 35.**

4. **Download Directory Server Enterprise Edition Bundle Patch 6.3.1.1.2.**

   See "Getting the Software" on page 23 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.**

   Before upgrading Directory Server Enterprise Edition, you must install 119254-38 on Solaris 10 SPARC and 119255-38 on Solaris 10 x64. See "Getting the Software" on page 23 for information on downloading patches.

   Alternatively, use `-G` with the patchadd command on Solaris 10 SPARC and Solaris 10 x64 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
   ```

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.**

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

Upgrading Directory Server Enterprise Edition to 6.3.1.1.2 Using ZIP distribution

▼ To Upgrade Directory Server Enterprise Edition to Bundle Patch 6.3.1.1.2 Using ZIP Distribution

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

Note – In general, it is a good practice to back up the directory databases regularly, and particularly before upgrading the Directory Server. You cannot restore an earlier Directory Server configuration later. This advice applies to both Zip and Native Packages installations. See the *Sun Java System Directory Server Enterprise Edition 6.3 Administration Guide* for information about backing up the database.

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 6.3.1.1.2.

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.

   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 Bundle Patch 6.3.1.1.2**

   a. **Use the `dsee_deploy` command from the Directory Server Enterprise Edition Bundle Patch 6.3.1.1.2 zip distribution, with the same installation path and the same CACAO port used in**

your previous installation of Directory Server Enterprise Edition 6.3.1. 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	126748-07
Solaris 10 x64 and AMD x64	126750-07
Red Hat Linux	126751-07
SuSE Linux	126751-07
HP-UX	126752-07
Windows	126753-07

ii. Install the prerequisite patches or service packs for your platform, as described in "Operating System Requirements" on page 25.

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` command.

```
$ ./dsee_deploy install -i install-path -p cacao-port 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 the *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 the *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.

Upgrading Directory Server Enterprise Edition 6.3.1 Native Packages to a 6.3.1.1.2 Zip installation

To upgrade Directory Server Enterprise Edition 6.3.1 Linux or Windows native packages to a 6.3.1.1.2 zip installation, you must complete the following procedures:

- "To Complete Pre-Upgrade Steps" on page 41
- "To Install Directory Server Enterprise Edition Bundle Patch 6.3.1.1.2" on page 43
- "To Upgrade DSCC" on page 43

▼ To Complete Pre-Upgrade Steps

Before You Begin In general, it is a good practice to back up the directory databases regularly, and particularly before upgrading the Directory Server. You cannot restore an earlier Directory Server configuration later. This advice applies to both Zip and Native Packages installations. See the *Sun Java System Directory Server Enterprise Edition 6.3 Administration Guide* for information about backing up the database.

1 Record Common Agent Container settings.

```
# cacaoadm-path list-params
```

2 Record DSCC registry port numbers.

```
# dsadm-path info ads-path
```

3 Export DSCC registry content.

- On Linux

```
# /opt/sun/ds6/bin/dsconf export -p port cn=dscc /tmp/dscc.ldif
```

- On Windows

```
# "C:\Program Files\Sun\JavaES5\DSEE\ds6\bin\dsconf.exe"
export -p port -e cn=dscc c:\temp\dscc.ldif
```

4 Stop Directory Server services.

- Stop all running Directory Servers (including DSCC registry).

```
# dsadm-path stop instance-path
# dsadm-path stop ads-path
```

- Stop all running Directory Proxy Servers.

```
# dpadm-path stop instance-path
```

5 Disable features specific to the native packages.

a. (Linux only) Disable start at boot.

- For any Directory Server instance registered to start at boot, type the following command:

```
# /opt/sun/ds6/bin/dsadm autostart --off instance-path
```

- For any Directory Proxy Server instance registered to start at boot, type the following command:

```
# /opt/sun/dps6/bin/dpadm autostart --off instance-path
```

b. (Windows only) Disable Windows services.

- For any Directory Server instance registered to start at boot, type the following command:

```
# "C:\Program Files\Sun\JavaES5\DSEE\ds6\bin\dsadm.exe"
disable-service --type WIN_SERVICE instance-path
```

- For any Directory Proxy Server instance registered to start at boot, type the following command:

```
# "C:\Program Files\Sun\JavaES5\DSEE\dps6\bin\dpadm.exe"
disable-service --type WIN_SERVICE instance-path
```

6 Unregister the DSCC Agent from the Common Agent Container.

```
# dsccsetup-path cacao-unreg
```

7 If you use the Common Agent Container only for Directory Server Enterprise Edition, then stop the Common Agent Container.

```
# cacaoadm-path stop
```

8 Unregister DSCC application from Java Web Console.

```
# dsccsetup-path console-unreg
```

To Install Directory Server Enterprise Edition Bundle Patch 6.3.1.1.2

Run the following command:

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

This command works properly only if a Common Agent Container is not yet running on the default port, 11162. If you don't stop your previous Common Agent Container (step 7 of previous section), specify a different port using the `-p` option.

```
# dsee_deploy install -i install-path  -p port options
```

This command installs a Common Agent Container with the local Directory Service Control Center agent as well, allowing you to use DSCC to create server instances.

▼ To Upgrade DSCC

1 Check Common Agent Container configuration.

a. If you used the Common Agent Container only for DSEE, check that port numbers are recorded ports.

```
# install-path/dsee6/cacao_2/cacao/bin/cacaoadm list-params
```

Update if needed:

```
# install-path/dsee6/cacao_2/cacao/bin/cacaoadm stop
# install-path/dsee6/cacao_2/cacao/bin/cacaoadm set-param
  snmp-adaptor-port=snmp-port
# install-path/dsee6/cacao_2/cacao/bin/cacaoadm set-param
  snmp-adaptor-trap-port=snmp-trap-port
# install-path/dsee6/cacao_2/cacao/bin/cacaoadm set-param
  jmxmp-connector-port=jmxmp-port
# install-path/dsee6/cacao_2/cacao/bin/cacaoadm start
```

b. If you should keep the native Common Agent Container alive, check that there is no conflict on port numbers with recorded ports.

```
# install-path/dsee6/cacao_2/cacao/bin/cacaoadm list-params
```

Update if needed:

```
# install-path/dsee6/cacao_2/cacao/bin/cacaoadm stop
# install-path/dsee6/cacao_2/cacao/bin/cacaoadm set-param
  snmp-adaptor-port=snmp-port
# install-path/dsee6/cacao_2/cacao/bin/cacaoadm set-param
  snmp-adaptor-trap-port=snmp-trap-port
# install-path/dsee6/cacao_2/cacao/bin/cacaoadm set-param
```

```
  jmxmp-connector-port=jmxmp-port
# install-path/dsee6/cacao_2/cacao/bin/cacaoadm start
```

2 Configure the DSCC registry.

a. Create the DSCC registry using recorded ports.

```
# install-path/dscc6/bin/dsccsetup ads-create -p port -P secure-port
```

b. Import the `/tmp/dscc.ldif` file.

- On Linux

```
# install-path/ds6/bin/dsconf import -p port /tmp/dscc.ldif cn=dscc
```

- On Windows

```
# install-path\ds6\bin\dsconf.exe import -p port -e c:\temp\dscc.ldif cn=dscc
```

c. If new port numbers are used for Common Agent Container, then:

i. Unregister all the servers from DSCC registry.

```
# install-path/dscc6/bin/dsccreg remove-server instance_path
```

ii. Register all the servers in DSCC registry.

```
# install-path/dscc6/bin/dsccreg add-server instance_path
```

3 Deploy Directory Service Control Center.

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.

- To Deploy the WAR File with Sun Java System Application Server

  a. Create an application server instance.

```
$ mkdir /local/domainroot
$ setenv AS_DOMAINS_ROOT /local/domainroot
$ cd app-server-install-path/bin
$ asadmin create-domain --domaindir ${AS_DOMAINS_ROOT} --adminport 3737 \
--adminuser boss dscc
```

  b. Edit the `server.policy` file.

    a. Open the `server.policy` file.

```
$ vi ${AS_DOMAINS_ROOT}/dscc/config/server.policy
```

    b. Add the following statements to the end of the file:

```
// Permissions for Directory Service Control Center
grant codeBase "file:${com.sun.aas.instanceRoot}/
applications/j2ee-modules/dscc/-"
{
    permission java.security.AllPermission;
};
```

This configures the application server to grant all of the Java permissions to the DSCC application.

1. Deploy the WAR file in your application server instance.

```
$ asadmin start-domain --domaindir ${AS_DOMAINS_ROOT} --user boss dscc
$ cp install-path/var/dscc6/dscc.war ${AS_DOMAINS_ROOT}/dscc/autodeploy
```

For more information about creating and configuring application server instances and deploying the WAR file, refer to the Sun Java System Application Server Online Help.

2. Open DSCC.

Use `http://hostname:8080/dscc` or `https://hostname:8181/dscc` based on the configuration of your application server.

The Directory Service Manager Login page displays.

- To Deploy the WAR File with Tomcat

a. Identify your Tomcat installation and instance.

```
$ setenv CATALINA_HOME tomcat-install-path
$ setenv CATALINA_BASE tomcat-instance-path
$ setenv JAVA_HOME jdk-home-dir
```

For installing Tomcat and creating instances, refer to the Tomcat documentation.

b. Deploy the WAR file.

a. Create the DSCC directory as shown below:

```
$ mkdir ${CATALINA_BASE}/webapps/dscc
```

b. Copy the `dscc.war` file into newly created DSCC folder and unzip the `dscc.war` file.

```
$ unzip -d ${CATALINA_BASE}/webapps/dscc install-path/var/dscc6/dscc.war
```

c. Add the emphasized text in the `${CATALINA_BASE}/conf/web.xml` file as shown below:

```
...
    <servlet>
        <servlet-name>jsp</servlet-name>
        <servlet-class>org.apache.jasper.servlet.JspServlet</servlet-class>
        <init-param>
            <param-name>fork</param-name>
            <param-value>false</param-value>
        </init-param>
        <init-param>
            <param-name>xpoweredBy</param-name>
            <param-value>false</param-value>
        </init-param>
    ...
        <init-param>
            <param-name>enablePooling</param-name>
            <param-value>false</param-value>
        </init-param>
        <init-param>
            <param-name>enablePooling</param-name>
```

```
            <param-value>false</param-value>
        </init-param>
        <load-on-startup>3</load-on-startup>
    </servlet>    ....
```

d. Verify the permissions of `startup.sh` (`tomcat5.exe` on Windows) and run the following command:

```
$ ${CATALINA_HOME}/bin/startup.sh
```

1. Use `http://hostname:8080/dscc` to connect to DSCC.

   The Directory Service Manager Login page displays.

Uninstallation Instructions

If you plan to uninstall Directory Server Enterprise Edition, see the chapter "Uninstalling Directory Server Enterprise Edition" in the *Sun Java System Directory Server Enterprise Edition Installation Guide* for the version you are uninstalling. For a comprehensive list of Directory Server Enterprise Edition documentation libraries, go to the Legacy Sun Identity Management Documentation page (`http://www.oracle.com/technetwork/documentation/legacy-sun-identity-mgmt-193462.html`).

◆ ◆ ◆ 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 Bundle Patch 6.3.1.1.2

This section lists the bugs fixed since Directory Server Enterprise Edition 6.3.1.1.2.

TABLE 3–1 Bugs Fixed in Directory Server Enterprise Edition Bundle Patch 6.3.1.1.2

Oracle Bug ID	Sun Bug ID	Synopsis
16523310	None	Issue resolved.
14673804	None	Improve the handling of "... CSNGEN_ADJUST_TIME: Adjustment limit exceeded"
14258153	None	Issue resolved.
14147844	None	Directory Server ns-slapd dumps core during LDIF import.
13932346	None	Issue resolved.
13924884	None	Rounding errors in memory sizing prevent correct instance sizing.
13833118	None	Memory leak can occur in a moddn operation if the moved entry has an entryid smaller than the new superior entry.
13632964	None	Issue resolved.
13242112	None	Data of type octetstring is corrupted by DSCC.

TABLE 3–1 Bugs Fixed in Directory Server Enterprise Edition Bundle Patch 6.3.1.1.2 *(Continued)*

Oracle Bug ID	Sun Bug ID	Synopsis
13065581	None	Directory Server crashes after failing to perform an LDAP write request due to a memory leak in the retro changelog.
12708119	None	Database entry cannot be read after being written with invalid nsuniqueid.
12245898	6737227	DSEE 6.3 crashes under load during DN normalization.
12232791	2160773	Smartheap v8.0 returns invalid address to realloc with buffer greater than 10Mb.
12211339	6601267	Destructive restore. Perform restore by moving files instead of copying files.
11826441	None	Memory leak in retro changelog when failing to perform an LDAP write request.

Known Problems and Limitations in Directory Server

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

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. (6830908/12268025)

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. (6886089/12279861)

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 Bundle Patch 6.3.1.1.2

This section lists the known issues that are found at the time of Directory Server Bundle Patch 6.3.1.1.2 release. Each issue in the following list is identified with a two-part ID using the following form: *Sun BugTrack ID*/*Oracle BugDB ID*.

2129151/12132482 The Directory Server hangs when running the `stop-slapd` command.

2151022/12206730 If certificates contain localized names, the certificate cannot be deleted properly. They also cannot be listed properly.

4979319/12096337 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 My Oracle Support.

6358392/12144749 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*.

6401484/12157832 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.

6410741/12160475 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.

6412131/12160953 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.

6416407/12162287 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.

6446318/12171105 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`.

6449828/12172126 Directory Service Control Center does not properly display `userCertificate` binary values.

6461602/12174839 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.

6468074/12177035 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.

6469154/12177381 On Windows, the output of `dsadm` and `dpadm` commands, and help messages are not localized in Simplified and Traditional Chinese languages.

6469296/12177450 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.

6469688/12177565 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.

6478568/12180348 The `dsadm enable-service - -` type CLUSTER command does not configure the cluster agent the properly; it is missing a dependency on the file system.

As a workaround, manually add the dependency. Example:

```
scrgadm -c -j ds--global-iplanet-sc1-ldap1vol1-jls-ds-1389 -y
Resource_dependencies=disks
```

where:

- `ds--global-iplanet-sc1-ldap1vol1-jls-ds-1389` is the name of the Directory Server created by `dsadm`.
- disks is the name of the `HAStoragePlus` resource as created by the user.

6480753/12181017 The `dsee_deploy` command has been seen to hang while registering the Monitoring Framework component into the Common Agent Container.

6483290/12181717 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`.

6485560/12182309 Directory Service Control Center does not allow you to browse a suffix that is configured to return a referral to another suffix.

6488197/12182934 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.

6488284/12182971 For the HP-UX platform, Directory Server Enterprise Edition man pages for the following sections cannot be accessed from the command line:

- `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.

6490557/12183619 An attempt to enter an invalid CoS Template results in a crash in versions of Directory Server 6.

6490653/12183629 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.

6492894/12184342 On Red Hat systems, the `dsadm autostart` command does not always ensure that the server instances start at boot time.

6494997/12185015 The `dsconf` command does not prompt for the appropriate `dsSearchBaseDN` setting when configuring DSML.

6495004/12185018 On Windows systems, Directory Server has been seen to fail to start when the base name of the instance is `ds`.

6497053/12185665 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`.

6497894/12186005 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`.

6501320/12186925 When creating an index on custom schema, a suffix level change of the *all-ids-threshold* is not permeated completely by the DSCC.

6503509/12187484 Some output displayed by the `dsccmon`, `dsccreg`, `dsccsetup`, and `dsccrepair` commands is not localized.

6503546/12187497 Changing the locale of the system and starting DSCC, does not display the pop-up window message in the locale that you selected.

6504180/12187685 On Solaris 10, the password verification fails for instances with multi-byte characters in their DN on English and Japanese locales.

6504549/12187763 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`.

6520646/12191946 Clicking Browse DSCC online help does not display the online help when you are using Internet Explorer.

6527999/12193852 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.

6539650/12196778 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.

6541040/12197180 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.

6542857/12197665 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.

6547992/12199102 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
```

6550543/12199716 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.

6551672/12200025 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.

6551685/12200029 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`.

6557480/12201146 On Solaris 9 and Windows, when you access the online help from the console configured using Web archive file (WAR), it displays an error.

6559825/12201643 If you modify the port number using DSCC on a server that has replicated suffixes, problems arise when setting replication agreement between servers.

6571672/12204509 If unzip is unavailable on the system, `dsee_deploy` does not install any product.

6583131/12207124 To use a localized Directory Service Control Center, apply the Directory Server Enterprise Edition Bundle Patch 6.3.1.1.2 localized patch before the Directory Server Enterprise Edition Bundle Patch 6.3.1.1.2 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 Bundle Patch 6.3.1.1.2 localized patch before the Directory Server Enterprise Edition Bundle Patch 6.3.1.1.2 patch.

For zip based installation, the Directory Server Enterprise Edition Bundle Patch 6.3.1.1.2 localized patch is not automatically applied to the Directory Service Control Center. As a workaround, undeploy and then redeploy the WAR file.

6587801/12208166 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
```

6594285/12209724 On HP_UX, the Directory Service Control Center has no RBAC capability.

6595805/12210057 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.

6630897/12218292 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.

6630924/12218303 The output of the `dsadm show-*-log` command is not correct if some lines in the log contain more than 1024 characters.

6634397/12219425 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.

6637242/12220200 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`

6638990/12220674 and 6641357/12221256 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.

6640755/12221093 In Windows, in the Korean locale, the `dsadm start` command does not display the `nsslapd` error log when `ns-slapd` fails to start.

6644161/12221900 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?
```

6648240/12223329 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.

6650105/12223892 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)
```

6658483/12226102 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.

6663685/12227613 In the Directory Service Control Center, the Copy Suffix Configuration operation can produce erroneous pop-up windows.

6687375/12234166 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.

6689290/12234693 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.

6696857/12236820 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. See "VERITAS File System (VxFS) Versions 4.1 and 5.0 Running on Solaris 9 and Solaris 10 May Experience Degraded I/O Performance While Synchronizing to Disk" (`https://support.oracle.com/CSP/main/article?cmd=show&type=NOT&doctype=ALERT&id=1000932.1`)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.

6705472/12238767 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.

6707789/12239527 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'
```

6712064/12240595 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

6720595/12242408 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.

6723208/12243134 An attempt to edit an attribute value containing a carriage return results in corruption of the value.

6723590/12243224 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.

6725346/12243611 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.

6742347/12246882 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
```

6750837/12248623 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.

6751354/12248728 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.

6752475/12249011 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).

6752625/12249065 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.

6753020/12249137 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.

6753742/12249325 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 the *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.

6755852/12249699 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
   ```

6756152/12249760 LDAP commands do not work on Windows (IPv6 enable)

6772879/12253695 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`.

6776034/12254403 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.`

6777338/12254781 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 the *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.

6786078/12257619 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.

6791372/12258920 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
```

6827661/12267366 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 startc`ommand locally.

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

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

6831959/12268259 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 the *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 the *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 the *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
   [...]
```

6834291/12268817 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,*
```

6872923/12277234 The First Login Password Policy scenario described in "To Set Up a First Login Password Policy" in the*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`.

6876315/12277925 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.

6902940/12283417 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=
```

6920893/12287170 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).

6928378/12288685 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 in Bundle Patch 6.3.1.1.2

This section lists the bugs fixed in Directory Proxy Server in Bundle Patch 6.3.1.1.2.

TABLE 4–1 Bugs Fixed in Directory Proxy Server in Bundle Patch 6.3.1.1.2

Oracle Bug ID	Sun ID	Synopsis
15866235	None	When all Directory Proxy Server 11.1.1.5.1 worker threads are busy, new client requests become backlogged and cannot be properly assigned.
14598827	None	Client connections hang and the following is reported in the Directory Proxy Server error log: "EXCEPTION - ERROR - Fatal uncaughtException in Worker Thread 29. Abandon current operation."
14393779	None	Directory Proxy Server 6.3.1.1 is significantly slower when dealing with large search result sets.
14268650	None	Issue resolved.
13932346	None	Issue resolved.
13392299	None	Using JDBC with Oracle 10g, add hire_date returns constraint violation.
13360543	None	Directory Proxy Server should abandon first bind, or abandon the search, if a second bind occurs.

TABLE 4–1 Bugs Fixed in Directory Proxy Server in Bundle Patch 6.3.1.1.2 *(Continued)*

Oracle Bug ID	Sun ID	Synopsis
12940451	None	Client-side sizelimits are ignored when setting a resource policy using DSCC.
12921731	None	DPS disconnects active connections incorrectly as idle-timeout
12307452	7016257	Directory Proxy Server 6.3.1: Silent bind fails when the password contains a special character.
12280079	6887397	Directory Proxy Server is server deadlocked, does not respond to requests.

Known Problems and Limitations in Directory Proxy Server

This section lists known problems and limitations at the time of Directory Server Enterprise Edition Bundle Patch 6.3.1.1.2 release.

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.

5042517/12080966
: The modify DN operation is not supported for LDIF, JDBC, join and access control data views.

6355714/12143951
: Currently, `getEffectiveRight` control is supported only for LDAP data views and does not yet take into account ACIs local to the proxy.

6439604/12080966
: After configuring alerts, you must restart Directory Proxy Server for the change to take effect.

Known Directory Proxy Server Issues in Bundle Patch 6.3.1.1.2

This section lists the known issues that are found at the time of Directory Proxy Server Bundle Patch 6.3.1.1.2 release.

6360059/12145232
: 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.

6383532/12152515
: Directory Proxy Server must be restarted when the authentication mode configuration is changed.

6386073/12153217
: After generation of a CA-Signed Certificate request, when you refresh, the certificate is displayed as a self-signed certificate.

6388022/12153788
: 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.

6390118/12154346
: 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.

6390220/12154371
: 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.

  The "" character is removed by the shell. The workaround is to escape it typing `base-dn:\"\"`

6428448/12165809
: The `dpconf` command has been seen to display the `Enter "cn=Directory Manager" password:` prompt twice when used in interactive mode.

6447554/12171555
: Directory Proxy Server fails to rename an entry moving to another data view when numeric or lexicographic data distribution is configured.

6458935/12174132
: 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.
6461510/12174791	In Directory Proxy Server, referral hop limit does not work.
6469154/12177381	On Windows, the output of `dsadm` and `dpadm` commands, and help messages are not localized in Simplified and Traditional Chinese languages.
6469780/12177599	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. The workaround is to create the JDBC data view before creating the JDBC server
6488197/12182934	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.
6488284/12182971	For the HP-UX platform, Directory Server Enterprise Edition, man pages for the `man5dpconf` section cannot be accessed from the command line: 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.
6488297/12182980	On Windows, DSCC initialization can only be performed by Administrator user.
6490763/12183676	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 property in the `AMConfig.properties` file:

	Increase `com.iplanet.am.event.connection.delay.between.retries`, which represents the number of milliseconds delay between attempts. The default is 3000 milliseconds.
6490853/12183727	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.
6491133/12183792	When creating a self-signed certificate using Directory Service Control Center, do not use multi-byte characters for the certificate names.
6491845/12184019	The default LDAP controls allowed through Directory Proxy Server are not displayed by Directory Service Control Center.
6493349/12184479	Directory Service Control Center removes commas when changing the DN for an existing excluded subtree, or alternate search base.
6494540/12184892	After enabling or disabling non secure LDAP access for the first time, you must restart Directory Proxy Server for the change to take effect.
6497547/12185916	Time limit and size limit settings work only with LDAP data sources.
6497992/12186047	After using the command `dpadm set-flags cert-pwd-store=off`, Directory Proxy Server cannot be restarted using Directory Service Control Center.
6501867/12187067	The `dpadm start` command has been seen to fail when used with a server instance name combining both ASCII and multi-byte characters.
6505112/12187920	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.
6510583/12189379	Unlike previous versions, as stated in the manual page *Sun Java System Directory Server Enterprise Edition 6.3 Man Page Reference*, 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.

6511264/12189496 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`.

6520368/12191889 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`

6527010/12193636 Directory Proxy Server cannot write JDBC attributes implying many-to-many (N:N) relationship between tables in the JDBC database.

6539650/12196778 Directory Proxy Server instances with multi-byte DN and created using DSCC, fail to start on Linux.

6542857/12197665 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.

6547755/12199009 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.

6547759/12199011 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.

6551076/12199855 Console does not retrieve the backend status of the Directory Proxy Server instance if a machine has multiple host names.

6565106/12202887 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.

6567644/12203547 DPS constructs illegal DB requests.

6573439/12204943 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.

6583798/12207253 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`.

6588319/12208289 In DSCC configured using Tomcat server, the title of the Help and Version pop-up windows displays the multi-byte strings garbled.

6590460/12208740 The string `owner` in the output of the `dpadm show-cert` *dps-instance-path* command is not translated in Simplified Chinese and Traditional Chinese.

6597598/12210440 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)
```

6639674/12220848 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.

6642559/12221511	Writing virtual transformations does not work for the `remove-attr-value` transformation model.
6642578/12221519	Writing virtual transformations does not work as expected when an entry is modified.
6649984/12223839	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.
6711054/12240375	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.
```

Known Problems and Limitations in Directory Proxy Server in Bundle Patch 6.3.1.1.2

This section lists the known problems and limitations that are found at the time of the Directory Proxy Server Bundle Patch 6.3.1.1.2 release.

Note – Known issues and limitations in Directory Proxy Server Bundle Patch 6.3.1.1.2 persist even after the patch for Directory Proxy Server Bundle Patch 6.3.1.1.2 is applied. Refer to "Known Problems and Limitations in Directory Proxy Server" on page 74 for information about these issues.

Known Limitations in Directory Proxy Server Bundle Patch 6.3.1.1.2

This section lists the known limitation that is found at the time of the Directory Proxy Server Bundle Patch 6.3.1.1.2 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 Bundle Patch 6.3.1.1.2

This section lists the known problems that are found at the time of the Directory Proxy Server Bundle Patch 6.3.1.1.2 release.

6728746/12244278 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 6636463/12219995. 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
```

6826694/12267142 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 the *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 the *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 the *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
   ```

6854861/12273133 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.

Identity Synchronization for Windows 6.0 Service Pack 1 is the latest Identity Synchronization for Windows 6.0 version that delivers bug fixes. For more information read *Installation Instructions for Identity Synchronization for Windows 6.0 Service Pack 1* (`http://download.oracle.com/docs/cd/E19656-01/821-1581/index.html`).

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 35.

Identity Synchronization for Windows Bugs Fixed and Known Problems

Identity Synchronization for Windows 6.0 Service Pack 1 is the latest Identity Synchronization for Windows 6.0 version that delivers bug fixes. For more information read *Installation Instructions for Identity Synchronization for Windows 6.0 Service Pack 1* (`http://download.oracle.com/docs/cd/E19656-01/821-1581/index.html`).

This section lists known problems and limitations exposed in Identity Synchronization for Windows product after the release of Directory Server Enterprise Edition Bundle Patch 6.3.1.1.2.

6572575/12204713	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.
6721443/12242656	If debug logs for ISW connectors are activated, connectors fail to reach synchronization step.

6879679/12278588

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 Bundle Patch 6.3.1.1.2 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 91

Known Problems and Limitations in Directory Server Resource Kit

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

5081543/12090467	`searchrate` crashes on Windows systems when using multiple threads.
5081546/12090468	`modrate` crashes on Windows systems when using multiple threads.
5081549/12090469	`authrate` crashes on Windows systems when using multiple threads.
5082507/12090777	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.
6379087/12151094	NameFinder has been seen to fail to deploy in Application Server on Windows systems.
6393554/12155522	NameFinder has been seen to throw a page not found error after deployment. To work around this issue, rename `nsDSRK/nf` to `nsDSRK/NF`.
6393586/12155532	Cannot add more than two users to My Selections list in NameFinder.

6393596/12155538	NameFinder search should fetch entries for values other than Last Name, First Name, Email, and Given Name.
6393599/12155540	NameFinder search should allow searches for groups.
6565893/12203090	The `idsktune` command does not support SuSE Enterprise Linux 10.
6576045/12205589	Killing `modrate` and `searchrate` launcher does not kill actual `modrate` and `searchrate` processes respectively.

6754994/12249520	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.`